УДК 681.3.067

doi:10.15217/issn1684-8853.2015.1.50

ИССЛЕДОВАНИЕ ВЕРОЯТНОСТНЫХ ХАРАКТЕРИСТИК ИЗМЕНЕНИЯ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА НАРУШИТЕЛЕЙ

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

Цель: *прогнозирование состояния защищенности информационной системы от несанкционированного доступа нарушителей для определения периодичности управления средствами защиты информации.* ***Методы:*** *использованы представление процессов возникновения и предотвращения угроз информационной безопасности в виде потоков случайных событий с заданными статистическими характеристиками и формализованное описание динамики изменения состояния защищенности информационной системы во времени вероятностной моделью конфликтного взаимодействия с нарушителем.* ***Результаты:*** *доказана необходимость использовать в условиях априорной неопределенности экспоненциальное распределение времени преодоления защиты нарушителем. Разработана модель, позволяющая обосновать необходимый период управления средствами защиты информации, а также описать изменение состояния защищенности информационной системы при заданных функциях распределения вероятностей обеспечения и преодоления защиты без наложения ограничений на вид этих распределений.* ***Практическая значимость:*** *на основе анализа изменения вероятностных характеристик защищенности информационной системы во времени может быть реализовано гибкое управление средствами защиты от несанкционированного доступа с учетом прогнозируемого уровня защищенности.*

Ключевые слова *— информационная безопасность, несанкционированный доступ, конфликтное взаимодействие, управление средствами защиты информации.*

Введение

В современных информационно-управляющих системах при передаче и обработке критической информации могут быть использованы различные методы защиты информации, обеспечивающие достижение определенного уровня информационной безопасности (ИБ) [1, 2]. В то же время в условиях информационного противоборства объективным свойством защищенности информационных систем является ее постепенное снижение при неизменном составе средств защиты или при фиксированных их параметрах [3]. Так, при перехвате зашифрованных сообщений и постоянном ведении криптоанализа нарушитель накапливает информацию об используемом методе шифрования, что в отсутствие смены ключей шифрования приводит к снижению уровня защищенности передаваемых сообщений и увеличению вероятности несанкционированного доступа (НСД) к ним нарушителя [4, 5]. В связи с этим необходимо с определенной периодичностью контролировать состояние защищенности информационных систем, своевременно проводить соответствующее текущим условиям управление средствами защиты информации (настройку их параметров) и тем самым поддерживать требуемый уровень защищенности системы от действующих или потенциальных угроз. Это относится как к техническим, так и к организационным мерам обеспечения ИБ, и в общем случае такое управление может рассматриваться как оптимизация состава средств защиты [6] или пересмотр мероприятий по защите информации [7].

Процессы реализации и предотвращения угроз ИБ могут быть описаны методами теории конфликта [8, 9]. Вероятностные модели составляют один из видов моделей конфликтного взаимодействия, применимый к широкому классу организационно-технических систем. Их достоинством является описание изменения состояния защищенности анализируемой системы при заданных функциях распределения вероятностей реализации и предотвращения угроз без наложения ограничений на вид этих распределений. В настоящей статье представлено описание вероятностной модели изменения защищенности информационной системы в условиях конфликтного взаимодействия с нарушителем. Модель позволяет определить периодичность контроля защищенности системы и управления используемыми средствами защиты информации, обеспечивающую требуемый уровень защищенности от действующих угроз, например от НСД нарушителя к передаваемой или обрабатываемой критической информации.

Определение вероятности обеспечения защиты информации за заданное время в условиях конфликтного взаимодействия с нарушителем

Требуемый уровень защищенности информационных систем, функционирующих в условиях информационного противоборства и угроз ИБ, обеспечивается использованием и поддержанием в работоспособном состоянии комплексов средств защиты информации (КСЗИ). В общем случае состав КСЗИ определяют, исходя из требований к ИБ системы, ожидаемых угроз и целей нарушителя. При этом высокая степень неопределенности процесса информационного противоборства, носящего характер конфликтного взаимодействия, приводит к необходимости принимать упреждающие меры по обеспечению требуемого уровня защищенности и сведению к минимуму возможного ущерба от действий нарушителя. Механизм поддержания требуемого состояния защищенности информационной системы должен функционировать так, чтобы через определенный интервал времени, выбираемый исходя из допустимого снижения вероятности нормального функционирования системы, проводилась проверка защищенности и при необходимости управление КСЗИ (настройка параметров входящих в его состав средств).

В постановке задачи моделирования изменения состояния защищенности информационной системы в условиях конфликтного взаимодействия с нарушителем [10, 11] функционирование КСЗИ информационной системы рассматривается как деятельность стороны защиты по обеспечению защиты, а попытки реализации угроз ИБ — как деятельность стороны нападения по преодолению защиты. При этом обе стороны осуществляют одновременно те или иные мероприятия с учетом текущей обстановки и поведения противоположной стороны. На основе формализованного описания изменения во времени защищенности информационной системы от угроз нарушителя рассмотрим вероятностные характеристики защищенности, позволяющие прогнозировать значения вероятностей обеспечения защиты в течение заданного интервала времени с целью определить периодичность контроля защищенности и управления (настройки параметров) КСЗИ. При предотвращении угроз НСД к системам передачи информации такое управление средствами защиты заключается в смене ключей шифрования [4, 5].

Общая постановка задачи определения необходимого момента управления КСЗИ при вероятностном описании его конфликтного взаимодействия с нарушителем состоит в следующем [10]. Заданы функции распределения $F_{з\,k}(t_k)$, $k = 1, ..., K$, случайных моментов времени t_k реализации K вариантов защиты и функции распределения $F_{н\,n}(\tau_n)$, $n = 1, ..., N$, случайных моментов времени τ_n реализации N вариантов нападения. Для определения момента времени управления КСЗИ в интересах обеспечения требуемого уровня ИБ необходимо оценивать условия достижения при конфликтном взаимодействии выигрыша защиты. При информационном конфликте k-го и n-го вариантов действий противоборствующих сторон выигрыш защиты $L_{з\,kn}(T)$ на интервале времени длительностью T заключается в реализации своего варианта действий раньше, чем будет реализован соответствующий вариант нападения.

Общее выражение для выигрыша защиты на интервале времени T для k-го и n-го вариантов действий противоборствующих сторон имеет следующий вид:

$$L_{çkn}(T) = \int_0^T F_{çk}(\tau_n)\mathrm{d}F_{ín}(\tau_n). \qquad (1)$$

Усреднение выигрыша защиты (1) по всем возможным альтернативам k и n представляет собой показатель эффективности заложенных в КСЗИ вариантов защиты на интервале времени T:

$$L_ç(T) = \sum_{k=1}^{K}\sum_{n=1}^{N}\int_0^T F_{çk}(\tau_n)\mathrm{d}F_{ín}(\tau_n)Q_nP_{k|n}, \qquad (2)$$

где Q_n — вероятности предотвращения КСЗИ угроз стороны нападения, соответствующие каждому из N вариантов нападения; $P_{k|n}$ — условные вероятности выбора k-го варианта защиты при условии реализации нарушителем n-го варианта нападения.

Выражение (2) учитывает взаимосвязь между вариантами действий защиты и нападения, обусловленную наличием у стороны защиты той или иной информации о стороне нападения, которую сторона защиты использует при принятии решений. На практике эта информация появляется у стороны защиты в результате анализа угроз и уязвимостей информационной системы в изменяющихся условиях ее функционирования и является функцией от длительности анализируемого интервала времени T. Отсюда следует постановка вариационных задач максимизации выигрыша защиты $L_з(T)$ и определения наибольшего интервала времени T, на котором выигрыш защиты $L_з(T)$ не менее заданного допустимого значения $L_{з.доп}$.

Если полагать, что начальный момент анализируемого интервала времени соответствует моменту времени $t_{упр\ i}$, в который произошло очередное i-е управление КСЗИ, то интервал времени до следующего $(i + 1)$-го управления КСЗИ $T_i = t_{упр\ i+1} - t_{упр\ i}$ должен удовлетворять условию $L_з(T) \geq L_{з.доп}$ для всех $T \in T_i$. Практически вместо обобщенного показателя выигрыша

защиты $L_з(T)$, определяемого выражением (2) и являющегося функционалом от функций распределения $F_{з\,k}(t_k)F_{н\,n}(\tau_n)$, могут быть максимизированы монотонно связанные с ним показатели. В качестве такого показателя, отражающего суть конфликтного взаимодействия сторон защиты и нападения, примем вероятность $P_{защ}(T)$ пребывания стороны защиты в состоянии выигрыша в течение интервала времени T. От этой вероятности в дальнейшем может быть осуществлен переход к зависимости вероятности обеспечения защиты от времени $P_з(t)$, где моменту времени $t_{упр\,i}$ соответствует $t = 0$, а интервал времени $T_i = t_{упр\,i+1} - t_{упр\,i}$ соответствует условию $P_з(t) \geq P_{з.доп}$ превышения вероятности обеспечения защиты допустимого уровня $P_{з.доп}$ для всех $t \leq T_i$. Исходя из этого условия по зависимостям $P_з(t)$ непосредственно осуществляется определение периода управления средствами защиты информации. При этом чем выше вероятность обеспечения защиты $P_{защ}(T)$ при фиксированной величине T, тем медленнее убывают соответствующие им зависимости $P_з(t)$ и тем реже необходимо управлять КСЗИ для поддержания требуемого уровня защищенности информационной системы.

При вероятностном подходе к описанию процесса конфликтного взаимодействия процессы возникновения и предотвращения угроз ИБ представляются в виде потоков случайных событий с заданными статистическими характеристиками. Условия конфликтного взаимодействия при попытке реализации нарушителем определенной угрозы ИБ характеризуются плотностями распределения вероятностей обеспечения и преодоления защиты $w_{защ}(t)$ и $w_{нап}(t)$ соответственно. Данные плотности распределения отражают возможности используемого КСЗИ обеспечивать защиту информации при попытке нарушителем реализовать соответствующую угрозу ИБ, а нарушителя — исполнить данную угрозу на рассматриваемом интервале времени T. Вероятность обеспечения защиты в течение интервала времени T определяется выражением

$$P_{çàù}(T) = \int_0^T w_{çàù}(\tau)\left[1 - \int_0^\tau w_{íàï}(t)dt\right]d\tau. \qquad (3)$$

На практике имеют место конечное время изменения условий функционирования информационной системы, связанных с попытками нарушителя реализовать угрозы ИБ, и конечная оперативность управления КСЗИ для их предотвращения. Величина вероятности обеспечения защиты $P_{защ}(T)$, определяемая выражением (3), зависит от временных масштабов изменения процессов преодоления и обеспечения защиты, описываемых плотностями распределения вероятностей $w_{защ}(t)$ и $w_{нап}(t)$. Задачей защиты является увеличение величины $P_{защ}(T)$ при поведении нарушителя, характеризуемом плотностью распределения вероятностей преодоления защиты $w_{нап}(t)$, за счет выбора соответствующего своего поведения, характеризуемого плотностью распределения вероятностей обеспечения защиты $w_{защ}(t)$, что эквивалентно критерию управления КСЗИ

$$Ð_{çàù}(Ò) = \int_0^T w_{çàù}(\tau)\left[1 - \int_0^\tau w_{íàï}(t)dt\right]d\tau \to \max_{w_{çàù}(\tau)}.$$

Максимальное значение вероятности обеспечения защиты $P_{защ}(T) = 1$ достигается в двух случаях:

1) если на анализируемом интервале времени T полностью отсутствуют воздействия нападения — при $w_{нап}(t) = 0$;

2) если на анализируемом интервале времени T защита обеспечивает полностью бесконфликтное функционирование с нападением — при

$$\int_0^T w_{çàù}(\tau)\int_0^\tau w_{íàï}(t)dtd\tau = 0.$$

Первый из указанных случаев соответствует бесконечно медленному изменению условий функционирования информационной системы, когда ее КСЗИ обеспечивает предотвращение всех возможных угроз ИБ со стороны нарушителя. В этом случае управление (настройка) КСЗИ не требуется. Второй из указанных случаев соответствует бесконечно быстрой упреждающей реакции КСЗИ на изменение условий функционирования информационной системы. В этом случае управление (настройка) КСЗИ происходит мгновенно и обеспечивает предотвращение всех возможных угроз ИБ.

Определение зависимостей $P_з(t)$ по зависимостям $P_{защ}(T)$ осуществляется следующим образом. Если положить в выражении вида (3) $w_{защ}(\tau) = \delta(\tau - T_{защ})$ и $T > T_{защ}$, то зависимости $P_з(t)$ будет соответствовать зависимость $P_{защ}(T_{защ})$ с заменой переменной $T_{защ}$ на переменную t. Полученные зависимости $P_з(t)$ имеют единичное значение при $t = 0$ и стремятся к нулю при $t \to \infty$, что отражает снижение с течением времени уровня защищенности информационной системы после управления КСЗИ в момент времени $t = 0$. Тогда интервал времени безопасного функционирования информационной системы T_0 является решением относительно t уравнения $P_з(t) = P_{з.доп}$ (полагаем $t_{упр\,i} = 0$). Найденные таким образом значения T_0 соответствуют требуемой периодичности управления КСЗИ, необходимой для своевременной его настройки — внесения изменений, соответствующих текущим условиям функционирования.

Достоинством вероятностного описания процесса конфликтного взаимодействия является отсутствие ограничений на вид используемых распределений вероятностей обеспечения и пре-

одоления защиты. Это позволяет задавать и проводить расчеты для различных стандартных и экспериментальных законов распределения. В то же время особенности и свойства вероятностных характеристик изменения защищенности информационных систем во времени могут быть рассмотрены по результатам анализа влияния на вероятности $P_{\text{защ}}(T)$ и $P_{\text{з}}(t)$ параметров плотностей распределения $w_{\text{защ}}(t)$ и $w_{\text{нап}}(t)$ для типовых законов распределения вероятностей преодоления и обеспечения защиты.

Результаты исследования изменения во времени вероятностных характеристик защищенности информационной системы

С использованием общего выражения (3) было исследовано влияние вида и параметров законов распределения вероятностей обеспечения защиты (для стороны защиты) и преодоления защиты (для стороны нападения) на динамику изменения защищенности информационной системы во времени. В качестве типовых рассматривались законы распределения вероятностей преодоления и обеспечения защиты трех видов:

1) усеченное гауссово распределение с функциями плотности распределения вероятностей

$$w_{\text{çàù}}(t)=\frac{1}{A_{\text{çàù}}\sqrt{2\pi}\sigma_{\text{çàù}}}\exp\left[-\frac{(t-T_{\text{çàù}})^2}{2\sigma^2_{\text{çàù}}}\right] \text{ и}$$

$$w_{\text{íàï}}(t)=\frac{1}{A_{\text{íàï}}\sqrt{2\pi}\sigma_{\text{íàï}}}\exp\left[-\frac{(t-T_{\text{íàï}})^2}{2\sigma^2_{\text{íàï}}}\right],$$

определяемыми для области значений $t \ge 0$, с параметрами: $T_{\text{защ}}$ и $T_{\text{нап}}$ — средние значения времени обеспечения и преодоления защиты, $\sigma_{\text{защ}}$ и $\sigma_{\text{нап}}$ — среднеквадратические значения времени обеспечения и преодоления защиты, $A_{\text{защ}}$ и $A_{\text{нап}}$ — нормировочные коэффициенты, обеспечивающие при переходе от стандартного к усеченному гауссову распределению выполнение условий нормировки $\int_0^\infty w_{\text{çàù}}(t)\mathrm{d}t=1$ и $\int_0^\infty w_{\text{íàï}}(t)\mathrm{d}t=1$;

2) экспоненциальное распределение с функциями плотности распределения вероятностей

$$w_{\text{çàù}}(t)=\frac{1}{T_{\text{çàù}}}\exp\left(-\frac{t}{T_{\text{çàù}}}\right) \text{ и}$$

$$w_{\text{íàï}}(t)=\frac{1}{T_{\text{íàï}}}\exp\left(-\frac{t}{T_{\text{íàï}}}\right),$$

определенными в области значений $t \ge 0$, с параметрами: $T_{\text{защ}}$ и $T_{\text{нап}}$ — средние значения времени обеспечения и преодоления защиты;

3) распределение с функциями плотности распределения вероятностей вида δ-функции

$$w_{\text{çàù}}(t)=\delta\left(t-T_{\text{çàù}}\right) \text{ и } w_{\text{íàï}}(t)=\delta\left(t-T_{\text{íàï}}\right),$$

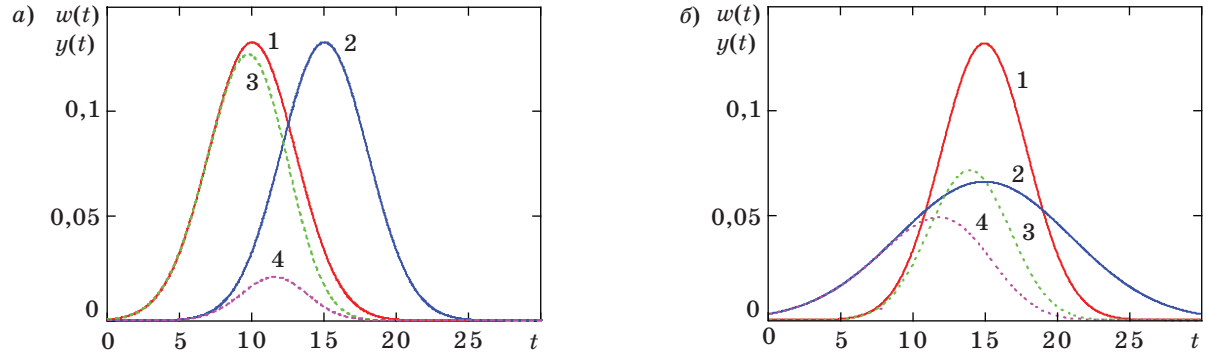
задаваемыми в области значений $t \ge 0$, соответствующее детерминированным моментам времени $T_{\text{защ}}$ и $T_{\text{нап}}$ обеспечения и преодоления защиты.

Гауссово распределение, являющееся двухпараметрическим, позволяет при описании конфликтного противодействия оценить влияние на результирующую величину вероятности обеспечения защиты средних и среднеквадратических значений времени обеспечения и преодоления защиты. Необходимость использовать усеченное гауссово распределение обусловлена тем, что плотности распределения вероятностей $w_{\text{защ}}(t)$ и $w_{\text{нап}}(t)$ должны задаваться в области положительных значений времени $0 \le t < \infty$, в то время как стандартное гауссово распределение задается в области $-\infty < t < \infty$. Нормировочные коэффициенты $A_{\text{защ}}$ и $A_{\text{нап}}$ для усеченного гауссова распределения, определяемого в области $0 \le t < \infty$, в соответствии с правилами теории вероятностей [12] рассчитываются по формулам

$$A_{\text{çàù}}=\frac{1}{\sqrt{2\pi}\sigma_{\text{çàù}}}\int_0^\infty \exp\left[-\frac{(t-T_{\text{çàù}})^2}{2\sigma^2_{\text{çàù}}}\right]\mathrm{d}t;$$

$$A_{\text{íàï}}=\frac{1}{\sqrt{2\pi}\sigma_{\text{íàï}}}\int_0^\infty \exp\left[-\frac{(t-T_{\text{íàï}})^2}{2\sigma^2_{\text{íàï}}}\right]\mathrm{d}t.$$

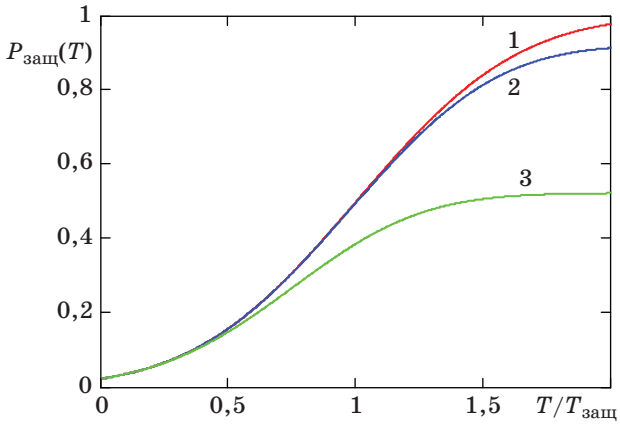
На рис. 1 приведены графики гауссовых плотностей распределения вероятностей $w(t)$ с различным сочетанием параметров T и σ, в качестве которых могут выступать $T_{\text{защ}}$ или $T_{\text{нап}}$ и $\sigma_{\text{защ}}$ или $\sigma_{\text{нап}}$ соответственно, а также функций вида $y(t)=w_{\text{çàù}}(t)\left[1-\int_0^t w_{\text{íàï}}(\tau)\mathrm{d}\tau\right]$, представляющих собой подынтегральное выражение внешнего интеграла в выражении (3) для вероятности обеспечения защиты $P_{\text{защ}}(T)$. На рис. 1, *а*: кривая *1* — гауссова плотность вероятности $w_1(t)$ с параметрами $T = 10$, $\sigma = 3$; кривая *2* — гауссова плотность вероятности $w_2(t)$ с параметрами $T = 15$, $\sigma = 3$; кривая *3* — функция $y(t)$, определяемая в предположении, что $w_1(t)=w_{\text{защ}}(t)$, $w_2(t)=w_{\text{нап}}(t)$; кривая *4* — функция $y(t)$, определяемая в предположении, что $w_1(t) = w_{\text{нап}}(t)$, $w_2(t) = w_{\text{защ}}(t)$. На рис. 1, *б*: кривая *1* — гауссова плотность вероятности $w_1(t)$ с параметрами $T = 15$, $\sigma = 3$; кривая *2* — гауссова плотность вероятности $w_2(t)$ с параметрами $T = 15$, $\sigma = 6$; кривая *3* — функция $y(t)$, определяемая в предположении, что $w_1(t) = w_{\text{защ}}(t)$, $w_2(t) = w_{\text{нап}}(t)$; кривая *4* — функция $y(t)$, определяемая в предположении, что $w_1(t) = w_{\text{нап}}(t)$, $w_2(t) = w_{\text{защ}}(t)$.



■ ***Рис. 1.*** Гауссова плотность распределения вероятности обеспечения защиты $w(t)$ и функции $y(t)$ при различных соотношениях между параметрами T и σ: *а* — значения T различные; *б* — значение T фиксированно

С учетом введенного обозначения $y(t)$ вероятность обеспечения защиты за заданное время T определяется выражением $P_{\text{çà ù}}(T) = \int_0^T y(t)\mathrm{d}t$, а при $T \to \infty$ ей соответствует площадь под кривыми *3* и *4*. Из графиков видно, что определяющими параметрами, от соотношения между которыми зависят результирующие значения вероятности обеспечения защиты $P_{\text{защ}}(T)$, являются средние значения времени обеспечения и преодоления защиты $T_{\text{защ}}$ и $T_{\text{нап}}$. Именно от их сочетания зависит способность защиты противостоять угрозам нападения, и управление КСЗИ должно быть направлено, прежде всего, на уменьшение отношения $T_{\text{защ}}/T_{\text{нап}}$, что соответствует упреждающей стратегии защиты. От соотношения между среднеквадратическими значениями времени обеспечения и преодоления защиты $\sigma_{\text{защ}}$ и $\sigma_{\text{нап}}$ результирующие значения вероятности обеспечения защиты $P_{\text{защ}}(T)$ зависят слабо. Так, при $T \to \infty$ функциям $y(t)$, представленным кривыми *3* и *4* на рис. 1, *а*, соответствуют значения $P_{\text{защ}}(T)$, равные 0,88 и 0,12, а обеим функциям $y(t)$, представленным кривыми *3* и *4* на рис. 1, *б* — значения $P_{\text{защ}}(T)$ около 0,5. Доминирующим останется влияние на величину $P_{\text{защ}}(T)$ отношения $T_{\text{защ}}/T_{\text{нап}}$ и при различных средних $T_{\text{защ}}$ и $T_{\text{нап}}$ и среднеквадратических $\sigma_{\text{защ}}$ и $\sigma_{\text{нап}}$ значениях времени обеспечения и преодоления защиты. При этом уменьшение $\sigma_{\text{защ}}$ приводит к более медленному нарастанию $P_{\text{защ}}(T)$ в области значений $T < T_{\text{защ}}$, а увеличение $\sigma_{\text{защ}}$ приводит к уменьшению величины $P_{\text{защ}}(T)$ при $T \to \infty$.

Зависимости вероятности обеспечения защиты $P_{\text{защ}}(T/T_{\text{защ}})$ (рис. 2) рассчитаны в соответствии с выражением (3) для гауссовых плотностей распределения вероятностей $w_{\text{защ}}(t)$ и $w_{\text{нап}}(t)$ при различных отношениях средних значений $T_{\text{защ}}/T_{\text{нап}}$ и среднеквадратических значениях $\sigma_{\text{защ}} = \sigma_{\text{нап}} = 0{,}5T_{\text{защ}}$. Из графиков видно, что



■ ***Рис. 2.*** Зависимости вероятности обеспечения защиты $P_{\text{защ}}(T)$ для гауссовых плотностей распределения вероятностей $w_{\text{защ}}(t)$ и $w_{\text{нап}}(t)$ при соотношениях $T_{\text{защ}}/T_{\text{нап}}$, равных 0,1 (кривая *1*), 0,5 (кривая *2*) и 1 (кривая *3*)

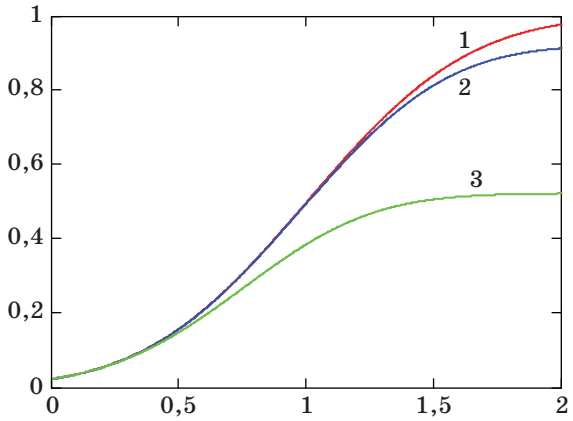
возможности достижения значений $P_{\text{защ}}(T) \approx 1$ существенным образом зависят от отношения $T_{\text{защ}}/T_{\text{нап}}$ вследствие насыщения зависимостей $P_{\text{защ}}(T)$ на некотором уровне, который тем ниже, чем меньше отношение $T_{\text{защ}}/T_{\text{нап}}$.

Экспоненциальное распределение и распределение вида δ-функции являются однопараметрическими и характеризуются одним параметром, определяющим среднее значение времени обеспечения $T_{\text{защ}}$ или преодоления $T_{\text{нап}}$ защиты для экспоненциального распределения и детерминированные моменты времени обеспечения $T_{\text{защ}}$ и преодоления $T_{\text{нап}}$ защиты для распределения вида δ-функции. При задании в выражении (3) плотностей распределения вероятностей $w_{\text{защ}}(t)$ и $w_{\text{нап}}(t)$, соответствующих экспоненциальному распределению и распределению вида δ-функции, могут быть получены простые аналитические выражения для вероятности обеспечения защиты $P_{\text{защ}}(T)$ в зависимости от относительных параметров $T/T_{\text{защ}}$ и $T_{\text{защ}}/T_{\text{нап}}$.

Экспоненциальное распределение соответствует простейшему потоку событий и описанию переходов между состояниями защищенности информационной системы марковскими случайными процессами [12]. Вычисление вероятности обеспечения защиты за заданное время T в соответствии с выражением (3) для экспоненциальных функций плотности распределения вероятностей $w_{\text{защ}}(t)$ и $w_{\text{нап}}(t)$ с параметрами $T_{\text{защ}}$ и $T_{\text{нап}}$ дает

$$P_{\text{çàù}}(T) = \frac{1}{1 + T_{\text{çàù}} / T_{\text{íàï}}} \times \times \left\{1 - \exp\left[-\frac{T\left(1 + T_{\text{çàù}} / T_{\text{íàï}}\right)}{T_{\text{çàù}}}\right]\right\}. \quad (4)$$

Зависимости вероятности обеспечения защиты $P_{\text{защ}}(T/T_{\text{защ}})$ (рис. 3) рассчитаны по формуле (4) при различных отношениях $T_{\text{защ}}/T_{\text{нап}}$. Из графиков видно, что при описании конфликтного взаимодействия экспоненциальными распределениями моментов обеспечения и преодоления защиты требования к быстроте реакции КСЗИ на изменение условий функционирования оказываются более жесткими, чем при использовании для описания конфликтного взаимодействия гауссовых распределений, особенно в области значений $P_{\text{защ}}(T) > 0{,}5$. Так, при использовании экспоненциальных распределений вероятность обеспечения защиты $P_{\text{защ}}(T) = 0{,}5$ в случае $T_{\text{защ}}/T_{\text{нап}} = 0{,}1$ достигается при $T \approx 0{,}8T_{\text{защ}}$, в случае $T_{\text{защ}}/T_{\text{нап}} = 0{,}5$ – при $T \approx T_{\text{защ}}$, в случае $T_{\text{защ}}/T_{\text{нап}} = 1$ — при $T \approx 2T_{\text{защ}}$, при этом даже в случае $T_{\text{защ}}/T_{\text{нап}} = 0{,}1$ при $T = 2T_{\text{защ}}$ достигается только $P_{\text{защ}}(T) = 0{,}8$. Для сравнения: при использовании гауссовых распределений вероятность обеспечения защиты $P_{\text{защ}}(T) = 0{,}5$ в случаях $T_{\text{защ}}/T_{\text{нап}} = 0{,}1$ и $T_{\text{защ}}/T_{\text{нап}} = 0{,}5$ достигается при $T \approx T_{\text{защ}}$, в случае $T_{\text{защ}}/T_{\text{нап}} = 1$ — при $T \approx 1{,}2T_{\text{защ}}$, а в случае $T_{\text{защ}}/T_{\text{нап}} = 0{,}1$ при $T = 2T_{\text{защ}}$ достигается $P_{\text{защ}}(T) \approx 1$. Поэтому экспоненциальное распределение вероятностей обеспечения и преодоления защиты может рассматриваться как предельный вариант случайного изменения условий функционирования информационных систем.



■ ***Рис. 3.*** Зависимости вероятности обеспечения защиты $P_{\text{защ}}(T)$ для экспоненциальных плотностей распределения вероятностей $w_{\text{защ}}(t)$ и $w_{\text{нап}}(t)$ при соотношениях $T_{\text{защ}}/T_{\text{нап}}$, равных 0,1 (кривая *1*), 0,5 (кривая *2*) и 1 (кривая *3*)

Использование распределения с функциями плотности распределения вероятности вида δ-функции соответствует детерминированным моментам обеспечения (для стороны защиты) и преодоления (для стороны нападения) защиты и позволяет описать скачкообразное изменение вероятности обеспечения защиты между двумя состояниями — защищенным и незащищенным. Вычисление вероятности обеспечения защиты за заданное время T в соответствии с выражением (3) для функций плотности распределения вероятностей $w_{\text{защ}}(t)$ и $w_{\text{нап}}(t)$ вида δ-функции с параметрами $T_{\text{защ}}$ и $T_{\text{нап}}$ дает

$$P_{\text{çàù}}(\dot{O}) = \begin{cases} 1, & 0 \le \dot{O}_{\text{çàù}} / \dot{O}_{\text{íàï}} < 1 \\ 0, & T_{\text{çàù}} / \dot{O}_{\text{íàï}} \ge 1 \end{cases}. \quad (5)$$

Выражение (5) отражает тот факт, что при принятых допущениях о характере изменения условий конфликтного взаимодействия при $T_{\text{защ}} < T_{\text{нап}}$ упреждающая защита всегда позволяет обеспечить полностью защищенное состояние информационной системы, а при $T_{\text{защ}} \ge T_{\text{нап}}$ опережающее нападение всегда достигает своих целей вследствие незащищенного состояния системы.

Возможно использование комбинации различных законов распределения для описания процессов преодоления защиты (для стороны защиты) и обеспечения защиты (для стороны нападения), например, экспоненциального распределения и распределения вида δ-функции. При этом экспоненциальное распределение с параметром $T_{\text{нап}}$ может описывать случайные моменты преодоления защиты нарушителем, а распределение вида δ-функции с параметром $T_{\text{защ}}$ — детерминированные моменты обеспечения защиты, что характерно для периодического управления параметрами КСЗИ. Вычисление вероятности обеспечения защиты за заданное время T в соответствии с выражением (3) для соответствующих функций плотности распределения вероятностей дает

$$P_{\text{çàù}}(\dot{O}) = \begin{cases} \exp(-\dot{O}_{\text{çàù}} / \dot{O}_{\text{íàï}}), & T / \dot{O}_{\text{çàù}} > 1 \\ 0, & 0 \le T / T_{\text{çàù}} \le 1 \end{cases}. \quad (6)$$

Выражение (6) показывает, что детерминированный характер моментов обеспечения защиты

при случайном характере попыток преодоления ее нарушителем приводит к незащищенному состоянию системы в моменты времени $T < T_{\text{защ}}$. Нулевые значения вероятности $P_{\text{защ}}(T)$ при $T < T_{\text{защ}}$ соответствуют наличию неустраненной уязвимости на интервале времени, когда имеется отличная от нуля вероятность преодоления защиты нарушителем. Эта уязвимость устраняется в момент времени $T_{\text{защ}}$, и при $T > T_{\text{защ}}$ устанавливается стационарное значение вероятности обеспечения защиты, которое тем выше, чем меньше отношение $T_{\text{защ}}/T_{\text{нап}}$: при $T > T_{\text{защ}}$ в случае $T_{\text{защ}}/T_{\text{нап}} = 0{,}1$ достигается $P_{\text{защ}}(T) \approx 0{,}9$, в случае $T_{\text{защ}}/T_{\text{нап}} = 0{,}5$ достигается $P_{\text{защ}}(T) \approx 0{,}6$, в случае $T_{\text{защ}}/T_{\text{нап}} = 1$ достигается $P_{\text{защ}}(T) \approx 0{,}37$. Ситуация, когда $w_{\text{защ}}(t) = \delta(t - T_{\text{защ}})$, имеет также важное значение с той точки зрения, что позволяет осуществить переход от вероятности обеспечения защиты $P_{\text{защ}}(T)$, определяемой для условий конфликтного взаимодействия сторон защиты и нападения, к зависимости вероятности обеспечения защиты от времени $P_{\text{з}}(t)$, к которой при проектировании и эксплуатации информационных систем задаются требования вида $P_{\text{з}}(t) \ge P_{\text{з.доп}}$ [3].

Практический интерес представляет определение по зависимости вероятности обеспечения защиты от времени $P_{\text{з}}(t)$ необходимого момента управления (настройки) КСЗИ с учетом ожидаемой динамики угроз (воздействий) нарушителя. Для определения зависимостей $P_{\text{з}}(t)$ по найденным зависимостям $P_{\text{защ}}(T)$ положим $w_{\text{защ}}(t) = \delta(t - T_{\text{защ}})$. Тогда зависимости $P_{\text{з}}(t)$ будет соответствовать зависимость $P_{\text{защ}}(T_{\text{защ}})$ с заменой переменной $T_{\text{защ}}$ на переменную t. После преобразований получаем:

$$P_{\text{ç}}(T) = 1 - \frac{1}{A_{\text{íàï}}}\left[\hat{\text{O}}\left(\frac{t - T_{\text{íàï}}}{\sigma_{\text{íàï}}}\right) - \hat{\text{O}}\left(-\frac{T_{\text{íàï}}}{\sigma_{\text{íàï}}}\right)\right] \qquad (7)$$

для усеченного гауссова распределения времени преодоления защиты, где $\hat{\text{O}}(z) = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{z} \exp\left(-\frac{x^2}{2}\right)dx$ — гауссов интеграл ошибок;

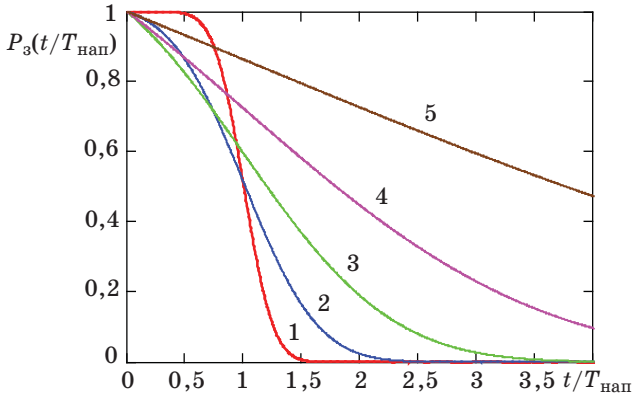
$$P_{\text{ç}}(T) = \exp\left(-t / T_{\text{íàï}}\right) \qquad (8)$$

для экспоненциального распределения времени преодоления защиты;

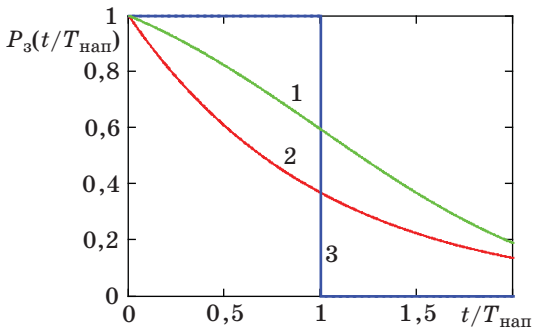
$$P_{\text{ç}}(t) = \begin{cases} 1, & t/T_{\text{íàï}} < 1 \\ 0, & t/T_{\text{íàï}} \ge 1 \end{cases} \qquad (9)$$

для распределения времени преодоления защиты с плотностью распределения вероятностей вида δ-функции.

Все полученные зависимости $P_{\text{з}}(t)$ имеют единичное значение при $t = 0$ и стремятся к нулю при $t \to \infty$, что отражает снижение уровня защищенности системы после настройки ее КСЗИ в момент времени $t = 0$. Зависимости $P_{\text{з}}(t/T_{\text{нап}})$ при различных плотностях распределения $w_{\text{нап}}(t)$ представлены на рис. 4 и 5. На рис. 4 показаны зависимости $P_{\text{з}}(t/T_{\text{нап}})$, соответствующие усеченной гауссовой плотности распределения вероятностей $w_{\text{нап}}(t)$.



■ ***Рис. 4.*** Зависимости вероятности обеспечения защиты $P_{\text{з}}(t/T_{\text{нап}})$ для гауссовой плотности распределения вероятностей $w_{\text{нап}}(t)$ при соотношениях $\delta_{\text{нап}}/T_{\text{нап}}$, равных 0,2 (кривая *1*), 0,5 (кривая *2*), 1 (кривая *3*), 2 (кривая *4*) и 5 (кривая *5*)



■ ***Рис. 5.*** Зависимость вероятности обеспечения защиты $P_{\text{з}}(t/T_{\text{нап}})$ при различных законах распределения времени преодоления защиты: *1* — усеченная гауссова плотность распределения; *2* — экспоненциальная плотность распределения; *3* — плотность распределения вида δ-функции

На рис. 5 приведены зависимости $P_{\text{з}}(t/T_{\text{нап}})$, соответствующие различным видам плотности распределения $w_{\text{нап}}(t)$ при фиксированном среднем значении времени преодоления защиты. Кривая *1* соответствует усеченной гауссовой плотности распределения вероятностей при $\sigma_{\text{нап}}/T_{\text{нап}} = 1$, кривая *2* — экспоненциальной плотности распределения вероятностей, кривая *3* — плотности распределения вероятностей вида δ-функции. Из графиков видно, что наихудшим с точки зрения характера изменения во времени t вероятности

обеспечения защиты $P_з(t)$ является экспоненциальное распределение времени преодоления защиты нарушителем. При гауссовом распределении времени преодоления защиты нарушителем и том же среднем времени преодоления защиты $T_{нап}$ вероятность обеспечения защиты $P_з(t)$ уменьшается с течением времени t медленнее, особенно при больших $\sigma_{нап}/T_{нап}$. Так, при $t = 0{,}2T_{нап}$ в случае экспоненциального распределения $P_з(t) = 0{,}82$, а в случае гауссова распределения ($\sigma_{нап}/T_{нап} = 1$) $P_з(t) = 0{,}94$, при $t = 0{,}5T_{нап}$ $P_з(t) = 0{,}61$ и $0{,}82$ соответственно.

Интервал времени безопасного функционирования информационной системы T_0 при заданной величине $P_{з.доп}$ соответствует $P_з(T_0) = P_{з.доп}$. Найденные таким образом значения интервалов времени T_0 определяют требуемую в текущих условиях функционирования информационной системы периодичность контроля состояния ее ИБ или управления (настройки) КСЗИ. Необходимыми исходными данными для определения величины T_0 являются плотности распределения вероятностей обеспечения и преодоления защиты $w_{защ}(t)$ и $w_{нап}(t)$ в текущих условиях функционирования информационной системы. При этом, как следует из зависимостей, приведенных на рис. 5, вид закона распределения существенным образом влияет на зависимость $P_з(t)$ и величину T_0, обеспечивающую выполнение условия $P_з(t) \geq P_{з.доп}$. При управлении параметрами КСЗИ с фиксированным периодом $w_{защ}(t) = \delta(t - T_{защ})$, и условие $P_з(t) \geq P_{з.доп}$ выполняется при периоде управления (настройки) КСЗИ $T_{защ} = T_0$.

Наиболее жесткие требования к величине $T_{защ}$ будут иметь место в случае экспоненциального распределения времени преодоления защиты нарушителем. Исходя из выражения (8), период управления КСЗИ, обеспечивающий выполнение требования $P_з(t) \geq P_{з.доп}$ при заданной величине $T_{нап}$, составляет

$$T_{защ} = -T_{нап}\ln P_{з.доп} \approx T_{нап}(1 - P_{з.доп}), \qquad (10)$$

где приближенное равенство соответствует линейной аппроксимации логарифмической функции при типовых требованиях к вероятности обеспечения защиты, характеризующихся значениями $P_{з.доп}$, близкими к единице, и $(1 - P_{з.доп}) << 1$. В силу того, что экспоненциальное распределение времени преодоления защиты нарушителем является наименее благоприятным с точки зрения изменения вероятности обеспечения защиты во времени, требования к периодичности управления КСЗИ, определяемые выражением (10), могут рассматриваться как гарантированные.

Заключение

Рассмотренное вероятностное описание изменения защищенности информационной системы во времени может быть использовано в тех случаях, когда условия конфликтного взаимодействия при попытках реализации нарушителем угроз ИБ и их предотвращении с помощью КСЗИ характеризуются плотностями распределения вероятностей обеспечения и преодоления защиты. Такое описание получает широкое распространение при анализе защищенности от угроз НСД систем и сетей передачи информации и вычислительных сетей [10, 11] и является основой реализации упреждающей стратегии управления средствами защиты от НСД с учетом прогнозируемого уровня защищенности. В статье показано, как на основе анализа изменения вероятностных характеристик защищенности информационной системы во времени может быть обоснован период управления (настройки параметров) КСЗИ при поддержании требуемого уровня защищенности, например, смена ключей шифрования для предотвращения НСД к передаваемой информации.

Представленные результаты могут найти применение при обосновании организационных и технических решений по защите критической информации в информационно-управляющих системах различного назначения на этапе их проектирования и в процессе эксплуатации.

Литература

1. **Романец Ю. В., Тимофеев П. А., Шаньгин В. Ф.** Защита информации в компьютерных системах и сетях. — М.: Радио и связь, 2001. — 376 с.
2. **Петренко С. А., Симонов С. В.** Управление информационными рисками: Экономически оправданная безопасность. — М.: Ай-Ти-Пресс, 2004. — 381 с.
3. **Малюк А. А.** Информационная безопасность: концептуальные и методологические основы защиты информации. — М.: Горячая линия-Телеком, 2004. — 280 с.
4. **Ростовцев А. Г., Маховенко Е. Б.** Теоретическая криптография. — СПб.: Профессионал, 2003. — 479 с.
5. **Панасенко С. П.** Алгоритмы шифрования. Специальный справочник. — СПб.: БХВ-Петербург, 2009. — 576 с.
6. **Мальцев Г. Н., Теличко В. В.** Оптимизация состава средств защиты в информационно-управляющей системе с каналами беспроводного доступа на основе графа реализации угроз // Информационно-управляющие системы. 2008. № 4. С. 29–33.
7. **Осипов В. Ю., Носаль И. А.** Обоснование периода пересмотра мероприятий по защите информации //

Информационно-управляющие системы. 2014. № 1. С. 63–69.
8. **Дружинин В. В., Конторов Д. С., Конторов М. Д.** Введение в теорию конфликта. — М.: Радио и связь, 1989. — 288 с.
9. **Владимиров В. И., Лихачев В. П., Шляхин В. М.** Антагонистический конфликт радиоэлектронных систем. Методы и математические модели. — М.: Радиотехника, 2004. — 384 с.
10. **Гаценко О. Ю.** Защита информации. Основы организационного управления. — СПб.: Сентябрь, 2001. — 228 с.
11. **Радько Н. М., Скобелев И. О.** Риск-модели информационно-телекоммуникационных систем при реализации угроз удаленного и непосредственного доступа. — М.: РадиоСофт, 2010. — 232 с.
12. **Ветцель Е. С.** Теория вероятностей. — М.: Высш. шк., 1998. — 576 с.

UDC 681.3.067
doi:10.15217/issn1684-8853.2015.1.50

Probabilistic Characteristics of Information System Security Changes under Unauthorized Access

Maltsev G. N.[a], Dr. Sc., Tech., Professor, georgy_maltsev@mail.ru
Pankratov A. V.[a], PhD, Tech., pankratov-av@rambler.ru
Lesniak D. A.[a], PhD, Tech., Laboratory Chief, denislesnyk@mail.ru
[a]A. F. Mozhaiskii Military Space Academy, 13, Zhdanovskaia St., 197082, Saint-Petersburg, Russian Federation

Purpose: Forecasting information system security in respect to violators' unauthorized access, and determining the periodicity of information security management. **Method:** The emergence and prevention of the information security threats are represented in the form of streams of random events with preset statistical characteristics. The security dynamics is formally described by a probabilistic model of conflict interaction with a violator. **Results:** Under prior uncertainty, it is recommended to postulate exponential distribution of time necessary for a violator to break the protection. A model is developed to ground the best period for managing an information security system and describe how it changes its state with preset distribution functions for the probabilities of providing and overcoming the protection without imposing any restrictions on the type of these distributions. **Practical relevance:** The analysis of changing probabilistic characteristics can help in organizing flexible security management to prevent an unauthorized access taking into account the predicted security level.
Keywords — Information Security, Unauthorized Access, Conflict Interaction, Management of Information Security System.

References

1. 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).
2. Petrenko S. A., Simonov S. V. *Upravlenie informatsionnymi riskami: Ekonomicheski opravdannaia bezopasnost'* [Management of Information Risks: Economically Justified Safety]. Moscow, Ai-Ti-Press Publ., 2004. 381 p. (In Russian).
3. 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).
4. Rostovtsev A. G., Makhovenko E. B. *Teoreticheskaia kriptografiia* [Theoretical Cryptography]. Saint-Petersburg, Professional Publ., 2003. 479 p. (In Russian).
5. Panasenko S. P. *Algoritmy shifrovaniia. Spetsial'nyi spravochnik* [Algorithms of Enciphering. Special Reference Book]. Saint-Petersburg, BKhV-Peterburg Publ., 2009. 576 p. (In Russian).
6. Maltsev G. N., Telichko V. V. Optimization of Information Protection Means in the Informational-Command System with Wireless Channels Access Based on Threats Realization Graph. *Informatsionno-upravliaiushchie sistemy*, 2008, no. 4, pp. 29–33 (In Russian).
7. Osipov V. Yu., Nosal I. A. Substantiation of the Period of Revision of Information Security Measures. *Informatsionno-upravliaiushchie sistemy*, 2014, no. 1, pp. 63–69 (In Russian).
8. Druzhinin V. V., Kontorov D. S., Kontorov M. D. *Vvedenie v teoriiu konflikta* [Introduction to the Theory of Conflict]. Moscow, Radio i sviaz' Publ., 1989. 288 p. (In Russian).
9. Vladimirov V. I., Likhachev V. P., Shliakhin V. M. *Antagonisticheskii konflikt radioelektronnykh sistem. Metody i matematicheskie modeli* [Antagonistichesky Conflict of Radio-Electronic Systems. Methods and Mathematical Models]. Moscow, Radiotekhnika Publ., 2004. 384 p. (In Russian).
10. Gatsenko O. Iu. *Zashchita informatsii. Osnovy organizatsionnogo upravleniia* [Basics of Organizational Management]. Saint-Petersburg, Sentiabr' Publ., 2001. 228 p. (In Russian).
11. 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, Radio-Soft Publ., 2010. 232 p. (In Russian).
12. Vettsel' E. S. *Teoriia veroiatnostei* [Probability Theory]. Moscow, Vysshaia shkola Publ., 1998. 576 p. (In Russian).