19. *GOST R ISO/MEK 27005-2010*. Informatsionnaya tekhnologiya. Metody i sredstva obespecheniya bezopasnosti. Menedzhment riska informatsionnoy bezopasnosti. Trebovaniya [State Standard R ISO/MEK 27005-2010. Information technology. Methods and means of security. Risk management of information security. Requirements]. Moscow: Standartinform, 2011, 51 p.
20. *Pashchenko I.N., Vasil'ev V.I.* Razrabotka trebovaniy k sisteme zashchity informatsii v intellektual'noy seti Smart Grid na osnove standartov ISO/IEC 27001 i 27005 [Design of requirements to smart grid security system on the basis of ISO/IEC 27001 and 27005 standards], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2013, No. 12 (149), pp. 117-126.

Статью рекомендовал к опубликованию к.т.н. А.А. Бакиров.

**Пащенко Иван Николаевич** – Уфимский государственный авиационный технический университет; e-mail: iv.pashchenko@gmail.com; 450000, Уфа, ул. К. Маркса, 70; тел.: +73472730672; кафедра вычислительной техники и защиты информации; аспирант.

**Васильев Владимир Иванович** – e-mail: vasilyev@ugatu.ac.ru; кафедра вычислительной техники и защиты информации; зав. кафедрой; д.т.н.; профессор.

**Гузаиров Мурат Бакеевич** – e-mail: guzairov@rb.ru; кафедра вычислительной техники и защиты информации; д.т.н.; профессор.

**Pashchenko Ivan Nikolaevich** – Ufa State Aviation Technical University; e-mail: iv.pashchenko@gmail.com; 12, K. Marxa street, Ufa, 450000, Russia; phone: +73472730672; the department of computer science and information security; postgraduate student.

**Vasyliev Vladimir Ivanovich** – e-mail: vasilyev@ugatu.ac.ru; the department of computer science and information security; head of department; dr. of eng. sc.; professor.

**Guzairov Murat Bakeevich** – e-mail: guzairov@rb.ru; the department of computer science and information security; dr. of eng. sc.; professor.

УДК 004.771

**Е.Н. Тищенко, К.А. Буцик, В.В. Деревяшко**

## МОДЕЛЬ ДОВЕРЕННОЙ СЕТЕВОЙ ЗАГРУЗКИ «ТОНКОГО КЛИЕНТА» С НЕЙТРАЛИЗАЦИЕЙ «ВНУТРЕННЕГО НАРУШИТЕЛЯ»

*Описана концепция и модель организации доверенной сетевой загрузки образа операционной системы в память рабочих станций, препятствующей атакам внутреннего нарушителя. Модель актуальна для существующих автоматизированных систем клиент-серверной архитектуры с терминальным доступом, построенных по технологии тонкий клиент (сетевая загрузка PXE и линии связи 100/1000Base-TX). Приводятся результаты анализа традиционных моделей и методов организации доверенной загрузки и возможностей внутреннего нарушителя по их обходу. Под традиционными моделями понимается использование специализированных программных и аппаратно-программных модулей доверенной загрузки, а также модифицированного программного обеспечения BIOS (UEFI). Для каждого метода (модели) приводятся актуальные направления (векторы) атак внутреннего нарушителя, что определяет недостатки использования метода. По результатам анализа предлагается концепция и технологическая реализация новой модели доверенной сетевой загрузки, лишенная выявленных недостатков. В базисе новой модели лежит контроль временных интервалов штатного обмена запросами на загрузку операционной системы между рабочей станцией и сервером. Новая модель основана на использовании периферийных сетевых модулей и центрального контроллера совместно с рабочими станциями и серверным массивом соответственно, что позволяет управлять состоянием межсетевого экрана и сервера сетевой загрузки в режиме реального времени и обеспечивает мгновенную блокировку прохождения сетевого трафика к защищаемым узлам автоматизиро-*

*ванной системы в случае выявления активности, характерной для атак внутреннего нарушителя. В заключении статьи приводятся: а) структурная схема новой модели; б) алгоритм работы новой модели; в) примеры нейтрализации атак внутреннего нарушителя, успешных в случае использования традиционных моделей и методов.*

*«Тонкий клиент»; «внутренний нарушитель»; терминальная операционная система; доверенная сетевая загрузка; временной интервал; периферийный сетевой модуль; специализированный сетевой контроллер; некриптографические методы защиты информации.*

**E.N. Tishenko, K.A. Butsik, V.V. Derevyashko**

## MODEL OF A THIN-CLIENTS TRUSTED NETWORK BOOTING FOR INSIDER'S CAPABILITIES NEUTRALIZATION

*The article describes the concept and logical model of a trusted network boot for operating system image to prevent insider's attacks. The model is developed for existing automated systems of client-server architecture with terminal access, built on thin client technology (PXE network boot and link 100 / 1000Base-TX). The article presents the results of the analysis of traditional models and methods of a trusted network boot and insider's opportunities for their deception. Traditional model means the use of specialized software and hardware software modules of trusted boot, as well as modification of software BIOS (UEFI). For each method (model) are determined an actual directions (vectors) insider's attacks that determines a disadvantages of this method. The conception and technological state of a new model of trusted network boot without such deficiencies are defined as the analysis results. The basis of the new model is control of time slots of regular requests exchanging between the workstation and the server. The new model is based on a peripheral network modules and a central controller in conjunction with workstations and servers respectively. This method allows you to control the state of the firewall and the network boot server and provides blocking network traffic of protected sites of the automated system in case of activity characteristic of insider attacks. The research findings indicate: a) structure and technology of the new model realization; b) algorithm of the new model; c) examples of neutralizing insider's attacks that are successful in case of using of traditional models and methods.*

*"Thin-client"; terminal operating system; trusted (secure) network boot; peripheral network module; special network controller; non-cryptographic methods of information security.*

**Введение.** Понятие «доверенная загрузка» означает обеспечение однозначной передачи в память рабочей станции (далее – РСТТК) образа терминальной операционной системы (далее – ТОС), защищенного от ложной модификации, подмены и внедрения вредоносного кода [1].

Ключевой проблемой защищенности доверенной загрузки в системе тонкого клиента является «однонаправленность» передачи образа ТОС со стороны сервера сетевой загрузки (далее – ССЗ) на рабочую станцию [2]. Процесс запроса на загрузку, его обработки, передачи и получения образа ТОС контролируется исключительно на основе полученных из запроса данных и служебной сетевой информации.

Внутренний нарушитель на время проведения рабочего сеанса в автоматизированной системе (далее – АС) располагает штатными идентификаторами и правами доступа, а также «машинным временем». При наличии достаточного времени на подготовку такой нарушитель способен подменить образ ТОС на образ собственной операционной системы [3], содержащей средства перехвата информации или проведения межсетевых атак (далее – «ядовитая ТОС»). При этом возможно определить основные направления (векторы) атак внутреннего нарушителя в типовой АС [4]:

1. Инициализация запроса и загрузки образа ТОС из заведомо загруженной на рабочей станции «ядовитой ТОС» с целью регистрации ложной информации в системе защиты.
2. Внедрение в сетевую структуру АС собственного сервера сетевой загрузки образов ТОС (далее – «ядовитый ССЗ») с целью перехвата и перенаправления запросов на загрузку штатных образов ТОС.

3. Подключение нештатной ПЭВМ, содержащей встроенные средства перехвата информации, к каналу связи с целью загрузки ТОС для последующей обработки защищаемой информации.

Использование современных некриптографических методов обеспечения доверенной загрузки зачастую либо не применимо в уже существующих АС, либо не позволяет полностью исключить представленные действия внутреннего нарушителя. Анализ указанных методов (далее – традиционных методов) представлен ниже.

Целью исследования является разработка концепции и модели обеспечения доверенной сетевой загрузки ТОС в память рабочих станций с однозначной нейтрализацией представленных векторов атак внутреннего нарушителя.

**Анализ традиционных методов.** Традиционные модели доверенной загрузки основаны на использовании (интеграции в структуру АС) следующих средств защиты информации:

а) программных средств уровня ТОС;

б) аппаратно-программных модулей доверенной загрузки (далее – АМДЗ);

в) модифицированного ПО BIOS рабочих станций.

**Программные средства доверенной загрузки.** К программным средствам доверенной загрузки ТОС относятся средства шифрования образа ТОС с выполнением условий аппаратной «привязки». Дешифрование и распаковка образа в оперативную память происходит только при совпадении некоторого числа уникальных аппаратных признаков рабочей станции, определяемых ТОС в процессе загрузки [5].

Однако внутренний нарушитель не имеет временных ограничений, связанных с изучением технологического процесса работы АС и используемых средств защиты, и поэтому способен реализовать следующие направления атак:

1. Симуляция средствами загруженной «ядовитой ТОС» сетевых запросов к серверному массиву, подтверждающих успешность загрузки штатной ТОС.
2. Загрузка «ядовитой ТОС» со встроенной средой виртуализации с целью эмуляции аппаратных «привязок», необходимых для проведения процедур распаковки и дешифрования.

**Модификация ПО BIOS (UEFI).** Специальная модификация ПО BIOS за счет установки программного модуля доверенной загрузки (далее – МДЗ) препятствует атакам нарушителя, направленным на обход защитных механизмов, поскольку полностью игнорировать процесс исполнения ПО BIOS на рабочей станции невозможно [6]. Однако установка МДЗ связана с рядом ограничений и проблем безопасности:

а) внедрение защитных механизмов допустимо далеко не для всех версий ПО BIOS и материнских плат;

б) после проведения процедуры модификации ПО BIOS существует заранее неизвестная вероятность отказа запуска (работы) материнской платы;

в) возможность модификации ПО BIOS сама по себе является каналом осуществления атаки – нарушитель способен провести обратный процесс и внедрить в него собственные утилиты перехвата, эмуляции и т.п. [7].

Последняя проблема особенно характерна для ПО UEFI, пришедшего на смену ПО BIOS в современных материнских платах. Если для ПО BIOS разнородность внедряемых версий являлась положительным аспектом безопасности, поскольку усложняла аналитическую задачу нарушителю, то разнородность UEFI наоборот усложняет задачу по интеграции в его среду любых защитных механизмов.

Следует также отметить многократное увеличение недокументированного кода, лежащего в основе каждого образа UEFI (до 16 Мбайт), по отношению к типовому ПО BIOS (256–1024 Кбайт). При встраивании в ПО UEFI защитных механизмов невозможно гарантировать отсутствие «черного хода», специально внесенного разработчиками конкретного ПО UEFI для выполнения служебных операций [7, 8].

**Аппаратно-программные модули доверенной загрузки.** Традиционный АМДЗ представляется технологической платой с типовым разъемом подключения (PCI, PCI-E, miniPCI-E), которая [9]:

а) инициализирует защитные механизмы на этапе инициализации ПО BIOS (UEFI);

б) обеспечивает дополнительную идентификацию и аутентификацию пользователей системы;

в) контролирует целостность ПО BIOS (UEFI) с целью продолжения или приостановки процесса загрузки системы;

г) контролирует неизменность загрузочной области;

д) перехватывает прерывание 0000:7C00H, передающее управление загрузочной области встроенного или съемного носителя;

е) обеспечивает проверку контрольных сумм программной среды загружаемой в дальнейшем операционной системы.

Однако последние три механизма не являются актуальными для случая сетевой загрузки ТОС. Поскольку на момент инициализации АМДЗ ТОС еще не загружена в память рабочей станции, постольку:

а) отсутствует информация о загрузочной области;

б) отсутствует информация о контрольных суммах программной среды;

в) прерывание ПО BIOS отличается от 0000:7C00H и при использовании ПО UEFI заранее неизвестно [10].

Таким образом, для АС, оборудованной АМДЗ, характерны следующие направления атак внутреннего нарушителя:

1. Вход в конфигурационную среду ПО BIOS (UEFI) за счет компрометации пароля или эксплуатации уязвимости «черного хода». Отключение механизма инициализации разъемов рабочей станции, к которым подключена плата АМДЗ. Загрузка рабочей станции со съемного носителя, в памяти которого расположена «ядовитая ТОС».

2. Внедрение в сетевую структуру АС «ядовитого ССЗ». Штатная авторизация в среде АМДЗ. Сетевая загрузка «ядовитой ТОС» в память рабочей станции.

В настоящее время нейтрализация указанных направлений атак производится за счет размещения ТОС в памяти самого АМДЗ или на отдельном съемном носителе, защищенном от несанкционированной модификации [11, 12]. Однако такая реализация лишает применение в АС технологии «тонкий клиент» основных преимуществ [13]:

1. Нарушается гибкость централизованного администрирования рабочих станций – обновление ТОС необходимо осуществлять отдельно для каждой станции.

2. Многократно увеличиваются экономические и технологические затраты на аппаратную модернизацию АС в части оснащения каждой рабочей станции АМДЗ.

Для сохранения преимуществ гибкости производители предлагают различные решения в области централизованного администрирования АМДЗ [3, 14, 15]. Ключевым недостатком такого подхода является необходимость внедрения в АС дополнительных линий связи, совместимого программного обеспечения и криптографических средств защиты информации, что также приводит к увеличению экономических и технологических затрат.

В свою очередь, с целью отказа от встраивания АМДЗ, возможно внедрение МДЗ с аналогичным функционалом в сетевые карты рабочих станций [16]. Однако такой подход автоматически наследует недостатки использования МДЗ совместно с ПО BIOS, перечисленные ранее, и, следовательно, не подходит для большинства уже существующих АС.

**Результаты анализа.** На основании вышеизложенных данных допустимо определить следующие недостатки традиционных моделей доверенной загрузки относительно воздействий внутреннего нарушителя:

1. Применение программных МДЗ, встраиваемых в ТОС, не влияет на защищенность процесса загрузки.

2. Модификация ПО BIOS или сетевых карт рабочих станций неактуальна для большинства уже существующих АС.

3. Применение традиционных АМДЗ, направленных на перехват прерываний ПО BIOS и контроль целостности образа ТОС, не влияет на защищенность процесса загрузки.

4. Применение АМДЗ, в памяти которых располагается образ ТОС, снижает экономическую и функциональную эффективности использования в АС технологии «тонкий клиент».

Таким образом, в основе новой концепции и модели обеспечения доверенной сетевой загрузки тонкого клиента должны лежать следующие принципы:

1. Использование периферийных (не встроенных) средств защиты.

2. Централизация и автоматизация средств управления ключевыми сетевыми устройствами АС (межсетевые экраны, терминальные серверы, сервер сетевой загрузки).

3. Использование существующих в АС линий и каналов связи для организации взаимодействия между средствами защиты.

4. Блокировка любой сетевой активности рабочей станции при отключении периферийных средств защиты.

5. Блокировка любой сетевой активности рабочей станции при обнаружении подозрительных действий на сетевом, аппаратном или программном уровнях работы АС.

6. К подозрительным действиям для каждой рабочей станции АС следует отнести:

а) инициализацию соединения с терминальным сервером до отправки запроса на загрузку ТОС;

б) сетевую активность рабочей станции после отключения периферийного средства защиты.

**Новая модель.** С целью нейтрализации векторов атак внутреннего нарушителя, рассмотренных для традиционных моделей доверенной загрузки, предлагается производить контроль временных интервалов процесса штатной загрузки – от включения рабочей станции до отправки запроса на получение образа ТОС к серверу. В зависимости от конечной реализации АС указанный интервал варьируется в диапазоне от 5 до 20 секунд, из которых большую часть времени занимает инициализация ПО BIOS (UEFI) рабочей станции [18]. Это позволяет блокировать атаки нарушителя, направленные на загрузку «ядовитой ТОС» в память рабочей станции со сторонних носителей или по сети.

Технологическая реализация новой модели сводится к внедрению в структуру АС периферийных модулей (далее – Модуль), центрального контроллера (далее – Контроллер) и специального программного обеспечения. Модуль подключается к LAN-порту (разъем 8P8C) каждой РСТТК, Контроллер размещается совместно с серверным массивом АС. Для связи Контроллера и Модулей предлагается исполь-

зовать существующие в АС линии связи 100/1000Base-TX между рабочими станциями и коммутационным оборудованием. Специальное программное обеспечение инсталлируется на ССЗ и выполняет функции обработки управляющих команд Контроллера и передачи управляющих команд межсетевому экрану АС, выполненному в виде отдельного узла сети или программного обеспечения ССЗ [1, 17].

Структурная схема и алгоритм работы новой модели доверенной сетевой загрузки ТОС представлены на рис. 1 и 2 соответственно.

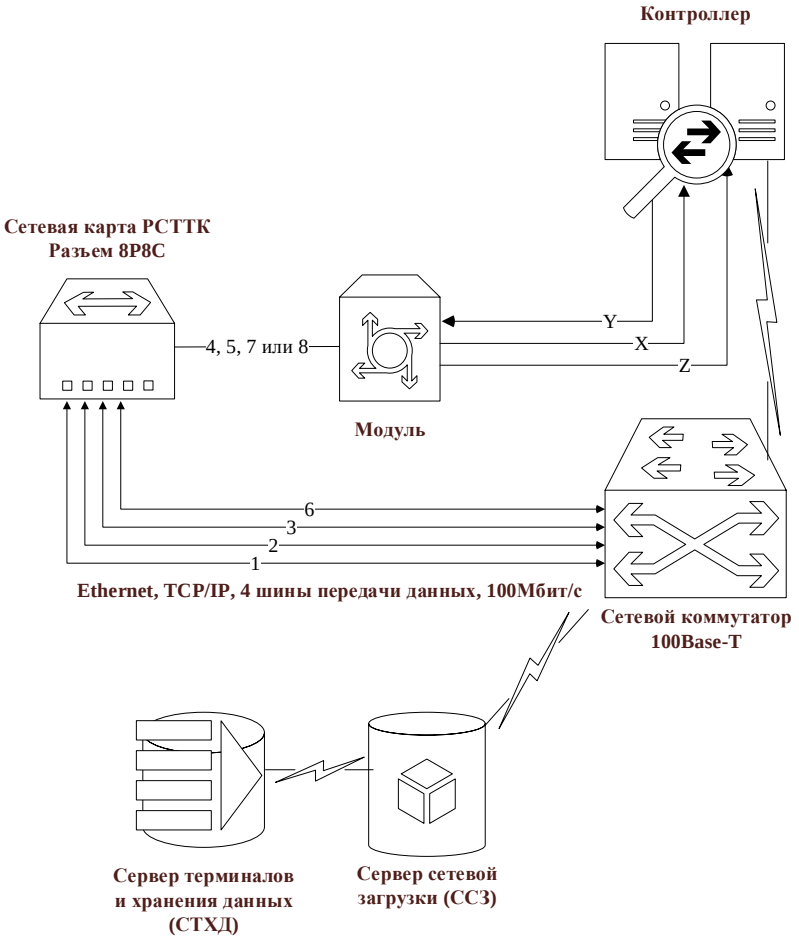


*Рис. 1. Структурная схема модели доверенной сетевой загрузки*

Технологическая группа «Модуль – Контроллер» в режиме реального времени фиксирует следующие состояния работы РСТТК:

а) рабочая станция включена, Модуль подключен (состояние 1);

б) рабочая станция выключена, Модуль подключен (состояние 2);

в) Модуль отключен (состояние 3).

Во внутренней энергонезависимой памяти Модуля содержатся 3 уникальных цифровых кода, соответствующих приведенным состояниям. Питание Модуля осуществляется Контроллером по линии «Y». Внутреннее устройство Модуля предполагает:

а) передачу уникальных кодов для состояний 1 и 2 по линии «X» в импульсном режиме в момент изменения режима работы сетевой карты РСТТК;

б) передачу уникального кода для состояния 3 по линии «Z» в постоянном режиме после подключения Модуля к сетевой карте РСТТК;

в) использование оболочки разъема 8P8C сетевой карты РСТТК для соединения линий «Y» и «Z».

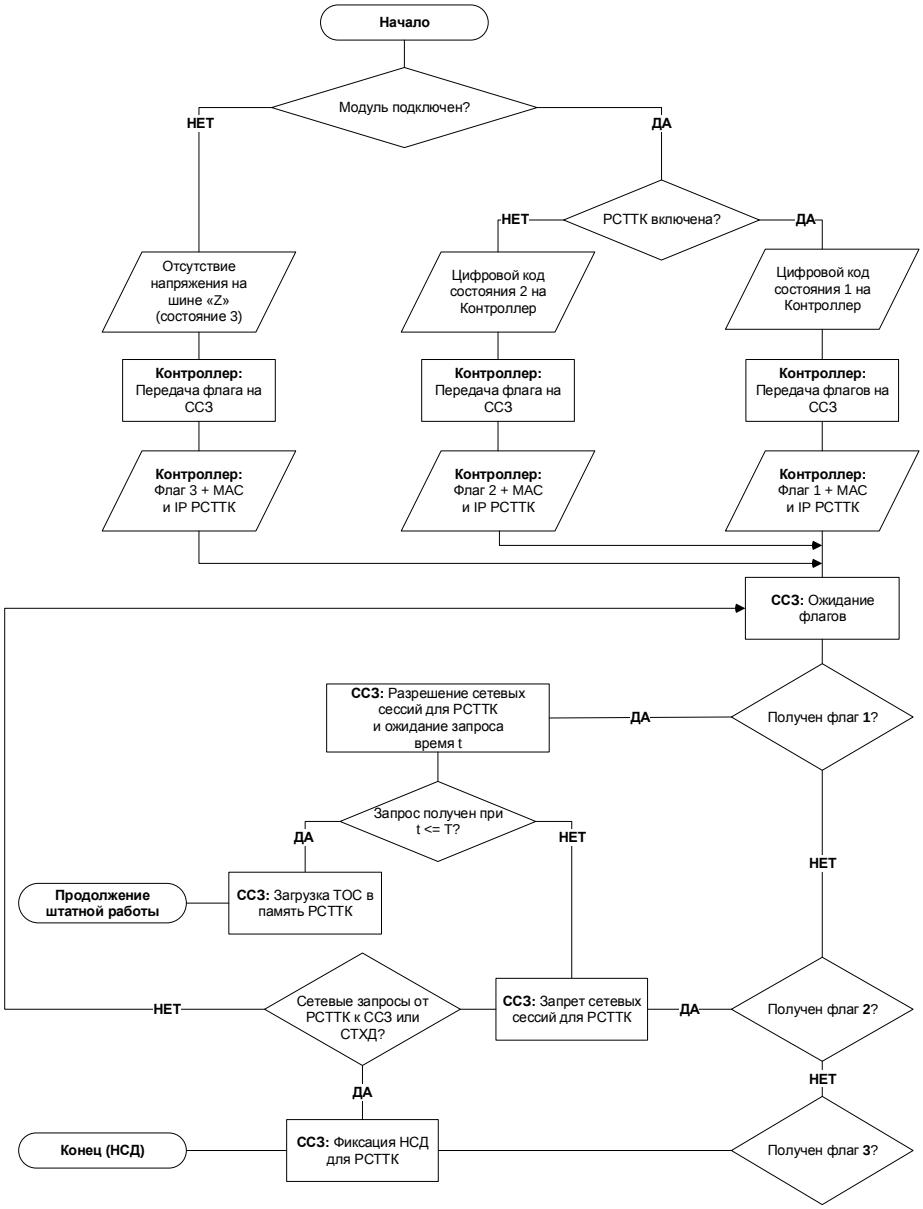


*Рис. 2. Функциональный алгоритм модели доверенной сетевой загрузки*

В энергонезависимой памяти Контроллера содержатся все уникальные цифровые коды для каждого используемого в системе Модуля. В случае использования нарушителем другого цифрового кода (симуляция штатной работы Модуля при его отсутствии), Контроллер игнорирует его и продолжает штатную работу в соответствии с приведенным на рис. 2 алгоритмом действий.

В памяти ССЗ запускается управляющее программное обеспечение, а также хранится заранее определенный для каждой рабочей станции АС временной интервал Т. В случае получения сетевого запроса от рабочей станции по истечении времени Т, ССЗ переходит в состояние блокировки сетевой активности с данной рабочей станцией и фиксирует событие НСД.

**Заключение.** В работе представлена разработка концепции и модели обеспечения доверенной сетевой загрузки ТОС в память рабочих станций с однозначной нейтрализацией представленных векторов атак внутреннего нарушителя. Предлагаемая модель доверенной сетевой загрузки «тонкого клиента» с нейтрализацией «внутреннего нарушителя» позволяет нейтрализовать атаки внутреннего нарушителя, направленные на обход установленных средств защиты информации. Разработаны сценарии использования новой модели с целью нейтрализации атак, характерных для традиционных методов обеспечения доверенной загрузки, которые представлены в табл. 1–3.

Таблица 1

**Сценарий изменения настроек ПО BIOS (UEFI)**

| № | Действие нарушителя | Реакция системы |
|---|---|---|
| 1 | Включение РСТТК | Фиксация включения РСТТК (состояние 1). Ожидание запроса на загрузку ТОС на стороне ССЗ, период времени Т |
| 2 | Несанкционированный вход в настройки ПО BIOS (UEFI) | В случае превышения периода ожидания Т, ССЗ блокирует сетевые запросы от РСТТК и фиксирует событие НСД! |
| 3 | Изменение параметров ПО BIOS (UEFI) | |
| 4 | Выключение РСТТК | Фиксация выключения РСТТК (состояние 2) |
| 5 | Подключение съемного носителя с образом «ядовитой ТОС» | Реакция отсутствует |
| 6 | Включение РСТТК | Фиксация включения РСТТК (состояние 1) |
| 7 | Загрузка «ядовитой ТОС» в память РСТТК | Время ожидания запроса на загрузку ТОС будет больше Т. ССЗ блокирует сетевые запросы от РСТТК и фиксирует событие НСД! |
| 8 | Попытка подключения к сетевым ресурсам АС средствами «ядовитой ТОС» | |

Таблица 2

**Сценарий внедрения в сетевую структуру «ядовитого ССЗ»**

| № | Действие нарушителя | Реакция системы |
|---|---|---|
| 1 | Подключение к кабельной сети АС «ядовитого ССЗ» | Реакция отсутствует |
| 2 | Включение РСТТК | Фиксация включения РСТТК (состояние 1) |
| 3 | Загрузка «ядовитой ТОС» в память РСТТК с «ядовитого ССЗ» | Ожидание запроса на загрузку ТОС, период времени Т на стороне ССЗ. При этом время ожидания будет больше Т. ССЗ блокирует сетевые запросы от РСТТК и фиксирует событие НСД! |
| 4 | Попытка подключения к сетевым ресурсам АС средствами «ядовитой ТОС» | |

Таблица 3

**Сценарий отключения Модуля от РСТТК**

| № | Действие нарушителя | Реакция системы |
|---|---|---|
| 1 | Отключение Модуля от РСТТК | Фиксация отсутствия сигнала на линии «Z» (состояние 3) |
| 2 | Загрузка «ядовитой ТОС» в память РСТТК любым возможным способом | Контроллер передает на ССЗ MAC и IP адрес РСТТК и команду блокировки любых сетевых запросов |
| 3 | Подключение Модуля к РСТТК | Контроллер фиксирует состояние 1, но ССЗ уже внес РСТТК в список блокировки |
| 4 | Попытка подключения к сетевым ресурсам АС средствами «ядовитой ТОС» | ССЗ блокирует сетевые запросы от РСТТК и фиксирует событие НСД! |

БИБЛИОГРАФИЧЕСКИЙ СПИСОК


1. *Nasimuddin A., Shekhar T., Neeraj A.* Practical Handbook of Thin-Client Implementation // New Age International. – 2005. – P. 214.
2. *Счастный Д.Ю.* Построение систем защиты от несанкционированного доступа к терминальным системам // Information Security/Информационная безопасность. – 2008. – № 2. – С. 48-49.
3. *Муха М.Д.* Система контроля целостности и аутентичности образов операционных систем, загружаемых по сети // Комплексная защита информации: Сборник мат. XII Международной конференции (Ярославль, 13–16 мая 2008 г.). – М., 2008. – С. 139-140.
4. *Kohlenberg T., Ben-Shalom O., Dunlop J., Rub J.* Evaluating Thin-Client Security in a Changing Threat Landscape // Intel Information Technology. Business Solutions. – 2010. – P. 8.
5. *Kelly E.* Thin Client 280 Success Secrets. – Emereo Publishing, 2014. – 206 p.
6. *Деревяшко В.В., Буцик К.А.* Проблемы защиты информации от несанкционированного доступа, современные средства защиты от НСД, перспективы и пути дальнейшего развития СЗИ от НСД // Актуальные вопросы информационной безопасности регионов в условиях глобализации информационного пространства: Сборник мат. III Всероссийской науч.-практ. конференции (Волгоград, 24–25 апреля 2014 г.). – Волгоград, 2014. – С. 201-206.
7. *Wojtczuk R., Kallenberg C.* Attacks on UEFI security, inspired by Darth Venamis's misery and Speed Racer // CanSecWest. – Vancouver, 2015.
8. *Юсупов Р.* Можно ли защититься от слежки и кражи данных при использовании информационных технологий? // Международная специализированная выставка-конференция по информационной безопасности Infobez-expo. – 2013. – 17 с.
9. *Счастный Д.Ю.* Аппаратная защита терминальных сессий // Комплексная защита информации: Сборник мат. X Международной конференции (Суздаль, 4–7 апр. 2006 г.). – Минск, 2006. – С. 135-136.
10. *Синякин С.А.* Особенности совместимости АККОРД-АМДЗ и современных СВТ // Комплексная защита информации: Сборник мат. XVIII Международной конференции (Брест, 21–24 мая 2013 г.). – Брест, 2013. – С. 102-105.
11. *Счастный Д.Ю.* Терминальные клиенты: начала защиты // Комплексная защита информации: Сборник мат. XIV Международной конференции (Минск, 19–22 мая 2009 г.). – Минск, 2009. – С. 210-211.
12. *Дударев Д.А., Полетаев В.М., Полтавцев А.В., Романцев Ю.В., Сырчин В.К.* Устройство создания доверенной среды для компьютеров информационно-вычислительных систем // Патент РФ № 2013131871/08, 11.07.2013.
13. *Reynolds G., Schwarzbacher A.* Th. Reducing IT Costs through the Design and Implementation of a Thin Client Infrastructure in Educational Environments // IEE Irish Signals and Systems Conference. – Dublin, 2006. – P. 28-30.
14. *Чугринов А.В.* Доверенные сеансы связи и средства их обеспечения // Information Security/Информационная безопасность. – 2010. – № 4. – С. 54-55.

15. Технология «Защищенный тонкий клиент» // Презентация компании «ANCUD». – Режим доступа: http://ancud.ru/presentation.html (дата обращения 13.11.2014).
16. *Гатчин Ю.А., Теплоухова О.А.* Реализация контроля целостности образа операционной системы, загружаемого по сети на тонкий клиент // Сборник тезисов докладов конгресса молодых ученых. Электронное издание. – СПб.: Университет ИТМО, 2015.
17. *Hocking M.* Feature: Thin client security in the cloud // Network Security. – 2011. – Issue 6. – P. 17-19.

REFERENCES

1. *Nasimuddin A., Shekhar T., Neeraj A.* Practical Handbook Of Thin-Client Implementation, *New Age International*, 2005, pp. 214.
2. *Schastnyy D.Yu.* Postroenie sistem zashchity ot nesanktsionirovannogo dostupa k terminal'nym sistemam [Building systems to protect against unauthorized access to the terminal systems], *Informatsionnaya bezopasnost'* [Information Security], 2008, No. 2, pp. 48-49.
3. *Mukha M.D.* Sistema kontrolya tselostnosti i autentichnosti obrazov operatsionnykh sistem, zagruzhaemykh po seti [Control system the integrity and authenticity of the operating system images that are downloaded over the network], *Kompleksnaya zashchita informatsii: Sbornik mat. XII Mezhdunarodnoy konferentsii (Yaroslavl', 13–16 maya 2008 g.)* [Integrated data protection: proceedings of the XII International conference (Moscow, 13-16 may 2008)]. Moscow, 2008, pp. 139-140.
4. *Kohlenberg T., Ben-Shalom O., Dunlop J., Rub J.* Evaluating Thin-Client Security in a Changing Threat Landscape, *Intel Information Technology. Business Solutions*, 2010, pp. 8.
5. *Kelly E.* Thin Client 280 Success Secrets. Emereo Publishing, 2014, 206 p.
6. *Derevyashko V.V., Butsik K.A.* Problemy zashchity informatsii ot nesanktsionirovannogo dostupa, sovremennye sredstva zashchity ot NSD, perspektivy i puti dal'neyshego razvitiya SZI ot NSD [Problems of information protection against unauthorized access, a modern means of protection against unauthorized access, Outlook, and ways of further development of GIS from unauthorized access], *Aktual'nye voprosy informatsionnoy bezopasnosti regionov v usloviyakh globalizatsii informatsionnogo prostranstva: Sbornik mat. III Vserossiyskoy nauch.-prakt. konferentsii (Volgograd, 24–25 aprelya 2014 g.)* [Current issues of information security of regions in the conditions of globalization of information space: Collection of materials of the III all-Russian scientific-practical conference (Volgograd, April 24-25, 2014). Volgograd, 2014, pp. 201-206.
7. *Wojtczuk R., Kallenberg C.* Attacks on UEFI security, inspired by Darth Venamis's misery and Speed Racer, *CanSecWest*.Vancouver, 2015.
8. *Yusupov R.* Mozhno li zashchitit'sya ot slezhki i krazhi dannykh pri ispol'zovanii informatsionnykh tekhnologiy? [Is it possible to defend against spying and data theft when using information technology?], *Mezhdunarodnaya spetsializirovannaya vystavka-konferentsiya po informatsionnoy bezopasnosti Infobez-expo* [International specialized exhibition-conference of information security Infobez-expo], 2013, 17 p.
9. *Schastnyy D.Yu.* Apparatnaya zashchita terminal'nykh sessiy [Hardware protection terminal sessions], *Kompleksnaya zashchita in-formatsii: Cbornik mat. X Mezhdunarodnoy konferentsii (Suzdal', 4–7 apr. 2006 g.).* [Integrated data protection: proceedings of the X International conference (Suzdal, 4-7 April 2006)]. Minsk, 2006, pp135-136.
10. *Sinyakin S.A.* Osobennosti sovmestimosti AKKORD-AMDZ i sovremennykh SVT [Features compatibility CHORD-ASGM and modern SVT], *Kompleksnaya zashchita informatsii: Sbornik mat. XVIII Mezhdunarodnoy konferentsii (Brest, 21–24 maya 2013 g.)* [Comprehensive protection of information: a Compilation of the Mat. XVIII International conference (Brest, 21-24 may 2013)]. Brest, 2013, pp. 102-105.
11. *Schastnyy D.Yu.* Terminal'nye klienty: nachala zashchity [Terminal clients: start protection], *Kompleksnaya zashchita informatsii: Sbornik mat. XIV Mezhdunarodnoy konferentsii (Minsk, 19-22 maya 2009 g.)* [Comprehensive protection of information: a Compilation of the Mat. XIV International conference (Minsk, may 19-22, 2009)]. Minsk, 2009, pp. 210-211.
12. *Dudarev D.A., Poletaev V.M., Poltavtsev A.V., Romantsev Yu.V., Syrchin V.K.* Ustroystvo sozdaniya doverennoy sredy dlya komp'yuterov informatsionno-vychislitel'nykh sistem [The device creating trusted environments for computers, information and computing systems]. Patent RF No. 2013131871/08, 11.07.2013.

13. *Reynolds G., Schwarzbacher A.* Th. Reducing IT Costs through the Design and Implementation of a Thin Client Infrastructure in Educational Environments, *IEE Irish Signals and Systems Conference*. Dublin, 2006, pp. 28-30.
14. *Chugrinov A.V.* Doverennye seansy svyazi i sredstva ikh obespecheniya [Trusted sessions and their means of support], *Informatsionnaya bezopasnost'* [Information Security], 2010, No. 4, pp. 54-55.
15. Tekhnologiya «Zashchishchennyy tonkiy klient» [Technology "Secure thin client", *Prezentatsiya kompanii «ANCUD»* [Company presentation "ANCUD"]. Available at: http://ancud.ru/presentation.html (Accessed 13 November 2014).
16. *Gatchin Yu.A., Teploukhova O.A.* Realizatsiya kontrolya tselostnosti obraza operatsionnoy sistemy, zagruzhaemogo po seti na tonkiy klient [Implementation monitoring the integrity of the operating system image that is loaded over the network to the thin client], *Sbornik tezisov dokladov kongressa molodykh uchenykh. Elektronnoe izdanie* [The book of abstracts of the Congress of young scientists. Electronic edition]. St. Petersburg: Universitet ITMO, 2015.
17. *Hocking M.* Feature: Thin client security in the cloud, *Network Security,* 2011, Issue 6, pp. 17-19.

Статью рекомендовал к опубликованию к.т.н. А.П. Еремеев.

**Тищенко Евгений Николаевич** – ФГБОУ ВПО «РГЭУ (РИНХ)»; e-mail: celt@inbox.ru; 344002, г. Ростов-на-Дону, ул. Большая Садовая, 69; тел.: 89281440403; профессор; зав. кафедрой.

**Буцик Кирилл Александрович** – e-mail: akademik@spark-mail.ru; тел.: 89094084213; аспирант.

**Деревяшко Вадим Вадимович** – e-mail: godzevs@mail.ru; тел.: 89185340736; аспирант.

**Tishenko Evgeniy Nikolaevich** – FGBOU VPO "RSUE (RINH)"; e-mail: celt@inbox.ru; 69, Bolshaya Sadovaya street, Rostov-on-Don, 344002, Russia; phone: +79281440403; professor; head of department.

**Butsik Kirill Alexandrovich** – e-mail: akademik@spark-mail.ru; phone: +79094084213; postgraduate student.

**Derevyashko Vadim Vadimovich** – e-mail: godzevs@mail.ru; phone: +79185340736; postgraduate student.

УДК 004.771

**Р.В. Сёмин, В.А. Новосядлый**

## ИССЛЕДОВАНИЕ ЗАДАЧИ АКТИВНОГО АУДИТА ПАРОЛЬНОЙ ПОЛИТИКИ В КОМПЬЮТЕРНЫХ СЕТЯХ

*На настоящий момент угрозам информационной безопасности в компьютерных сетях уделяется большое внимание. Различные утечки баз данных с паролями показывают, что даже хорошо построенная система безопасности может быть уязвима по причине слабой парольной политики. Для обнаружения слабых сторон в парольной безопасности применяются методы активного аудита, а именно тесты на проникновение. В статье рассматривается непосредственно фаза атаки на объекты компьютерной сети. На результаты проведения тестов могут негативно влиять ряд факторов, которые приводят к возникновению так называемых «ложных срабатываний», вызванных ненадёжностью или недостаточной скоростью работы тех или иных узлов сети. К таким факторам, например, относится как само использование компьютерных сетей, так и использование прокси-серверов при проведении аудита. Особое внимание уделяется именно влиянию прокси-серверов на систему проведения аудита. Цель данного исследования – выявление характерных особенностей процесса активного аудита парольной политики и конструирование*