УДК 004

**К.А. Буцик, Е.Н. Тищенко**

Россия, Ростов-на-Дону, Ростовский государственный
экономический университет (РИНХ)

# МАТЕМАТИЧЕСКАЯ МОДЕЛЬ НАРУШИТЕЛЯ ПРОЦЕССА ДОВЕРЕННОЙ ЗАГРУЗКИ «АППАРАТНОГО ТОНКОГО КЛИЕНТА»

Разрабатывается формальная модель нарушителя – условное математическое представление их воздействий на процесс доверенной загрузки. Определяются недостатки современных систем доверенной загрузки, основанных исключительно на контроле состояний внедренных защитных механизмов. В качестве альтернативы предлагается контролировать не состояния (реакции) защитных механизмов, но временные характеристики штатного процесса загрузки. Это 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.

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].

Исходя из утверждения, что при любой реализации автоматизированной система (далее по тексту – АС) полное отсутствие уязвимостей в ее компонентах принципиально невозможно ($\sum(V) \neq 0$), 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 [1], 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:

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

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

Также следует учесть, что приведенное выше выражение 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 ™, каналы связи и коммутационное оборудование (K) и серверы терминалов и хранения данных (D) [2]. 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:

$$S_{\text{СИБ}} = \sum_{i=1}^{n} S_{Ri} \cup \sum_{i=1}^{n} S_{Ki} \cup \sum_{i=1}^{n} S_{Di} .$$

Принимая во внимание преимущества технологии «аппаратный тонкий клиент», одним из которых является использование терминальной 75нновационной среды (далее по тексту – ТОС), справедливо утверждать, что в составе СИБ на стороне рабочей станции имеется только две компоненты: доверенная загрузка (ДЗ) и ограничение программной среды ТОС (ОПС):

$$S_R = \max\left\{\sum_{i=1}^{n} S_{\text{ДЗ}i} ; \sum_{i=1}^{n} S_{\text{ОПС}i}\right\}.$$

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. Точки смены формул такой функции 76нновются началом исполнения каждого последующего этапа $x_i$, где $i \in \{1,2,\dots,7\}$ в случае локальной загрузки и $i \in \{1,2,\dots,9\}$ – 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.

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:

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

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

$$f'(P,s) = \lim_{\Delta t \to 0} \frac{S\text{дз}(t+\Delta t) - S\text{дз}(t)}{\Delta t} = 0.$$

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

На основании рассмотренных выше данных допустимо сформулировать основную задачу идеального процесса «доверенной загрузки» как обеспечение стабильной нейтрализации ($S_{ДЗ} = 0$) 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 ($j$). 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 ($k$) оказывать противодействие атакам нарушителя. Т.е. идеальная современная система ДЗ в рамках рассмотренной выше взаимосвязи с условной моделью нарушителя может быть представлена следующим образом:

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

Однако это выражение не позволяет описать процесс доверенной загрузки при $t \neq t_j$, т.е. в периоды времени, не связанные с работой защитных механизмов. Тогда, принимая во внимание уровень подготовки нарушителя, допустимо сделать вывод, что $t \neq t_j \rightarrow 0 < S_{ДЗ}(t) \leq \max(M)$. 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: $S_{ДЗ} = S(t_a) + S(t_b) = \max(M)$, где $b > a \; u \; t_a, t_b \neq t_j$.

Таким образом, достижение свойств идеальной модели для современных систем доверенной загрузки возможно исключительно за счет повышения 77нчественно-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 77нмой 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».

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:

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

Внутренний нарушитель по отношению к внешнему характеризуется рядом принципиальных преимуществ, более подробно описанных в исследованиях отечественных и зарубежных специалистов:

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: $S_{ДЗ} = \max(M)\ при\ f_j^{'}(P,s) = 0$.

С учетом указанных преимуществ необходимо уточнить, что приведенные выражения 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.

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 $x_i$:

$$S_{ДЗ} = \begin{cases} \sum f(\mathrm{s}), \\ s(t) \to 1, \\ t \leq t_{норм}. \end{cases}$$

По результатам проведенного моделирования справедливо утверждать, что подход, основанный на контроле исключительно внедренных (встроенных) в процесс штатной загрузки защитных механизмов не является оптимальным. Проблема оптимизация 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.

## Литература

1. Щеглов А.Ю. Математические модели и методы формального проектирования систем защиты информационных систем / А.Ю. Щеглов, К.А. Щеглов – СПб.: Университет ИТМО, 2015. – 93 с.

2. Буцик К.А. Модель доверенной сетевой загрузки тонкого клиента с нейтрализацией возможностей внутреннего нарушителя / Е.Н. Тищенко, К.А. Буцик, В.В. Деревяшко // Известия ЮФУ. Технические науки – 2015. – Вып.5 (166) – С. 37-47.