УДК 681.3.067
doi:10.15217/issn1684-8853.2017.3.67

ПРИМЕНЕНИЕ СТРАТЕГИЙ ПОДДЕРЖАНИЯ ЗАЩИЩЕННОСТИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Г. Н. Мальцев[a], *доктор техн. наук, профессор*
Д. А. Лесняк[a], *канд. техн. наук, старший преподаватель*
[a]*Военно-космическая академия им. А. Ф. Можайского, Санкт-Петербург, РФ*

Постановка проблемы: *обеспечение информационной безопасности является важным условием функционирования любой информационной системы, в которой циркулирует критически важная информация. Процесс поддержания состояния информационной безопасности в условиях угроз ее нарушения носит характер конфликтного взаимодействия между средствами защиты и нарушителем. При этом возможны различные стратегии поддержания защищенности информационных систем исходя из характера возможных действий, средств и целей нарушителей.* ***Цель:*** *анализ условий применения упреждающей стратегии обеспечения информационной безопасности, основанной на прогнозировании действий нарушителя и принятии упреждающих мер по обеспечению требуемого уровня защищенности системы.* ***Результаты:*** *сравнительный анализ стратегий поддержания защищенности информационной системы на основе контроля ее текущего состояния и прогнозирования показал, что обе рассмотренные стратегии имеют свои преимущества и недостатки и должны исходить из характера возможных действий, средств и целей нарушителя, однако стратегия поддержания защищенности на основе прогнозирования ее текущего состояния оказывается единственно возможной при поддержании защищенности критически важных информационных систем. Исследованы вероятностно-временные характеристики состояния защищенности при реализации упреждающей стратегии ее поддержания и смене параметров средств защиты на основе прогнозирования изменения уровня защищенности системы, позволяющие обосновать необходимый период управления средствами защиты информации.* ***Практическая значимость:*** *использование методики расчета вероятностно-временных характеристик состояния защищенности на основе вероятностного описания конфликтного взаимодействия значительно повышает защищенность информационных систем, реализующих гибкое управление средствами защиты от несанкционированного доступа в процессе их функционирования.*

Ключевые слова *— информационная безопасность, информационное противоборство, уровень защищенности, стратегия поддержания защищенности.*

Введение

Функционирование информационных систем (ИС), в которых циркулирует критически важная информация, неразрывно связано с обеспечением их информационной безопасности (ИБ) и защищенности информационных ресурсов [1, 2]. Проблема поддержания защищенности ИС особенно остро стоит в тех случаях, когда имеет место ее постоянное функционирование в условиях угроз нарушения ИБ. Это имеет место в распределенных ИС: в сетевых телекоммуникационных системах с большим числом точек доступа и неконтролируемыми уязвимостями, а также в радиотехнических системах передачи информации и системах беспроводного доступа вследствие их электромагнитной доступности [3, 4]. Точки доступа и беспроводные каналы передачи информации оказываются наиболее уязвимыми звеньями распределенных ИС, и их защищенность может быть определяющей для ИБ системы в целом.

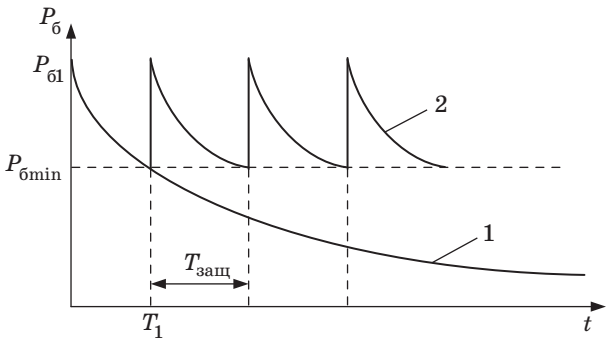
В рамках принятой классификации угроз ИБ целями действий нарушителя могут быть перехват (кража), уничтожение (прерывание), подмена (модификация или фальсификация) информации [1, 5]. Первичной угрозой ИБ является перехват и связанный с ним несанкционированный доступ (НСД) нарушителя к информации. НСД, как угроза ИБ, имеет самостоятельное значение, а также является первой фазой реализации других угроз ИБ, в частности, угроз модификации и фальсификации информации.

Как показывает практика, даже при внедрении современных технологий защиты информации не удается обеспечить гарантированную защищенность систем обработки, хранения и передачи критической информации. Это связано с современными достижениями криптоанализа [6], а также с тем, что взаимодействие между средствами защиты и нарушителем носит конфликтный характер информационного противоборства, при котором обе стороны действуют одновременно, совершая те или иные действия с учетом текущей обстановки и действий противоположной стороны, и обладают информированностью о действиях друг друга [7]. В этих условиях возможны различные стратегии поддержания защищенности ИС исходя из характера возможных действий, средств и целей нарушителей. В настоящей статье обосновывается применение упреждающей стратегии обеспечения ИБ, основанной на прогнозировании состояния ИБ с учетом ожидаемых действий и возможностей нарушителя и принятия упреждающих мер по обеспечению требуемого уровня защищенности ИС.

Общий принцип и стратегии поддержания уровня защищенности ИС

В общем случае требуемый уровень защищенности информации обеспечивается созданием и поддержанием в работоспособном состоянии комплекса средств защиты информации (КСЗИ) ИС, включающего как технические, так и организационные методы обеспечения ИБ [2, 3]. Состав КСЗИ определяется исходя из требований к ИБ системы, ожидаемых угроз и целей нарушителей. Взаимодействие между средствами защиты и нарушителем в условиях постоянного действия угроз ИБ и применения средств защиты может быть описано моделями конфликтного взаимодействия [7, 8]. Нападающая сторона — нарушитель — накапливает информацию и постоянно ведет анализ действий защищающей стороны, что объективно приводит к изменению с течением времени среды безопасности, а именно к снижению защищенности ИС. Защищающаяся сторона — средства защиты — для поддержания состояния защищенности ИС с определенной периодичностью контролирует состояние ИБ и при необходимости вносит изменения (настройки) в КСЗИ, соответствующие текущим условиям функционирования. При этом под правильным функционированием средств защиты понимается предотвращение ими реализации нарушителем угроз ИБ.

Принцип поддержания требуемого уровня защищенности ИС в условиях действия угроз ИБ представлен на рис. 1. Он соответствует подходу к анализу ИБ с использованием теории надежности [9, 10]. Кривая *1* соответствует снижению с течением времени t вероятности обеспечения ИБ $P_б$ без внесения изменений в КСЗИ, кривая *2* соответствует поддержанию вероятности обеспечения ИБ не ниже минимально допустимой $P_{б\,min}$ за счет периодического внесения изменений в КСЗИ. Чтобы гарантировать требуемый уровень ИБ, механизм контроля состояния защищенности ИС должен функционировать так, чтобы необходимые изменения в КСЗИ проводились через определенный интервал времени $T_{защ}$, выбираемый исходя из допустимого снижения вероятности обеспечения ИБ при правильном функционировании средств защиты [6].



■ ***Рис. 1.*** Измерение во времени вероятности обеспечения ИБ в отсутствие и при наличии настройки КСЗИ

В случае, когда поддержание уровня защищенности ИС с течением времени не осуществляется, даже при начальном полностью защищенном состоянии системы ($P_б(0) = P_{б1} = 1$) через интервал времени T_1 вероятность защищенного состояния системы достигнет минимально допустимого значения $P_{б\,min}$ и будет продолжать снижаться на всем жизненном цикле ИС. Характер изменения (снижения) вероятности $P_б$ от времени t будет определяться темпами ведения нападающей стороной — нарушителем — анализа деятельности защищающейся стороны по поддержанию уровня защищенности ИС.

В случае, когда осуществляется поддержание уровня защищенности ИС с течением времени t, с периодичностью $T_{защ}$ производится изменение параметров КСЗИ таким образом, чтобы вероятность защищенного состояния системы не опускалась ниже минимально допустимого значения $P_{б\,min}$. Полагается, что внесение изменений в КСЗИ соответствует устранению обнаруженных нарушителем уязвимостей и приводит к тому, что система возвращается в полностью защищенное состояние ($P_б(nT_{защ}) = 1$, $n = 1, 2, ...$). Очевидно, что чем меньше интервал времени между изменениями параметров КСЗИ, тем больше гарантий защиты. При этом основной задачей становится определение периода изменения параметров КСЗИ $T_{защ}$, при котором в любой момент времени t в течение длительности жизненного цикла ИС выполняется условие $P_б(t) < P_{б\,min}$.

Рассмотренный принцип поддержания требуемого уровня защищенности ИС предопределяет необходимость учета динамики изменения состояния ее ИБ (текущей среды безопасности) для правильного выбора периодичности управления используемыми в КСЗИ средствами защиты информации $T_{защ}$.

Для поддержания защищенности ИС на требуемом уровне в условиях изменения среды безопасности должна быть предусмотрена соответствующая стратегия поддержания защищенности [2, 7]. Для ее реализации КСЗИ должен допускать управление своими функциями и характеристиками отдельных средств для настройки под текущую среду безопасности по результатам контроля или прогнозирования состояния защищенности ИС. При этом оценивание действующих угроз и текущего состояния защищенности системы соответствует контролю и анализу текущей среды безопасности, а настройка и внесение изменений в состав КСЗИ соответствуют управ-

лению средствами защиты в целях противодействия действующим угрозам ИБ. Результатом функционирования КСЗИ является защищенное (защита обеспечена) или незащищенное (защита не обеспечена) состояние ИС.

В общем случае контроль и анализ защищенности ИС предполагает мониторинг и оценку текущего состояния защищенности от действующих угроз. Управление КСЗИ по результатам мониторинга и оценки текущего состояния защищенности осуществляется таким образом, чтобы состояние ИБ системы поддерживалось на требуемом уровне. При этом принципиальное значение приобретает возможность оперативного — в реальном времени или с допустимой задержкой — выполнения мониторинга текущего состояния защищенности ИС от действующих угроз. Под допустимой задержкой понимается задержка, соответствующая так называемому критическому сроку жизни информации — интервалу времени, необходимому нарушителю для ее использования в своих целях.

Поскольку любая угроза ИБ реализуется в результате НСД к ИС, контроль ее защищенности наряду с оценкой текущего уровня защищенности должен включать в себя обнаружение воздействий (атак) нарушителей и фактов их НСД. От того, существует ли возможность эффективно оперативно выполнять эти операции соответствующими аппаратными или программными средствами, входящими в состав КСЗИ, зависит стратегия поддержания защищенности ИС. Можно выделить две основные стратерии поддержания защищенности ИС: на основе контроля и на основе прогнозирования ее текущего состояния.

При наличии возможности оперативного обнаружения средствами КСЗИ атак нарушителей и фактов их НСД в ИС реализуется стратегия поддержания защищенности на основе контроля ее текущего состояния. В соответствии с классификацией систем и процессов защиты информации [2, 7] данная стратегия соответствует оперативно-диспетчерскому управлению процессами функционирования систем защиты информации. Она получает широкое распространение в сетевых системах связи и передачи данных, в том числе в радиосетях с интенсивным трафиком и высокой частотой атак нарушителей, направленных на реализацию широкого спектра угроз ИБ. Для этого средствами защиты многоуровневого КСЗИ осуществляются совместный контроль событий безопасности и активности абонентов, мониторинг защищенности сетей доступа и технологических сетей управления предоставлением услуг. В большинстве случаев характер угроз позволяет их обнаружить и локализовать НСД с допустимыми потерями в качестве обслуживания абонентов сети, а накопление статистических данных об обнаруженных атаках позволяет эффективно им противодействовать при управлении (настройке) КСЗИ [3, 11].

В отсутствие возможности оперативного обнаружения средствами КСЗИ атак нарушителей и фактов их НСД в ИС реализуется стратегия поддержания защищенности на основе прогнозирования ее текущего состояния. В соответствии с классификацией систем и процессов защиты информации [2, 7] по принципу реализации данная стратегия соответствует календарно-плановому управлению процессами функционирования систем защиты информации. Она получает широкое распространение при поддержании защищенности информационно-вычислительных систем от отдельных угроз ИБ, например, при обновлении антивирусной защиты, а также при предотвращении НСД к информации в результате криптоанализа при реализации алгоритмов прямого перебора, временная сложность которых известна [6, 12]. При этом определяемый по результатам прогнозирования защищенности ИС календарный период управления (настройки) КСЗИ на длительных интервалах времени может изменяться при изменении на этих интервалах используемых при прогнозировании исходных данных, например, ожидаемой активности нарушителя.

Обе рассмотренные стратегии поддержания защищенности имеют свои преимущества и недостатки. Достоинством стратегии поддержания защищенности на основе контроля ее текущего состояния является то, что она реализуется как процесс адаптации к реально действующим (обнаруженным) угрозам ИБ, что соответствует непосредственной оценке текущего состояния защищенности ИС. В то же время по своему характеру данная стратегия является оборонительной — она реагирует на обнаружение атак и попыток НСД, а не предотвращает их вообще. Недостатком стратегии поддержания защищенности на основе прогнозирования ее текущего состояния является то, что она реализуется как процесс предотвращения не реальных, а ожидаемых угроз ИБ по результатам прогноза, который, строго говоря, не может быть полностью достоверным. В то же время данная стратегия оказывается единственно возможной при поддержании защищенности критически важных ИС. По своему характеру данная стратегия является упреждающей и направлена на недопущение реализации угроз ИБ.

Существует ряд ИС, в которых возможности использования стратегии поддержания защищенности на основе контроля ее текущего состояния ограничены. Это обусловлено следующими причинами. Во-первых, высокой ценой риска реализации угроз НСД, который может привести к серьезным последствиям и значительному

ущербу в критически важных сферах деятельности. Во-вторых, требованиями обеспечить количественные характеристики защищенности на высоком уровне, достижение которого может быть проверено только аналитическими методами. В таких ИС необходимо использовать стратегию поддержания защищенности на основе прогнозирования ее текущего состояния. При этом на основе математических моделей изменения условий функционирования ИС могут быть рассчитаны вероятностно-временные характеристики состояния защищености и на их основе определены интервалы времени, в течение которых обеспечивается требуемый (заданный) уровень защищенности ИС.

Вероятностно-временные характеристики состояния защищенности ИС при управлении параметрами средств защиты на основе ее прогнозирования

Вероятностные модели являются одним из основных видов моделей конфликтного взаимодействия и применимы к широкому классу ИС [5, 6]. Они позволяют описать изменения состояния противоборства конфликтующих сторон при заданных функциях плотности распределения вероятностей их действий, направленных на достижение превосходства, без наложения существенных ограничений на вид этих распределений. Если параметрами распределений являются средние времена обеспечения защиты и реализации угроз, то вероятностные модели позволяют определить соотношение между этими параметрами, при которых достигается требуемый уровень результативности действий сторон защиты и нападения [9], в рассматриваемом случае — результативность применения КСЗИ.

Вероятностное описание процесса конфликтного взаимодействия сторон защиты и нападения осуществляется с использованием функций распределения вероятностей случайных моментов времени применения средств защиты и реализации угроз нападения [13, 14]. Выигрыш той или иной стороны на некотором интервале времени длительностью T заключается в реализации своего варианта действий раньше, чем будет реализован соответствующий вариант действий противоположной стороны. Для заданных плотностей вероятности случайных моментов времени применение средств защиты $\varphi_{\text{защ}}(t)$ и реализации угроз нападения $\varphi_{\text{нап}}(t)$ вероятности пребывания в состоянии выигрыша на интервале времени $[0, T]$ стороны нападения $P_{\text{нап}}(T)$ и стороны защиты $P_{\text{защ}}(T)$ определяются следующими выражениями:

$$P_{\text{нап}}(T) = \int_0^T \varphi_{\text{нап}}(\tau)\left(1 - \int_0^\tau \varphi_{\text{защ}}(t)\,dt\right)d\tau; \qquad (1)$$

$$P_{\text{защ}}(T) = \int_0^T \varphi_{\text{защ}}(\tau)\left(1 - \int_0^\tau \varphi_{\text{нап}}(t)\,dt\right)d\tau. \qquad (2)$$

Определение вероятностей успешного преодоления средств защиты $P_{\text{нап}}(T)$ и недопущения преодоления средств защиты $P_{\text{защ}}(T)$ в соответствии с выражениями (1) и (2) формализовано для интервала времени длительностью T с началом действий в момент времени $t = 0$ и некоторых фиксированных на данном интервале плотностей вероятности случайных моментов применения средств защиты $\varphi_{\text{защ}}(t)$ и реализации угроз нападения $\varphi_{\text{нап}}(t)$. Для любого значения T выполняется $P_{\text{нап}}(T) + P_{\text{защ}}(T) = 1$.

Если полагать, что в случае реализации угрозы осуществляется доступ к защищаемому ресурсу, а в случае обеспечения защиты доступ исключается, то рассматриваемый случай сводится к описанию реализации одиночной угрозы и одиночного применения средств защиты. Конфликтное противоборство складывается из многократных попыток реализации угроз и постоянного применения средств защиты на последовательности временных интервалов T_1, T_2, ... Для описания общего случая реализации угроз в условиях применения средств защиты выражение (1) последовательно применяется к интервалам времени T_1, T_2, ... Для каждого интервала времени задаются плотности вероятности $\varphi_{\text{защ}}(t)$ и $\varphi_{\text{нап}}(t)$, а при расчете вероятностей $P_{\text{нап}}(T)$ и $P_{\text{защ}}(T)$ в соответствии с выражениями (1) и (2) полагается, что началу каждого интервала времени соответствует $t = 0$.

Для анализа условий реализации угроз нападения осуществляется переход от вероятности успешного преодоления средств защиты $P_{\text{нап}}(T)$ на интервале времени $[0, T]$ к вероятности НСД нарушителя $P_{\text{НСД}}(t)$ в текущий момент времени t. В наихудшем с точки зрения нарушителя случае при очередном применении средств защиты происходит полное обновление параметров системы защиты анализируемых ресурсов. Тогда результаты мониторинга ИС, накопленные нарушителем на интервале времени длительностью $t_{\text{защ}\,i}$, в течение которого применялся i-й набор параметров системы защиты, при смене набора параметров системы защиты становятся устаревшими и неинформативными и, начиная с момента времени $t = \sum_{i=0}^{n} t_{\text{защ}\,i}$, $n = 1, 2, ...$, нарушителю нужно начинать мониторинг сначала. Чем больше интервал времени $t_{\text{защ}\,i}$, в течение которого применяется i-й набор параметров системы защиты, тем больших значений достигает на этом интервале вероятность $P_{\text{НСД}}(t)$.

В общем случае длительность случайных интервалов времени применения изменяемых пара-

метров системы защиты $t_{\text{защ}\,i}$ описывается плотностью распределения вероятностей применения средств защиты $\varphi_{\text{защ}}(t)$. При фиксированном периоде применения средств защиты $t_{\text{защ}\,i} = T_{\text{защ}}$ и $\varphi_{\text{защ}}(t) = \delta(t - T_{\text{защ}})$. При принятых допущениях переход от вероятности $P_{\text{нап}}(T)$ к вероятности $P_{\text{НСД}}(t)$ осуществляется следующим образом. Исходной является полученная в результате описания процесса НСД нарушителя к ИС, как конфликтного взаимодействия, функциональная зависимость от аргумента T вероятности реализации угрозы $P_{\text{нап}}(T)$. Вероятность НСД нарушителя $P_{\text{НСД}}(t)$ в текущий момент времени t в общем случае определяется зависимостью $P_{\text{нап}}(T)$ с заменой аргумента T на аргумент $t - \sum_{i=0}^{n} t_{\text{защ}\,i}$:

$$P_{\text{НСД}}(t) = P_{\text{нап}}\left(t - \sum_{i=0}^{n} t_{\text{защ}\,i}\right),$$

$$\sum_{i=0}^{n} t_{\text{защ}\,i} \le t \le \sum_{i=0}^{n+1} t_{\text{защ}\,i},\ n=1, 2, \ldots . \qquad (3)$$

Для перехода от зависимости $P_{\text{нап}}(T)$ к зависимости $P_{\text{НСД}}(t)$ необходимо задание моментов времени $t_{\text{защ}\,i}$, $i = 1, 2, \ldots$. В общем случае получаем:

$$P_{\text{НСД}}(t) = P_{\text{нап}}(t) \text{ при } 0 \le t \le t_{\text{защ1}};$$

$$P_{\text{НСД}}(t) = P_{\text{нап}}(t - t_{\text{защ1}}) \text{ при } t_{\text{защ1}} \le t \le t_{\text{защ1}} + t_{\text{защ2}};$$

$$P_{\text{НСД}}(t) = P_{\text{нап}}(t - t_{\text{защ1}} - t_{\text{защ2}})$$

$$\text{при } t_{\text{защ1}} + t_{\text{защ2}} \le t \le t_{\text{защ1}} + t_{\text{защ2}} + t_{\text{защ3}} \text{ и т. д.}$$

При фиксированном периоде $T_{\text{защ}}$ смены параметров системы защиты вероятность НСД нарушителя $P_{\text{НСД}}(t)$ в текущий момент времени t определяется зависимостью $P_{\text{нап}}(T)$ с заменой аргумента T на аргумент $(t - nT_{\text{защ}})$:

$$P_{\text{НСД}}(t) = P_{\text{нап}}(t - nT_{\text{защ}})$$

$$\text{при } nT_{\text{защ}} \le t \le (n + 1)T_{\text{защ}},\ n = 1, 2, \ldots .$$

В данном случае $t_{\text{защ}\,i} = T_{\text{защ}}$, $i = 1, 2, \ldots$, и для перехода от зависимости $P_{\text{нап}}(t)$ к зависимости $P_{\text{НСД}}(t)$ необходимо задание величины $T_{\text{защ}}$. В результате получаем

$$P_{\text{НСД}}(t) = P_{\text{нап}}(t) \text{ при } 0 \le t \le T_{\text{защ}};$$

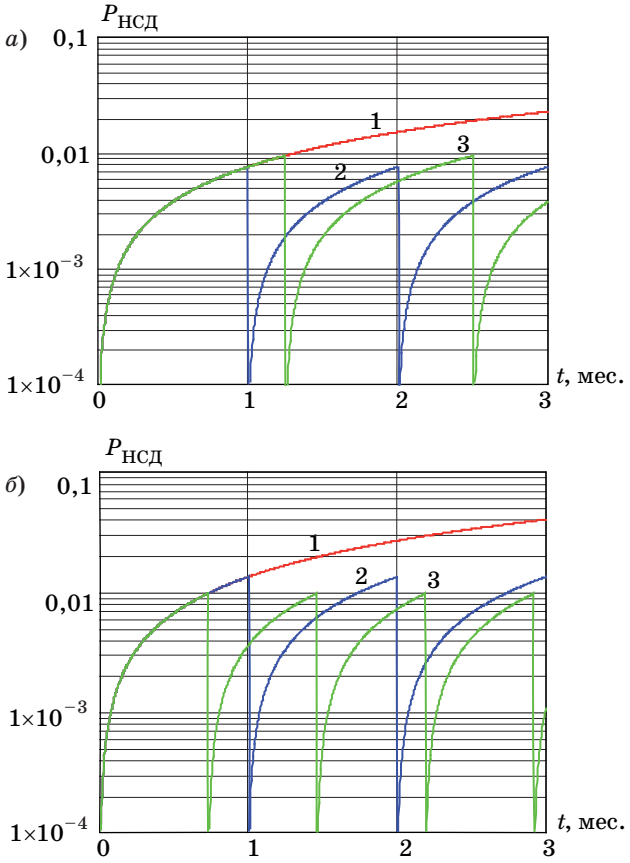
$$P_{\text{НСД}}(t) = P_{\text{нап}}(t - T_{\text{защ}}) \text{ при } T_{\text{защ}} \le t \le 2T_{\text{защ}};$$

$$P_{\text{НСД}}(t) = P_{\text{нап}}(t - 2T_{\text{защ}}) \text{ при } 2T_{\text{защ}} \le t \le 3T_{\text{защ}} \text{ и т. д.}$$

На основе выражений (1) и (3) проведены расчеты вероятности НСД нарушителя $P_{\text{НСД}}(t)$ для различных соотношений между постоянными времени применения средств защиты $T_{\text{защ}}$ и реализации угроз нападения $T_{\text{нап}}$. Действия стороны нападения характеризовались экспоненциальным законом распределения вероятностей случайных моментов времени реализации угроз нападения $\varphi_{\text{нап}}(t) = \frac{1}{T_{\text{нап}}} \exp\left(-\frac{t}{T_{\text{нап}}}\right)$, действия стороны защиты — законом распределения вероятностей применения средств защиты типа δ-функции $\varphi_{\text{защ}}(t) = \delta(t - T_{\text{защ}})$, что соответствует календарному принципу смены параметров КСЗИ.

В качестве примера рассматривался КСЗИ с типичным директивно установленным периодом управления параметрами (смены параметров) $T_{\text{защ}} = 1$ мес. Полагалось, что нарушитель предпринимает попытки по преодолению КСЗИ с постоянной времени реализации угроз нападения $T_{\text{нап}}$, изменяющейся в зависимости от обстановки, в которой ведется информационное противоборство. Задавалось $T_{\text{нап}} = 10$ лет для нормальной обстановки и $T_{\text{нап}} = 6$ лет для обстановки обострения информационного противоборства. Во втором случае имеет место активизация действий нарушителя, и за счет качественного и количественного увеличения привлекаемых им средств для анализа действий защищающейся стороны, преодоления защиты и доступа к защищаемым ресурсам величина $T_{\text{нап}}$ уменьшается.

В качестве приемлемого уровня защищенности, который должен обеспечивать КСЗИ в любой момент времени, рассматривалась вероятность НСД нарушителя $P_{\text{НСД}} = 10^{-2}$. Проведенные расчеты показали, что при выбранных исходных данных требуемый уровень защищенности обеспечивается при $T_{\text{защ}} = 37$ сут в нормальной обстановке и $T_{\text{защ}} = 22$ сут в обстановке обострения информационного противоборства. Таким образом, период управления параметрами КСЗИ $T_{\text{защ}} = 1$ мес. в первом случае гарантированно обеспечивает требуемый уровень защищенности, а во втором случае является недостаточным. Отметим, что на практике приемлемый уровень вероятности НСД нарушителя $P_{\text{НСД}}$ может изменяться в широких пределах в зависимости от типа ИС, характера угроз и защищаемых информационных ресурсов. Так, допустимая вероятность вскрытия ключей шифрования в системах криптографической защиты информации может составлять очень малые величины. Допустимый уровень вероятности НСД нарушителя $P_{\text{НСД}} = 10^{-2}$ выбран для примера, демонстрирующего степень защищенности при рассмотренном соотношении между величинами $T_{\text{защ}}$ и $T_{\text{нап}}$ — ежемесячная смена параметров КСЗИ при случайном характере реализации угроз нападения с постоянной времени в несколько лет.



■ ***Рис. 2.*** Зависимость вероятности НСД от времени в нормальной обстановке (*а*) и в обстановке обострения информационного противоборства (*б*)

На рис. 2, *а* и *б* представлены зависимости вероятности НСД нарушителя к ИС от времени $P_{НСД}(t)$ для рассмотренных случаев функционирования КСЗИ с календарной сменой параметров в различные периоды действия нарушителя, совершающего попытки преодоления КСЗИ и реализации НСД к ИС.

На рис. 2, *а* представлены расчетные зависимости $P_{НСД}(t)$ в нормальной обстановке при $T_{нап} = 10$ лет. Кривая *1* соответствует использованию одних и тех же параметров КСЗИ, кривая *2* — смене параметров КСЗИ с периодом $T_{защ0} = 1$ мес. (30 сут), кривая *3* — смене параметров КСЗИ с периодом $T_{защ1} = 1{,}23$ мес. (37 сут). На рис. 2, *б* представлены расчетные зависимости $P_{НСД}(t)$ в обстановке обострения информационного противоборства при $T_{нап} = 6$ лет. Кривая *1* соответствует использованию одних и тех же параметров КСЗИ, кривая *2* — смене параметров КСЗИ с периодом $T_{защ0} = 1$ мес. (30 сут), кривая *3* — смене параметров КСЗИ с периодом $T_{защ1} = 0{,}73$ мес. (22 сут). На обоих рисунках момент времени $t = 0$ соответствует началу жизненного цикла ИС или очередному обновлению параметров ее КСЗИ.

Практический интерес представляет выигрыш в ИБ, который имеет место в тех случаях, когда с учетом текущего состояния защищенности ИС требуется более частый контроль и внесение изменений в КСЗИ, чем с периодичностью, определяемой директивно. Если задаваемый по календарному принципу период обновления параметров КСЗИ составляет $T_{защ0}$, а период обновления параметров КСЗИ, требуемый с учетом текущего уровня защищенности ИС, составляет $T_{защ1}$, то выигрыш в ИБ имеет место при $T_{защ0} > T_{защ1}$ и составляет

$$B = \begin{cases} (T_{защ0} - T_{защ1}) / T_{защ0}, & T_{защ0} > T_{защ1}; \\ 0, & T_{защ0} \le T_{защ1}. \end{cases} \quad (4)$$

Величина выигрыша в информационной безопасности B, определяемая выражением (4), есть доля времени, в течение которого при управлении параметрами КСЗИ по календарному принципу с периодом $T_{защ0}$ вероятность НСД нарушителя к ИС выше требуемого уровня. Эта величина изменяется от 0 до 1 и может быть выражена в процентах. В рассмотренном примере в нормальной обстановке ежемесячное обновление параметров КСЗИ обеспечивает поддержание требуемого уровня вероятности НСД нарушителя, а в обстановке обострения информационного противоборства за счет более частого управления параметрами КСЗИ с учетом текущего состояния защищенности ИС обеспечивается выигрыш $B = 0{,}27$ — при обновлении параметров КСЗИ без учета текущего состояния защищенности ИС вероятность НСД нарушителя оказывается выше требуемого уровня в течение 27 % времени.

Предельные значения величины B соответствуют выполнению требований по ИБ при управлении параметрами КСЗИ по календарному принципу ($B = 0$ при $T_{защ0} \le T_{защ1}$) и значительному превышению периода управления параметрами КСЗИ по сравнению с требуемым периодом управления с учетом текущего уровня защищенности ИС ($B \to 1$ при $T_{защ0} >> T_{защ1}$). Если в течение жизненного цикла ИС управление параметрами КСЗИ не предусматривается, то в качестве $T_{защ0}$ необходимо рассматривать длительность всего жизненного цикла.

При $T_{защ0} < T_{защ1}$ положительный эффект при управлении параметрами КСЗИ с учетом текущего состояния защищенности ИС может состоять в возможности увеличения в $T_{защ1}/T_{защ0}$ раз периода обновления параметров КСЗИ при сохранении требуемого уровня ИБ. В рассмотренном примере в нормальной обстановке приемлемый уровень защищенности, характеризуемый требуемой вероятностью НСД нарушителя, сохраняется при увеличении периода обновления параметров КСЗИ в 1,23 раза. При управлении пара-

метрами аппаратуры криптозащиты увеличение допустимого периода обновления параметров позволяет более «экономно» использовать ключи, не отнесенные в результате предшествующего криптоанализа к «слабым» [6, 12].

Заключение

В условиях информационного противоборства планирование применения определенной стратегии поддержания защищенности ИС должно исходить из характера возможных действий, средств и целей нарушителя и предусматривать управление механизмами защиты, гарантирующее требуемый уровень защищенности. Это достигается выбором стратегии обеспечения ИБ. Рассмотренные стратегии обеспечения ИБ в условиях изменяющейся обстановки (среды безопасности) предполагают контроль и анализ защищенности ИС на основе мониторинга и оценки текущего состояния защищенности от действующих угроз. Управление КСЗИ по результатам мониторинга и оценки текущего состояния защищенности осуществляется таким образом, чтобы состояние ее ИБ системы поддерживалось на требуемом уровне. Рассмотренный принцип поддержания защищенности ИС с использованием упреждающей стратегии обеспечения ИБ на основе прогнозирования ее текущего состояния может быть рекомендован для использования в КСЗИ широкого класса ИС, к которым предъявляются директивные требования по обеспечению заданного уровня защищенности в процессе их функционирования.

Литература

1. **Устинов Г. Н.** Основы информационной безопасности систем и сетей передачи данных. — М.: СИНТЕГ, 2000. — 248 с.
2. **Малюк А. А.** Информационная безопасность: концептуальные и методологические основы защиты информации. — М.: Горячая линия–Телеком, 2004. — 280 с.
3. **Романец Ю. В., Тимофеев П. А., Шаньгин В. Ф.** Защита информации в компьютерных системах и сетях. — М.: Радио и связь, 2001. — 376 с.
4. **Щербаков В. Б., Ермаков С. А.** Безопасность беспроводных сетей: стандарт IEEE 802.11. — М.: РадиоСофт, 2010. — 256 с.
5. **Столлингс В.** Криптография и защита сетей: принципы и практика: пер. с англ. — М.: Вильямс, 2001. — 672 с.
6. **Ростовцев А. Г., Маховенко Е. Б.** Теоретическая криптография. — СПб.: Профессионал, 2003. — 479 с.
7. **Гаценко О. Ю.** Защита информации. Основы организационного управления. — СПб.: Сентябрь, 2001. — 228 с.
8. **Владимиров В. И., Лихачев В. П., Шляхин В. М.** Антагонистический конфликт радиоэлектронных систем. Методы и математические модели. — М.: Радиотехника, 2004. — 384 с.
9. **Шахов В. Г., Елизарова Ю. М.** Анализ и расчет информационной безопасности. — Омск: Изд-во ОмГТУ, 2010. — 136 с.
10. **Радько Н. М., Скобелев И. О.** Риск-модели информационно-телекоммуникационных систем при реализации угроз удаленного и непосредственного доступа. — М.: РадиоСофт, 2010. — 232 с.
11. **Зима В. М., Молдовян А. А., Молдовян Н. А.** Безопасность глобальных сетевых технологий. — СПб.: Изд-во СПбГУ, 1999. — 368 с.
12. **Корниенко А. А., Еремеев М. А., Ададуров С. Е.** Средства защиты информации на железнодорожном транспорте. (Криптографические методы и средства). — М.: Маршрут, 2006. — 256 с.
13. **Мальцев Г. Н., Панкратов А. В., Лесняк Д. А.** Исследование вероятностных характеристик изменения защищенности информационной системы от несанкционированного доступа нарушителей // Информационно-управляющие системы. 2015. № 1. С. 50–59. doi:10.15217/issn1684-8853.2015.1.50
14. **Мальцев Г. Н., Панкратов А. В.** Вероятностное описание возможностей доступа к защищенным ресурсам с использованием средств инженерного анализа // Проблемы информационной безопасности. Компьютерные системы. 2015. № 2. С. 37–46.

UDC 681.3.067
doi:10.15217/issn1684-8853.2017.3.67

Security Maintenance Strategies in Information Systems

Maltsev G. N.[a], Dr. Sc., Tech., Professor, georgy_maltsev@mail.ru
Lesnyak D. A.[a], PhD, Tech., Lecturer, denislesnyk@mail.ru
[a]A. F. Mozhaiskii Military Space Academy, 13, Zhdanovskaia St., 197198, Saint-Petersburg, Russian Federation

Introduction: Ensuring information security is an important functioning condition in any information system where crucial information circulates. The process of maintaining information security under threats of its violation looks like a conflict interaction between the means of protection and a violator. Security maintenance can follow various strategies, proceeding from the nature of

possible actions, tools and purposes of the violators. **Purpose:** We analyze the conditions of using an anticipatory strategy of information security maintenance based on predicting the violator's actions and taking preventive measures to ensure the required level of system security. **Results:** Comparative analysis of information system security maintenance strategies on the basis of monitoring or prediction has shown that both the considered strategies have their own advantages and disadvantages and must take into account the possible actions, tools and purposes of the violator. However, the strategy based on prediction of the system state is the only possible one to maintain the security of crucial information systems. The probabilistic and temporal characteristics of the security condition have been studied for the case of implementing the anticipatory strategy when the parameters of the protection tools vary on the basis of predicting the changes in the system security level. This allows you to substantiate the necessary period of control over the information protection tools. **Practical relevance:** Calculating the probabilistic and temporal characteristics of the security condition on the basis of a probabilistic description of the conflict interaction considerably improves the security of information systems with flexible control over their protection tools.

Keywords — Information Security, Informational Antagonism, Security Level, Security Maintenance Strategy.

References

1. Ustinov G. N. *Osnovy informatsionnoi bezopasnosti sistem i setei peredachi dannykh* [Bases of Information Security of Systems and Data Transmission Networks]. Moscow, SINTEG Publ., 2000. 248 p. (In Russian).
2. Maliuk A. A. *Informatsionnaia bezopasnost': kontseptual'nye i metodologicheskie osnovy zashchity informatsii* [Information Security: Conceptual and Methodological Bases of Information Security]. Moscow, Goriachaia liniia–Telecom Publ., 2004. 280 p. (In Russian).
3. Romanets Iu. V., Timofeev P. A., Shan'gin V. F. *Zashchita informatsii v komp'iuternykh sistemakh i setiakh* [Information Security in Computer Systems and Networks]. Moscow, Radio i sviaz' Publ., 2001. 376 p. (In Russian).
4. Shherbakov V. B., Ermakov S. A. *Bezopasnost' besprovodnykh setei: standart IEEE 802.11* [Safety of Wireless Networks]. Moscow, RadioSoft Publ., 2010. 256 p. (In Russian).
5. Stallings W. Cryptography and Network Security Principles and Practices. New Jersey, Prentice Hall, 2000. 592 p.
6. Rostovtsev A. G., Makhovenko E. B. *Teoreticheskaia kriptografiia* [Theoretical Cryptography]. Saint-Petersburg, Professional Publ., 2003. 479 p. (In Russian).
7. Gatsenko O. Iu. *Zashchita informatsii. Osnovy organizatsionnogo upravleniia* [Information security. Basics of Organizational Management]. Saint-Petersburg, Sentiabr' Publ., 2001. 228 p. (In Russian).
8. Vladimirov V. I., Likhachev V. P., Shliakhin V. M. *Antagonisticheskii konflikt radioelektronnykh sistem. Metody i matematicheskie modeli* [Antagonisticheskiy Conflict of RadioElectronic Systems. Methods and Mathematical Models]. Moscow, Radiotekhnika Publ., 2004. 384 p. (In Russian).
9. Shahov V. G., Elizarova Ju. M. *Analiz i raschet informatsionnoi bezopasnosti* [Analysis and Calculation of Informational Safety]. Omsk, OmGTU Publ., 2010. 136 p. (In Russian).
10. Rad'ko N. M., Skobelev I. O. *Risk-modeli informatsionno-telekommunikatsionnykh sistem pri realizatsii ugroz udalennogo i neposredstvennogo dostupa* [Risk-Models of Information and Telecommunication Systems at Realization of Threats of Remote and Direct Access]. Moscow, RadioSoft Publ., 2010. 232 p. (In Russian).
11. Zima V. M., Moldovjan A. A., Moldvjan N. A. *Bezopasnost' global'nykh setevykh tekhnologii* [Safety of Global Network Technologies]. Saint-Petersburg, SPbGU Publ., 1999. 368 p. (In Russian).
12. Korniyenko A. A., Yeremeyev M. A., Adadurov S. E. *Sredstva zashchity informatsii na zheleznoorozhnom transporte. (Kriptograficheskie metody i sredstva)* [Information Means of Protection on Railway Transport: Cryptographic Methods and Means]. Moscow, Marshrut Publ., 2006. 256 p. (In Russian).
13. Maltsev G. N., Pankratov A. V., Lesnyak D. A. Probabilistic Characteristics of Information System Security Changes under Unauthorized Access. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2015, no. 1, pp. 50–59 (In Russian). doi:10.15217/issn1684-8853.2015.1.50
14. Maltsev G. N., Pankratov A. V. The Probability Description of Opportunities of Access to the Protected Resources with use of Means of the Engineering Analysis. *Problemy informatsionnoi bezopasnosti. Komp'iuternye sistemy*, 2015, no. 2, pp. 37–46 (In Russian).

УВАЖАЕМЫЕ АВТОРЫ!

Научные базы данных, включая SCOPUS и Web of Science, обрабатывают данные автоматически. С одной стороны, это ускоряет процесс обработки данных, с другой — различия в транслитерации ФИО, неточные данные о месте работы, области научного знания и т. д. приводят к тому, что в базах оказывается несколько авторских страниц для одного и того же человека. В результате для всех по отдельности считаются индексы цитирования, снижая рейтинг ученого.

Для идентификации авторов в сетях Thomson Reuters проводит регистрацию с присвоением уникального индекса (ID) для каждого из авторов научных публикаций.

Процедура получения ID бесплатна и очень проста: входите на страницу http://www.researcherid.com, слева под надписью «New to ResearcherID?» нажимаете на синюю кнопку «Join Now It's Free» и заполняете короткую анкету. По указанному электронному адресу получаете сообщение с предложением по ссылке заполнить полную регистрационную форму на ORCID. Получаете ID.