DOI: https://doi.org/10.15688/jvolsu10.2017.4.4

УДК 004.771
ББК 32.81

ИССЛЕДОВАНИЕ И МОДЕЛИРОВАНИЕ СИСТЕМ ДОВЕРЕННОЙ ЗАГРУЗКИ «ТОНКОГО КЛИЕНТА»

Евгений Николаевич Тищенко

Доктор экономических наук,
заведующий кафедрой информационных технологий и защиты информации,
Ростовский государственный экономический университет (РИНХ)
celt@rsue.ru
ул. Большая Садовая, 69, 344002 г. Ростов-на-Дону, Российская Федерация

Кирилл Александрович Буцик

Аспирант кафедры информационных технологий и защиты информации,
Ростовский государственный экономический университет (РИНХ)
celt@rsue.ru
ул. Большая Садовая, 69, 344002 г. Ростов-на-Дону, Российская Федерация

Аннотация. В статье рассматривается процесс доверенной загрузки «аппаратного тонкого клиента» в типовой автоматизированной системе. Рассматривается процесс загрузки операционной системы в память рабочих станций с использованием как съемных носителей, так и технологии сетевой загрузки PXE. Проводится аналитическое моделирование указанного процесса с позиции воздействий внутреннего и внешнего нарушителей. Разрабатывается формальная модель нарушителей – условное математическое представление их воздействий на процесс доверенной загрузки. Определяются факторы, характеризующие повышенную опасность атак внутреннего нарушителя. Проводится моделирование идеального процесса доверенной загрузки, характеризуемого полным противодействием атакам нарушителей. Определяются факторы, необходимые любому процессу доверенной загрузки для приближения к идеальному состоянию, и недостатки современных систем доверенной загрузки, основанных исключительно на контроле состояний внедренных защитных механизмов. Приводится перечень характеристик, требующих оптимизации, с целью разработки альтернативного метода обеспечения доверенной загрузки «аппаратного тонкого клиента». В качестве альтернативы предлагается контролировать не состояния (реакции) защитных механизмов, но временные характеристики штатного процесса загрузки. Указанные характеристики подвергаются нормированию – получению и записи штатных значений на основании собранной статистики в период функционирования автоматизированной системы при отсутствии воздействий нарушителей. В ходе каждого последующего запуска процесса загрузки его временные характеристики сравниваются с нормированными значениями. На основании допустимой или недопустимой разницы значений делается вывод о возможном воздействии внутреннего нарушителя на процесс загрузки, что позволяет полноценно контролировать все этапы процесса доверенной загрузки, а не только состояния защитных механизмов, занимающих только часть этапов.

Ключевые слова: нарушитель, уязвимость, успешность атаки, этап загрузки, время исполнения.

Формальная модель нарушителя

Современные подходы к математическому описанию нарушителей в автоматизированных (информационных) системах предполагают, что любая атака любого нарушителя зависит от следующих факторов: наличие уязвимости в атакуемой системе или компоненте системы (V), вероятность обнаружения такой уязвимости нарушителем (P) и способность нарушителя к успешной эксплуатации выявленной уязвимости (s) [1; 2].

Исходя из утверждения, что при любой реализации автоматизированной системы (далее по тексту – АС) полное отсутствие уязвимостей в ее компонентах принципиально невозможно ($\Sigma(V) \neq 0$), допустимо от использования бинарного параметра $V = \{0,1\}$ перейти к параметру n – количеству имеющихся уязвимостей в атакуемой АС или ее компонентах.

Приняв за основу результаты моделирования атак нарушителей, изложенные в работах [2] и [9], а также утверждение, что любая атака может рассматриваться как совокупность реализаций атак на каждую выявленную нарушителем уязвимость, допустимо представить результирующую способность нарушителя к совершению успешной атаки (S) следующим образом:

$$S = \sum_{i=1}^{n} \left(P_i, s_i\right) \qquad (1)$$

Следует отметить, что в любой АС, оборудованной комплексной системой информационной безопасности (далее по тексту – СИБ), задача нарушителя по выявлению и эксплуатации уязвимостей в первую очередь переносится в пространство самой СИБ. То есть $S = S_{\text{СИБ}} + C$, где C – константа, определяющая уязвимости АС, не зависящие от внедрения СИБ. При этом представление $S_{\text{СИБ}}$ аналогично выражению (1).

Также следует учесть, что выражение (1) и его интерпретация в части СИБ справедливы лишь для абстрактной АС. В АС, построенной на базе технологии «аппаратный тонкий клиент», существует принципиальное разделение на направления поиска уязвимостей нарушителем: рабочая станция пользователя (R), каналы связи и коммутационное оборудование (K) и серверы терминалов и хранения данных (D) [3]. Следовательно, результирующую успешность атаки на компоненты СИБ такой АС возможно принципиально (без уточнения приоритетов нарушителя и критичности уязвимостей) представить совокупностью успешных атак в указанных направлениях:

$$S_{\text{СИБ}} = \sum_{i=1}^{n} S_{Ri} \text{ Y} \sum_{i=1}^{n} S_{Ki} \text{ Y} \sum_{i=1}^{n} S_{Di} \qquad (2)$$

Принимая во внимание преимущества технологии «аппаратный тонкий клиент», одним из которых является использование терминальной операционной среды (далее по тексту – ТОС), справедливо утверждать, что в составе СИБ на стороне рабочей станции имеются только две компоненты: доверенная загрузка (ДЗ) и ограничение программной среды ТОС (ОПС):

$$S_R = \max\left\{\sum_{i=1}^{n} S_{\text{ДЗ}i}; \sum_{i=1}^{n} S_{\text{ОПС}i}\right\} \qquad (3)$$

Идеальная модель

Для описания идеальной модели доверенной загрузки «аппаратного тонкого клиента» необходимо определиться с функциональным видом (выражением) самого процесса доверенной загрузки. Анализ типового процесса загрузки ТОС в память рабочей станции, а также результаты анализа современных отечественных систем и алгоритмов доверенной загрузки позволяют представить процесс доверенной загрузки кусочно-заданной функцией на заранее определенном множестве интервалов – конечном числе этапов работы штатного процесса загрузки ТОС [4]. Точки смены формул такой функции являются началом исполнения каждого последующего эта-

па x_i, где i {1, 2, ..., 7} в случае локальной загрузки и i {1, 2, ..., 9} – в случае сетевой.

Важно понимать, что $x_1 \neq 0$ и $x_i = x_i(t)$, где t – время исполнения этапов загрузки ($t_0 > 0$). Это означает, что в нулевой момент времени и ранее ($t \leq 0$) функция не существует (не задана), поскольку с технической точки зрения начало процесса доверенной загрузки совпадает с одновременным использованием всех ключевых элементов АС (рабочая станция, носитель ТОС, коммутационное оборудование и т. д.), что в целом соответствует понятию «доверенная загрузка», утвержденному ФСТЭК России [5].

Однако помимо прямой зависимости от этапов штатной загрузки, ключевой задачей процесса доверенной загрузки является противостояние атакам нарушителей. Учитывая рассмотренную выше условную модель нарушителя, это означает снижение вероятности и способности нарушителя к эксплуатации уязвимостей на каждом этапе штатного процесса загрузки до допустимого минимума. При этом вероятность выявления и способность эксплуатации уязвимостей нарушителем также можно представить параметрическими функциями от времени исполнения каждого этапа. Следовательно, процесс доверенной загрузки можно определить через функцию успешности совершения атаки нарушителем:

$$S_{\text{ДЗ}} \leftrightarrow \begin{cases} f(P,s) \\ P(t) \\ s(t) \end{cases} \qquad (4)$$

Тогда для *идеального* случая (полная нейтрализация атак нарушителей): $S_{\text{ДЗ}} = 0$ при $\forall t \in x_i$. Из чего допустимо сделать вывод о характере непрерывности загрузки и возможности ее дифференцирования на любом временном отрезке существования. То есть процесс доверенной загрузки должен быть задан кусочно-гладкой функцией, для которой в идеальном случае (рис. 1):

$$f'(P,s) = \lim_{\Delta t \to 0} \frac{S_{\text{ДЗ}}(t+\Delta t) - S_{\text{ДЗ}}(t)}{\Delta t} = 0 \qquad (5)$$

В свою очередь, реальный процесс доверенной загрузки с учетом воздействий (атак) нарушителя однозначно характеризуется $f'(P, s) \neq 0$ (рис. 2).

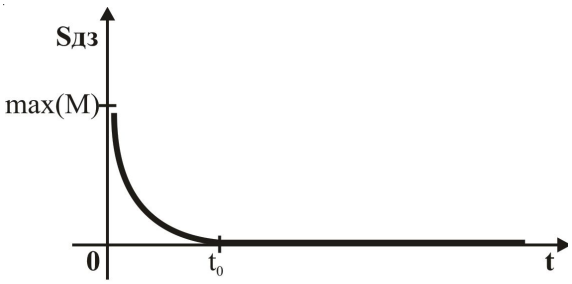

Рис. 1. Условное представление идеального процесса доверенной загрузки

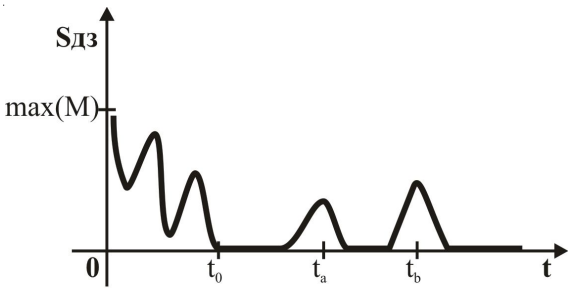

Рис. 2. Условное представление реального процесса доверенной загрузки

Современные системы

На основании рассмотренных выше данных допустимо сформулировать основную задачу идеального процесса «доверенной загрузки» как обеспечение стабильной нейтрализации ($S_{\text{ДЗ}} = 0$) возможностей нарушителя по выявлению ($P(t) = 0$) и эксплуатации ($s(t) = 0$) уязвимостей в любых временных периодах исполнения каждого этапа штатного процесса загрузки ($\forall t \in x_i$).

Современные отечественные СИБ решают указанную задачу за счет последовательного внедрения и эксплуатации защитных механизмов (j) [6]. По времени исполнения такие механизмы занимают либо часть определенного этапа x_i, либо весь этап. При этом оценка эффективности ДЗ определяется суммарной оценкой для совокупности внедренных защитных механизмов (k) возможности оказывать противодействие атакам нарушителя [7; 8]. То есть идеальная современная система ДЗ в рамках рассмотренной выше взаимосвязи с условной моделью нарушителя может быть представлена следующим образом:

$$S_{\text{ДЗ}} = \begin{cases} \sum_{j=1}^{k} f_j(P,s) = 0 \\ f_j'(P,s) = 0 \end{cases} \quad (6)$$

Однако выражение (6) не позволяет описать процесс доверенной загрузки при $t \neq t_j$, то есть в периоды времени, не связанные с работой защитных механизмов. Тогда, принимая во внимание уровень подготовки нарушителя, допустимо сделать вывод, что $t \neq t_j \rightarrow 0 < S_{\text{ДЗ}}(t) \leq \max(M)$. Это может являться критичным в случаях, когда результирующая успешность атаки нарушителя на всю систему доверенной загрузки зависит от реализации *косвенных* (потенциально опасных) атак на различных этапах штатного процесса загрузки: $S_{\text{ДЗ}} = S(t_a) + S(t_b) = \max(M)$, где $b > a$ и t_a, $t_b \neq t_j$ (рис. 3). Простейшим примером может являться успешная загрузка нештатной ТОС со стороннего съемного носителя после проведения успешной атаки по модификации ПО BIOS.

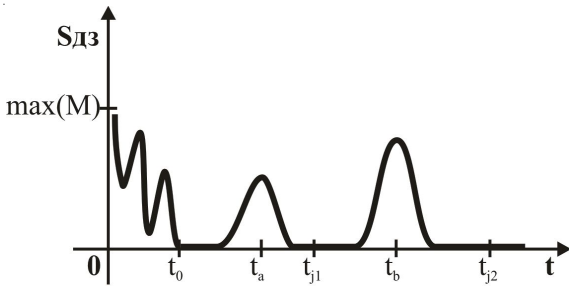

Рис. 3. Условное представление современных систем доверенной загрузки

Таким образом, достижение свойств идеальной модели для современных систем доверенной загрузки возможно исключительно за счет повышения качественно-количественных характеристик внедряемых защитных механизмов с целью противодействия атакам нарушителей, направленным на выявление и эксплуатацию новых (0-day) уязвимостей как в компонентах АС, так и в самой СИБ. Что в целом подтверждает выводы Теории Игр в части представления противостояния «нарушитель – администратор» в качестве ориентированного графа с целью моделирования процесса «игры на опережение» [8; 10].

Однако как только нарушитель получит ключевое преимущество, связанное с возможностью эксплуатации выявленной уязвимости в штатном процессе загрузки ТОС безотносительно уязвимостей в защитных механизмах, эффективность реализованной системы доверенной загрузки примет нулевое значение, а результирующая успешность атаки нарушителя – максимальное:

$$S_{\text{ДЗ}} = \begin{cases} \sum_{j=1}^{k} f_j(P,s) = 0 \\ f_j'(P,s) = 0 \\ \sum f_i(P,s) = \max(M) \\ f_j'(P,s) \neq 0 \\ t_i \neq t_j \end{cases} \quad (7)$$

Внутренний нарушитель

Внутренний нарушитель по отношению к внешнему характеризуется рядом принципиальных преимуществ, более подробно описанных в исследованиях отечественных и зарубежных специалистов [7], [11], [13] и [14]:

а) отсутствие временных ограничений на проведение атаки при ее разделении на несколько самостоятельных этапов;

б) достаточность времени на изучение структуры и функционала СИБ;

в) возможность использования любых компонент СИБ, выданных пользователю АС в штатном порядке (например, ключевые носители).

Следует отметить, что в зависимости от реализации процесса ДЗ преимущество «в» зачастую позволяет внутреннему нарушителю игнорировать часть защитных механизмов: $S_{\text{ДЗ}} = \max(M)$ при $f'(P, s)=0$.

С учетом указанных преимуществ необходимо уточнить, что выражения (4), (6) и (7) в полной мере актуальны только для внешнего нарушителя. В действительности, поскольку возможности выявления $P(t)$ и эксплуатации $s(t)$ уязвимостей – параметрические функции, зависящие от времени исполнения этапов штатного процесса загрузки, постольку преимущества внутреннего нарушителя «а» и «б» позволяют ему игнорировать стадию выявления уязвимостей ($\sum P(t) = 1, \forall t \geq 0$). Для

внутреннего нарушителя штатная загрузка ТОС и, как следствие, доверенная загрузка представляются периодическим процессом с практически неограниченным периодом повтора этапов x_i. Фактически, это означает отсутствие временных ограничений внутри каждого этапа на выявление уязвимостей вне зависимости от величины конечного времени исполнения любого этапа. Следовательно, внутренний нарушитель способен повторять весь процесс «доверенной загрузки» заново до тех пор, пока не выявит все возможные уязвимости: $\lim_{T\to\infty} P(t)=1$, где $T=\sum t, t\in x_i$.

Однако в части $s(t)$ внутренний нарушитель не имеет преимуществ перед внешним. Это утверждение верно, поскольку эксплуатация любой уязвимости всегда является активным методом воздействия на компоненты уязвимой системы и, как следствие, требует некоторого количества времени на реализацию [12; 15]. При этом в случае неудачной эксплуатации уязвимости нарушитель рискует быть обнаруженным СИБ. Следовательно, число повторных исполнений штатных этапов для внутреннего нарушителя конечно ($T \neq \infty$), а рост $s(t)$ влечет за собой увеличение временной задержки на исполнение этапа.

Таким образом, при условии фиксации и последующей оценке – нормировании – штатного значения времени исполнения для каждого этапа успешность атаки внутреннего нарушителя будет определяться совокупностью его способностей по эксплуатации выявленных уязвимостей, не выходя за границы нормированных значений времени исполнения каждого этапа x_i:

$$S_{\text{ДЗ}} = \begin{cases} \sum f(s) \\ s(t) \to 1 \\ t \le t_{\text{норм}} \end{cases} \qquad (8)$$

Результаты и выводы

По результатам проведенного моделирования справедливо утверждать, что подход, основанный на контроле исключительно внедренных (встроенных) в процесс штатной загрузки защитных механизмов не является оптимальным. Проблема оптимизации такого подхода заключается в отсутствии контроля временных характеристик, определяющих связь между эффективной работой защитных механизмов и вероятностью выявления и способностью эксплуатации нарушителем уязвимостей как в самих механизмах, так и в структуре процесса штатной загрузки и компонентах АС. То есть попытка реализации замкнутого технологического процесса средствами внедрения защитных механизмов СДЗ обречена на постоянный (монотонный) рост числа защитных механизмов с целью максимального покрытия пространства возможностей нарушителя.

С целью оптимизации (модернизации) системы доверенной загрузки «аппаратного тонкого клиента» необходимо разработать и реализовать метод, позволяющий:

- фиксировать нормированные значения времени исполнения каждого этапа штатного процесса загрузки «тонкого клиента» ($x_{\text{норм}}(t)$);
- контролировать время исполнения каждого этапа штатного процесса загрузки «тонкого клиента» ($x(t)$, $t_0 > 0$);
- фиксировать любые отклонения времени исполнения на каждом этапе процесса штатной загрузки;
- выносить непротиворечивые решения на основании собранных данных по каждому зафиксированному случаю временных отклонений;
- приостанавливать процесс штатной загрузки при условии подозрения на атаку нарушителя ($f_i'(P,s) \neq 0$);
- отказаться от качественной оценки эффективности защитных механизмов непосредственно на этапах штатного процесса загрузки;
- отказаться от использования защитных механизмов внутри пространства, доступного нарушителю для компрометации.

Разработанный метод и/или его техническая реализация должны также учитывать состояние системы при $0 \le t < t_0$, то есть контролировать активность нарушителя до момента включения рабочей станции. Это опосредовано возможностью нарушителя реализовать атаку до начала фактического исполнения процесса штатной загрузки ($S_{\text{ДЗ}}(t) = \max(M)$, $t < t_0$) – например, подключить к коммутационному оборудованию АС стороннюю рабочую станцию.

СПИСОК ЛИТЕРАТУРЫ

1. Гатчин, Ю. А. Реализация контроля целостности образа операционной системы, загружаемого по сети на тонкий клиент / Ю. А. Гатчин, О. А. Теплоухова // Научно-технический вестник информационных технологий, механики и оптики. – 2015. – Т. 15, № 6. – С. 1115–1121.

2. Деревяшко, В. В. Проблемы защиты информации от несанкционированного доступа, современные средства защиты от НСД, перспективы и пути дальнейшего развития СЗИ от НСД / В. В. Деревяшко, К. А. Буцик // Актуальные вопросы информационной безопасности регионов в условиях глобализации информационного пространства : сб. материалов III Всерос. науч.-практ. конф. (г. Волгоград, 24–25 апр. 2014 г.). – Волгоград : Изд-во ВолГУ, 2014. – С. 48–49.

3. Муха, М. Д. Система контроля целостности и аутентичности образов операционных систем, загружаемых по сети / М. Д. Муха // Комплексная защита информации : сб. материалов XII Междунар. конф. (г. Ярославль, 13–16 мая 2008 г.). – М., 2008. – С. 139–140.

4. Синякин, С. А. Особенности совместимости АККОРД-АМДЗ и современных СВТ / С. А. Синякин // Комплексная защита информации : сб. материалов XVIII Междунар. конф. (г. Брест, 21–24 мая 2013 г.). – Брест, 2013. – С. 102–105.

5. Счастный, Д. Ю. Аппаратная защита терминальных сессий / Д. Ю. Счастный // Комплексная защита информации : сб. материалов X Междунар. конф. (г. Суздаль, 4–7 апр. 2006 г.). – Минск, 2006. – С. 135–136.

6. Счастный, Д. Ю. Построение систем защиты от несанкционированного доступа к терминальным системам / Д. Ю. Счастный // Information Security/Информационная безопасность. – 2008. – № 2. – С. 201–206.

7. Счастный, Д. Ю. Терминальные клиенты: начала защиты / Д. Ю. Счастный // Комплексная защита информации : сб. материалов XIV Междунар. конф. (г. Минск, 19–22 мая 2009 г.). – Минск, 2009. – С. 210–211.

8. Технология «Защищенный тонкий клиент» // [Презентации компании «ANCUD»]. – Электрон. дан. – Режим доступа: http://ancud.ru/presentation.html (дата обращения: 13.11.2014). – Загл. с экрана.

9. Устройство создания доверенной среды для компьютеров информационно-вычислительных систем : пат. № 2538329 Российская Федерация / Д. А. Дударев, В. М. Полетаев, А. В. Полтавцев, Ю. В. Романцев, В. К. Сырчин ; патентообладатель Общество с ограниченной ответственностью Фирма «АНКАД» (RU). – № 2013131871/08 ; заявл. 11.07.2013 ; опубл. 10.01.2015, Бюл. № 1. – 22 с. : ил.

10. Чугринов, А. В. Доверенные сеансы связи и средства их обеспечения / А. В. Чугринов // Information Security/Информационная безопасность. – 2010. – № 4. – С. 54–55.

11. Юсупов, Р. Можно ли защититься от слежки и кражи данных при использовании информационных технологий? : [презентация на Международной специализированной выставке-конференции по информационной безопасности «Infobez-expo 2013»] / Р. Юсупов. – Электрон. дан. – М., 2013. – 17 с. – Режим доступа: https://www.slideserve.com/melvyn/4087724. – Загл. с экрана.

12. Evaluating Thin-Client Security in a Changing Threat Landscape / T. Kohlenberg, O. Ben-Shalom, J. Dunlop, J. Rub // Intel Information Technology. Business Solutions. – 2010. – P. 8.

13. Hocking, M. Feature: Thin client security in the cloud / M. Hocking // Network Security. – 2011. – Iss. 6. – P. 17–19.

14. Kelly, E. Thin Client 280 Success Secrets / E. Kelly. – Emereo Publishing, 2014. – 206 p.

15. Nasimuddin, A. Practical Handbook of Thin-Client Implementation / A.Nasimuddin, T. Shekhar, A. Neeraj // New Age International. – 2005. – P. 214.

16. Reynolds, G. Reducing IT Costs through the Design and Implementation of a Thin Client Infrastructure in Educational Environments / G. Reynolds, A. Th. Schwarzbacher // IEE Irish Signals and Systems Conference. – Dublin, 2006. – P. 28–30.

17. Wojtczuk, R. Attacks on UEFI security, inspired by Darth Venamis's misery and Speed Racer /R. Wojtczuk, C. Kallenberg // CanSecWest. – Vancouver, 2015.

REFERENCES

1. Gatchin Yu.A., Teploukhova O.A. Realizatsiya kontrolya tselostnosti obraza operatsionnoy sistemy, zagruzhaemogo po seti na tonkiy klient [Controlling the Integrity Operating System Image Loaded over the Network to the Thin Client]. *Nauchno-tekhnicheskiy vestnik informatsionnykh tekhnologiy, mekhaniki i optiki*, 2015, vol. 15, no. 6, pp. 1115-1121.

2. Derevyashko V.V., Butsik K.A. Problemy zashchity informatsii ot nesanktsionirovannogo dostupa, sovremennye sredstva zashchity ot NSD, perspektivy i puti dalneyshego razvitiya SZI ot NSD [Problems of Information Protection from Unauthorized Access, Modern Means of Protection Against Unauthorized Access, Prospects and Ways of Further Development of SZI from NSD]. *Aktualnye voprosy informatsionnoy bezopasnosti regionov v usloviyakh globalizatsii informatsionnogo prostranstva: sb. materialov III Vseros. nauch.-prakt. konf. (g. Volgograd, 24–25 apr. 2014 g.)* [Current Issues

of Information Security of Regions in the Conditions of Globalization of Information Space: Collected Materials of the 3rd All-Russian Research and Practice Conference (Volgograd, April 24-25, 2014)]. Volgograd, Izd-vo VolGU, 2014, pp. 48-49.

3. Mukha M.D. Sistema kontrolya tselostnosti i autentichnosti obrazov operatsionnykh sistem, zagruzhaemykh po seti [The System of Controlling the Integrity and Authenticity of the Operating System Images that Are Downloaded over the Network]. *Kompleksnaya zashchita informatsii: sb. materialov XII Mezhdunar. konf. (g. Yaroslavl, 13–16 maya 2008 g.)* [Complex Protection of Information: Collected Materials of the 12th International Conference (Yaroslavl, May 13-16, 2008)]. Moscow, 2008, pp. 139-140.

4. Sinyakin S.A. Osobennosti sovmestimosti AKKORD-AMDZ i sovremennykh SVT [Features of Compatibility of ACCORD-ASGM and Modern SVT]. *Kompleksnaya zashchita informatsii: sb. materialov XVIII Mezhdunar. konf. (g. Brest, 21–24 maya 2013 g.)* [Complex Protection of Information: Collected Materials of the 18th International Conference (Brest, May 21-24, 2013)]. Brest, 2013, pp. 102-105.

5. Schastnyy D.Yu. Apparatnaya zashchita terminalnykh sessiy [Hardware Protection of Terminal Sessions]. *Kompleksnaya zashchita informatsii: sb. materialov X Mezhdunar. konf. (g. Suzdal, 4–7 apr. 2006 g.)* [Complex Protection of Information: Collected Materials of the 10th International Conference (Suzdal, April 4-7, 2006)]. Minsk, 2006, pp. 135-136.

6. Schastnyy D.Yu. Postroenie sistem zashchity ot nesanktsionirovannogo dostupa k terminalnym sistemam [The Construction of Systems of Protection Against Unauthorized Access to the Terminal Systems]. *Informatsionnaya bezopasnost* [Information Security], 2008, no. 2, pp. 201-206.

7. Schastnyy D.Yu. Terminalnye klienty: nachala zashchity [Terminal Clients: Start Protection]. *Kompleksnaya zashchita informatsii: sb. materialov XIV Mezhdunar. konf. (g. Minsk, 19–22 maya 2009 g.)* [Complex Protection of Information: Collected Materials of the 14th International Conference (Minsk, May 19-22, 2009)]. Minsk, 2009, pp. 210-211.

8. Tekhnologiya «Zashchishchennyy tonkiy klient» [Technology "Secure Thin Client"]. *ANCUD Company's Presentation*. URL: http://ancud.ru/presentation.html (accessed November 13, 2014).

9. Dudarev D.A., Poletaev V.M., Poltavtsev A.V., Romantsev Yu.V., Syrchin V.K. *Ustroystvo sozdaniya doverennoy sredy dlya kompyuterov informatsionno-vychislitelnykh sistem: pat. № 2538329 Rossiyskaya Federatsiya* [The Device for Creating a Trusted Environment for Computers, Information and Computing Systems: Patent 2538329 Russian Federation]. Patent owner: ANKAD Ltd.; no. 2013131871/08 ; published on January 10, 2015, Bull. no. 1. 22 p.

10. Chugrinov A.V. Doverennye seansy svyazi i sredstva ikh obespecheniya [Trusted Sessions and Means of Their Support]. *Informatsionnaya bezopasnost* [Information Security], 2010, no. 4, pp. 54-55.

11. Yusupov R. Mozhno li zashchititsya ot slezhki i krazhi dannykh pri ispolzovanii informatsionnykh tekhnologiy? [Can People Protect Themselves From Surveillance and Data Theft When Using Information Technology?]. *Prezentatsiya na Mezhdunarodnoy spetsializirovannoy vystavke-konferentsii po informatsionnoy bezopasnosti «Infobez-expo 2013»* [Presentation at the International Specialized Exhibition-Conference on Information Security "Infobez-expo 2013"], 2013. 17 p.

12. 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.

13. Hocking M. Feature: Thin client security in the cloud. *Network Security*, 2011, iss. 6, pp. 17-19.

14. Kelly E. *Thin Client 280 Success Secrets*. Emereo Publishing, 2014. 206 p.

15. Nasimuddin A., Shekhar T., Neeraj A. Practical Handbook of Thin-Client Implementation. *New Age International*, 2005, p. 214.

16. 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.

17. WojtczukR., Kallenberg C. Attacks on UEFI security, inspired by Darth Venamis's misery and Speed Racer. *CanSecWest*. Vancouver, 2015.

INVESTIGATION AND MODELING OF THIN-CLIENT TRUSTED PLATFORM SYSTEM

Evgeniy Nikolaevich Tishchenko

Doctor of Economic Sciences,
Head of Department of Information Technologies and Information Protection,
Rostov State Economic University
celt@rsue.ru
Bolshaya Sadovaya St., 69, 344002 Rostov-on-Don, Russian Federation

Kirill Aleksandrovich Butsik

Postgraduate Student,
Department of Information Technologies and Information Protection,
Rostov State Economic University
celt@rsue.ru
Bolshaya Sadovaya St., 69, 344002 Rostov-on-Don, Russian Federation

Abstract. The article discusses the process of trusted boot "hardware thin client" in a typical automated system. The process of loading the operating system into memory workstations is carried out using removable media, and technology network PXE boot. The analytical modeling of this process is performed from the perspective of the impacts of internal and external violators. The authors develop a formal model of the violators – a conditional mathematical representation of their impacts on the process of trusted boot. The factors that characterize the increased risk of attack from internal intruder, are outlined. An ideal boot process, characterized by the complete counter-attacks of the violators is simulated. The factors required of any trusted boot process for the approximation to the ideal state, are outlined. The authors identify the limitations of the modern systems for trusted boot based solely on the control of implemented protective mechanisms. The research provides a list of characteristics that require optimization with the aim of developing an alternative method of ensuring trusted boot "hardware thin client". Alternatively, it is proposed to control not conditions (reactions) of defense mechanisms, but the temporal characteristics of the regular boot process. These characteristics are subjected to standardization – obtaining and recording staffing values based on statistics collected during the operation of the automated system in the absence of effects offenders. During each subsequent run of the boot process, its transient characteristics are compared with normalized values. On the basis of valid or invalid values differences, the conclusion about the possible impact of domestic violator on the boot process is made. That enables controlling all stages of boot, and not just the status of the protective mechanisms that occupies only part of the stages.

Key words: intruder, vulnerability, success of attack, loading stage, time of execution.