DOI: 10.18137/RNU.V9187.22.04.P.165 УДК 004.056.53+004.056.57

А.С. Швецов, В.Г. Терехов, А.Н. Соколовский

# МЕТОД ОЦЕНИВАНИЯ КАЧЕСТВА ФУНКЦИОНИРОВАНИЯ АДАПТИВНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

**Аннотация.** Рассматриваются вопросы качества функционирования систем адаптивного управления процессами защиты информации в автоматизированных системах управления при деструктивных информационных воздействиях. Предложен метод оценивания функционирования адаптивной системы защиты информации, который заключается в использовании комплексного многокритериального подхода для одновременного оценивания как статической, так и динамической составляющих рассматриваемой системы. Для динамической составляющей определены критерии оценивания, события, возникающие в процессе адаптации, и показатель защищенности, представляющий собой вероятность неотклонения активного профиля защиты от состояния, которое является результатом правильной конфигурации защиты и эффективной реализации алгоритма выбора активного профиля защиты.

*Ключевые слова:* автоматизированные системы управления, адаптивное управление, деструктивные информационные воздействия, защита информации, оценивание показателя защищенности.

A.S. Shvetsov, V.G. Terekhov, A.N. Sokolovsky

# THE METHOD OF ASSESSING THE QUALITY OF FUNCTIONING OF THE ADAPTIVE INFORMATION SECURITY SYSTEM

**Abstract.** The issues of assessing the quality of functioning of information security systems and adaptive control of information security processes in automated control systems during destructive information impacts are considered. A method for evaluating the quality of functioning of an adaptive information security system is proposed, which consists in using an integrated multi-criteria approach for the simultaneous evaluation of both the static and dynamic components of the information security system under consideration. For the dynamic component, evaluation criteria are defined, events that occur during the adaptation process and a security indicator, which is the probability that the active protection profile does not deviate from the state that is the result of the correct configuration of protection profiles and the effective implementation of the active selection algorithm.

*Keywords:* automated control systems, adaptive control, destructive information impacts, information security, assessment of the security indicator.

## *Введение*

Любая система защиты информации (далее – СЗИ), реализованная на основе динамических технологий, требует специального подхода к оцениванию качества ее функционирования. Для СЗИ, в том числе адаптивных, основным показателем качества функционирования является показатель защищенности объекта. В связи с тем, что адаптивная система защиты информации (далее – АСЗИ) является динамической (меняющейся во времени), методики оценивания показателя защищенности, которые применяются для неадаптивных (неизменяемых) СЗИ, не могут использоваться, так как не в полном объеме учитывают процессы, происходящие в АСЗИ. Поэтому ниже будет рассмотрен один из возможных подходов к оцениванию показателя защищенности АСЗИ с целью адекватной оценки качества ее функционирования. Оценивание показателя защищенности рас-

**Швецов Александр Сергеевич**
кандидат технических наук, доцент, доцент кафедры информационно-вычислительных систем и сетей. Военно-космическая академия имени А.Ф. Можайского, Санкт-Петербург. Сфера научных интересов: компьютерные сети; защита информации в информационно-вычислительных сетях. Автор более 20 опубликованных научных работ.
Электронный адрес: mysash@yandex.ru

**Терехов Владимир Геннадиевич**
кандидат военных наук, доцент, старший преподаватель кафедры информационно-вычислительных систем и сетей. Военно-космическая академия имени А.Ф. Можайского, Санкт-Петербург. Сфера научных интересов: надежность программного обеспечения; защита информации в информационно-вычислительных сетях. Автор более 20 опубликованных научных работ.
Электронный адрес: vter2@rambler.ru

**Соколовский Алексей Николаевич**
кандидат технических наук, преподаватель кафедры информационно-вычислительных систем и сетей. Военно-космическая академия имени А.Ф. Можайского, Санкт-Петербург. Сфера научных интересов: компьютерные технологии; защита информации в информационно-вычислительных сетях. Автор более 20 опубликованных научных работ.
Электронный адрес: sokolovskij@rambler.ru

сматривается применительно к особенностям реализации АСЗИ на основе перераспределения вычислительных ресурсов и маскирования уязвимостей [7].

*Функционирование адаптивной системы защиты информации*

Рассматриваемая АСЗИ основывается на том факте, что деструктивные информационные воздействия (далее – ДИВ) осуществляются на заранее известный в плане аппаратно-программного обеспечения объект, например, автоматизированную систему управления (далее – АСУ). Это связано с тем, что в определенном целевом объекте известны его уязвимости. Местоположение уязвимости связано с задействованными ей определенными аппаратно-программными ресурсами, то есть зависит от активной конфигурации АСУ и ее СЗИ. С изменением конфигурации может измениться местоположение уязвимости. Следовательно, любые изменения, в том числе и на уровне настроек, могут привести к тому, что раннее успешные ДИВ станут неэффективными [1]. Таким образом, конфигурация (совокупность всех настроек аппаратно-программного обеспечения) АСУ и ее СЗИ рассматривается как защита – профиль защиты от ДИВ. Один профиль защиты будет отличаться от другого, если хотя бы одна настройка конфигурации какого-либо аппаратно-программного обеспечения была изменена. Количество профилей защиты зависит от количества контролируемых точек в конфигурации АСУ и ее СЗИ. Своевременная смена профилей защиты способна предотвратить как новые, неизвестные, так и известные (обнаруживаемые) ДИВ [5].

Целью функционирования АСЗИ является поддержание во времени высокой вероятности отражения (не менее заданной руководящими документами) ДИВ, то есть нахождение в профиле защиты, который обеспечит максимальную вероятность отражения ДИВ к данному моменту времени [3]. Для соблюдения этого условия необходимо по-

стоянно выполнять прогнозирование уровня защищенности в каждом профиле защиты и перспективное планирование или оценку возможных ситуаций. Чтобы АСЗИ качественно выполняла свои функции, необходим постоянный контроль эффективности использования, который заключается в проверке соответствия принятых мер защиты требованиям по защищенности [4]. При этом задачи контроля рассматриваются как задачи анализа выполнения требований по защищенности АСУ в каждом профиле защиты. Этот процесс протекает во времени, и при снижении защищенности АСУ необходимо принимать соответствующие меры для ее повышения до максимально возможного в этот момент уровня.

С целью учета процессов, происходящих в АСЗИ, применительно к особенностям реализации АСЗИ на основе перераспределения вычислительных ресурсов и маскирования уязвимостей для оценивания показателя защищенности АСУ целесообразно использовать комплексный многокритериальный подход, то есть одновременно оценивать как статическую, так и динамическую составляющую СЗИ. Это связано с тем, что в любой дискретный момент времени АСЗИ представляется как обычная (статическая составляющая) СЗИ, к которой применимы все существующие подходы к оцениванию показателя защищенности информации. Если АСЗИ рассматривать относительно изменения времени, то на показатель защищенности информации значительное влияние будут оказывать особенности реализации принципов и алгоритмов адаптации (динамическая составляющая), количество и качество профилей защиты, используемые алгоритмы поиска и смены профилей защиты, от которых будет зависеть время, необходимое на реконфигурацию АСУ и ее СЗИ и изменение показателя защищенности.

*Динамическая составляющая адаптивной системы защиты информации*

В связи с тем, что вопросам оценивания показателя защищенности информации при использовании обычных (статических) СЗИ посвящено много работ, далее основное внимание будет сосредоточено на рассмотрении динамической составляющей АСЗИ.

Для оценивания качества функционирования АСЗИ применительно к особенностям реализации выше изложенной АСЗИ будет использоваться одновременно три критерия (требования):

1. Обеспечение вероятности отражения ДИВ не менее заданной руководящими документами. Для ее оценивания вводится показатель абсолютного отклонения вероятности отражения ДИВ от единицы в активном профиле защиты: $\Delta\eta^{абс}_{актив} = 1 - P^{АСЗИ}_{актив}$. Для идеальной АСЗИ $\Delta\eta^{абс}_{актив} \approx 0$, но не более допустимого отклонения, то есть $\Delta\eta^{абс}_{актив} \le \Delta\eta^{доп}$.

2. Нахождение АСЗИ в профиле защиты, который обеспечит максимальную вероятность отражения ДИВ к данному моменту времени. Для его оценивания вводится показатель относительного отклонения вероятности отражения ДИВ в активном профиле защиты от максимально возможной вероятности отражения ДИВ относительно всех сконфигурированных профилей защиты: $\Delta\eta^{отн}_{актив} = P^{АСЗИ}_{макс} - P^{АСЗИ}_{актив}$. Для идеальной АСЗИ значение $\Delta\eta^{отн}_{актив} = 0$.

3. Обеспечение низкого уровня риска при смене профилей защиты. Для его оценивания вводится показатель динамической защищенности $D_m$, который для идеальной АСЗИ в момент смены профиля защиты имеет всегда максимальное значение.

Анализ последовательности смены профилей защиты АСЗИ относительно вышеизложенных критериев создает следующие возможные события (см. Таблицу) [8].

*Таблица*

**События, возникающие в результате смены профилей защиты АСЗИ**

| № | Описание события | Выражение |
|---|---|---|
| C1 | Осуществлен переход в профиль защиты с максимальной вероятностью отражения ДИВ, значение которой не ниже допустимого | $\begin{cases} P_{актив}^{АСЗИ} = P_{отр.}^{max} \\ P_{актив}^{АСЗИ} \geq P_{отр.}^{задан.} \end{cases}$ |
| C2 | Осуществлен переход в профиль защиты не с максимальной вероятностью отражения ДИВ, значение которой не ниже допустимого | $\begin{cases} P_{актив}^{АСЗИ} < P_{отр.}^{max} \\ P_{актив}^{АСЗИ} \geq P_{отр.}^{задан.} \end{cases}$ |
| C3 | Осуществлен переход в профиль защиты не с максимальной вероятностью отражения ДИВ, значение которой ниже допустимого, при условии, что у профиля защиты с максимальной вероятностью отражения ДИВ, значение не ниже допустимого | $\begin{cases} P_{актив}^{АСЗИ} < P_{отр.}^{max} \\ P_{актив}^{АСЗИ} < P_{отр.}^{задан.} \\ P_{отр.}^{max} \geq P_{отр.}^{задан.} \end{cases}$ |
| C4 | Осуществлен переход в профиль защиты с максимальной вероятностью отражения ДИВ, значение которой ниже допустимого | $\begin{cases} P_{актив}^{АСЗИ} = P_{отр.}^{max} \\ P_{актив}^{АСЗИ} < P_{отр.}^{задан.} \end{cases}$ |
| C5 | Осуществлен переход в профиль защиты не с максимальной вероятностью отражения ДИВ, значение которой ниже допустимого, при условии, что у профиля защиты с максимальной вероятностью отражения ДИВ значение ниже допустимого | $\begin{cases} P_{актив}^{АСЗИ} < P_{отр.}^{max} \\ P_{актив}^{АСЗИ} < P_{отр.}^{задан.} \\ P_{отр.}^{max} < P_{отр.}^{задан.} \end{cases}$ |

Событие C1 является результатом правильной конфигурации профилей защиты и эффективной реализации алгоритма выбора активного. Это событие является наилучшем из всех возможных. Постоянное поддержание состояния, в котором следуют только такие события, является целью функционирования АСЗИ.

Событие C2 является результатом правильной конфигурации профилей защиты, неэффективной реализации алгоритма выбора активного, но сохраняется вероятность отражения ДИВ в допустимых пределах.

Событие C3 является результатом правильной конфигурации профилей защиты, неэффективной реализации алгоритма выбора активного и в результате не обеспечивает минимально допустимую вероятность отражения ДИВ.

Событие C4 является результатом эффективной реализации алгоритма выбора активного, но неправильной конфигурации профилей защиты и в результате не обеспечивает минимально допустимую вероятность отражения ДИВ.

Событие C5 является результатом неэффективной реализации алгоритма выбора активного, неправильной конфигурации профилей защиты и в результате не обеспечивает минимально допустимую вероятность отражения ДИВ. Это событие является худшим из всех возможных.

В результате анализа возможных событий можно заключить, что при появлении событий с C2 по C5 требуется дополнительная настройка АСЗИ, хотя событие C2 является вполне приемлемым с точки зрения поддержания заданного уровня вероятности отражения ДИВ.

Показателем защищенности $\psi$ АСЗИ следует считать вероятность неотклонения активного профиля защиты от состояния С1, и следовательно, непоявления событий с С2 по С5:

$$\psi = 1 - P(\Delta\eta^{отн}_{актив} > 0) = 1 - P(C2 \cup C3 \cup C4 \cup C5).$$

Введем ограничения на нестационарный поток ДИВ. Будем считать его потоком однородных событий, ординарным и без последействий. Тогда с учетом нестационарного пуассоновского потока ДИВ и марковского случайного процесса адаптации СЗИ рассчитываем вероятность того, что за время $\tau$, начиная с момента времени $t$, произойдет, соответственно, ровно $k$, $l$, $m$, $n$ событий С2, С3, С4, С5 [6]:

$$P_k^{C2}(\tau,t) = \frac{a_{C2}^k}{k!} e^{-a_{C2}}, P_l^{C3}(\tau,t) = \frac{a_{C3}^l}{l!} e^{-a_{C3}},$$

$$P_m^{C4}(\tau,t) = \frac{a_{C4}^m}{m!} e^{-a_{C4}}, \; P_n^{C5}(\tau,t) = \frac{a_{C5}^n}{n!} e^{-a_{C5}}, (k, l, m, n = 0, 1, 2, \ldots).$$

Здесь $a_{C2} = \int_{t_0}^{t_0+\tau} \lambda_{c2}(t)dt$, $a_{C3} = \int_{t_0}^{t_0+\tau} \lambda_{c3}(t)dt$ – математические ожидания числа событий С2, С3, С5 и С6 на участке от $t$ до $t+\tau$ соответственно; $\lambda_{C2}(t)$, $\lambda_{C3}(t)$ – интенсивности потоков событий для С2, С3, С4 и С5.

Учитывая разный уровень опасности возникновения событий С2, С3, С4 и С5, введем для них соответствующие коэффициенты опасности $\partial^{задан}$.

В итоге получим показатель защищенности:

$$\psi(\tau,t) = 1 - \delta_{C2}^{задан} \frac{a_{C2}^k}{k!} e^{-a_{C2}} - \delta_{C3}^{задан} \frac{a_{C3}^l}{l!} e^{-a_{C3}} - \delta_{C4}^{задан} \frac{a_{C4}^m}{m!} e^{-a_{C4}} - \delta_{C5}^{задан} \frac{a_{C5}^n}{n!} e^{-a_{C5}}.$$

Оценивание изменения показателя защищенности АСЗИ в условиях нестационарного потока ДИВ с учетом возможной важности защищаемых объектов с точки зрения рисков для обеспечения их низкого уровня при смене профилей защиты осуществляется с помощью показателя динамической защищенности $D_m = \frac{R_{актив}(p)}{R_m(p)}$, который отображает изменение риска в новом профиле защиты ($R_m$) относительно активного ($R_{актив}$); здесь $m = \overline{1,i}$ – номер нового профиля защиты, $i = 2^\beta$, где $i$ – число сконфигурированных профилей защиты, $\beta$ – число контролируемых точек на средствах АСУ и ее СЗИ.

Расчет риска потенциальных потерь от угроз защищенности при выборе неэффективного профиля защиты происходит по следующей формуле [2]:

$$R(p) = CQV,$$

где $C$ – стоимость информационно-временных потерь; $Q$ – вероятность реализации угрозы информационной безопасности (появления опасного ДИВ в общем потоке), причем:

$$Q = \frac{\lambda}{\Lambda},$$

где $\lambda$ – плотность потока опасных ДИВ к информации; $\Lambda$ – общая плотность потока ДИВ к информации; $V$ – вероятность попадания в уязвимость, причем если рассматривать эту вероятность относительно смены профилей защиты, то есть маскирования уязвимостей, тогда

$$V = 1 - P$$

где $P$ – вероятность того, что к моменту появления опасного ДИВ местоположение уязвимости будет изменено.

Потенциальные потери $R_m(p)$ от всех ( $r$ ) ДИВ в профиле защиты $m = \overline{1,i}$ можно обозначить как

$$R_m(p) = \sum_{k=1}^{r} R_k(p) = \sum_{k=1}^{r} C_k^m Q_k^m (1 - P_k^m) .$$

В итоге получаем

$$D_m = \frac{\sum_{k=1}^{r} C_k^{актив} Q_k^{актив} (1 - P_k^{актив})}{\sum_{k=1}^{r} C_k^m Q_k^m (1 - P_k^m)} = \frac{\sum_{k=1}^{r} C_k^{актив} \lambda_k^{актив} (1 - P_k^{актив})}{\sum_{k=1}^{r} C_k^m \lambda_k^m (1 - P_k^m)} .$$

*Заключение*

Таким образом, показатель защищенности АСУ зависит от вероятности нахождения АСЗИ в профиле защиты, обеспечивающем максимальную вероятность отражения ДИВ, которая, в свою очередь, зависит от внешних изменений (от стратегии поведения противника) и качества профилей, их количества и эффективности реализации алгоритма выбора активного, реализованных в АСЗИ. Предложенный метод оценивания учитывает процессы, происходящие в АСЗИ, поэтому с его помощью можно корректно оценивать качество ее функционирования.

## Литература

1. *Антонов В.Н., Терехов В.Г., Тюкин Ю.И.* Адаптивное управление в технических системах. СПб.: Изд-во Санкт-Петербургского университета, 2001. 244 с.

2. ГОСТ Р ИСО/МЭК 27005–2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. М.: Стандартинформ, 2011. 51 с.

3. Информационная модель для оценки эффективности применения автоматизированных систем специального назначения на основе аппарата нечетких множеств / А.С. Швецов, Т.И. Белая, А.С. Васильев, В.Г. Терехов // Современные проблемы науки и образования. 2014. № 6. С. 117–118.

4. *Маслова Н.А., Шамаев В.В.* Принципы адаптации в защите корпоративных систем // Искусственный интеллект. 2010. № 3. С. 64–72.

5. *Швецов А.С.* Применение адаптивных технологий в системах защиты информации в информационных сетях // Проблемные вопросы сбора, обработки, передачи и защиты информации в сложных радиотехнических системах: сб. трудов VII Межведомственной научно-технической конференции, 22 ноября 2005 г. СПб.: ПВИРЭ КВ, 2005. С. 168–170.

6. *Швецов А.С., Соколовский А.Н.* Метод повышения защищенности сложных информационно-вычислительных систем // Труды Военно-космической академии имени А.Ф.Можайского. 2016. № 654. С. 118–123.

7. *Швецов А.С., Терехов В.Г., Белая Т.И.* Метод обеспечения адаптивной защиты информации на основе перераспределения вычислительных ресурсов и маскирования уязвимостей автоматизированных систем управления // Современные проблемы науки и образования. 2015. № 1. С. 187–188.

8. *Швецов А.С., Терехов В.Г., Белая Т.И.* Метод оценивания показателя защищенности автоматизированных систем управления на основе модели равновесия динамической системы защиты // Естественные и технические науки. 2015. № 1. С. 99–101.

## References

1. Antonov V.N., Terekhov V.G., Tyukin Yu.I. (2001) *Adaptivnoe upravlenie v tekhnicheskih sistemah* [Adaptive management in technical systems]. St. Petersburg, Publishing House of St. Petersburg University, 244 p. (in Russian).

2. GOST R ISO/MEK 27005-2010. *Informacionnaya tekhnologiya. Metody i sredstva obespecheniya bezopasnosti. Menedzhment riska informacionnoj bezopasnosti* [Information technology. Methods and means of ensuring security. Information security risk management]. Moscow, Standartinform Publishing, 2011, 51 p. (in Russian).

3. Shvetsov A.S., Belaya T.I., Vasiliev A.S., Terekhov V.G. (2014) *Informacionnaya model' dlya ocenki effektivnosti primeneniya avtomatizirovannyh system special'nogo naznacheniya na osnove apparata nechetkih mnozhestv* [An information model for evaluating the effectiveness of the use of automated systems for special purposes based on the apparatus of fuzzy sets]. *Sovremennye problemy nauki i obrazovanija*, No. 6, pp. 117–118 (in Russian).

4. Maslova N.A., Shamaev V.V. (2010) *Principy adaptacii v zashchite korporativnyh sistem* [Principles of adaptation in the protection of corporate systems]. *Iskusstvennyj intellekt*, No. 3, pp. 64–72 (in Russian).

5. Shvetsov A.S. (2005) *Primenenie adaptivnyh tekhnologij v sistemah zashchity informacii v informacionnyh setyah* [Application of adaptive technologies in information security systems in information networks]. Proc. of the seventh Interdepartmental Scientific and Technical Conference "Problematic issues of collecting, processing, transmitting and protecting information in complex radio engineering systems", November 22, 2005. St. Petersburg, PVIRE KV, pp. 168–170 (in Russian).

6. Shvetsov A.S., Sokolovsky A.N. (2016) *Metod povysheniya zashchishchennosti slozhnyh informacionno-vychislitel'nyh sistem* [Method of increasing the security of complex information and computing systems]. Proc. of the Military Space Academy named after A.F.Mozhaisky, No. 654, pp. 118–123 (in Russian).

7. Shvetsov A.S., Terekhov V.G., Belaya T.I. (2015) *Metod obespecheniya adaptivnoj zashchity informacii na osnove pereraspredeleniya vychislitel'nyh resursov i maskirovaniya uyazvimostej avtomatizirovannyh system upravleniya* [Method of providing adaptive information protection based on redistribution of computing resources and masking vulnerabilities of automated control systems]. *Sovremennye problemy nauki i obrazovanija*, no. 1, pp. 187–188 (in Russian).

8. Shvetsov A.S., Terekhov V.G., Belaya T.I. (2015) *Metod ocenivaniya pokazatelya zashchishchyonnosti avtomatizirovannyh system upravleniya na osnove modeli ravnovesiya dinamicheskoj sistemy zashchity* [A method for estimating the security index of automated control systems based on the "equilibrium" model of a dynamic protection system]. *Estestvennye i tehnicheskie nauki*, no. 1, pp. 99–101 (in Russian).