УДК 004.056.53+004.056.57

МЕТОД ОБЕСПЕЧЕНИЯ АДАПТИВНОЙ ЗАЩИТЫ ИНФОРМАЦИИ НА ОСНОВЕ ПЕРЕРАСПРЕДЕЛЕНИЯ ВЫЧИСЛИТЕЛЬНЫХ РЕСУРСОВ И МАСКИРОВАНИЯ УЯЗВИМОСТЕЙ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ

Терехов В.Г.[1], Белая Т.И.[1], Швецов А.С. [1]

[1]*Военно-космическая академия имени А.Ф. Можайского, Санкт-Петербург, e-mail: studentszip@yandex.ru*

Рассматривается метод обеспечения адаптивной защиты информации на основе перераспределения вычислительных ресурсов и маскирования уязвимостей автоматизированных систем управления. Каждая конфигурация (профиль защиты) автоматизированной системы управления представляется как совокупность аппаратно-программного обеспечения, которое можно характеризовать некоторым множеством уязвимостей, имеющих своё чётко определённое местоположение в автоматизированной системе управления. Показателем качества функционирования является показатель защищённости автоматизированной системы управления, зависящий от профиля защиты, в котором находится система защиты. Для обеспечения максимальной (из всех возможных) вероятности отражения деструктивных информационных воздействий необходимо, чтобы изменение показателя защищенности нового профиля защиты, относительно текущего было максимально.

Ключевые слова: адаптивная защита информации, маскирование уязвимостей, защита систем управления

METHOD OF ENSURING ADAPTIVE INFORMATION SECURITY ON THE BASIS OF REDISTRIBUTION OF COMPUTING RESOURCES AND MASKING OF VULNERABILITIES OF AUTOMATED CONTROL SYSTEMS

Terehov V.G.[1], Belaya T.I.[1], Shvecov A.S.[1]

[1] *Military space academy of A.F.Mozhaysky, Sankt-Peterburg, e-mail: studentszip@yandex.ru*

The method of ensuring adaptive information security on the basis of redistribution of computing resources and masking of vulnerabilities of automated control systems is considered. Each configuration (a protection profile) of an automated control system is represented as set of firmware which can be characterized by some set of the vulnerabilities having the accurately certain location in an automated control system. An indicator of quality of functioning is the indicator of security of an automated control system depending on a protection profile in which there is a system of protection. Maximum (from all possible) it is necessary for probability of reflection of destructive information influences for providing that change of an indicator of security of a new profile of protection, rather current was maximum.

Keywords: adaptive information security, masking of vulnerabilities, protection of control systems

Постоянное совершенствование информационных технологий определяет необходимость разработки новых систем защиты информации (СиЗИ). Современные СиЗИ для эффективного отражения деструктивных информационных воздействий (ДИВ) должны отвечать требованиям гибкости и адаптируемости к изменяющимся условиям.

Каждую конфигурацию (профиль защиты) АСУ, как совокупность аппаратно-программного обеспечения, можно характеризовать некоторым множеством уязвимостей, которые имеют своё чётко определённое местоположение в АСУ. К каждому случайному моменту времени $\hat{t}$ злоумышленник может применить только множество W ДИВ на множество H уязвимостей. Местоположение уязвимости зависит от выбранной конфигурации (распределения информационных ресурсов) аппаратно-программной части АСУ. Таким образом, каждое, отдельно взятое ДИВ, нацелено на определённую конфигурацию и, следовательно, саму конфигурацию можно рассматривать как защиту от

ДИВ. При изменении конфигурации аппаратно-программной части АСУ ранее успешные ДИВ станут неэффективными [1]. Поэтому, каждая конфигурация, с точки зрения защищённости, характеризуется вероятностью появления опасного ДИВ w_r^* $(w_r^* \in W)$, направленного точно на уязвимость (местоположение уязвимости). Следовательно, к любому, отдельно взятому, случайному моменту времени $\hat{t}$, каждый профиль защиты будет иметь свою вероятность $P_{u_m},\ m = \overline{1,i}$ отражения ДИВ, где i – количество профилей защиты. Для поддержания высокой вероятности отражения ДИВ АСУ необходимо всегда находиться в профиле защиты, который обеспечит максимальную вероятность отражения ДИВ к данному моменту времени [2].

Профиль защиты АСУ характеризуется настройками конфигурации всех аппаратно-программных средств АСУ, к которым относятся как средства защищаемого объекта, предназначенные для целевой обработки, хранения и передачи информации, так и средства защиты информации, предназначенные для обеспечения безопасности работы АСУ.

Один профиль защиты будет отличаться от другого, если хотя бы одна настройка конфигурации какого-либо аппаратно-программного средства была изменена. С изменением настройки конфигурации изменится местоположение уязвимости, что может стать достаточным для успешного отражения ДИВ. Хотя предлагаемый метод не устраняет уязвимость полностью и не решает окончательно вопрос безопасности АСУ, но он позволяет быстро реагировать на меняющуюся обстановку и сохранить работоспособность АСУ в условиях применения деструктивных воздействий [3].

Конфигурация аппаратно-программной части АСУ может меняться путём добавления новых компонентов в структуру или путём изменения уже существующих (реконфигурация). Количество профилей защиты зависит от количества контролируемых точек в конфигурации АСУ. Каждая контролируемая точка может иметь два состояния: активна и неактивна. Совокупность всех контролируемых точек составляет определённую конфигурацию АСУ [4]. Зависимость между количеством контролируемых точек и объёмом таблицы профилей защиты выражается формулой

$$i = 2^{\beta} \tag{1}$$

где i – общее число возможных профилей защиты, β – число контролируемых точек на средствах АСУ. Общее количество возможных стратегий смены профилей защиты определяется по формуле

$$\alpha = (i-1)! \tag{2}$$

Для реализации эффективной защиты, СиЗИ необходимо ликвидировать уязвимость, т.е. сменить профиль защиты, за время меньшее, по сравнению со временем, которое затратит злоумышленник на обнаружение уязвимости и осуществление ДИВ.

Для повышения эффективности работы СиЗИ и устойчивости АСУ к ДИВ предлагается автоматизировать процесс ликвидации уязвимостей, который можно реализовать с использованием метода обеспечения адаптивной защиты информации на основе перераспределения вычислительных ресурсов и маскирования уязвимостей [5].

Метод обеспечения адаптивной защиты информации на основе перераспределения вычислительных ресурсов и маскирования уязвимостей АСУ основывается на двух гипотезах:

1. Все ДИВ направляются на уязвимости, которые имеют определённое местоположение согласно установленной конфигурации аппаратно-программных средств АСУ.

2. Конечная конфигурация аппаратно-программных средств АСУ может иметь некоторое множество $U^* = \{u_1^*, \ \ldots, \ u_i^*\}$ решений (профилей защиты, где $U^* \in U$), удовлетворяющих заданным требованиям по реализации необходимых функций защищаемым объектом.

Основными данными, которые необходимы для функционирования метода, являются, количество времени, прошедшее с момента последней смены профиля защиты (обуславливается понижением вероятности отражения ДИВ во времени), и результаты работы системы обнаружения вторжений (СОВ).

Вероятность отражения ДИВ, в каждом отдельно взятом сконфигурированном профиле защиты u_i^*, равна вероятности появления опасного ДИВ w_r^* в неадаптивной СиЗИ, т.е.

$$P_{u_m^*}^{\text{отр}}(t) = 1 - P_u^{w_r^*}(t) \tag{3}$$

где $m = \overline{1, i}$.

Введём ограничения на нестационарный поток ДИВ. Будем его считать потоком однородных событий, ординарным и без последействий. Тогда с учётом нестационарного пуассоновского потока ДИВ и Марковского случайного процесса адаптации СиЗИ рассчитываем вероятность того, что за время τ, начиная с момента времени t, произойдёт ровно k_i опасных ДИВ w_r^* в профиле защиты u_i^* по формуле

$$P_{u_m^*}^{k_m w_r^*}(\tau, t) = \frac{[a_m]^{k_m}}{k_m!} \cdot e^{-a_m} \tag{4}$$

где $m = \overline{1, i}$; $a_m = \int_t^{t+\tau} \lambda_m(t)dt -$ математические ожидания числа событий на участке от t до $t+\tau$; $\lambda(\tau, t)$ – плотность потока w_r^* на интервале времени (τ, t) ; $k = 1, \ldots$.

Вероятности перехода из $u_m^{\text{актив}}$ в u_m^* при $t_0 = 0$ (начальный момент времени, при отсутствии информации о злоумышленнике) будет равна:

$$P(u_m^{\text{актив}} \to u_m^*) = \frac{1}{i^*} \quad (5)$$

где $m = \overline{1,i}$; i^* – количество сконфигурированных профилей защиты.

При $t_0 \neq 0$ и $\lambda_m \neq \lambda_{\text{актив}}$, $P(u_m^{\text{актив}} \to u_m^*) = P_{u_m^*}^{\text{отр}}$, где $m = \overline{1,i}$.

С учётом формулы (1) для выявления последовательности благоприятных профилей защиты u_m^{**} получим:

$$\Theta(u_m^{\text{актив}};\ u_m^{**}) = \frac{\gamma\left(P_{u_m^{**}}^{k_m w_r^*}\right)}{\gamma\left(P_{u_m^{\text{актив}}}^{k_{\text{актив}} w_r^*}\right)} = \frac{\gamma\left(\frac{[a_m^{**}]^{k_m}}{k_m!}\right)\cdot e^{-a_m^{**}}}{\gamma\left(\frac{[a_m^{\text{актив}}]^{k_{\text{актив}}}}{k_{\text{актив}!}}\right)\cdot e^{-a_m^{\text{актив}}}} \quad (6)$$

Вероятность реализации каждой стратегии защиты $\Omega_n, n = \overline{1,\alpha}$ при $t_0=0$ на интервале времени (τ, t) будет равна:

$$P_{\Omega_n}(\tau, t) = \frac{1}{\alpha} \quad (7)$$

где $n = \overline{1,\alpha}$; α – количество стратегий профилей защиты. По мере функционирования адаптивных СиЗИ (АСиЗИ) вероятность реализации каждой стратегии смены профилей защиты будут изменяться.

Упорядочивание профилей защиты в процессе функционирования АСиЗИ производится согласно выражению $\langle u_{\text{актив}}, \dots, u_{m-1}, u_m \rangle$ при

$$P_{k_{m-1}}^{u_{m-1}^* w_r^*}(\tau, t) < P_{k_m}^{u_m^* w_r^*}(\tau, t),$$

где $m = \overline{1,i}$.

Корректируя стратегию переходов с учётом возможной важности защищаемых объектов с точки зрения рисков, получаем следующее:

R – потенциальные потери от угроз защищённости, при выборе неэффективного профиля защиты (риск):

$$R(p) = C_{\text{инф}} \cdot p_{\text{взл}} \quad (8)$$

где $C_{инф}$ – стоимость информационно-временных потерь, $p_{взл}$ - вероятность взлома.

Потери в единицу времени:

$R(\lambda) = C_{\text{инф}} \cdot \lambda_{\text{взл}}$, где $\lambda_{\text{взл}}$– плотность потока ДИВ злоумышленника к информации;

$p_{\text{взл}} = \frac{\lambda_{\text{взл}}}{\Lambda}$, где Λ – общая плотность потока ДИВ злоумышленника к информации;

D – коэффициент защищённости, отображающий относительное уменьшение риска в новом u_m профиле защиты относительно активного $u_{актив}$,

$$D_m = \frac{R_m}{R_{\text{актив}}}, \quad (9)$$

где $m = \overline{1,i}$; R_m – риск в профиле защиты u_m, $R_{актив}$ – риск в активном профиле защиты.

$$R_m(p) = \sum_1^r R_k\,(p) = \sum_1^r C_k \cdot p_{\text{ДИВ}_k}\,,$$

где $R_k(p)$ – коэффициент потерь от ДИВ w_r в m-м профиле защиты.

$$R_m(\lambda) = \sum_1^r R_k\,(\lambda) = \sum_1^r C_k \cdot \lambda_{\text{ДИВ}_k},$$

где $R_k(\lambda)$ – коэффициент потерь в m-м профиле защиты в единицу времени от ДИВ w_r.

В итоге получаем:

$$D_m = \frac{\sum_1^r C_k^m \cdot Q_k^m \cdot (1-p_k^m)}{\sum_1^r C_k^{\text{актив}} \cdot Q_k^{\text{актив}} \cdot (1-p_k^{\text{актив}})} = \frac{\sum_1^r C_k^m \cdot \lambda_k^m \cdot (1-p_k^m)}{\sum_1^r C_k^{\text{актив}} \cdot \lambda_k^{\text{актив}} \cdot (1-p_k^{\text{актив}})} \quad (10)$$

Коррекция упорядочивания профилей защиты в процессе функционирования АСиЗИ производится согласно выражению $\langle u_{\text{актив}}, \dots, u_{m-1}^*, u_m^* \rangle$, при $D_{m-1} > D_m$, где $m = \overline{1,i}$.

Показателем качества функционирования является показатель защищённости АСУ, который в свою очередь зависит от профиля защиты, в котором находится СиЗИ. Для обеспечения максимальной (из всех возможных) вероятности отражения ДИВ необходимо, чтобы изменение показателя защищенности нового профиля защиты, относительно текущего было максимально.

Список литературы

1. Антонов В.Н., Терехов В.Г., Тюкин Ю.И. Адаптивное управление в технических системах. – СПб.: изд-во Санкт-Петербургского университета, 2001. – 244с.
2. Белая Т.И, Васильев А.С., Терехов В.Г., Швецов А.С. Информационная модель для оценки эффективности применения автоматизированных систем специального назначения на основе аппарата нечетких множеств // Современные проблемы науки и образования. - 2014. - №6: URL: http://www.scince-education.ru/120-15979 (дата обращения: 13.12.2014).
3. Швецов А.С. Применение адаптивных технологий в системах защиты информации в информационных сетях. // Сб. трудов седьмой межведомственной научно-технической конференции «Проблемные вопросы сбора, обработки, передачи и защиты информации в сложных радиотехнических системах», 22 ноября 2005. – СПб.: ПВИРЭ КВ, 2005. – С.168-170.
4. Швецов А.С. Применение адаптивных технологий в системах защиты информации в информационно-управляющей системе КВ. // Труды научно-практической конференции

«Военно-космическая деятельность России – истоки, состояния, перспективы», 2005.– СПб.: Изд-во «Левша. Санкт-Петербург», 2005. – С.186-187.

5. Юревич Е.И. Теория автоматического управления. - СПб.: БХВ-Петербург, 2007. – 560 с.

Рецензенты:

Пророк В.Я., д.т.н., профессор 95 кафедры ВКА имени А.Ф. Можайского, г. Санкт-Петербург;

Дроздов В.Н., д.т.н., профессор кафедры ТПП СПГУТД СЗИП, г. Санкт-Петербург.