УДК 004.056.5(045)

МЕТОДОЛОГИЯ ПОСТРОЕНИЯ И АНАЛИЗА СОСТОЯНИЯ КОМПЛЕКСА ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ С ВЕРОЯТНОСТНОЙ НАДЕЖНОСТЬЮ И УЧЕТОМ ВРЕМЕННЫХ ПОПЫТОК ВЗЛОМА

Борис Журиленко

В данной работе проведено теоретическое обоснование методологии проектирования одиночной (ОТЗИ) и комплексной технической защиты информации (КТЗИ), основанной на количественных оценках качества защиты. Методология базируется на таких обобщающих физических параметрах как финансовые затраты на организацию, построение или модернизацию КТЗИ, эффективности построенной защиты, количества попыток взлома и времени, при котором произошли эти попытки взлома. На базе этих параметров предложена методология построения КТЗИ с количественной оценкой в виде вероятностной надежности качества защиты информации. В результате исследования было получено выражение распределения вероятности взлома и максимума вероятности взлома от попытки и времени этой попытки взлома, предложен метод определения коэффициента эффективности ОТЗИ и КТЗИ. Исследовано влияние эффективности защиты на вероятность взлома ОТЗИ и КТЗИ, показано, каким должен быть предельный коэффициент эффективности защиты, чтобы система была взломана на бесконечности либо не была взломана до нужной попытки и времени этой попытки взлома. Определено, как направление взлома может повлиять на реальный процесс взлома КТЗИ. Установлено, что реальный процесс взлома с выбранными проектируемыми условиями может происходить по линии пересечения двух поверхностей - максимума вероятности взлома и вероятности, определяемой реальной попыткой взлома. Точка взлома определяется пересечением линии направления взлома и линии пересечения двух поверхностей.

Ключевые слова: *комплекс технической защиты информации, коэффициент эффективности защиты, распределение максимума вероятности взлома, попытка взлома, время попытки взлома, линия направления взлома.*

Введение. Развитие методов защиты информации требует методологии построения и анализа состояния этой защиты с количественной ее оценкой во времени. В настоящее время в анализе комплекса технической защиты информации (КТЗИ) или одиночной технической защиты информации (ОТЗИ) используется большое количество исходных параметров, которые только качественно оценивают степень защищенности информации. Построение КТЗИ или ОТЗИ требует выбора таких параметров, которые при наименьшем их количестве наиболее полно отражали свойства защищенности информации. Кроме того желательно иметь количественную оценку технической защиты информации (ТЗИ), например, вероятностную надежность защиты, чтобы можно было адекватно оценивать ее, сравнивать между собой выбранные или проектируемые КТЗИ или ОТЗИ и обеспечить выбор оптимального варианта защиты информации в период разработки, проектирования, модернизации и в процессе выполнения защитных функций. Приемлемым вариантом для оценки ТЗИ может служить вероятностная характеристика взлома. С одной стороны она может характеризоваться количеством попыток взлома и временем, когда эти попытки происходят, а с другой – все затраченные усилия на создание, проектирование, модернизацию и другие работы по защите информации, могут быть оценены финансовыми затратами на организацию этой защиты. Оценить эффективность вложенных финансовых затрат в КТЗИ или ОТЗИ можно с помощью коэффициента эффективности защиты, поскольку не всегда вложенные финансовые затраты в организацию защиты однозначно определяют ее эффективность. Таким образом, вложенное финансирование и эффективность защиты будут определять возможности КТЗИ, а попытки взлома и время этой попытки будут определять параметры возможного взлома. Вероятностная оценка их совместного действия даст количественную оценку КТЗИ.

Используя рассмотренные и перечисленные выше параметры, можно получить количественную вероятностную оценку КТЗИ, которая позволит проектировать, анализировать, оценивать и предсказывать время и попытку взлома защиты на этапе ее эксплуатации.

В работе [2] предложена общая идеология оценки вероятностной надежности КТЗИ и ОТЗИ с использованием выбранных параметров, но без учета финансовых затрат на защиту информации. В [4] рассмотрен метод проектирования ОТЗИ и ее оценки, но также без учета финансовых затрат на защиту информации. В данной работе предлагается методология построения, анализа и количественной оценки защищенности КТЗИ с учетом вложенного финансирования в защиту.

Целью работы является попытка создания методологии проектирования, анализа состояния, оценивания вероятностной надежности, связанной с количественной оценкой защиты инфор-

мации, и предсказания времени и попытки взлома защиты на этапе эксплуатации КТЗИ.

Теоретическое обоснование методологии проектирования, анализа состояния, оценивания вероятностной надежности, связанной с количественной оценкой защиты информации, и предсказания времени и попытки взлома защиты на этапе эксплуатации КТЗИ.

Для достижения поставленной цели работы, необходимо определить вероятность распределения случайных дискретных величин, от которых оно зависит, поскольку каждая конкретная задача может приводить к тому или иному распределению, но получающаяся математическая модель может иметь различные толкования. В данном случае с рассмотренными выше параметрами случайными дискретными величинами являются попытка взлома, время попытки взлома. Выбираемыми являются вложенные финансовые затраты и определяемый – коэффициент эффективности защиты информации.

В основу определения вероятности распределения случайной дискретной величины положим следующие предположения.

Пусть ведутся попытки взлома информации до первого осуществленного взлома, причем вероятность взлома при каждой попытке не зависит от результатов предыдущих попыток и сохраняет постоянное значение вероятности p $(0<p<1)$. Число X попыток взлома будет случайной величиной, возможными значениями которой являются все натуральные числа. Найдем закон распределения ее вероятности. Событие $X=1$ означает взлом с первой попытки, поэтому его вероятность равна p: $P(X=1)=p$. Событие $X=2$ означает взлом со второй попытки и, значит, отсутствие взлома при первой попытки. По правилу умножения вероятностей в силу условия независимости получим

$$P(X=2)=p\cdot q;$$

где $q=1-p$.

Продолжение этих рассуждений приводит к общему закону распределения вероятностей

$$P(X=m)=q^{m-1}\cdot p, \qquad (1)$$

где $m=1, 2, \ldots,$ который можно назвать геометрическим законом распределения вероятностей. Ряд вероятностей (1) представляет собой бесконечно убывающую геометрическую прогрессию со знаменателем $0<q<1$; он сходится, и его сумма равна единице:

$$p+p\cdot q+p\cdot q^2+\ldots+p\cdot q^{m-1}+\ldots=p\cdot\frac{1}{1-q}=1.$$

Найдем математическое ожидание числа X проведенных попыток взлома защиты информации:

$$MX=\sum_{i=1}^{\infty}x_i\cdot p_i=1\cdot p+2\cdot p\cdot q+$$
$$+3\cdot p\cdot q^2+\ldots+m\cdot p\cdot q^{m-1}+\ldots=$$
$$=(1-q)+2\cdot(q-q^2)+3\cdot(q^2-q^3)+$$
$$+\ldots+m\cdot(q^{m-1}-q^m)+\ldots$$

Так как частичная сумма этого ряда равна

$$1+q+q^2+q^3+\ldots+q^m-m\cdot q^m$$

и так как из $0<q<1$ следует, что $m\cdot q^m\to 0$ при $m\to\infty$, то сумма выписанного выше ряда для MX равна

$$MX=\frac{1}{1-q}=\frac{1}{p}.$$

Итак, математическое ожидание числа попыток взлома есть число, обратное вероятности попыток взлома.

Выражение распределения вероятности (1) позволяет объединить вероятность любого процесса взлома или защиты с количеством попыток взломов, поэтому все выбранные параметры взлома ТЗИ можно объединить в одном математическом выражении. Следует заметить, что выражение (1) позволяет использовать не только выбранные в данной работе параметры взлома, но и другие параметры, которые зависят от количества попыток взлома или определяются ими.

На основании выражения (1) в работе [1] было получено распределение вероятности взлома в зависимости от попыток взлома и финансовых затрат на создание ОТЗИ

$$P_{взлі}(x_i)=(p_{хз})^{m_c-1}\cdot p_x=\left(\frac{x_i}{H_i+x_i}\right)^{m_c-1}\cdot\frac{H_i}{H_i+x_i}, \qquad (2)$$

где x_i – финансовые затраты на создание ОТЗИ; H_i – первоначальные финансовые потери при взломе и отсутствии защиты, m_c – попытка взлома.

Исследования (2) на экстремум показали, что максимум вероятности взлома $P_{взлі}(x_i)$ от вложенного финансирования x_i для i-ой защиты на m_c – той попытке, будет определяться выражением

$$x_i=(m_c-1)\cdot H_i \qquad (3)$$

или для приведенных значений финансовых затрат X_i к финансовым потерям при отсутствии защиты H_i

$$X_i = \frac{x_i}{H_i} = (m_c\text{-}1) \ . \qquad (4)$$

Учитывая (3), (4), выражение (2) для максимумов вероятностей взлома защиты от вложенного финансирования можно представить в виде

$$P_{взлі}(X_i) = \frac{X_i^{X_i}}{(1+X_i)^{1+X_i}} . \qquad (5)$$

В случае, если для защиты одного объекта используются две одинаковые по стоимости защитные системы, то максимум вероятности их взлома будет определяться выражением

$$P^2_{взлі}(X_i) = \{\frac{X_i^{X_i}}{(1+X_i)^{1+X_i}}\}^2 . \qquad (5а)$$

На рис. 1 представлены результаты расчета по формуле (2) вероятности события проникновения через защиту $P_{взлі(xi)}$=$P2_{взл}$(X) от попытки взлома m_c=*1* и вложенного финансирования в защиту x_i, где X=X_i из (4). И соответственно $P_{взлі(xi)}$=$P3_{взл}$(X) при попытках взлома m_c=*2*, $P_{взлі(xi)}$=$P4_{взл}$(X) при m_c=*3*, $P_{взлі(xi)}$=$P5_{взл}$(X) при m_c=*4*. Эти вероятности $P2_{взл}$(X), $P3_{взл}$(X), $P4_{взл}$(X), $P5_{взл}$(X) представлены тонкими сплошной, пунктирной, штрихпунктирной и точечной линиями соответственно. Толстая сплошная $P_{взл}$(X) и толстая прерывистая P^2*взл*(X) линии проходит через максимумы распределения вероятностей попыток взлома и строятся по формулам (5) и (5а) соответственно.

Анализ выражений (2), (5), (5а) и графики рисунка 1 показали, что ТЗИ обеспечивается при бесконечном финансировании защиты, а значение вероятности $P_{взлі(Xi)}$ стремится к нулю [1].

$$\lim_{X_i \to \infty} P_{взлі}(X_i) = \lim_{X_i \to \infty} \frac{X_i^{X_i}}{(1+X_i)^{1+X_i}} = 0 .$$

В этом случае попытки взлома m_c, согласно (4), стремятся к бесконечности. На практике бесконечные затраты на ТЗИ не реальны. Однако более оптимальные затраты на организацию ТЗИ можно определить, используя величину рисков потерь информации при затратах на ТЗИ, которые соответствуют следующим выражениям:

$$R_{общ}(x_i) = P_{взлі}(X_i) \cdot (H_i + x_i) \qquad (6)$$

– соответствует величине рисков полных финансовых потерь в случае взлома защиты;

$$R^*_{общ}(m_c) = R^*_{общ}(X_i) = \frac{R_{общ}(x_i)}{H_i} = P_{взлі}(X_i) \cdot (1+X_i) \qquad (6а)$$

– соответствует величине приведенных рисков полных финансовых потерь в случае взлома защиты. И

$$R_{вл}(x_i) = P_{взлі}(X_i) \cdot x_i \qquad (7)$$

– соответствует величине рисков финансовых потерь, вложенных в построение ТЗИ;

$$R^*_{вл}(m_c) = R^*_{вл}(X_i) = \frac{R_{вл}(x_i)}{H_i} = P_{взлі}(X_i) \cdot X_i \qquad (7а)$$

– соответствует величине приведенных рисков финансовых потерь, вложенных в построение ТЗИ. Для двухуровневой защиты, имеющей одинаковую вероятность взлома одиночных защит и одинаковые финансовые затраты и обеспечивающих защиту одного и того же объекта, величина общих рисков будет

$$R^{*2}_{общ}(m_c) = R^{*2}_{общ}(X_i) = \frac{R^2_{общ}(x_i)}{H_i} = P^2_{взлі}(X_i) \cdot (1+X_i) \qquad (8)$$

и соответственно вложенных

$$R^{*2}_{вл}(m_c) = R^{*2}_{вл}(X_i) = \frac{R^2_{вл}(x_i)}{H_i} = P^2_{взлі}(X_i) \cdot X_i \ . \qquad (8а)$$

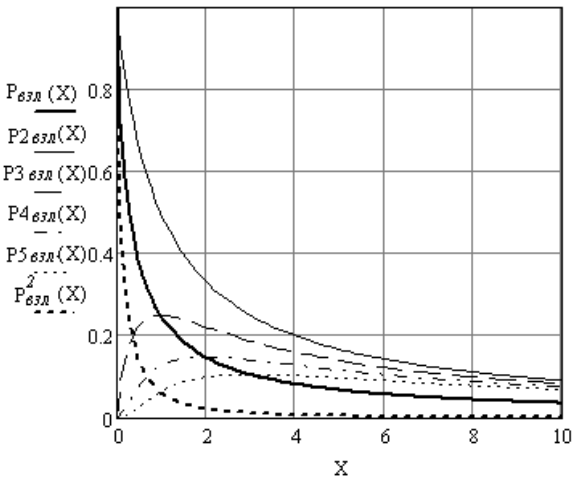

Рис. 1. Расчет вероятности события проникновения через защиту в зависимости от вложенного финансирования и попыток взлома: $P2_{взл}$(X) – при m = *1*; $P3_{взл}$(X) – при m = *2*; $P4_{взл}$(X) – при m = *3*; $P5_{взл}$(X) – при m = *4*; $P_{взл}$(X) - кривая, определяющая максимальные значения вероятности проникновения через одиночную защиту; P^2*взл*(X) - кривая, определяющая максимальные значения вероятности проникновения через двухуровневую защиту

Результаты расчета величины приведенных рисков потерь представлены на рис. 2. Толстая сплошная линия $R^*_{общ}(X_i)$=R0(X) соответствует величине приведенных рисков полных финансовых потерь в случае взлома защиты; толстая пунктирная линия $R^*_{вл}(X_i)$=R1(X) соответствует величине рисков финансовых потерь, вложенных в построение ТЗИ. Для двухуровневой системы защиты тонкая сплошная соответствует расчетам выражения (8), а точки – выражению (8а).

Определим пределы, к которым стремятся величины приведенных рисков полных финансовых потерь (6а) и величины приведенных рисков вложенных финансовых потерь (7а), при стремлении их попыток взлома m_c к бесконечности. Для этого вместо X_i в выражения (6а) и (7а) подставим условие экстремума (4). Получим

$$\lim_{m_c \to \infty} R^*_{общ}(m_c) = \lim_{m_c \to \infty} \frac{(m_c - 1)^{m_c - 1} \cdot m_c}{m_c^{m_c}} = \frac{1}{e} \approx 0{,}37, \quad (9)$$

$$\lim_{m_c \to \infty} R^*_{вл}(m_c) = \lim_{m_c \to \infty} \frac{(m_c - 1)^{m_c - 1} \cdot (m_c - 1)}{m_c^{m_c}} = \frac{1}{e} \approx 0{,}37. \quad (10)$$

Отсюда видно, что величины приведенных рисков полных потерь и потерь финансирования, вложенных в построение одной ТЗИ, при бесконечных попытках взлома m_c и, следовательно, бесконечного финансирования имеют предельное значение величины рисков, равное 1/e ≈ 0,37 (рис. 2 прямая тонкая пунктирная линия). В выражениях (6) и (7) величины рисков будут равны ≈ 0,37H_i, то есть предельные величины рисков полных потерь и предельные величины рисков потерь вложенного финансирования при бесконечных попытках взлома и бесконечном финансировании для одной ТЗИ будут ≈ 0,37H_i. Стремление обоих рисков к одному общему пределу для одиночной ТЗИ говорит о том, что после финансовых вложений порядка X≥3÷4 или защиты от попыток взлома с m_c≥4÷5 дальнейшие финансовые затраты идут в основном не на уменьшение общих рисков финансовых потерь, а на поддержание рисков или защиты собственно вложенного финансирования x_i.

Рассмотрим случай использования двух защит, имеющих одинаковую вероятность взлома и одинаковые финансовые затраты и обеспечивающие один и тот же объект защиты. Риски финансовых потерь этих защит будут определяться выражениями (8) и (8а). Предельные значения рисков потерь будут

$$\lim_{m_c \to \infty} R^{*2}_{общ}(m_c) = \lim_{m_c \to \infty} [\frac{(m_c - 1)^{m_c - 1}}{m_c^{m_c}}]^2 \cdot m_c = \lim_{m_c \to \infty} \frac{1}{e^2 \cdot m_c} = 0 \quad (11)$$

и

$$\lim_{m_c \to \infty} R^{*2}_{вл}(m_c) = \lim_{m_c \to \infty} [\frac{(m_c - 1)^{m_c - 1}}{m_c^{m_c}}]^2 \cdot (m_c - 1) = \lim_{m_c \to \infty} \frac{m_c - 1}{e^2 \cdot m_c} = 0. \quad (12)$$

Из графиков рис. 2 и проведенных вычислений (9), (10), (11), (12) можно сделать вывод, что одиночная защита не сможет обеспечить требуемый уровень защиты даже при бесконечных финансовых затратах на защиту. Необходимый уровень защиты сможет обеспечить только многоуровневая защита, начиная с двухуровневой, так как только начиная с двухуровневой защиты бесконечные финансовые затраты обеспечивают риски общих финансовых потерь равные нулю.

Анализируя графики рис. 1 и рис. 2 можно сделать еще одно важное заключение. Если строить двухуровневую защиту по частям, то при затратах на одну X=0,3 (на две = 0,6) приведенные риски общих финансовых потерь будут равны 0,37, что для одиночной защиты может быть достигнуто только при бесконечных финансовых затратах. Следовательно, используя двухуровневую защиту по частям, можно значительно сэкономить при создании КТЗИ и понизить вероятность его взлома. При рассмотренных равных финансовых затратах на защиту объекта отношение максимумов вероятностей взломов одиночной защиты и двухуровневой будет равно 1,4.

В работе [4] на основании выражения (1) было получено распределение максимума вероятности взлома в зависимости от попытки взлома и времени взлома этой попытки для ОТЗИ

$$P_{взлі}(m,t) = (\frac{f_i(m,t)}{f_i(m,t)+t})^{\frac{f_i(m,t)}{t}} \cdot (\frac{t}{f_i(m,t)+t}), \quad (13)$$

и $$f_i(m,t)=[t_1+\frac{t_2-t_1}{m_2-m_1}\cdot(m-m_1)]\cdot(m-1)\,, \quad (14)$$

где $f_i(m,t)$ – характеристическая функция, присущая данной системе защиты, определяющая ее защитные свойства и направление взлома, m_1, t_1, m_2, t_2 – могут быть выбранные или конкретные попытки взлома и время этих попыток взлома соответственно. Эти параметры либо выбираются при проектировании или модернизации КТЗИ, либо определяются взломом в случае анализа процесса взлома или анализа состояния КТЗИ; m, t – текущие значение попытки и времени взлома. В случае отсутствия взлома по его конкретным параметрам попыток можно определить направление процесса взлома и провести его анализ [5].

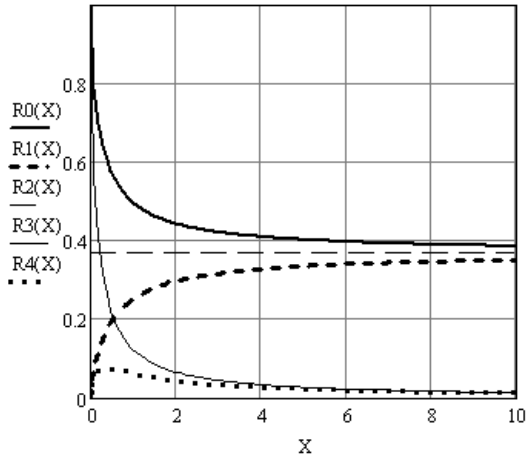

Рис. 2. Расчет величины рисков потерь: $R^*_{общ}(X_i)$=R0(X) соответствует величине приведенных рисков полных финансовых потерь в случае взлома защиты; $R^*_{вл}(X_i)$=R1(X) соответствует величине рисков финансовых потерь, вложенных в построение ТЗИ; $R^{*2}_{общ}(X_i)$=R3(X) и $R^{*2}_{вл}(X_i)$=R4(X) – соответственно величины рисков для двухуровневой системы защиты; R2(X) – предельное значение рисков потерь

Поскольку вероятности $P_{взлі}(X_i)$ и $P_{взлі}(m,\ t)$ независимы друг от друга и определяют одну и ту же систему ТЗИ, то вероятность взлома ОТЗИ будет определяться произведением этих вероятностей. Вероятность взлома для КТЗИ, согласно работе [4], может быть представлена выражением

$$P_{взлКТЗИ}=\prod_{i=1}^{n}[P_{взлі}(X_i)\cdot P_{взлі}(m,t)]^{\alpha_i}\,, \quad (15)$$

где α_i – коэффициент эффективности защиты; n – количество защит, i – индекс параметра текущей защиты.

Рассмотрим влияние эффективности защиты на вероятность взлома ТЗИ.

Вероятность взлома любой защиты информации (ОТЗИ или КТЗИ) на m – той попытке будет иметь вид

$$P(m)=\frac{1}{m}\,. \quad (16)$$

С другой стороны вероятность взлома ОТЗИ будет определяться вероятностью взлома $P_{взлКТЗИ}$ с $i=n=1$, то есть

$$P_{взлКТЗИ}=P(m)\,. \quad (17)$$

Как и в работе [4], в результате решения уравнения (17) относительно α_i с учетом финансовых вложений X_i в ОТЗИ, можно получить выражение для коэффициента эффективности ОТЗИ

$$\alpha=\frac{\ln[P(m)]}{\ln[P_{взлі}(m,t)]+\ln[P_{взлі}(X_i)]}\,, \quad (18)$$

где $P_{взлі}(m,\ t)$ и время t необходимо выразить через попытки взлома m. В выражении (13) время $t=t(m)$, согласно работе [4], может быть выражено в следующем виде

$$t(m)=\frac{\sqrt{A^2+\frac{4}{\varpi}\cdot f(m,t)}-A}{2}\,,\ A=t_1+\frac{m_1-1}{\varpi}\,,$$

$$\varpi=\frac{m_2-m_1}{t_2-t_1}\,.$$

Более подробные исследования коэффициента эффективности и методы его определение будут опубликованы в последующих работах.

На рис. 3 представлена зависимость коэффициента эффективности ОТЗИ от вложенного в защиту финансирования и от попытки, на которой произошел ее взлом. Сплошные линии с точками представляют расчеты: 1 обозначены расчеты, полученные при $X=0$; 2, 3 и 4 получены при $X=1$, $X=2$ и $X=3$ соответственно. Сплошная линия 5 представляет расчет коэффициента эффективности для двух одинаковых ОТЗИ с приведенными финансовыми вложениями при $X=1$.

Сплошными линиями и точками обозначены расчеты при направлениях попыток взлома $\omega=\omega1=2$ и $\omega=\omega2=4,5$ соответственно в координатах m и t. Из рисунка видно, что при различных направлениях взлома коэффициент эффективности ТЗИ зависит только от финансовых вложений в защиту и не зависит от направления попыток взлома. Из рисунка также видно, что если взлом произошел на первой попытке, то эффективность ОТЗИ будет равна нулю. При одной и той же попытке взлома эффективность взлома будет тем меньше, чем больше вложено

финансирования в защиту информации. И если же эффективность ОТЗИ остается постоянной, то взлом наступит при большей попытке, то есть при больших финансовых вкладах в ТЗИ получается большая эффективность защиты информации. Наиболее эффективная и экономная защита получается, когда используется многоуровневый КТЗИ, например, с двумя равными по эффективности защитами (это линия 5), но с меньшими финансовыми затратами на каждую из них. Из зависимости 5 рис. 3 видно, что использование многоуровневой защиты увеличивает попытку возможного взлома защиты информации даже при небольших коэффициентах эффективности защиты α_i. С увеличением коэффициента эффективности защиты информации существенно увеличивается возможная попытка взлома информации.

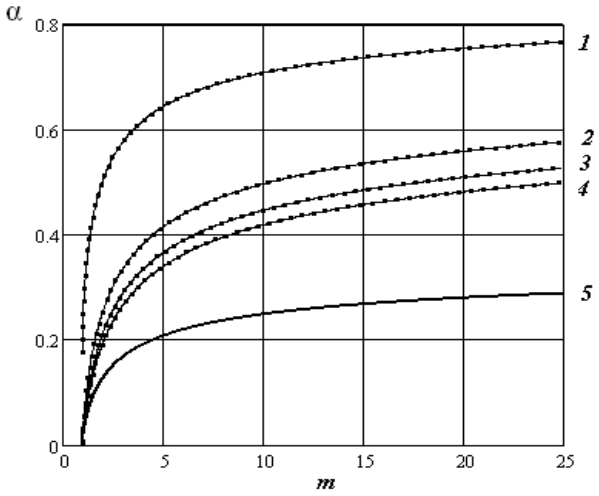

Рис. 3. Представлена зависимость коэффициента эффективности ОТЗИ от вложенного в защиту финансирования и от попытки, на которой произошел ее взлом. Сплошными линиями обозначены расчеты при направлениях попыток взлома $\omega=\omega 1=2$, и точками - $\omega=\omega 2=4{,}5$. 1 обозначены расчеты, полученные при $X=0$; 2, 3 и 4 получены при $X=1$, $X=2$ и $X=3$ соответственно. 5 – расчет двухуровневой защиты из двух одинаковых ОТЗИ при $X=1$

Определим, какая должна быть эффективность коэффициента защиты ОТЗИ, чтобы взлом произошел на бесконечной попытке. Для этого в выражении (14) проведем замены $m_2=m$ так как взлом должен произойти на бесконечной попытке, когда $m \to \infty$, и t_2 на t, где t время бесконечной попытки взлома. В результате таких замен получим

$$f_i(m,t) = t \cdot (m-1). \qquad (19)$$

Учитывая выражение (19) для $f_i(m,t)$, подставим его в выражение (13), а затем в (15) и (16). В соответствие с формулой (17) для ОТЗИ получим

$$[P_{взлі}(X_i) \cdot (\frac{m-1}{m})^{m-1} \cdot (\frac{1}{m})]^{\alpha_i} = \frac{1}{m}. \qquad (20)$$

Из выражения (20) можно определить эффективность α_i единичной защиты информации от попытки взлома на бесконечности и вложенного в защиту финансирования. Для этого возьмем логарифм выражения (20) и определим α_i. Получим

$$\alpha_i = \frac{\ln(m)}{m \cdot \ln(m) - (m-1) \cdot \ln(m-1) - \ln[P_{взлі}(X_i)]}. \qquad (21)$$

Рассмотрим предел выражения (21) при $m \to \infty$. Воспользовавшись правилом Лопиталя продифференцировав дважды числитель и знаменатель, получим

$$\lim_{m \to \infty} (\alpha_i) = \lim_{m \to \infty} [\frac{-\frac{1}{m^2}}{-\frac{1}{m \cdot (m-1)}}] = 1.$$

В результате проведенного анализа можно сделать следующее заключение. Защита информации обеспечивается, если эффективность коэффициента взлома ОТЗИ будет больше или равна единице. В случае если она меньше единицы, то возможен взлом ТЗИ, причем, чем меньше эффективность, тем на меньшей попытке произойдет взлом.

Важным выводом проведенного выше анализа является применение многоуровневой защиты, обеспечивающей намного большую эффективность защиты при малых затратах на каждую, чем одноуровневая защита со значительными финансовыми вкладами в нее. В этом случае общая эффективность взлома будет равна произведению $\alpha_i \cdot n$, что увеличивает эффективность защиты.

Выражение (15) дает поверхность максимумов вероятностей взлома в координатах попыток взлома и времени этих попыток взлома. Кроме того, эта поверхность зависит от вложенного в защиту финансирования и эффективности данной защиты. Результаты расчета этой поверхности представлены на рис. 4.

Для расчетов поверхности максимумов вероятностей взлома (серая поверхность) использовались следующие исходные данные: для рис. 4а использовались $m_1=1$, $t_1=0$, $m_2=7$, $t_2=3$ $X=10$, $\alpha_i=0{,}301$, $n=1$; для рис. 4б – $m_1=1$, $t_1=0$, $m_2=7$, $t_2=3$ $X=0{,}1$, $\alpha_i=0{,}301$, $n=1$; для рис. 4в – $m_1=1$, $t_1=0$, $m_2=7$, $t_2=3$ $X=0{,}1$, $\alpha_i=0{,}301$, $n=3$. При про-

ектировании этих поверхностей предполагалось направление взлома, которое будет проходить по линии 1. Направление взлома автоматически получалось при выборе исходных данных. Взлом ТЗИ произойдет в точке пересечения линии направления взлома и линии пересечения поверхностей взлома (светлой, рассчитанной по формуле (16) и серой поверхностей). В случае если реальный взлом пошел в другом направлении, например, $m_1=1$, $t_1=0$, $m_2=7$, $t_2=6$, (линия 2 рис. 4), то и реальный взлом произойдет в другой точке отличной от планируемой и при других значениях попытки взлома m и времени взлома t. Этот результат будет очень полезен при анализе состояния работающего КТЗИ.

Анализируя представленные на рис. 4 результаты, можно сделать следующие заключения. Из анализа рис. 4а и рис. 4в можно сказать, что большой вклад финансовых затрат в ОТЗИ менее эффективен, чем малые финансовые вложения в многоуровневые КТЗИ. Следующее заключение – большое количество попыток взлома в течение малого времени или малое количество попыток взлома в течение большого времени не приведут к быстрому взлому ОТЗИ или КТЗИ. Наиболее опасна и эффективна атака по взлому ТЗИ, когда она проводится систематически и целенаправленно с оценкой состояния ТЗИ.

Если бы эффективность защиты была равна нулю, то поверхность взлома $P_{взлКТЗИ}$ (серая поверхность) представляла бы плоскость на уровне единицы вероятности, и взлом происходил бы с первой попытки. В реальных условиях это не всегда так.

Результаты, представленные на рис. 4б, указывают на то, что даже малые финансовые затраты способствуют защите ТЗИ. Эти малые затраты могут возникать даже без создания специальной ТЗИ за счет реализации без сбойного функционирования самого объекта.

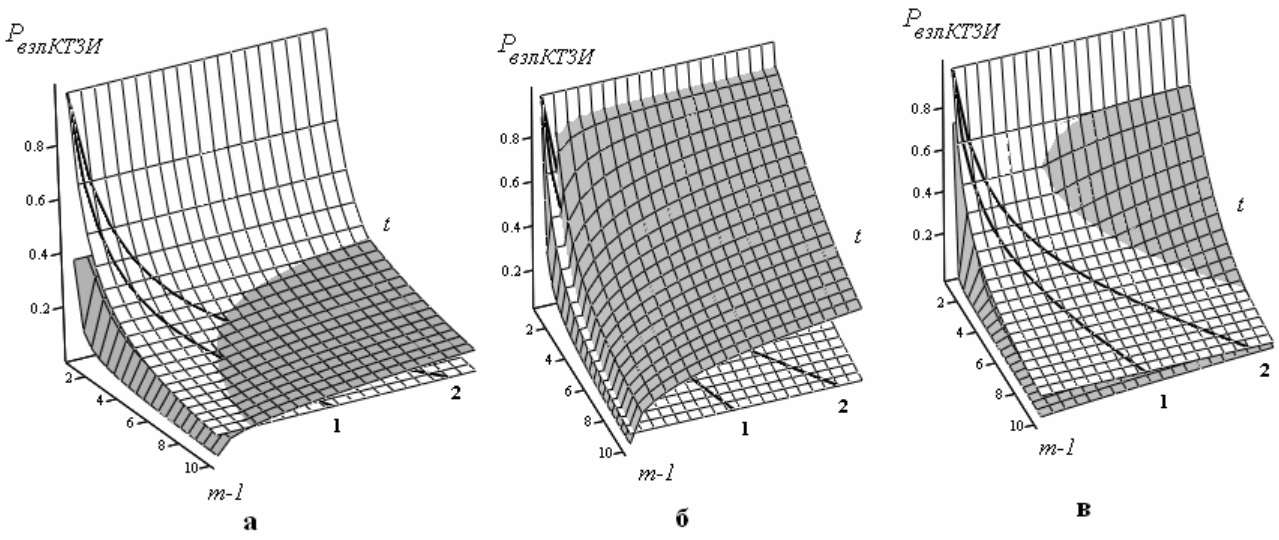

Рис. 4. Представлены расчеты поверхностей максимума вероятностей взлома (серая поверхность), вероятности взлома защиты (белая поверхность). Линия 1 определяет направление проектируемого взлома, линия 2 – возможного реального взлома. Для расчетов **а** – использовались параметры $m_1=1$, $t_1=0$, $m_2=7$, $t_2=3$ $X=10$, $\alpha_i=0{,}301$, $n=1$; **б** - $m_1=1$, $t_1=0$, $m_2=7$, $t_2=3$ $X=0{,}1$, $\alpha_i=0{,}301$, $n=1$; **в** - $m_1=1$, $t_1=0$, $m_2=7$, $t_2=3$ $X=0{,}1$, $\alpha_i=0{,}301$, $n=3$

На рис. 4б показаны два направления взлома, которые определяются случайным процессом, одно направление дает взлом на второй попытке, второе на третьей, а в некоторых случаях на других направлениях взлома и при других попытках. На рис. 4 точка взлома $m_{взл}=m-1$. Отсюда попытка на которой произошел взлом будет $m=m_{взл}+1$. Таким образом, даже малая объектная защищенность и случайность направления взлома в реальных условиях не всегда позволяют осуществить взлом сразу с первой попытки.

Методология построения ТЗИ.

Проведенные исследования позволяют предложить методологию построения КТЗИ.

На первом этапе, в соответствие с техническими требованиями, задаются исходные параметры КТЗИ $m_1=1$, $t_1=0$, и проектируемые, которые требуются по взлому m_2, и времени взлома t_2. Из исходных и проектируемых данных по формуле (14) находится характеристическая функция $f_i(m,t)$ и проектируемое направление взлома.

Затем задается количество ОТЗИ n и финансовые затраты X_i на каждую из одиночных защит.

На третьем этапе определяется коэффициент эффективности α_i каждого ОТЗИ по формуле (21), если финансовые затраты на защиту каждого ОТЗИ отличаются. Если не отличаются, тогда α_i определяется один раз. В случае применения n одинаковых по эффективности защит общая эффективность будет определяться произведением α_i и n.

С учетом формул (13), (14) по формулам (15), (16) строятся поверхности максимума вероятности взлома и вероятности взлома, по пересечению которых находится линия взлома защиты проектируемого КТЗИ. При необходимости строится линия направления взлома. При правильном построении проектируемого КТЗИ точка проектируемого взлома совпадет с точкой пересечения линий.

Графическое построение КТЗИ позволяет наглядно представить процесс взлома и защиты, а также при необходимости провести либо сравнительный анализ различных типов проектируемых КТЗИ, либо вести анализ комплекса защиты в процессе его работы.

Выводы. В данной работе проведено теоретическое обоснование методологии проектирования ОТЗИ и КТЗИ, основанной на количественных оценках качества защиты. Методология базируется на таких обобщающих физических параметрах как финансовые затраты на организацию, построение или модернизацию КТЗИ, эффективности построенной защиты, количества попыток взлома и времени, при котором произошли эти попытки взлома. На базе этих параметров предложена методология построения КТЗИ с количественной оценкой в виде вероятностной надежности качества защиты информации.

В результате исследования было получено выражение распределения вероятности взлома и максимума вероятности взлома от попытки и времени этой попытки взлома, предложен метод определения коэффициента эффективности ОТЗИ и КТЗИ. Исследовано влияние эффективности защиты на вероятность взлома ОТЗИ и КТЗИ; показано, каким должен быть предельный коэффициент эффективности защиты, чтобы система была взломана на бесконечности либо не была взломана до нужной попытки и времени этой попытки взлома. Определено, как направление взлома может повлиять на реальный процесс взлома КТЗИ. Установлено, что реальный процесс взлома с выбранными проектируемыми условиями может происходить по линии пересечения двух поверхностей - максимума вероятности взлома и вероятности, определяемой реальной попыткой взлома. Точка взлома определяется пересечением линии направления взлома и линии пересечения двух поверхностей.

ЛИТЕРАТУРА

[1]. Журиленко Б.Є. Оптимальные финансовые затраты и основные критерии построения или модернизации комплекса технической защиты информации / Журиленко Б.Є., Николаева Н.К., Пелих Н.С. // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – Київ, КПІ НДЦ «Тезіс», 2011. – Випуск 1 (22). – С.33-43.

[2]. Журиленко Б.Е. Математическая модель вероятностной надежности комплекса технической защиты информации / Б.Е. Журиленко // Безпека інформації: науково – практичний журнал – К.: НАУ, 2012. №2 (18). – С. 61-65.

[3]. Журиленко Б.Е. Определение вероятностной надежности единичной технической защиты информации из реальных попыток взлома / Б.Е. Журиленко // Безпека інформації. – К.: НАУ, 2013. №1 (19). – С.34-39.

[4]. Журиленко Б.Е. Метод проектирования единичной системы технической защиты информации с вероятностной надежностью и заданными параметрами взлома / Б.Е. Журиленко // Безпека інформації.– 2014. – №1(20). – С. 36-42.

[5]. Журиленко Б.Є. Определение направления взлома технической защиты информации по его параметрам / Журиленко Б.Є., Николаева Н.К.//Інформаційні управляючі системи та технології: міжнар. наук.-практ. конф., 23-25 вересня 2014 р.: тези доп. – С. 168-171.

REFERENCES

[1]. Zhurylenko B.E. Optimal financial costs and main criteria of construction or modernization of technical information security complex. Zhurilenko B.E., Nykolaeva N.K., Pelykh N.S.. Pravove, normatyvne ta metrologichne zabezpechennya systemy zakhystu informatsiyi v Ukrayini, №1(22), 2011, P.33-43.

[2]. Zhurylenko B.E. Mathematical model of reliable reliability for complex of technical information security. Zhurylenko B.E. Ukrainian Scientific Journal of Information Security, №2 (18), 2012, P. 61-65.

[3]. Zhurylenko B.E. Definition of reliable reliability of single technical information security from the real attack attempts. Zhurylenko B.E. Ukrainian Scientific Journal of Information Security, №1 (19), 2013, P. 34-39.

[4]. Zhurylenko B.E. Method of single technical information security system designing with probable reliability and given parameters of breaking.

Zhurylenko B.E. Ukrainian Scientific Journal of Information Security, №1 (20), 2014, P. 36-42.

[5]. Zhurylenko B.E. Direction finding of breaking of technical priv on his parameters. Zhurilenko B.E., Nykolaeva N.K. Materials of the III international scientific-practical conference "Information Control Systems and Technologies". Sept. 23-25, 2014 p.: report thesis, Odessa: ICST, ODESSA, 2014, P. 168-171.

МЕТОДОЛОГІЯ ПОБУДОВИ І АНАЛІЗУ СТАНУ КОМПЛЕКСУ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ З ІМОВІРНІСНОЮ НАДІЙНІСТЮ І ОБЛІКОМ ТИМЧАСОВИХ СПРОБ ЗЛОМУ

У цій роботі проведено теоретичне обґрунтування методології проектування поодинокого (ПТЗІ) і комплексного технічного захисту інформації (КТЗІ), заснованої на кількісних оцінках якості захисту. Методологія базується на таких узагальнених фізичних параметрах як фінансові витрати на організацію, побудову або модернізацію КТЗІ, ефективності побудованого захисту, кількості спроб злому і часу, при якому сталися ці спроби злому. На базі цих параметрів запропонована методологія побудови КТЗІ з кількісною оцінкою у вигляді імовірнісної надійності якості захисту інформації. В результаті дослідження було отримано вираз розподілу вірогідності злому і максимуму вірогідності злому від спроби і часу цієї спроби злому, запропонований метод визначення коефіцієнта ефективності ПТЗІ і КТЗІ. Досліджений вплив ефективності захисту на вірогідність злому ПТЗІ і КТЗІ, показано, яким має бути граничний коефіцієнт ефективності захисту, щоб система була зламана на нескінченності або не була зламана до потрібної спроби і часу цієї спроби злому. Визначено як напрям злому може вплинути на реальний процес злому КТЗІ. Встановлено, що реальний процес злому з обраними проектованими умовами може відбуватися по лінії перетину двох поверхонь - максимуму вірогідності злому і вірогідності, визначуваною реальною спробою злому. Точка злому визначається перетином лінії напряму злому і лінії перетину двох поверхонь.

Ключові слова: комплекс технічного захисту інформації, коефіцієнт ефективності захисту, розподіл максимуму вірогідності злому, спроба злому, час спроби злому, лінія напряму злому.

CONSTRUCTION AND ANALYSIS METHODOLOGY OF COMPLEX TECHNICAL INFORMATION SECURITY WITH PROBABILISTIC RELIABILITY AND COUNTING OF TEMPORAL BREAKING ATTEMPTS

In this work the theoretical substantiation of single design (SDM) and complex technical information security (CTIS) methodology, based on quantitative assessments of the security quality, are made. The methodology is based on such generalized physical parameters as financial costs for organization, bulding and modernization technical information security complex, efficiency built protection, the number of hacking attempts and the time at which these occurred hacking attempt. On the basis of these parameters proposed technical information security complex methodology with quantitative assessment in the form of probabilistic reliability data protection quality. As a result was received expression of the probability distribution of maximum hacking probability and of attempts and the time of the hacking attempt, the proposed determining the coefficient method efficiency and SDM and CTIS. The influence of effective protection on the probability hacking SDM and CTIS, shown how to be a limiting factor effective protection system to be broken at infinity or was broken to the desired time of attempts and hacking attempt. Been determined how hacking direction can influence the real process hacking CTIS. Established that the actual hacking process with the selected conditions can be projected along the line intersection of two surfaces - the maximum probability hacking and probability, determined actual hacking attempt. Break point determined by the intersection direction lines hacking and the intersection of two surfaces.

Index terms: complex technical information security, security effectiveness ratio, distribution of maximum hacking probability, hacking attempt, hacking attempt time, hacking direction line.

Журиленко Борис Евгеньевич, кандидат физико-математических наук, доцент кафедры средств защиты информации Национального авиационного университета.
E-mail: zhurilenko@mail.ru.

Журиленко Борис Євгенович, кандидат фізико-математичних наук, доцент кафедри засобів захисту інформації Національного авіаційного університету.

Zhurilenko Boris, PhD, Associate Professor of the Academic Department of information security tools National Aviation University.