Методический подход к оценке времени реакции системы выявления программно-технических воздействий на автоматизированную систему управления военного назначения

Соколовский С.П.
кандидат технических наук

Матвеев Д.С.
кандидат военных наук

Свистунов М.И.
Военно–воздушная академия имени проф. Н.Е. Жуковского и Ю.А. Гагарина» , г. Воронеж

Аннотация

Разработан методический подход к оценке эффективности применения системы выявления программно–технических воздействий на автоматизированную систему управления военного назначения, в основе которого лежит оценка времени реакции системы выявления, определяемого на основании формализованного описания процесса перехода этой системы из состояния в состояние.

Ключевые слова: воздействие; время реакции; информационная система; автоматизированная система управления; противодействие.

Введение

Возросший уровень информационных технологий, развитие и совершенствование концепций сетецентрических войн и сетецентрического управления войсками и оружием обусловили повышение ряда требований к качеству управления. Успешное решение задач совершенствования управления войсками, новыми видами оружия достигается внедрением в войска автоматизированных систем управления военного назначения (АСУ ВН). Однако, АСУ ВН, как и любая другая информационная система, обладает уязвимостями цифрового коммуникационного оборудования и используемого программного обеспечения, что обуславливает возможность осуществления на них программно-технического воздействия (ПТВ). Кроме того, к основным факторам, определяющим возможность осуществления ПТВ, относятся: территориально-распределенная структура АСУ; интенсивное развитие технологий и средств реализации ПТВ; вынужденная необходимость внедрения в АСУ программно-аппаратных средств иностранного производства, постоянно совершенствуемые и уже удачно реализуемые способы и средства осуществления ПТВ со стороны воинских формирований и организаций США и НАТО, а также ряда других государств, что вызывает необходимость совершенствования форм и способов информационной защиты АСУ наших войск, выражающуюся в необходимости создания и совершенствования перспективной системы защиты информации (СЗИ) АСУ. В связи с этим актуальной является задача разработки методов оценки эффективности применения системы выявления программно-технических воздействий на автоматизированную систему управления военного назначения.

Одним из главных показателей эффективности применения системы выявления ПТВ является время реакции, которое может быть определено на основании формализованного описания процесса перехода системы выявления ПТВ из состоянии S_i в S_{i+1} при реализации ПТВ [1-3].

$$t_i = t_{обн_i} + t_{анал_i} + t_{идент_i} + t_{под_i}, \quad (1)$$

где $t_{обн_i}$ – время обнаружения признаков ПТВ; $t_{анал_i}$ – время анализа признаков ПТВ; $t_{идент_i}$ – время идентификации ПТВ; $t_{под_i}$ – время подавления ПТВ.

Общее время реакции системы выявления ПТВ на оказанное воздействие представлено на рис. 1.

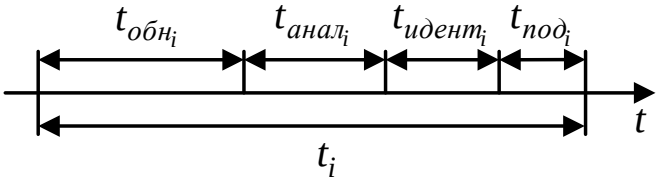

Рис. 1. Вариант временной диаграммы процесса противодействия ПТВ

Подавление ПТВ обычно осуществляется после процесса выявления. В большинстве случаев оно представляется в виде некого решающего правила из множества способов подавления ПТВ $M_{сп.под}$ и длится достаточно короткий промежуток времени, то есть можно записать, что $t_{под_i} \to 0$.

Время обнаружения признаков ПТВ во многом зависит от правильного распределения средств обнаружения признаков ПТВ. А этим процессом, в свою очередь, управляет система выявления ПТВ. Время реакции системы выявления ПТВ определяет ее способность к осуществлению процедур обнаружения признаков, их анализа, идентификации ПТВ за короткий ограниченный промежуток времени с последующим переходом системы в режим готовности к повтору указанных операций. Кроме того, необходимо учитывать, что ПТВ, в большинстве случаев, поступают от разных источников и с разных направлений. Они, как правило, не связаны друг с другом. Это позволяет вести речь о несвязных воздействиях. Исключение составляют массированные целенаправленные воздействия. Но если брать во внимание их хаотическое поступление (например, атаки DDOS), то их тоже можно отнести к разряду несвязных.

Время t_i зависит от многих факторов: особенностей реализации комплекса обнаружения признаков ПТВ, системы выявления ПТВ, производительности используемых технических средств АСУ ВН и т.д. То есть, можно отдельно рассмотреть составляющие слагаемых выражения (2). Так,

$$t_{обн_i} = f\,(M_{мет.\,обн}, M_{реал}, M_{призн}, M_{класс}), \tag{2}$$

где $M_{мет.обн}$ – множество методов обнаружения признаков ПТВ на АСУ ВН; $M_{реал}$ – множество способов реализации комплекса обнаружения ПТВ; $M_{призн}$ – множество признаков ПТВ; $M_{класс}$ – множество классов ПТВ.

Так как работа системы выявления ПТВ напрямую зависит от структуры комплекса обнаружения признаков ПТВ и имеет возможность гибко управлять его составом и соответственно методами обнаружения комплекса, то можно записать

$$t_{анал_i} = f\,(M_{мет.\,анал}, M_{мод}, \upsilon_{тс}, M_{призн}, M_{класс}), \tag{3}$$

где $M_{мет.анал}$ – множество методов анализа признаков ПТВ на АСУ ВН; $M_{мод}$ – множество моделей системы выявления ПТВ; $\upsilon_{тс}$ – показатель производительности системы выявления ПТВ.

$$t_{идент_i} = f\,(M_{мет.\,идент}, \upsilon_{тс}, M_{призн}, M_{класс}), \tag{4}$$

где $M_{мет.идент}$ – множество методов идентификации ПТВ на АСУ ВН.

Время подавления ПТВ $t_{ïîä_i}$ можно оценить как

$$t_{под_i} = f\,(\upsilon_{спд}, M_{сп.\,под}, M_{класс}), \tag{5}$$

где $\upsilon_{спд}$ – показатель скорости передачи данных в АСУ ВН; $M_{сп.под}$ – множество способов подавления ПТВ на АСУ ВН.

Таким образом,

$$t_i = f\,(M_{мет.\,обн}, M_{реал}, M_{призн}, M_{класс}, M_{мет.\,анал}, M_{мод}, \upsilon_{тс}, M_{мет.\,идент}, \upsilon_{спд}, M_{сп.\,под}). \tag{6}$$

То есть время однократного перехода системы t_i не является величиной постоянной.

Обозначим T_i – время реализации i-го ПТВ, которое определяется как

$$T_i = f\ (M_{призн}, M_{класс}, \upsilon_{тс}, \upsilon_{спд})\ . \tag{7}$$

При реализации несвязных ПТВ на АСУ ВН они будут обнаружены при выполнении условия

$$t_i \le T_i\ ,\ \forall i \in \overline{1,N}\ . \tag{8}$$

Учитывая поэтапную реализацию ПТВ на АСУ ВН, соответствующую условию связности, неравенство можно записать как

$$\sum_{i=1}^{N} t_i \le \sum_{i=1}^{N} T_i = T_{ПТВ}\ ,\ \forall i \in \overline{1,N}\ . \tag{9}$$

Согласно этому условию для обнаружения, выявления и предотвращения связных ПТВ достаточно выявить воздействие на одном из этапов. Пример определения ПТВ на АСУ ВН согласно четырехэтапной стратегии его осуществления приведен на рис. 2, где $T_{и.дост}$ – время исследования механизма доступа к элементам АСУ ВН, $T_{и.заи}$ – время исследования механизмов защиты информации в элементах АСУ ВН, $T_{и.проц}$ – время исследования информационных процессов в элементах АСУ ВН, $T_{манип}$ – время несанкционированного манипулирования информацией в элементах АСУ ВН. Жирной чертой выделено время t_3, когда ПТВ было выявлено.

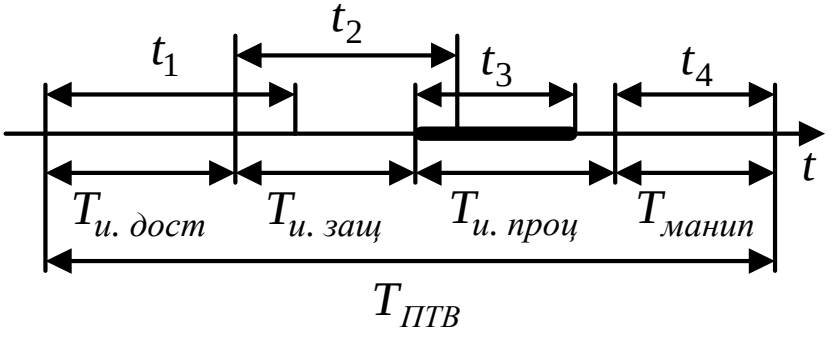

Рис. 2. Вариант временной диаграммы процесса выявления ПТВ, основанного на четырехэтапной стратегии (связные воздействия)

Принятие решений, согласно условию (9), связано с необходимостью многократного определения времени T_i. Поэтому для оценивания времени реакции целесообразно ввести показатель $t_{зад}$ – директивное время перехода системы из состояния S_i в S_{i+1} при реализации ПТВ. Причем,

$$t_{зад} = \frac{\sum_{i=1}^{N} T_i}{N}\ ,\ \forall i \in \overline{1,N}\ , \tag{10}$$

и должно однозначно определять требования для времени реакции системы выявления ПТВ на АСУ ВН

$$t_i \le t_{зад}\ . \tag{11}$$

Так как показатель производительности системы выявления ПТВ $\upsilon_{тс}$ и показатель скорости передачи данных $\upsilon_{спд}$ в конкретных АСУ ВН являются величинами постоянными, то время перехода системы из состоянии S_i в S_{i+1} при реализации ПТВ зависит преимущественно от типов и параметров реализуемых воздействий.

Достижение требований (9) при использовании сигнатурных методов выявления ПТВ возможно за счет оптимизации процессов поиска известных сигнатур и реагирования на них. Использование методов «обнаружения аномалий поведения» приводит к увеличению времени выявления за счет выполнения достаточно трудоемких процессов сбора и анализа информации. Обнаружение и распознавание ПТВ в условиях априорной неопределенности существенно затруднено в связи с необходимостью сбора большого количества информации, то есть контроля множества параметров.

Соответственно, выполнение требований (9) по обеспечению необходимого времени реакции системы выявления ПТВ определяется временем T_i (выражением (7)) и связано с совершенствованием методов обнаружения признаков, выявления ПТВ и оптимизацией структуры комплекса обнаружения.

Заключение

При разработке методического подхода к оценке времени реакции системы выявления ПТВ, определяющего способность системы к осуществлению процедур обнаружения признаков, их анализа, идентификации воздействия за короткий ограниченный промежуток времени с последующим переходом системы в режим готовности к повтору указанных операций, показано, что необходимо различать два вида воздействий на АСУ ВН: несвязные (поступающие от разных источников, с разных направлений и, как правило, не связанные друг с другом) и связные (реализующие поэтапную стратегию ПТВ на АСУ ВН, связанные друг с другом). При этом время обнаружения признаков ПТВ во многом зависит от правильного распределения средств обнаружения признаков ПТВ. На основе примера показано, что согласно четырехэтапной стратегии ПТВ для обнаружения, распознавания и предотвращения связных ПТВ достаточно выявить воздействие на одном из этапов.

Литература

1. Душкин А.В., Молоканов П.С., Соколовский С.П. Метод оценивания качества работы подсистемы распознавания угроз несанкционированного воздействия на защищенные информационные телекоммуникационные системы // Оптимизация и моделирование в автоматизированных системах. Межвузовский сборник научных трудов. Воронеж. ВГТУ. 2007. С. 205–208.

2. Душкин А.В., Соколовский С.П. Математическая модель процесса оптимизации структуры адаптивной системы распознавания угроз несанкционированного воздействия на защищенные информационные телекоммуникационные системы // Преступность в России: состояние, проблемы предупреждения и раскрытия преступлений. Ч. 2: Материалы Международной НПК. Воронеж: ВИ МВД России. 2008. С. 86–87.

3. Душкин А.В., Соколовский С.П. Практическая реализация процесса оптимизации структуры адаптивной системы распознавания угроз несанкционированного воздействия на защищенные информационные телекоммуникационные системы // Пути совершенствования ракетно-артиллерийских комплексов, средств управления войсками и оружием, их эксплуатации и ремонта: Материалы XVI Межвузовской НТК. Тула. 2008. С. 66–67.

Для цитирования:

Соколовский С.П., Матвеев Д.С., Свистунов М.И. Методический подход к оценке времени реакции системы выявления программно-технических воздействий на автоматизированную систему управления военного назначения // i-methods. 2015. Т. 7. № 4. С. 40–44.

Methods to evaluating the response time of the system of identifying software and hardware impacts on an automatic control system for military use

Sokolovsky S.P.
candidate of technical Sciences
Matveev D.S.
candidate of military Sciences
Svistunov I.M.
Air force Academy named after Professor N. E. Zhukovsky and Y. A. Gagarin" , Voronezh

Abstract
The developed methods to assessment of efficiency of application system of identifying software and hardware impacts on an automatic control system for military purposes, which is based on assessment of reaction time detection system, determined on the basis of a formalized description of the process of transition of the system from state to state.

Keywords: effects; reaction time; Information system; automated control system; opposition.

References
1. Dushkin A. V., Molokanov, P. S., Sokolovsky S. P. Method of evaluation of quality of work of a subsystem of recognition of the threats of unauthorized impact on the protected information and telecommunication systems // Optimization and modeling in automated systems. Interuniversity collection of scientific works. Voronezh. Vilnius Gediminas technical University. 2007. P. 205–208.
2. Dushkin A.V., Sokolovskiy, S. P. Mathematical model of structure optimization of adaptive systems of recognition of threats of unauthorized impact on the protected information and telecommunication systems // Crime in Russia: status, problems preventing and solving crimes. H. 2: Materials of International conference. Voronezh: VI the Ministry of internal Affairs of Russia. 2008. P. 86–87.
3. Dushkin A.V., Sokolovskiy, S. P. Practical implementation of process optimization of the structure of an adaptive system of recognition of threats of unauthorized impact on the protected information and telecommunication systems // Ways of improving missile and artillery systems, means of control of troops and weapons, operate, and repair: proceedings of the XVI Inter–University scientific and technical conference. Tula. 2008. P. 66–67.

For citation:
Sokolovsky S.P. Matveev D.S. Svistunov I.M. Methods to evaluating the response time of the system of identifying software and hardware impacts on an automatic control system for military use // i-methods. 2015. T.7. No. 4. Pp. 40–44.