

ЗАХИСТ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ОБЛАДНАННЯ / SOFTWARE & HARDWARE ARCHITECTURE SECURITY

ОПРЕДЕЛЕНИЕ КОЭФФИЦИЕНТА ЭФФЕКТИВНОСТИ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ ПО ЕЕ ПАРАМЕТРАМ

Борис Журиленко, Надежда Николаева

Национальный авиационный университет, Украина



ЖУРИЛЕНКО Борис Евгеньевич, к.ф.-м.н.

Год и место рождения: 1946 год, г. Чугуев Харьковской области, Украина.
Образование: Киевский государственный университет им. Т.Г. Шевченко, 1974 год.
Должность: доцент кафедры автоматизации и энергоменеджмента с 2014 года.
Научный интерес: методы съема и методы технической защиты информации.
Публикации: более 90 научных статей и патентов на изобретения.
E-mail: zhurilenko@mail.ru



НИКОЛАЕВА Надежда Константиновна

Год и место рождения: 1954 год, г. Киев, Украина.
Образование: Киевский институт инженеров гражданской авиации (НАУ с 2000 г.), 1980 год.
Должность: ведущий инженер кафедры телекоммуникационных систем с 2015 года.
Научный интерес: методы съема и методы технической защиты информации.
Публикации: 15 научных статей, тезисов и патентов на изобретения.
E-mail: nnikolaeva17@yandex.ru

Аннотация. В данной работе рассмотрены способы определения коэффициента эффективности технической защиты информации при проектировании и анализе функционирующей технической защиты. Сложность определения коэффициента эффективности защиты заключается в отсутствии всех необходимых исходных параметров. Поэтому рассматривались три основных возможных варианта. Первый, когда известны финансовые затраты, вложенные в защиту, попытка и время этой попытки взлома. Второй вариант – это, когда известны финансовые затраты на защиту и вероятность взлома технической защиты на первой попытке, которая известна. Вероятность взлома ТЗИ для начальных условий может вычисляться с помощью существующих других различных способов и методов оценки качества технической защиты информации. Третий вариант – наиболее общий, когда известны любые две попытки, время этих попыток взлома и вероятности взлома этих попыток. В результате исследований получены формулы, позволяющие по этим известным параметрам строить поверхности максимумов вероятностей взлома технической защиты информации, по которым можно определить параметры возможного взлома технической защиты информации для любого направления процесса взлома.

Ключевые слова: коэффициент эффективности защиты, техническая защита информации, приведенная вероятность максимумов взлома защиты, попытка взлома, время попытки взлома, комплекс технической защиты информации.

Введение

В настоящее время существуют различные способы и методы оценки качества технической

защиты информации (ТЗИ). Основная масса этих методов и способов дает качественную оценку ТЗИ, не учитывающих ни конкретных текущих попыток взлома, ни времени этих попыток взлома. Но есть

ряд работ [1,2], основанные на вероятностной надежности ТЗИ, которые дают количественную оценку защищенности информации и учитывают попытки и время взлома. В этих работах важным параметром, отвечающим за эффективность технической защиты информации с вероятностной надежностью, является коэффициент эффективности защиты (КЭЗ). Показано, что эффективность технической защиты зависит от величины значения КЭЗ. Если КЭЗ меньше единицы, то ТЗИ может быть взломана на конечной попытке меньше бесконечности. Причем, чем меньше значение КЭЗ, тем на меньшей конечной попытке будет взломана защита. Равенство КЭЗ единице дает теоретическую возможность взлома ТЗИ только при попытке равной бесконечности. Следовательно, при равенстве КЭЗ единице, вероятность взлома будет описываться функцией, которая определяет границу между взломом и не взломом, а также направление проектируемого или реального взлома ТЗИ. При КЭЗ больше единицы вероятность взлома ТЗИ будет значительно ниже, чем при значении равном единице, то есть реальный взлом может произойти при больших значениях попыток, в результате чего защищенность ТЗИ будет значительно выше. При проектировании ТЗИ с высоким уровнем защиты информации необходимо добиваться, чтобы КЭЗ был наиболее большим. Этого можно достичь, если использовать комплекс технической защиты информации (КТЗИ) [1].

Таким образом, КЭЗ является единственным параметром, который определяет эффективность защиты ТЗИ. В этом случае определение КЭЗ на этапе проектирования, модернизации и анализа состояния ТЗИ является актуальной задачей.

Целью данной работы является определение коэффициента эффективности защиты по имеющимся реальным параметрам, таким как: попытки взлома, время этих попыток взлома, финансовые затраты на создание и организацию технической защиты информации, известная вероятность взлома, которая получена или рассчитана другими методами или способами.

В реальных условиях из-за вероятностного процесса взлома и ограниченности сведений о параметрах по защите информации определение значения КЭЗ является довольно сложной задачей. Поэтому в каждом конкретном случае требуется свой подход по определению эффективности защиты информации.

Основная часть исследований

Как указывалось выше, наиболее трудно определяемым параметром в ТЗИ является КЭЗ. Для его нахождения необходимы дополнительные условия, которые в каждом конкретном случае рассматриваются индивидуально. Если же дополнительных условий в настоящее время нет, то КЭЗ либо выбирается априори, либо берется равным единице до появления дополнительных данных в виде вероятности при данной попытке взлома и времени этой попытки взлома.

Рассмотрим несколько конкретных вариантов и подходов к определению КЭЗ. Сложность определения КЭЗ связана с тем, что требуется знание или вычисление вероятности процесса взлома каким либо способом в некоторой точке с известными координатами попытки и времени этой попытки взлома. Один из вариантов определения КЭЗ связан с процессом проектирования взлома и анализа взлома ТЗИ и рассмотрен в работе [2]. В этом случае возможен, в основном, анализ взломанной ТЗИ, а метод определения КЭЗ может быть представлен в следующем виде.

Вероятность взлома для комплекса технической защиты информации (КТЗИ), согласно работе [1], может быть представлена выражением

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

где $P_{\text{взл}i}(X_i)$ – приведенная вероятность максимумов взлома защиты от вложенного финансирования

$$P_{\text{взл}i}(X_i) = \frac{X_i^{x_i}}{(1 + X_i)^{1 + X_i}}, \text{ и } X_i = \frac{x_i}{H_i} = (m_c - 1), \quad (2)$$

где x_i – финансовые затраты на создание одиночной технической защиты информации (ОТЗИ); H_i – первоначальные финансовые потери при взломе и отсутствии защиты; m_c – выбранная попытка взлома для финансовых затрат [1]. $P_{\text{взл}i}(m, t)$ – распределение максимумов вероятностей взлома в зависимости от попыток взлома m и времени взлома t этих попыток для ОТЗИ; α_i – коэффициент эффективности i -той защиты (КЭЗ); n – количество защит; i – индекс параметра текущей одиночной защиты.

Распределение максимумов вероятностей взлома в зависимости от попыток взлома и времени взлома этих попыток для ОТЗИ, согласно [2], может быть представлено в виде

$$P_{\text{взл}i}(m, t) = \left(\frac{f_i(m, t)}{f_i(m, t) + t} \right)^t \cdot \left(\frac{t}{f_i(m, t) + t} \right), \quad (3)$$

$$f_i(m, t) = [t_1 + \frac{t_2 - t_1}{m_2 - m_1} \cdot (m - m_1)] \cdot (m - 1), \quad (4)$$

где $f_i(m, t)$ – функция, присущая данной i -той системе защиты, определяющая ее защитные свойства и направление взлома; m_1, t_1, m_2, t_2 – параметры, которые могут быть выбраны при проектировании ТЗИ или реальные попытки взлома и время этих попыток взлома соответственно, для которых в (4) $m_{\text{взл}} = m_2 = m, t_{\text{взл}} = t_2 = t$. Эти параметры либо выбираются при проектировании или модернизации КТЗИ, либо определяются взломом в случае анализа процесса взлома или анализа состояния КТЗИ; m, t – текущие значения попытки и времени взлома; $m_1 = 1, t_1 = 0$ – тривиальные начальные или исходные условия процесса взлома. Взлом на m – той попытке позволяет определить вероятность процесса взлома ТЗИ.

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

$$P(m) = \frac{1}{m}. \quad (5)$$

Как и в работе [2], в результате решения уравнения (1) относительно a_i , можно получить выражение для КЭЗ ОТЗИ

$$\alpha = \frac{\ln[P(m)]}{\ln[P_{\text{взл}}(m,t)] + \ln[P_{\text{взл}}(X_i)]}, \quad (6)$$

где $P_{\text{взл}}(m, t)$ и время t необходимо выразить через попытки взлома m . В выражении (3) время $t=t(m)$, согласно работе [2], может быть выражено в следующем виде

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

$$\omega = \frac{m_2 - m_1}{t_2 - t_1}. \quad (7)$$

Построить поверхность вероятности максимумов взлома ОТЗИ или КТЗИ по формуле (1) можно, если есть все необходимые параметры ТЗИ.

На рис. 1 представлены расчеты поверхностей максимумов вероятностей взлома (серая поверхность) и вероятности взлома защиты (белая поверхность). Для построения поверхности максимумов вероятностей взлома, в качестве примера, было выбрано направление взлома с параметрами $m_1=1, t_1=0, m_2=3, t_2=2$ и финансовые затраты на ТЗИ x_i ; или приведенное финансирование $X_i=1$. Выбрав точку взлома ТЗИ в этом направлении с параметрами $m_{\text{взл}}=5, t_{\text{взл}}=4$ и подставив в формулу (4) вместо m и t , с помощью выражения (6) вычисляем КЭЗ, которое будет $a_i=0,414$. На рис. 1 направление взлома представлено сплошной линией. Поскольку выбранная точка взлома совпадает с направлением взлома, то пересечение поверхностей и линии дают точку $m_{\text{взл}}=5, t_{\text{взл}}=4$. Если же направления взлома будут идти в других направлениях для данной ТЗИ с КЭЗ $a_i=0,414$, то точки взлома ТЗИ будут располагаться по линии пересечения светлой и серой поверхностей.

Выбранная точка взлома ТЗИ и вычисленный КЭЗ, позволяют при проектировании найти необходимую вероятность взлома $P_{\text{взлОТЗИ}}(0)$ в начальных условиях при $m_1=1, t_1=0$. Получить необходимую вероятность взлома $P_{\text{взлОТЗИ}}(0)$ можно путем проектирования ТЗИ с соответствующими приведенными затратами на защиту $P_{\text{взл}}(X_i)$. Кроме того, при проектировании по этому параметру можно сравнивать различные проектируемые ТЗИ и выбрать лучший вариант.

В начальных условиях $P_{\text{взл}}(m, t)$ будет равно единице и, следовательно, (1) для ОТЗИ будет иметь вид

$$P_{\text{взлОТЗИ}}(0) = [P_{\text{взл}}(X_i)]^{\alpha_i}. \quad (8)$$

Отсюда получим вероятность взлома $P_{\text{взлОТЗИ}}(0)$ для начальных условий при $m_1=1$ и $t_1=0$.

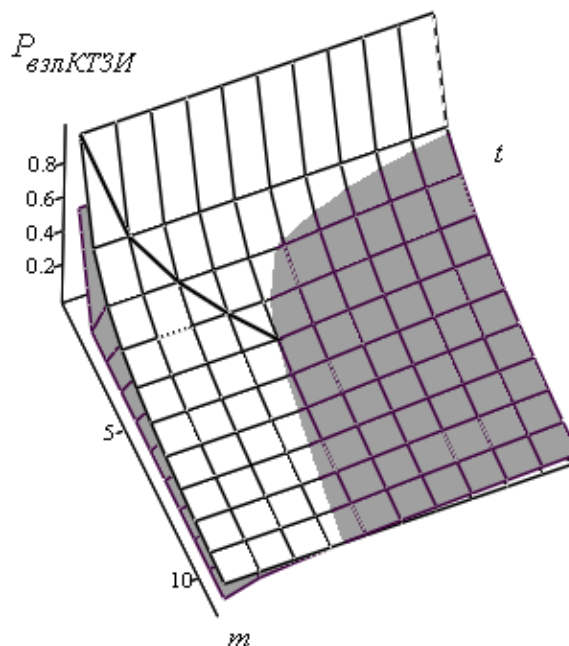


Рис. 1. Расчеты поверхностей максимумов вероятностей взлома (серая поверхность), вероятности взлома защиты (белая поверхность). Линия определяет направление проектируемого взлома. Для расчетов использовались параметры $m_1=1, t_1=0, m_2=3, t_2=2; X=1; a_i=0,414; n=1; m_{\text{взл}}=5, t_{\text{взл}}=4$

Рассмотрим следующий случай, когда известны только начальные условия: начальная попытка взлома $m_1=1$, время этой попытки взлома $t_1=0, x$ - финансовые затраты на создание ОТЗИ или приведенное финансирование X_i . Эти исходные параметры практически всегда известны и могут быть использованы при проектировании, анализе и сравнении различных ТЗИ, для выбора оптимального варианта защиты. Вероятность взлома ТЗИ для начальных условий может вычисляться с помощью существующих других различных способов и методов оценки качества технической защиты информации. Поскольку КЭЗ является отношением логарифма вероятностей в данной точке, то в начальных условиях появляется возможность вычислить КЭЗ и, следовательно, выбрав нужное направление взлома, оценить параметры будущей ТЗИ или оценить и сравнить ее с другими ТЗИ.

Одним из известных способов вычислим вероятность взлома ТЗИ для начальных условий $m_1=1$ и $t_1=0$, например, получим конкретное значение вероятности взлома $P_{\text{взлОТЗИ}}(0)$. Отсюда, аналогично (6), получим КЭЗ

$$\alpha = \frac{\ln[P_{\text{взлОТЗИ}}(0)]}{\ln[P_{\text{взл}}(X_i)]}. \quad (9)$$

Из известных начальных параметров и определенном по формуле (9) КЭЗ по выбранному направлению взлома определим попытку, на которой вероятен взлом ТЗИ и время этой попытки взлома. Для начальных условий несколько упростим выражения (4), (3), (1).

Подставив значения $m_1=1, t_1=0$ в выражение (4) получим

$$f(m,t) = \frac{t_2}{m_2 - 1} \cdot (m - 1)^2 = \frac{(m - 1)^2}{\omega_1}, \quad (10)$$

где $\omega_1 = \frac{m_2 - 1}{t_2}$.

Определим координату времени $t=t(m)$, по направлению которой происходит выбранный взлом в зависимости от попытки взлома, например, $m_2=3$, $t_2=2$. Легко показать, что в начальных условиях $A=0$. Следовательно,

$$t(m) = \frac{\sqrt{\frac{4}{\omega_1} \cdot f(m,t)}}{2} = \frac{\sqrt{\frac{4}{\omega_1} \cdot \frac{(m-1)^2}{\omega_1}}}{2} = \frac{(m-1)}{\omega_1}. \quad (11)$$

Подставив в (3), выражения (10), (11) получим вероятность $P_{\text{взл}}(m, t)$, зависящую только от координаты m попыток взлома

$$P_{\text{взл}}(m,t) = \frac{(m-1)^{(m-1)}}{m^m}. \quad (12)$$

Учитывая (12) в (1), получим распределение максимума вероятности взлома в зависимости от попытки взлома для ОТЗИ

$$P_{\text{взлОТЗИ}} = [P_{\text{взл}}(X_1) \cdot \frac{(m-1)^{(m-1)}}{m^m}]^{\alpha_i}. \quad (13)$$

Приравнявая выражение (13) к (5) и решая полученное уравнение относительно m , получим значение попытки взлома $m_{\text{взл}}$, при которой возможен взлом ТЗИ.

На рис. 2 представлено графическое решение уравнений (13) и (5).

С помощью выражения (11) можно определить время возможной попытки взлома, происходящей в выбранном направлении, в результате получим

$$t_{\text{взл}}(m_{\text{взл}}) = \frac{(m_{\text{взл}} - 1)}{\omega_1}. \quad (14)$$

Таким образом, планируя ОТЗИ с необходимыми направлениями взлома (попыткой и временем этой попытки взлома), можно спроектировать КТЗИ с необходимыми параметрами защиты.

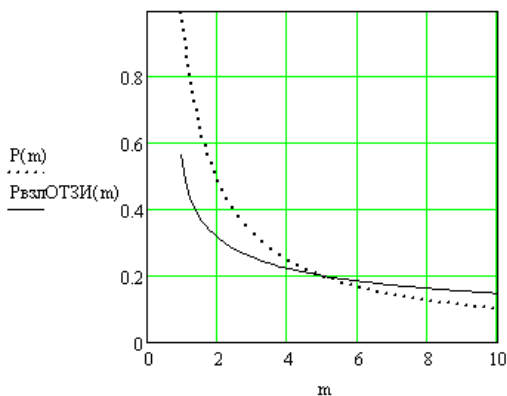


Рис. 2. Графическое совместное решение уравнений (13) и (5) с исходными начальными параметрами $m_1=1$, $t_1=0$, направлением взлома $m_2=3$, $t_2=2$; приведенными финансовыми затратами $X=1$; КЭЗ $a_i=0,414$; начальной вероятностью взлома $P_{\text{взлОТЗИ}}=0,563$; совместное решение уравнений дает $m_{\text{взл}}=5$, и время этой попытки взлома, вычисленное по формуле (14) $t_{\text{взл}}=4$

Рассмотрим теперь случай, когда начальные условия неизвестны, а известны параметры некоторых попыток и времени этих попыток взлома и вероятности для этих попыток взлома.

Пусть, например, параметры попыток взлома $m_1=2$, $t_1=3$, $m_2=5$, $t_2=6$ и вероятности для этих попыток взлома $P1=P1_{\text{взлОТЗИ}}(m_1=2, t_1=3)=0.22$ и $P2=P2_{\text{взлОТЗИ}}(m_2=5, t_2=6)=0.13$.

В данном случае считаем, что один и тот же процесс взлома проходит по известным точкам взлома, как и все реальные процессы. Для каждой точки взлома запишем распределение максимумов вероятностей взлома в зависимости от попыток взлома для ОТЗИ, приравняв их к значениям вероятности взлома в этих точках. Получим систему уравнений:

$$\begin{cases} P1 = [P_{\text{взл}}(X_1) \cdot P1(m_1)]^{\alpha_i} \\ P2 = [P_{\text{взл}}(X_1) \cdot P2(m_2)]^{\alpha_i} \end{cases}, \quad (15)$$

где введены обозначения вероятностей в соответствующих точках взлома и времени

$$P1(m_1) = P_{\text{взл}}(m_1, t_1) =$$

$$= \left(\frac{f_1(m_1, t_1)}{f_1(m_1, t_1) + t(m_1)} \right)^{t(m_1)} \cdot \left(\frac{t(m_1)}{f_1(m_1, t_1) + t(m_1)} \right)^{t(m_1)},$$

$$f_1(m_1, t_1) = t_1 \cdot (m_1 - 1), \quad t(m_1) = \frac{\sqrt{A^2 + \frac{4}{\omega} \cdot f_1(m_1, t_1)} - A}{2};$$

$$P2(m_2) = P_{\text{взл}}(m_2, t_2) =$$

$$= \left(\frac{f_2(m_2, t_2)}{f_2(m_2, t_2) + t(m_2)} \right)^{t(m_2)} \cdot \left(\frac{t(m_2)}{f_2(m_2, t_2) + t(m_2)} \right)^{t(m_2)},$$

$$f_2(m_2, t_2) = t_2 \cdot (m_2 - 1),$$

$$t(m_2) = \frac{\sqrt{A^2 + \frac{4}{\omega} \cdot f_2(m_2, t_2)} - A}{2}.$$

В системе уравнений два неизвестных $P_{\text{взл}}(X_i)$ и a_i . Так как оба уравнения описывают одну и ту же кривую, решаем их совместно путем деления первого уравнения на второе. Получим

$$\left(\frac{P1(m_1)}{P2(m_2)} \right)^{\alpha_i} = \frac{P1}{P2}. \quad (16)$$

Путем логарифмирования выражения (16) находим КЭЗ a_i

$$a_i = \frac{\ln P1 - \ln P2}{\ln P1(m_1) - \ln P2(m_2)}. \quad (17)$$

С известным параметром a_i из одного уравнения (15) получим вероятность приведенных затрат на ТЗИ

$$P_{\text{взл}}(X_1) = \exp\left[\frac{\ln P1}{a_i} - \ln P(m_1) \right]. \quad (18)$$

По вычисленным $P_{\text{взл}}(X_i)$ и a_i , известным параметрам некоторых попыток и времени этих попыток взлома, можно построить поверхность

максимумов вероятностей взломов по формуле (1). Пересечение этой поверхности с поверхностью вероятности взлома (5) даст линию возможного взлома ТЗИ с этими параметрами. Пересечение этих поверхностей дает линию взлома, которая описывается уравнением

$$[P_{\text{взл}}(X_1) \cdot P_{\text{взл}}(m, t)]^{\alpha_i} = \frac{1}{m}. \quad (19)$$

На рис. 3 представлены поверхности, рассчитанные по формулам (1) и (5). Серым цветом показана поверхность максимумов вероятностей взломов, рассчитанная по формуле (1) с известными и полученными для данного случая параметрами ТЗИ, светлым цветом - поверхность вероятностей взломов, рассчитанная по формуле (5). Линия пересечения этих поверхностей дает точки возможного взлома данного ТЗИ с попытками взлома в других направлениях и описывается уравнением (19). Получим выражения, позволяющие вычислить возможную вероятность взлома, попытку и время этой попытки взлома.

Определить значение попытки взлома можно так же, как и в предыдущем случае (рис. 2), то есть построить в координатной плоскости попыток взлома проекции поверхностей рассчитанных по формулам (1) и (5). Время попытки взлома вычисляется по кривой направления взлома. Для предыдущего случая это формула (14). Однако такой способ определения попытки взлома имеет определенный недостаток. При больших значениях попыток взлома обе кривые сильно сближаются (рис. 2) и, в этом случае из-за неточности вычисления (особенно при графических решениях), может возникать большая ошибка в определении попытки взлома, а, следовательно, и времени попытки взлома.

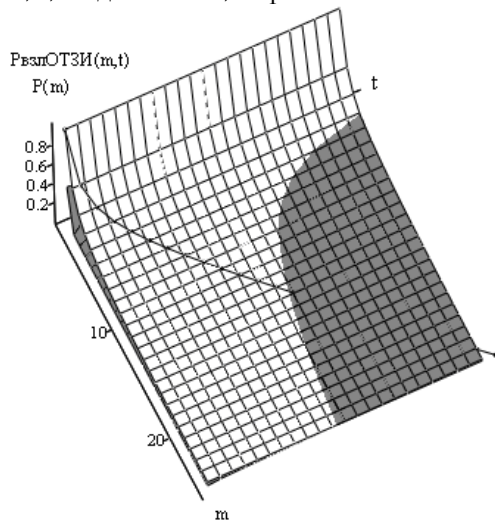


Рис. 3. Расчеты поверхностей максимумов вероятностей взломов (серая поверхность), вероятности взлома защиты (белая поверхность) с параметрами попыток взлома $m_1=2$, $t_1=3$, $m_2=5$, $t_2=6$; $P1=0.22$ и $P2=0.13$; $a=0,459$; $X=2$. Линия - направление взлома с точкой взлома ТЗИ на $m_{\text{взл}}=13,7$ попытке и времени $t_{\text{взл}}=11,8$

Для определения точки и времени взлома проведем некоторые преобразования выражения (19), после чего получим уравнение:

$$\frac{1}{m^{\alpha_i}} \cdot P_{\text{взл}}(m, t) = \frac{1}{P_{\text{взл}}(X_1)}. \quad (20)$$

Решая уравнение (20) графическим способом (рис. 4) или числовым методом последовательных приближений можно найти точку взлома $m_{\text{взл}}$.

Определяем время попытки взлома по попытке взлома и направлению процесса взлома с помощью выражению (7), подставив в него значение $m_{\text{взл}}$ получим

$$t(m_{\text{взл}}) = \frac{\sqrt{A^2 + \frac{4}{\omega} \cdot f(m_{\text{взл}}, t) - A}}{2}, \quad (21)$$

$$\text{где } f(m_{\text{взл}}, t) = [t_1 + \frac{t_2 - t_1}{m_2 - m_1} \cdot (m_{\text{взл}} - m_1)] \cdot (m_{\text{взл}} - 1).$$

На рис. 4 представлено графическое решение уравнения (20): линия 1 - расчет, выполненный по правой части уравнения (20), линия 2 - по левой части уравнения (20). Пересечение линий 1 и 2 дают точку взлома $m_{\text{взл}}=13,7$, то есть взлом ТЗИ вероятен между 13 или 14 попытками, а время при выбранном примере направлении взлома будет $t_{\text{взл}}=11,8$, то есть между 11 и 12 единицей времени.

Такое решение из-за большего угла между линиями позволяет более точно определять точку попытки взлома. Кроме того, такой подход дает возможность уменьшить время поиска решения уравнения (20) при больших значениях попыток взлома с помощью метода последовательных приближений.

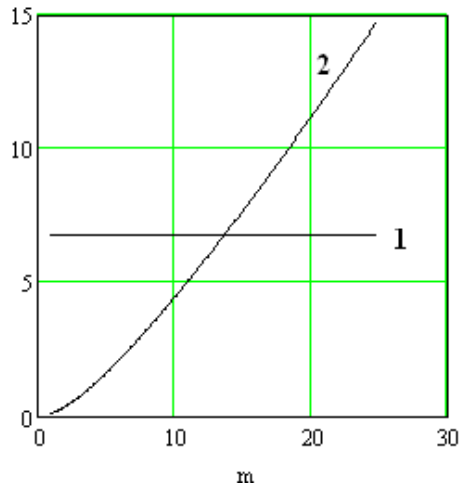


Рис. 4. Графическое решение уравнения (20): линия 1 - расчет, выполненный по правой части уравнения; линия 2 - по левой части уравнения. Взломом ТЗИ возможен на $m_{\text{взл}}=13,7$ попытке или между 13 и 14 попытками

Выводы

В работе рассмотрены способы определения коэффициента эффективности технической защиты информации. Рассмотрены три разных варианта получения КЭЗ. Первый - предполагает определение КЭЗ при проектировании ТЗИ. В этом случае при проектировании попытка взлома и время этой попытки взлома закладываются из требований технического задания. Необходимые финансовые затраты на защиту определяются из состава ТЗИ для

первой попытки взлома. Можно также определить КЭЗ, если произошел взлом реально работающей ТЗИ и известна попытка и время этой попытки взлома. Эти данные могут быть использованы для анализа ТЗИ.

Второй вариант определения КЭЗ, когда известна вероятность взлома ТЗИ с первой попытки, что позволяет не только определить КЭЗ, но и предсказать попытку и время попытки взлома, если известно направление взлома. Направление процесса взлома может быть определено по последующим реальным попыткам взлома.

И третий вариант, когда известны параметры промежуточных взломов и вероятности этих промежуточных попыток взлома, то есть не используются тривиальные параметры первой попытки взлома ($m_1=1$, $t_1=0$). В этом случае можно получить все необходимые параметры для данной ТЗИ: финансовые вложения в защиту, КЭЗ, и рассчитать попытку, время, вероятность возможного взлома, а также проанализировать состояние ТЗИ в

любой момент функционирования защиты.

Следует заметить, что получение КЭЗ возможно лишь в том случае, когда есть дополнительные сведения, связанные с известными значениями вероятности в любой момент функционирования защиты. Нахождение значения вероятности в любой момент функционирования защиты требует дополнительных исследований.

Литература

[1] Журиленко Б.Е. Математическая модель вероятностной надежности комплекса технической защиты информации / Б.Е. Журиленко // *Безпека інформації*. – 2012. №2 (18). – С. 61-65.

[2] 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.

УДК 004.056.5 (045)

Журиленко Б.Є., Ніколаєва Н.К. Визначення коефіцієнта ефективності технічного захисту інформації по її параметрах

Анотація. У цій роботі розглянуті способи визначення коефіцієнта ефективності технічного захисту інформації при проектуванні і аналізі функціонування технічного захисту. Складність визначення коефіцієнта ефективності захисту полягає у відсутності усіх необхідних початкових параметрів. Тому розглядалися три основні можливі варіанти. Перший, коли відомі фінансові витрати, вкладені в захист, спроба і час цієї спроби злому. Другий варіант - це, коли відомі фінансові витрати на захист і вірогідність злому технічного захисту на першій спробі, яка відома. Вірогідність злому ТЗИ для початкових умов може обчислюватися за допомогою існуючих інших різних способів і методів оцінки якості технічного захисту інформації. Третій варіант - найбільш загальний, коли відомі будь-які дві спроби, час цих спроб злому і вірогідності злому цих спроб. В результаті досліджень отримані формули, що дозволяють по цих відомих параметрах будувати поверхні максимумів вірогідності злому технічного захисту інформації, по яких можна визначити параметри можливого злому технічного захисту інформації для будь-якого напрямку процесу злому.

Ключові слова: коефіцієнт ефективності захисту, технічний захист інформації, приведена вірогідність максимумів злому захисту, спроба злому, час спроби злому, комплекс технічного захисту інформації.

Zhurilenko B., Nikolaieva N. Efficiency coefficient calculation for technical information security based on its parameters

Abstract. This paper shows ways to determine the efficiency coefficient for technical information security in the design stage and analysis of the functioning of technical security. The complexity of the determination of efficiency coefficient for technical information security is the lack of all necessary initial parameters. Therefore, we considered three main options. First, when we know the financial costs invested in the protection and time of the attempt to hacking attempts. The second option - it is when we know the financial costs of the defense and the possibility of breaking the technical security on the first try, which is known for. The probability of breaking proofing for the initial conditions can be calculated using various other existing methods and methods for assessing the quality of technical information security. The third option - the most common, where known, any two attempts, time of break-in attempts and the likelihood of hacking attempts. As a result of research we obtained formulas that allow for these known parameters to build a surface high probability of breaking technical information security, which can determine the parameters of a possible burglary technical information security for all processes of breaking.

Key words: coefficient for technical information security, technical information security, given the likelihood of a security breach high, breaking attempt, time for breaking attempt, complex of technical information security.

Отримано 8 жовтня 2015 року, затверджено редколегією 28 жовтня 2015 року