© Zhurilenko B. Method of single technical information security system designing with probable reliability and given parameters of breaking // Ukrainian Scientific Journal of Information Security, 2014, vol. 20, issue 1, p. 36-42.

МЕТОД ПРОЕКТИРОВАНИЯ ЕДИНИЧНОЙ СИСТЕМЫ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ С ВЕРОЯТНОСТНОЙ НАДЕЖНОСТЬЮ И ЗАДАННЫМИ ПАРАМЕТРАМИ ВЗЛОМА

Борис Журиленко

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 методов защиты информации с 2002 года.
Научный интерес: методы съема и методы технической защиты информации.
Публикации: более 90 научных статей и патентов на изобретения.
E-mail: zhurilenko@mail. ru

Аннотация. *В результате проведенной работы предложен метод проектирования единичной системы технической защиты информации (ТЗИ) с вероятностной надежностью и с заданными параметрами взлома. Установлена общая связь между попыткой и временем взлома при проектируемой частоте взлома. Показано, что параметр, определяющий вероятностную надежность ТЗИ, может быть не только постоянной величиной с размерностью времени, но и зависеть как от попыток взлома, так и времени этих попыток взлома. Через попытки и время взломов определены уравнения для оценки вероятностной надежности технической защиты с параметрами, присущими конкретной проектируемой системе защиты, которые учитывают исходные начальные и требуемые при проектировании ТЗИ данные. Получены выражения определения таких параметров, как значения вероятности, координаты попыток и времени для линии, по которой реализуется проектируемый взлом. Полученные параметры линии взлома позволяют не только проектировать ТЗИ, но и исследовать, контролировать и управлять самим процессом взлома по совпадению или отклонению от линии реально происшедших событий взлома*

Ключевые слова: *защита информации, надежность, вероятность взлома, техническая защита информации, заданные параметры взлома, кривая максимальной вероятности взлома, попытка взлома, время взлома, проектируемая система защиты.*

Введение

В настоящее время в литературе не приводятся и не описываются методы проектирования средств технической защиты информации (ТЗИ) с конкретными требованиями защищенности по количеству попыток взлома и времени взлома. Прежде чем проектировать построение той или иной ТЗИ желательно было бы знать ее проектируемую надежность, и в частности ее вероятностную надежность к взлому или защите. При проектировании основными параметрами понятными заказчику и проектировщику ТЗИ являются ее стоимость, попытка и время попытки, при которых возможен взлом ТЗИ. Влияние финансирования или стоимости ТЗИ на вероятность ее взлома можно оценить, используя результаты работ [1,2]. Для построения метода проектирования с учетом исходных требований по попытке взлома и времени, которые должны быть не меньше заданных, необходимы дополнительные исследования.

Анализ существующих исследований

В настоящее время в Украине теоретически разрабатываются методы защиты информации с использованием системного подхода, экспертной оценки анализа с помощью нечетких множеств, теории игр и другие [3].

В работе [3] предложен метод, позволяющий оценить вероятностную защищенность ТЗИ по

попыткам и времени взлома, и, соответственно, выработать необходимые рекомендации для модернизации или разработки новой ТЗИ.

Некоторый недостаток подхода к оценке вероятностной защищенности ТЗИ в данном методе связан с необходимостью решения задачи с построением трехмерного графика, что не всегда удобно на практике. Аппроксимация параметра, определяющего свойства технической защиты, была линейной, что может привести к существенным ошибкам при исследовании и проектировании ТЗИ. Кроме того, параметр, определяющий свойства технической защиты, выбирался постоянной величиной, хотя и с размерностью времени. Если осуществить определенную доработку подхода, данный метод может быть положен в основу метода проектирования ТЗИ с наперед заданными параметрами взлома.

Целью данной работы является разработка метода проектирования с вероятностной надежностью единичной системы технической защиты информации и с заданными параметрами взлома.

Теоретическое обоснование метода проектирования единичной системы технической защиты информации

Для создания метода проектирования ТЗИ с наперед заданными параметрами взлома по попыткам и времени проведем дополнительный анализ выражения вероятности взлома во времени для одной защиты.

В работах [4,5] было получено выражение распределения вероятности попыток взлома, которое подчиняется геометрическому закону распределения вероятностей из условия, что параметр t_0, определяющий свойство единичной ТЗИ, является величиной постоянной не зависящей от времени, но имеющий ее размерность.

В реальных условиях на практике параметр t_0 не является постоянной величиной и зависит как от количества попыток взлома, так и времени, при котором происходит этот взлом.

Рассмотрим случай, когда t_0 является не постоянной величиной, а дополнительно зависит от времени.

Пусть t_0 – параметр, определяющий свойства технической защиты информации во времени и связанный с надежностью ТЗИ. Конкретные свойства параметра t_0 определим несколько позже. t – текущее время, в течение которого осуществляется защита, $p_0(t)$ – вероятность защищенности ТЗИ во времени.

Определим свойства ТЗИ через риски защищенности во времени

$$(t_0 + t)\cdot p_0(t) = f(t), \qquad (1)$$

где $f(t)$ – произвольная положительная функция, зависящая от времени и имеющая размерность времени.

Анализируя выражение (1), можно сказать, что для обеспечения защиты информации функция $f(t)$, которую определим как функцию рисков по защите информации во времени, при увеличении времени t должна быть хотя бы постоянной. Постоянство $f(t)$ во времени обеспечивает предельно допустимый уровень ТЗИ. Если $f(t)$ со временем будет уменьшаться, то используемая ТЗИ является не эффективной и ее необходимо поменять на другую более эффективную систему защиты. В случае же если функция $f(t)$ увеличивается со временем, то такая ТЗИ является более эффективной. Причем, чем сильнее со временем увеличивается $f(t)$, тем эффективнее становится ТЗИ.

Из (1) запишем вероятность защищенности ТЗИ:

$$p_0(t) = \frac{f(t)}{t_0 + t}. \qquad (2)$$

Определим $f(t)$ из начальных условий. При $t=0$ вероятность защищенности $p_0(0)=1$. Отсюда

$$p_0(0) = \frac{f(t)}{t_0} = 1; \text{ или } f(t) = t_0. \qquad (3)$$

Выражение $f(t)$ из (1) является математическим ожиданием защищенности данной ТЗИ. А из (3) следует, что $f(t)$ сначала соответствует некоторым начальными условиями при $t=0$, а затем может увеличиваться или быть постоянной с увеличением временем.

Следовательно, вероятность защищенности ТЗИ во времени будет:

$$\mathrm{p}_0(\mathrm{t}) = \frac{f(t)}{f(t) + t}. \qquad (4)$$

Вероятность взлома во времени:

$$p(t) = \frac{t}{f(t) + t}. \qquad (5)$$

Выбираем независимость вероятности взлома от результатов предыдущих попыток. Если с очередной попытки взлом не произошел, то считаем, что вероятность взлома используемой защиты остается той же. Такое распределение попыток взлома будет подчиняться геометрическому закону распределения вероятностей, и в этом случае, согласно [6], вероятность события взлома на m – той попытке может быть записана как:

$$P_m(t) = [p_0(t)]^{m-1}\cdot p(t) = \left(\frac{f(t)}{f(t)+t}\right)^{m-1}\cdot\left(\frac{t}{f(t)+t}\right). \qquad (6)$$

Найдем кривую распределения максимумов вероятностей взлома $P_m(t)$. Для этого определим вероятность m – той попытки взлома во времени, приравняв нулю первую производную выражения (6). Получим:

$$\frac{\partial P_m(t)}{\partial t} = [f(t) + t\cdot(m-1)\cdot\frac{\partial f(t)}{\partial t} - t\cdot m\times \\ \times\frac{f(t)}{f(t)+t}\cdot\left(\frac{\partial f(t)}{\partial t}+1\right)]\cdot\frac{f^{m-2}(t)}{\left(f(t)+t\right)^m} = 0. \qquad (7)$$

Выражение $\frac{f^{m-2}(t)}{\left(f(t)+t\right)^m} \neq 0$, потому что $f(t)>0$ и $t\geq 0$. Сократив на это выражение и приравняв в уравнении (7) значение в квадратных скобках нулю, после определенных преобразований, получим

$$f(t) - t \cdot m \cdot \frac{f(t)}{f(t)+t} = \\ = [t \cdot m \cdot \frac{f(t)}{f(t)+t} - t \cdot (m-1)] \cdot \frac{\partial f(t)}{\partial t} \quad (8)$$

или

$$f(t) \cdot [f(t) - (m-1) \cdot t] = t \cdot [f(t) - (m-1) \cdot t] \cdot \frac{\partial f(t)}{\partial t}. \quad (9)$$

Из равенства (9) найдем одно из его решений, приравняв нулю выражение в квадратных скобках. Получим:

$$f(t) = (m-1) \cdot t. \quad (10)$$

Второе решение равенства (9) можно найти, если сократить обе его части на выражение в квадратных скобках. В результате несложных преобразований будем иметь

$$\frac{\partial t}{t} = \frac{\partial f(t)}{f(t)}. \quad (11)$$

Интегрируя выражение (11):

$$\lg[f(t)] = \lg t + const, \quad (12)$$

а затем, потенцируя равенство (12), получим второе решение уравнения (9)

$$f(t) = t \cdot const. \quad (13)$$

Сравнивая выражения (13) и (10) видим, что они будут равны, если *const = (m-1)*. Поскольку константа может быть любой величиной, то можно сделать вывод, что равенство (9) имеет одно решение, определяемое выражением (10). Одновременно выражение (10) определяет связь между попытками взлома *m* и временем этой попытки *t*.

Вторая производная распределения вероятностей взлома (6) по времени дает максимум в точке, определяемой выражением (10).

Таким образом, в процессе приведенных выкладок показано, что параметр t_0 равен *f(t)* и может быть переменной величиной, зависящей от произведения количества попыток взлома и времени взлома. Это важный результат, так как в реальных условиях одновременно возрастают и попытки взлома и время, при котором происходит взлом.

Используя полученный результат, также как и в работах [2-5] плотность вероятности взлома на *m* – той попытке во времени может быть записана как

$$P_m(t) = [(\frac{f(t)}{f(t)+t})^{m-1} \cdot (\frac{t}{f(t)+t})]^{\gamma}, \quad (14)$$

где *f(t)* – параметр, присущий данной системе защиты и определяющий ее защитные свойства; *t* – текущая координата времени; *m* – текущая попытка взлома; γ – определяет эффективность проектируемой защиты.

Выражение для максимумов вероятностей взлома во времени может быть получено из уравнения (14) путем замены степени *(m-1)* решением уравнения (10), которое и определяет максимум вероятности взлома в точке *(m-1)*

$$P(t) = [(\frac{f(t)}{f(t)+t})^{\frac{f(t)}{t}} \cdot (\frac{t}{f(t)+t})]^{\gamma}. \quad (15)$$

Как уже упоминалось, при проектировании ТЗИ без учета ее стоимости основными исходными данными могут быть любые два из следующих параметров – необходимая минимальная попытка взлома, время этой попытки взлома или средняя частота попыток взлома. Поскольку *f(t)* – параметр, присущий конкретной проектируемой системе защиты, то его необходимо определить через основные исходные данные - время и попытку взлома. Кроме того, необходимо найти связь между этими исходными данными.

Определим *f(t)* через время *t*, учитывая (10) и исходные данные: начальные $m_1=1$; $t_1=0$ и требуемые при проектировании ТЗИ m_2 и t_2, путем аппроксимации таким образом, чтобы *f(t)* принимало соответствующие значения при выбранных исходных данных. Аппроксимация выполняется согласно [7].

$$f(t) = [(m_1 - 1) + \frac{m_2 - m_1}{t_2 - t_1} \cdot (t - t_1)] \cdot t, \quad (16)$$

где $\omega = \frac{m_2 - m_1}{t_2 - t_1}$ средняя частота попыток взломов.

Если в выражение (16) подставить исходные данные времени t_1, t_2, то *f(t)* даст значения соответствующие попыткам взлома m_1 и m_2.

В уравнении (16) начальные условия не конкретизируются, так как они могут быть любыми. Кривая *f(t)* проходит через все точки, определяемые исходными данными.

С другой стороны аналогичным образом находится *f(m)* через попытки взлома *(m-1)* с учетом начальных и требуемых при проектировании исходных данных

$$f(m) = [t_1 + \frac{t_2 - t_1}{m_2 - m_1} \cdot (m - m_1)] \cdot (m - 1). \quad (17)$$

В этом случае, как и предыдущем, если в выражение (17) подставить исходные данные попыток взлома, то *f(m)* даст такие же значения, что и для выражения (16), при прохождении через все точки времени, определяемые исходными данными.

При равенстве *f(t)=f(m)* максимумы вероятности взлома выражения (15) будут давать линию, по которой будет происходить процесс взлома с выбранными исходными данными.

Используя выражения (16) и (17) можно построить поверхность, которая одновременно будет удовлетворять попыткам взлома и времени взлома проектируемого ТЗИ:

$$f(m,t) = \sqrt{f(t) \cdot f(m)}. \quad (18)$$

Если построить поверхности для выражений (16), (17) и (18), то можно показать, что проектируемый процесс взлома ТЗИ будет происходить по общей линии пересечения всех этих поверхностей.

На рис. 1 представлены поверхности, рассчитанные с помощью формул (16), (17) и (18).

Поскольку поверхности рис. 1 представлены в координатной оси по попыткам взлома с отсчетом, который начинается с *m'=m-1*, то проектируемые исходные данные на поверхности рис. 1 будут $t_2=3$ $m_2'=m_2-1=5-1=4$, и $m_1'=m_1-1=1-1=0$, $t_1=0$.

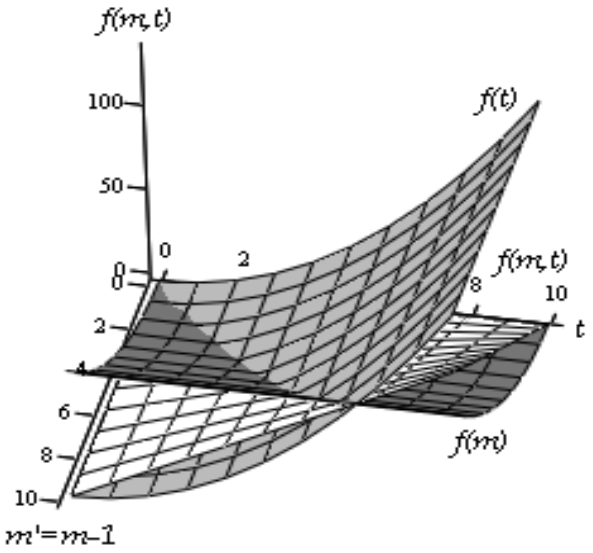

Рис. 1 Представлены поверхности, полученные по формулам (16), (17) и (18) с проектируемыми параметрами взлома $m_1=1$, $t_1=0$, $m_2=5$, $t_2=3$. Поверхность $f(t)$ представлена светло серым цветом, $f(m)$ - темно серым цветом и $f(m, t)$ - белым цветом

Реальный процесс взлома ТЗИ, определяемый физической природой с выбранными исходными данными, будет происходить по линии пересечения темно и светло серых поверхностей, то есть по линии пересечения, на которой выполняется условие $f(t)=f(m)$. Из этого условия для данного процесса взлома можно получить связь между попытками взлома и временем попыток взлома.

Определим время попытки взлома через среднюю частоту взлома и попытку взлома. Решая совместно уравнения (16) и (17), получим время попытки взлома $t(m)$ от самой попытки взлома:

$$t(m)=\frac{\sqrt{A^2+\frac{4}{\omega}\cdot f(m)}-A}{2}, \qquad (19)$$

где $A=t_1+\frac{m_1-1}{\omega}$.

Аналогично, определяем попытку взлома через среднюю частоту взлома и время попытки взлома, получим зависимость самой попытки взлома $m(t)$ от времени взлома:

$$m(t)=\frac{\sqrt{B^2+4\cdot\omega\cdot f(t)}-B}{2}+1, \qquad (20)$$

где $B=\omega\cdot t_1-(m_1-1)$.

Как и в работе [3], определим вероятность взлома проектируемой защиты информации на m – той попытке с помощью выражения:

$$P(m)=\frac{1}{m}. \qquad (21)$$

С другой стороны эту же вероятность взлома можно определить через процесс взлома, проектируемый ТЗИ во времени, с помощью формулы (20). Получим

$$P(m)=P(t)=\frac{1}{m(t)}. \qquad (22)$$

С помощью формул (16), (17), (18), (19), (20), (21), (22) можно перевести процесс проектирования с задачи в трехмерной области [3] в задачу двухмерной области и упростить процесс проектирования.

Проведем расчеты и построим поверхности вероятностей взлома с помощью выражения для максимумов вероятности взлома в виде

$$P(m,t)=[(\frac{f(m)}{f(m)+t})^{\frac{f(m)}{t}}\cdot(\frac{t}{f(m)+t})]^{\gamma} \qquad (23)$$

и выражений проектируемой вероятности взлома (21) и той же вероятности взлома выраженной через время (22). В расчетах использовались исходные данные $m_1=1$, $t_1=0$, $m_2=5$, $t_2=3$ и $\gamma=1$. Полученные результаты представлены на рис. 2. В работе [3] значение γ определяет критерий и является признаком эффективности использования ТЗИ. При $\gamma=1$ обеспечивается минимальное требование по защите.

Поверхность максимума вероятности взлома $P(m,t)$ по координатам m, t соответствует результатам, полученным в работах [3,4]. Однако полученный результат отличается от результата работы [3] тем, что на рис. 2 есть две линии, связанные с пересечениями поверхностей вероятностей взлома. По одной линии - пересечения белой и светло серой поверхностей, полученной с помощью выражений (21) и (22), осуществляться процесс взлома ТЗИ, который определяется исходными данными. В этом случае при $\gamma=1$ взлом возможен в основном на бесконечности.

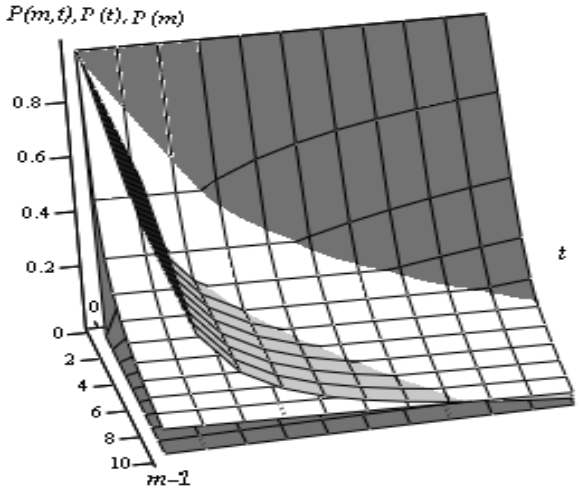

Рис. 2 Поверхности расчетов вероятностей взлома по формулам: (22) – $P(t)$ – поверхность светло серого цвета, (21) - $P(m)$ - поверхность белого цвета, (23) - $P(m,t)$- поверхность темно серого цвета. В расчетах использовались исходные данные $m_1=1$, $t_1=0$, $m_2=5$, $t_2=3$ и $\gamma=1$

Вторая линия – пересечение белой и темно серой поверхностей указывает на возможность взлома, если процесс пойдет по пути не определяемым исходными данными и $\gamma=1$. Такой процесс можно анализировать по реальным попыткам взлома, которые в данный момент времени не привели к взлому ТЗИ , но могут предсказать, когда взлом произойдет в будущем.

При проектировании ТЗИ в качестве исходных данных можно заложить либо необходимое время или попытку взлома при известной частоте попыток взлома, то есть заложить такие параметры взлома, ниже которых взлома не

должно быть. Если неизвестна частота попыток взлома, то можно заложить попытку $m_{вз}$ и ее время взлома $t_{вз}$.

Если взлом должен произойти при заданных исходных данных, то можно определить необходимую эффективность системы защиты γ. Для этого уравнение (21) приравнивается к уравнению (23), выполняется логарифмирование обеих частей равенства и из полученного равенства находится γ, причем, предварительно в (23) заменяется время t на выражение $t(m)$ (19). В этом случае решение уравнения (23) из трехмерного пространства переводится в двумерное пространство, в котором вероятность взлома зависит только от m, при условии, что процесс взлома идет в соответствие с выбранными исходными параметрами.

В результате решения равенства относительно γ после некоторых преобразований получим:

$$\gamma = \frac{t(m)\cdot \lg(m)}{\lg\left[\frac{f(m)+t(m)}{f(m)}\right]^{f(m)} + \lg\left[\frac{f(m)+t(m)}{t(m)}\right]^{t(m)}}. \quad (24)$$

Эффективность системы защиты γ можно определить и через временной параметр. Проделав аналогичные операции с выражениями (22), (23) и заменив в (23) функцию, зависящую от m на функцию, зависящую от t, получим:

$$\gamma = \frac{t\cdot \lg[m(t)]}{\lg\left[\frac{f(t)+t)}{f(t)}\right]^{f(t)} + \lg\left[\frac{f(t)+t)}{t}\right]^{t}}. \quad (25)$$

Если известны только требуемые параметры по взлому $m_{вз}$ и $t_{вз}$, то можно определить необходимую эффективность системы защиты, подставив эти параметры в выражения (24) или (25).

При проектировании ТЗИ возможны следующие случаи. Первые два случая, когда планируется частота взломов ω и один из начальных параметров либо взлом $m_{вз}$, либо время взлома $t_{вз}$. В этом случае по формулам (16) и (17) вычисляются функции $f(t)$ и $f(m)$, а затем с учетом выражений (19), (20) по формулам (24) и (25) вычисляется эффективность системы защиты γ. В расчетах используются подстановки $m=m_{вз}$ и $t=t_{вз}$. После определения всех необходимых параметров по формулам (21), (22), (23) строятся поверхности вероятностей взлома. Причем, если $\gamma<1$, то все поверхности взлома пересекутся в точке с координатами $m=m_{вз}-1$ и $t=t_{вз}$.

При проектировании ТЗИ параметры взлома которого задаются только исходными данными $m_1=1$; $t_1=0$, $m_{вз}=9$ и $t_{вз}=6$. В этом случае для проектируемой ТЗИ по формулам (16), (17) определяются $f(t)$ и $f(m)$ при соответствующих заменах $m_1=1$; $t_1=0$, $m_{вз}=m_2=m=9$ и $t_{вз}=t_2=t=6$, а затем вычисляется параметр эффективности системы защиты, который для выбранных исходных данных будет равен $\gamma=0,7$. Дальнейшее построение поверхностей взлома по формулам (21), (22), (23) даст пересечение всех поверхностей с координатами $m_{вз}=9-1=8$ и $t_{вз}=6$.

В отличие от результатов рис. 2 линия максимума вероятности, по которой будет происходить взлом, может быть получена с помощью других формул. В выражении (23) $f(m)$ заменяется выражением $f(m,t)$ (18). При такой замене выражение (23) будет создавать поверхность, зависящую только от m, а это позволит перейти от анализа защищенности ТЗИ из трех мерной в двумерную задачу. С учетом выражений (21), (22) и исходных данных $m_1=1$; $t_1=0$, $m_{вз}=m_2=m=9$ и $t_{вз}=t_2=t=6$, а также $\gamma=0,7$, получим поверхности максимумов вероятностей взлома представленные на рис. 3.

Также как и на рис. 2 по линии пересечения белой и светло серой поверхностей, полученных с помощью выражений (21) и (22), осуществляться процесс взлома ТЗИ, который определяется исходными данными. Темно серая поверхность получена с помощью выражения (23) с заменой $f(m)$ на $f(m,t)$. При проектировании ТЗИ точка пересечения всех поверхностей дает требуемую попытку взлома на девятой попытке и на шестой единице времени.

Линия вероятности взлома позволит не только проектировать ТЗИ, но и исследовать, контролировать и управлять самим процессом взлома по совпадению или отклонению происшедших событий взлома от линии взлома. Из результатов рис. 3 видно, что при исходных проектируемых параметрах и эффективности ТЗИ $\gamma=0,7$ взлом произойдет во времени при $t=6$ на $m'=m-1=8$ или $m=9$ попытке.

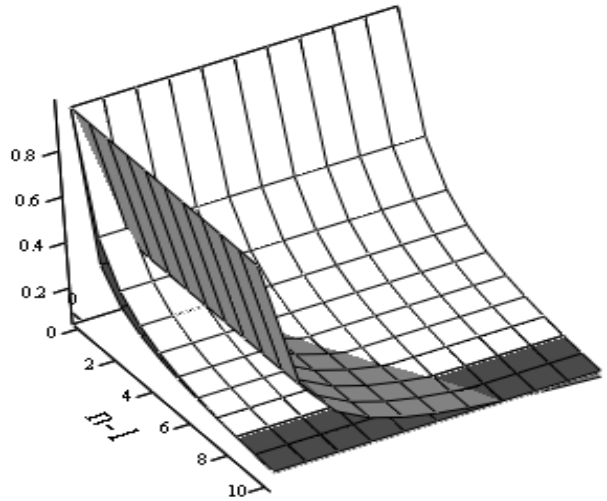

Рис. 3 Поверхности расчетов вероятностей взлома по формулам: (22) – $P(t)$ – поверхность светло серого цвета, (21) - $P(m)$ - поверхность белого цвета, (23) - $P(m,t)$- поверхность темно серого цвета с заменой $f(m)$ на $f(m,t)$. В расчетах использовались исходные данные $m_1=1$, $t_1=0$, $m_2=5$, $t_2=3$ и $\gamma=0.7$

Выводы

В результате проведенной работы показано, что t_0 – параметр, определяющий свойства технической защиты информации, может быть не только постоянной величиной с размерностью времени, но и функцией, зависящей как от попыток взлома, так и от времени этих попыток взлома.

Установлена общая связь между попытками взлома и временем этих взломов, которая имеет один и тот же вид как для постоянного значения параметра t_0, определяющего свойства ТЗИ, так и

для зависящего от попыток и времени взлома. Также установлена связь между попыткой взлома и временем этой попытки взлома при проектируемой частоте взлома.

Определен вид функций *f(m)*, *f(t)* и *f(m,t)* с параметрами, присущими конкретной проектируемой системе защиты, через попытки *m* и время *t* этих взломов, учитывающие исходные начальные $m_1=1$; $t_1=0$ и требуемые при проектировании ТЗИ m_2 и t_2 данные. С помощью этих исходных данных и полученных функций можно вычислить частоту попыток взлома, а так же вероятностную надежность технической защиты информации через частоту попыток взлома и одного из проектируемых параметров попыток взлома *m* или времени попыток взлома *t*, или только через проектируемые параметры попыток взлома $m_{в3}$ и времени взлома $t_{в3}$.

Показано что с помощью уравнений *f(m)*, *f(t)* и *f(m,t)* можно предсказать, в каком направлении идет проектируемый процесс взлома ТЗИ, и провести его анализ.

Предложен метод проектирования с вероятностной надежностью единичной системы технической защиты информации и с заданными параметрами взлома, который заключается в следующем:

1. Задается или вычисляется по начальным исходным данным средняя частота попыток взлома.
2. По формулам (16), (17) и (18) определяются значения выражений *f(m)*, *f(t)* и *f(m,t)*, отвечающие за вероятностные свойства проектируемой технической защиты информации.
3. По исходным данным с помощью выражений (24) или (25) рассчитывается проектируемая эффективность ТЗИ.
4. Затем строятся поверхности вероятностей взлома по формулам (21), (22) и (23), представленные на рис. 2 или рис. 3.
5. По пересечениям поверхностей рис. 2 определяются направление проектируемого процесса взлома и зона допуска попыток и времени взлома, отличающихся от реального процесса взлома и представленных на рис. 2 областью белой поверхности, заключенной между светло серой и серой поверхностями.

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. — К. : КПІ НДЦ «Тезіс», 2011. — Вип. 1 (22). — С. 33-43.

[2] Журиленко Б.Е. Математическая модель вероятностной надежности комплекса технической защиты информации / Б.Е. Журиленко // Безпека інформації. — 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. — 2013. — №1 (19). — С. 34-39.

[4] Журиленко Б.Е. Оценка стойкости технической защиты информации во времени / Б.Е. Журиленко, Н.К. Николаева, Н.С. Пелих // Захист інформації. — 2012. — №1(54). — С. 104-108.

[5] Журиленко Б.Е. Связь количества попыток взлома технической защиты информации и времени взлома / Журиленко Б.Е.// Матеріали Міжнар. наук.-практ. конф. «Інформаційні управляючі системи та технології» (ІУСТ-ОДЕСА-2013), м. Одеса, 8-10 жовтня 2013 р. — С.184-186.

[6] Румшинский Л.З. Элементы теории вероятностей / Румшинский Л.З. — М.: Изд-во «Наука», 1970. — 256 с.

[7] Ефимов Н.В. Краткий курс аналитической геометрии / Н.В. Ефимов. — М.: Госуд. изд. технико-теоретической литературы. — 1956. — 256 с.

УДК 004.056.5 (045)

Журиленко Б.Є. Метод проектування одиничної системи технічного захисту інформації з вірогідною надійністю та заданими параметрами злому

Анотація. *В результаті проведеної роботи запропонований метод проектування одиничної системи технічного захисту інформації (ТЗІ) з вірогідною надійністю і із заданими параметрами злому. Встановлений загальний зв'язок між спробою і часом злому при проектованій частоті злому. Показано, що параметр, який визначає вірогідну надійність ТЗІ, може бути не тільки постійною величиною з розмірністю часу, але і залежати як від спроб злому, так і часу цих спроб злому. Через спроби і час зломів визначені рівняння для оцінки вірогідної надійності технічного захисту з параметрами, властивими конкретній проектованій системі захисту, які враховують початкові первинні і необхідні при проектуванні ТЗІ дані. Отримані вирази визначення таких параметрів, як значення вірогідності, координати спроб і часу для лінії, по якій реалізується проектований злом. Отримані параметри лінії злому дозволяють не тільки проектувати ТЗІ, але і досліджувати, контролювати і управляти самим процесом злому по збігу або відхиленню від лінії подій злому, що реально відбулися.*

Ключові слова: *захист інформації, надійність, вірогідність злому, технічний захист інформації, задані параметри злому, крива максимальної вірогідності злому, спроба злому, час злому, проектована система захисту.*

Zhurilenko B. Method of single technical information security system designing with probable reliability and given parameters of breaking

Abstract. *As a result of the work was proposed a method of single technical information security (TIS) system designing with probable reliability and given parameters of breaking. The general dependence between effort and time of breaking by projected frequency of breaking was defined. It is shown that the parameter that determines the probable reliability of TIS may not only be a constant with the time dimension, but depends on both the attempt of breaking and time of breaking. Through the attempt of breaking*

and time of breaking by an equation for the estimation of the likely reliability of technical security options that are specific designed security system, taking into account the initial primary and essential data in the design of TIS. The expressions were given for determining parameters such as probability values, efforts and time coordinates for line, which is implemented by the projected breaking. These parameters allow not only the TIS design, but also to research, control and manage the process of breaking through coincidence or deviation from the line of breaking events that actually occurred.

Key words: *information security, reliability, breaking probability, technical information security, given parameters of breaking, curve of maximal breaking probability, attempt of breaking, time of breaking, designed security system.*

Отримано *20 січня 2014 року*, затверджено редколегією *18 лютого 2014 року*