DOI: 10.18372/2410-7840.23.16769
УДК 004.056.5(045)

ОЦЕНКА ПРОЕКТИРУЕМОЙ И РАБОТАЮЩЕЙ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ С ПОМОЩЬЮ МАТЕМАТИЧЕСКОЙ МОДЕЛИ РЕАЛЬНОГО ФИЗИЧЕСКОГО ПРОЦЕССА ВЗЛОМА ЗАЩИТЫ

Борис Журиленко

В данной работе показана возможность оценки проектируемой и работающей технической защиты информации (ТЗИ) с помощью математической модели реального физического процесса взлома защиты по полученным экспериментально попыткам и времени этих попыток взлома. Оценка многоуровневой работающей технической защиты информации осуществляется через эквивалентную ей одноуровневую защиту, которая может сравниваться с эквивалентной проектируемой многоуровневой защитой и определять ее эффективность. Для получения всех параметров эффективной одноуровневой математической модели реального процесса взлома ТЗИ необходимо, как минимум, три реальные попытки и их время взлома защиты. Как правило, после взлома, защита не используется, но параметры взлома становятся известны. Если получить данные трех попыток взлома ТЗИ с одинаковыми параметрами используемой защиты информации, то можно вычислить все необходимые параметры эквивалентной одноуровневой защиты, определяемой математической моделью реального физического процесса взлома. Поскольку, в открытой печати, нет экспериментальных результатов исследования процесса взлома технических защит, то для определения параметров исследуемой ТЗИ воспользовались следующей моделью. Выполнили расчет вероятности взлома с известными исходными параметрами взлома и построили одноуровневую защиту, из нее определили три попытки и их время взлома, направление процесса взлома, интенсивность попыток взлома и другие данные, определяемые из реального процесса взлома. С помощью этих данных была решена обратная задача и были получены все неизвестные параметры исследуемой ТЗИ, с достаточно высокой точностью, совпадающие с исходными данными, заложенными в модели при проектировании защиты.

Ключевые слова: *техническая защита информации, распределение вероятности взлома, математическая модель реального физического процесса взлома защиты, распределение Пуассона, распределение вероятности возможного взлома, реальный процесс взлома, линия направления взлома.*

ВВЕДЕНИЕ

Развитие информационных технологий и глобального информационного пространства требуют создания принципиально новой структуры защиты киберпространства, имеющей оптимальный, необходимый для защиты потенциал и играющий большую роль в экономическом и социальном развитии стран. Защита киберпространства и создание новой структуры защиты требует исследования реальных процессов взлома технической защиты информации (ТЗИ), создание математической модели взлома и новых подходов к оценке проектируемой и состояния работающей защиты информации.

Чтобы исключить возможную утечку информации, применяют различные системы защит [1-6]. Однако основное количество разрабатываемых защит, из-за отсутствия математической модели реального физического процесса взлома, более ориентированы на качественную оценку защиты, хотя некоторые из них и дают некоторую количественную оценку. В работах Б. Журиленко [7-14] достаточно подробно рассмотрены отдельные вопросы реального физического процесса взлома защиты информации, но не дано полное представления о расчетах оценки вероятности взлома ТЗИ с использованием его математической модели в процессе проектирования и анализа конечного состояния работающей ТЗИ.

Таким образом, в настоящее время проблемы кибербезопасности и киберзащиты являются актуальными и приобретают статус ключевых проблем. Следует заметить, что в настоящее время применяемые методы для проектирования и оценки технических защит информации (ТЗИ) не дают представления о реальных физических процессах взлома ТЗИ.

ФОРМУЛИРОВАНИЕ ЦЕЛИ ИССЛЕДОВАНИЙ

Целью работы является получение методологии оценки проектируемой и работающей ТЗИ с

помощью математической модели реального физического процесса взлома [15], что позволит оптимизировать, сравнивать различные виды одно- и многоуровневые защиты информации; исследовать, анализировать ТЗИ при их работе, проектировании и модернизации.

Актуальность работы заключается в том, что получение методологии оценки проектируемой и работающей ТЗИ с помощью математической модели реального физического процесса взлома, позволит осуществить новый подход к проектированию и анализу рабочего состояния и разработке одно- и многоуровневой ТЗИ, опирающийся на вероятностные оценки реальных физических процессов взлома информации.

Научная новизна заключается в разработке новой методологии проектирования, анализа рабочего состояния работающей одно- и многоуровневой ТЗИ с целью экономии финансовых затрат, вкладываемых в защиту, и повышение эффективности защиты информации при ее проектировании и использовании.

Задача исследования – разработка методологии и способа анализа распределений вероятностей взлома ТЗИ с учетом математической модели реального физического процесса взлома.

Объект исследования – процесс технической защиты информации.

Предмет исследования – оценка вероятностной надежности ТЗИ с учетом математической модели реального физического процесса взлома.

Методы исследования – основываются на математическом представлении реального процесса взлома защиты информации.

ПОСТАНОВКА И РЕШЕНИЕ ПРОБЛЕМЫ

В работе [15] представлена математическая модель реального физического процесса взлома защиты информации в виде выражений распределений вероятности и максимума вероятности взлома. В модели учитываются зависимости вероятности взлома: от вложенного в ТЗИ финансирования; от коэффициента эффективности построенной защиты; от направления попыток и времени этих попыток взлома; от вероятности возникновения той или иной попытки взлома; от вероятности взлома цифрового или другого кода. С помощью этой модели можно учесть и другие физические процессы, влияющие на вероятность защиты информации. Для этого необходимо знать вероятность влияния этого процесса на взлом защиты и учесть ее в формуле математической модели взлома защиты.

Следует заметить, что расчеты вероятности взлома, при оценке состояния проектируемой и работающей защиты, могут отличаться между собой в зависимости от требований поставленной задачи и исходных данных. Для расчета оценки вероятности взлома проектируемой защиты все исходные параметры для защиты могут быть известны. Тогда в выражение для математической модели реального процесса взлома достаточно будет подставить эти исходные параметры. С другой стороны, возможна ситуация, когда необходимо оценить проектируемую защиту на определенную попытку взлома или когда работающая ТЗИ была взломана и необходимо оценить и сравнить ее реальные параметры с проектируемой защитой. В случае взлома количество исходных данных будет ограничено. При реальном взломе ТЗИ могут быть известны только направление взлома, попытки и их время взлома.

Поскольку задача проектирования ТЗИ с известными исходными данными является достаточно простой и требует элементарных расчетов [15], то рассмотрим вторую обратную задачу с ограниченным количеством данных, которые могут быть получены из реальных попыток взлома.

В этом случае можно и необходимо провести анализ взломанной одно- или многоуровневой ТЗИ с оценкой параметров через одноуровневую защиту, чтобы сравнить их с параметрами проектируемой защиты [14]. Сравнение проектируемых и реальных параметров защит позволит улучшить используемые и создать новые ТЗИ.

Воспользуемся выражением математической модели физического процесса взлома ТЗИ, полученной в работе [15]

$$P_{взл}(m,t,n) = P_{взл}(m,t) \cdot P_m(t) \cdot P(n). \qquad (1)$$

Рассмотрим, что представляют собой вероятности, представленные произведением.

$P_m(X)$ – вероятность взлома от вложенного в защиту финансирования.

$$P_m(X) = \frac{X^X}{(1+X)^{1+X}} \cdot \qquad (2)$$

$X=x/H$ – приведенное вложенное в защиту финансирование; x – величина вложенного в защиту финансирования (например, в денежных единицах); H – финансовые потери без ТЗИ (в таких же денежных единицах).

Выражение для распределения вероятности взлома без учета вероятности возникновения этих попыток взлома будет иметь вид

$$P_{взл} = \{P_m(X) \cdot [\frac{f(m,t)}{f(m,t)+t}]^{\frac{f(m_c,t_c)}{t_c}} \cdot [\frac{t}{f(m,t)+t}]\}^{\gamma}, \quad (3)$$

и, соответственно, зависимости функции $f(m,t)$ от направления взлома m_1, t_1, m_2, t_2 и текущих координат m,t в том же выбранном направлении от текущих координат t и m:

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

$$\omega = \frac{t_2 - t_1}{m_2 - m_1}. \qquad (3а)$$

Сама же функция для распределения вероятности взлома в зависимости от направления времени и попытки взлома, выраженной через параметры конкретной максимальной попытки взлома, например, при максимуме взлома в координатах $m=m_c$, $t=t_c$, имеют вид:

$$f(m_c,t_c) = [t_1 + \frac{t_2 - t_1}{m_2 - m_1} \cdot (m_c - m_1)] \cdot (m_c - 1). \quad (4)$$

Коэффициент эффективности (γ) построенной защиты будет

$$\gamma = \frac{x}{x+H} = \frac{X}{1+X}. \qquad (5)$$

Вероятность процесса взлома (попыток и времени взлома) может быть описана распределением Пуассона, и полностью соответствует реальному физическому процессу взлома ТЗИ. Поскольку процесс взлома начинается с $m=1$, то распределение Пуассона для попыток взлома нужно записать в виде:

$$P_m(t) = \frac{(\lambda \cdot t)^{m-1}}{(m-1)!} \cdot e^{-\lambda \cdot t}. \lambda = \frac{m_2 - m_1}{t_2 - t_1}. \qquad (6)$$

Количество возможных цифровых кодов, используемых для защиты информации может быть вычислено с помощью формулы количества размещений $A^m_n = n^m$. В случае, когда из n цифр необходимо выбрать один код, то необходимо сделать $A^n_n = n^n$ раз возможных попыток взлома. Вероятность угадать нужный цифровой код будет

$$P(n) = (A^n_n)^{-1} = (n^n)^{-1}. \qquad (7)$$

Вероятность реального взлома ТЗИ на конкретной попытке определяется выражением:

$$P_{взл} = 1/m_в. \qquad (8)$$

Выражения (1-7) описывают распределение вероятности взлома с помощью математической модели физического процесса взлома.

В процессе работы ТЗИ возможен взлом защиты с вероятностью взлома определяемой выражением (8). Если выражение (8) приравнять выражению (1), то можно найти параметры реальной ТЗИ для одно- или многоуровневой защиты, которая будет определена через одноуровневую защиту [14]. Для того чтобы определить параметры спроектированной одно- или многоуровневой защиты, работающей в реальных условиях, необходимо решить обратную задачу с одноуровневой защитой и ограниченным количеством известных при взломе данных.

При реальном процессе взлома ТЗИ, как и в работе [7], можно определить направление попыток взлома, фиксируя попытки и время этих попыток взлома, то есть m_1, t_1, m_2, t_2 и так далее; можно определить интенсивность попыток взлома (требования или заявки) - λ (6) и величину обратную интенсивности взлома $\omega = 1/\lambda$, которая определяет функцию распределения вероятности взлома $f(m,t)$ (3а) от направления попыток взлома m_1, t_1, m_2, t_2 и текущих координат m, t. В реальных условиях взлома определяется также сама попытка взлома и ее время $m_в$, $t_в$. Если известно, что использовалась одна и та же спроектированная одно- или многоуровневая защита системы и направление взлома, то имея несколько попыток реального взлома систем, можно определить па-

раметры и построить эквивалентную одноуровневую поверхность вероятности взлома ТЗИ.

В качестве примера расчета параметров для эквивалентной одноуровневой ТЗИ рассмотрим одноуровневую защиту, которая описывается уравнением (1). Для этого предварительно построим поверхность распределения вероятности взлома, а затем решим обратную задачу.

Для построения поверхности вероятности взлома возьмем следующие параметры. Направление взлома будет определяться $m_1=1$, $t_1=0$, $m_2=9$, $t_2=6$; максимум вероятности взлома в выбранном направлении будет $m_c=9$, $t_c=6$; приведенное вложенное в защиту финансирование $X=0,1$; вероятность взлома от вложенного в защиту финансирования $P_m(X)=0,715267$; коэффициент эффективности $\gamma=0,090909$; интенсивность попыток взлома или среднее число событий поступающих в систему массового обслуживания в единицу времени при взломе ТЗИ $\lambda=1,333333$ или $\omega=0,75$; в данных вычислениях не будем вводить цифровой код, поэтому вероятность взлома при отсутствии кода будет $P(n)=1$.

Из приведенных исходных данных степень в выражении (3) будет $\alpha = \frac{f(m_c,t_c)}{t_c} = 8$. На основании выбранных исходных данных строим поверхность вероятности взлома.

На рис.1*а* темной поверхностью представлено распределение вероятности взлома ТЗИ по формуле (1), а светлой распределение реального процесса взлома по формуле (8). Линией 1 указано направление процесса взлома. На рис.1*в* представлены эти же поверхности в проекции сверху.

На рис.1*в* пересечение поверхностей указывает на вероятность взлома ТЗИ. Линия 1 определяет максимум вероятности взлома ТЗИ. В рабочих условиях при разных реальных направлениях взлома будет лишь одна точка взлома, связанная с направлением взлома и параметрами, заложенными при проектировании.

В этом случае, в реальных условиях после взлома ТЗИ ее дальнейшее использование не имеет смысла. Нужна другая защита или ее модификация.

Для решения уравнения (1) необходимы 3 значения попыток и их времени взлома, то есть нужно иметь, как минимум, 3 взлома одной и той же защиты, но для разных потребителей ТЗИ. Имея 3 точки с реальными направлениями взлома, можно определить параметры используемой ТЗИ через одноуровневую защиту информации.

Поскольку, в открытой печати, нет экспериментальных результатов исследования процесса взлома ТЗИ, то для определения параметров взломанной ТЗИ воспользуемся следующей моделью. На рис.1*b* выберем три точки на пересечении серой и светлой поверхностей, точках равных вероятностей взлома. В этом случае имеем заложенные при проектировании параметры и направление взлома.

Первая точка соответствует первому взлому по направлению линии 1 – $m_{в1}=10,649$, $t_{в1}=7,22644$. Вторую и третью точку взлома выберем по линии пересечения темной и светлой поверхностей: $m_{в2}=25,0$, $t_{в2}=21,3197$; $m_{в3}=23,0358$, $t_{в3}=13,88$ соответственно.

Эти три и более значения, которые можно контролировать в процессе защиты информации и могут быть известны из экспериментальных данных разных потребителей ТЗИ. Таким образом, получим уравнения (1) с координатами этих 3 точек.

Выражение (1) для одного из значений взлома можно записать в виде:

$$\{P_m(X)\cdot[\frac{f(m_{в1},t_{в1})}{f(m_{в1},t_{в1})+t_{в1}}]^{\alpha}\cdot[\frac{t_{в1}}{f(m_{в1},t_{в1})+t_{в1}}]\}^{\gamma}\cdot P(n)= \frac{1}{m_{в1}\cdot\frac{(\lambda\cdot t_{в1})^{m_{в1}-1}}{(m_{в1}-1)!}\cdot e^{-\lambda\cdot t_{в1}}} \quad (9)$$

И аналогично для двух остальных точек

$$\{P_m(X)\cdot[\frac{f(m_{в2},t_{в2})}{f(m_{в2},t_{в2})+t_{в2}}]^{\alpha}\cdot[\frac{t_{в2}}{f(m_{в2},t_{в2})+t_{в2}}]\}^{\gamma}\cdot P(n)= \frac{1}{m_{в2}\cdot\frac{(\lambda\cdot t_{в2})^{m_{в2}-1}}{(m_{в2}-1)!}\cdot e^{-\lambda\cdot t_{в2}}} \quad (9а)$$

$$\{P_m(X)\cdot[\frac{f(m_{в3},t_{в3})}{f(m_{в3},t_{в3})+t_{в3}}]^{\alpha}\cdot[\frac{t_{в3}}{f(m_{в3},t_{в3})+t_{в3}}]\}^{\gamma}\cdot P(n)= \frac{1}{m_{в3}\cdot\frac{(\lambda\cdot t_{в3})^{m_{в3}-1}}{(m_{в3}-1)!}\cdot e^{-\lambda\cdot t_{в3}}} \quad (9б)$$

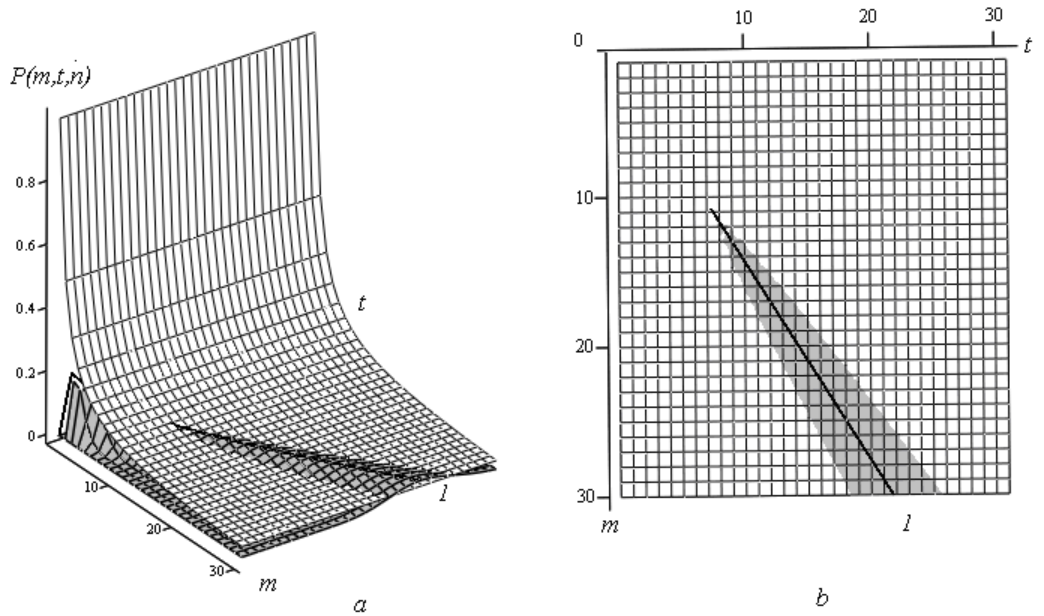

Рис.1 Поверхности распределений: серая – вероятность взлома ТЗИ; светлая – вероятность реального взлома защиты

Для выражений (9), (9а), (9б) вероятность для выбранного цифрового кода в расчетах поверхности распределения вероятности взлома (рис.1) было принято $P(n)=1$ и $\lambda = \frac{m_2 - m_1}{t_2 - t_1} = 1{,}333333$.

При решении обратной задачи в выражениях (9), (9а), (9б) неизвестными будут α, γ, $P_m(X)$ и $P(n)$. Следует заметить, что γ и $P_m(X)$ связаны между собой через приведенное вложенное в защиту финансирование X уравнения (2) и (5), и вероятность взлома от приведенного вложенного в защиту финансирования $P_m(X)$ может быть определена через коэффициент эффективности вложенного в защиту финансирования γ.

$$P(X) = \frac{(\frac{\gamma}{\gamma-1})^{\frac{\gamma}{\gamma-1}}}{(\frac{1}{1-\gamma})^{\frac{1}{1-\gamma}}}. \qquad (10)$$

Таким образом, из 4 неизвестных параметров остаются только 3, поэтому достаточно трех уравнений, чтобы определить все остальные параметры одноуровневой ТЗИ.

Чтобы определить параметры защиты информации через одноуровневую ТЗИ прологарифмируем выражения (9), (9а) и (9б)

$$\begin{aligned}
&\gamma \cdot ln(P_m(X)) + ln(P(n)) + \\
&\gamma \cdot \alpha \cdot ln(\frac{f(m_{в1}, t_{в1})}{f(m_{в1}, t_{в1}) + t_{в1}}) + \\
&\gamma \cdot ln(\frac{t_{в1}}{f(m_{в1}, t_{в1}) + t_{в1}}) = \\
&= ln(\frac{1}{m_{в1} \cdot \frac{(\lambda \cdot t_{в1})^{m_{в1}-1}}{(m_{в1}-1)!} \cdot e^{-\lambda \cdot t_{в1}}}) \\
&\gamma \cdot ln(P_m(X)) + ln(P(n)) + \\
&\gamma \cdot \alpha \cdot ln(\frac{f(m_{в2}, t_{в2})}{f(m_{в2}, t_{в2}) + t_{в2}}) + \\
&\gamma \cdot ln(\frac{t_{в2}}{f(m_{в2}, t_{в2}) + t_{в2}}) = \qquad (11) \\
&= ln(\frac{1}{m_{в2} \cdot \frac{(\lambda \cdot t_{в2})^{m_{в2}-1}}{(m_{в2}-1)!} \cdot e^{-\lambda \cdot t_{в2}}}) \\
&\gamma \cdot ln(P_m(X)) + ln(P(n)) + \\
&\gamma \cdot \alpha \cdot ln(\frac{f(m_{в3}, t_{в3})}{f(m_{в3}, t_{в3}) + t_{в3}}) + \\
&\gamma \cdot ln(\frac{t_{в3}}{f(m_{в3}, t_{в3}) + t_{в3}}) = \\
&= ln(\frac{1}{m_{в3} \cdot \frac{(\lambda \cdot t_{в3})^{m_{в3}-1}}{(m_{в3}-1)!} \cdot e^{-\lambda \cdot t_{в3}}})
\end{aligned}$$

Введем следующие обозначения:

$$y1=\gamma\cdot\ln(P_m(X))+\ln(P(n));\qquad y2=\gamma\cdot\alpha;$$

$$y3=\gamma.$$

$$A1=\ln(\frac{f(m_{в1},t_{в1})}{f(m_{в1},t_{в1})+t_{в1}});$$

$$B1=\ln(\frac{t_{в1}}{f(m_{в1},t_{в1})+t_{в1}});$$

$$C1=\ln(\frac{1}{m_{в1}\cdot\frac{(\lambda\cdot t_{в1})^{m_{в1}-1}}{(m_{в1}-1)!}\cdot e^{-\lambda\cdot t_{в1}}});$$

$$A2=\ln(\frac{f(m_{в2},t_{в2})}{f(m_{в2},t_{в2})+t_{в2}});$$

$$B2=\ln(\frac{t_{в2}}{f(m_{в2},t_{в2})+t_{в2}});$$

$$C2=\ln(\frac{1}{m_{в2}\cdot\frac{(\lambda\cdot t_{в2})^{m_{в2}-1}}{(m_{в2}-1)!}\cdot e^{-\lambda\cdot t_{в2}}});$$

$$A3=\ln(\frac{f(m_{в3},t_{в3})}{f(m_{в3},t_{в3})+t_{в3}});$$

$$B3=\ln(\frac{t_{в3}}{f(m_{в3},t_{в3})+t_{в3}});$$

$$C3=\ln(\frac{1}{m_{в3}\cdot\frac{(\lambda\cdot t_{в3})^{m_{в3}-1}}{(m_{в3}-1)!}\cdot e^{-\lambda\cdot t_{в3}}}).$$

Система уравнений (11) в новых обозначениях будет иметь вид:

$$\begin{aligned}&y1+y2\cdot A1+y3\cdot B1=C1;\\&y1+y2\cdot A2+y3\cdot B2=C2;\\&y1+y2\cdot A3+y3\cdot B3=C3.\end{aligned}\qquad(12)$$

Решаем эту систему уравнений методом Гаусса, получим:

$$\begin{aligned}&y1+y2\cdot A1+y3\cdot B1=C1;\\&y2+y3\cdot\frac{B1-B2}{A1-A2}=\frac{C1-C2}{A1-A2};\\&y3=\frac{\frac{C1-C2}{A1-A2}-\frac{C1-C3}{A1-A3}}{\frac{B1-B2}{A1-A2}-\frac{B1-B3}{A1-A3}}.\end{aligned}\qquad(13)$$

Из выражения (13) определяем коэффициент эффективности вложенного в защиту финансирования *y3=γ=0,09086 (γ=0,090909); y2=a·γ= 0,72653; a=7,99612 (a=8).* В соответствии с (10) определяем *P(X)=0,715369 (P(X)=0,715267).* В скобках приведены параметры, которые использовались для построения распределения вероятности ТЗИ.

С помощью выражения (5) определяем приведенное вложенное в защиту финансирование *X=0,09994 (X=0,1).* Учитывая, что в точке максимума попытки взлома в направлении взлома $a=m_c-1=7,99612$ $(m_c-1=8)$, максимум попытки взлома будет при $m_c=8,99612$ $(m_c=9)$. Вычислить время максимума попытки взлома можно с помощью формулы

$$\alpha=\frac{f(m_c,t_c)}{t_c}=[(m_1-1)+\frac{m_2-m_1}{t_2-t_1}\cdot(t_c-t_1)]=7,99612\qquad(14)$$

Вычисления дают $t_c=5,99709$ $(t_c=6)$. Осталось вычислить вероятность примененного кода *P(n).* Для этого воспользуемся первым уравнением из (13), учитывая, что $y1=\gamma\cdot\ln(P_m(X))+\ln(P(n))$.

Получим выражение

$$\gamma\cdot\ln(P_m(X))+\ln(P(n))+\alpha\cdot\gamma\cdot A1+\gamma\cdot B1=C1,$$

в котором *P(n)* неизвестно и, вычисляя его, получим *P(n)=0,908781 (P(n)=1).* В данном случае ошибка в определении вероятности взлома кода составляет 9,12%. Однако, следует заметить, что в простейшем случае, если нужно угадать код, например, 1 или 2, то вероятность правильного угадывания кода будет 0,5. В данных вычислениях вероятность составляет 0,9, что ближе к единице. Требуются дальнейшие исследования, чтобы выяснить, почему вычисления дали значение с ошибкой в 9,12%, а не более близкое к вероятности равной единице.

Остальные неизвестные параметры ТЗИ были определены со следующей точностью: коэффициент эффективности защиты γ – 0,054%; вероятность взлома от вложенного в защиту финансирования *P(X)* – 0,014%; попытка, при которой будет максимальное значение вероятности взлома в направлении процесса взлома, m_c – 0,043%; время, при котором будет максимальное значение вероятности взлома в направлении

процесса взлома, t_c – 0,049%; приведенное вложенное в защиту финансирование X – 0,06%.

ВЫВОДЫ

В результате выполненной работы с помощью одноуровневой математической модели физического процесса взлома ТЗИ, показана возможность определения всех неизвестных параметров этой модели по попыткам и времени этих попыток процесса взлома. Такой подход позволит по экспериментальным данным определять все параметры сложной многоуровневой системы ТЗИ через эквивалентную одноуровневую систему. Это позволит сравнивать проектируемые и работающие сложные системы защит и определять более эффективную защиту. В результате исследований были с достаточно высокой точностью определены неизвестные параметры ТЗИ такие как: коэффициент эффективности защиты γ – 0,054%; вероятность взлома от вложенного в защиту финансирования $P(X)$ – 0,014%; попытка максимального значения вероятности взлома в направлении процесса взлома, m_c – 0,043%; время, максимального значения вероятности взлома в направлении процесса взлома, t_c – 0,049%; приведенное вложенное в защиту финансирование X – 0,06%. Неясным остается вопрос, почему вероятность цифрового кода, которая была равна единице (то есть кода не было) дала достаточно большой процент ошибки вероятности взлома порядка $P(n)$ - 9,12%. С другой стороны эта точность ближе к единице, чем к вероятности 0,5 (44,98%), которая будет при угадывании простейшего цифрового кода, который состоит из двух однозначных цифр. Возможно, процент ошибки будет меньше при использовании вероятности кода намного меньше единицы. Следует заметить, что этот вопрос требует дальнейших исследований.

ЛИТЕРАТУРА

[1] Tawfik Mudarri, Samer Abdo AL-RABEEI,: Security fundamentals: access control models. *International journal of interdisciplinary in theory and practice*, ITPB - NR.: 7, 2015. - pp. 259-262.

[2] Jerome H. Saltzer, Michael D. Schroeder.: *The Protection of Information in Computer Systems*. URL: https://www.cs.virginia.edu/~evans/cs551/saltzer/.

[3] Bokova O. I., Drovnikov I. G., Popov A. D., Rogozin E. A.: *Model of the process of functioning of the information protection system from unauthorized access created in the software environment of imitation modeling "CPN TOOLS"*. URL: https://www.researchgate.net/publication/334492982_MODEL_OF_ THE_PROCESS_OF_FUNCTIONING_OF_THE_INFORMATION_PROTECTION_SYSTEM_FROM_UNAUTHORIZED_ACCESS_CREATED_IN_THE_SOFTWARE_ENVIRONMENT_OF_IMITATION_MODELING_CPN_TOOLS.

[4] Jerome H. Saltzer, Michael. Schroeder.: *The Protection of Information in Computer Systems*. URL: https://www.cl.cam.ac.uk/teaching/1011/R01/75-protection.pdf.

[5] Albert Caballero.: *Information Security Essentials for IT Managers: Protecting Mission-Critical Systems*. https://booksite. elsevier.com/samplechapters/97815974 95332/02~Chapter_1.pdf.

[6] Pierangela Samarati, Sabrina de Capitani di Vimercati.: *Access Control: Policies, Models, and Mechanisms*. URL: https://link.springer.com/content/pdf/10.1007%2F3-540-45608-2_3.pdf.

[7] Zhurilenko B.E.: Design method and evaluation of a single operational technical protection of information in the selected hacking direction. *Zahist Information*, vol 21, 2019. - pp. 143-149.

[8] Vasyanin V., Zhurilenko B., Nikolaev N et al.: *Information control systems and technologies. Problems and solutions*: monograph. Ecology, Odessa, 2019.

[9] Zhurilenko B.E.: The method of designing a single system of technical protection of information with probabilistic reliability and specified hacking parameters. *Bezpeka Information*, vol 20, 2014. - pp. 36-42.

[10] Zhurilenko B.E.: Estimation of financial costs for building an information protection system. *Zahist Information*, vol 20, 2018. - pp. 231-239.

[11] Borys Zhurylenko, Kirill Nikolaev Combined Multi-Level Information Protection with Probability Reliability *Proceedings of the 9th International Conference "Information Control Systems & Technologies"* Odessa, Ukraine, September 24–26, 2020 - pp. 241 – 251.

[12] Borys Zhurylenko, Kirill Nikolaev Combined Multi-Level Information Protection With Probability Reliability *Proceedings of the 9th International Conference "Information Control Systems & Technologies"* Odessa, Ukraine, September 24–26, 2020 - pp. 241 – 251.

[13] Borys Zhurylenko. *Design with Preset Parameters and Reliability Assessment of Single Level Personal Data Protection System*/ B. Zhurylenko, K. Nikolaev, M. Aleksander // CEUR-WS: 19-Aug-2020, pp. 838-849, http://ceur-ws.org/Vol-2654/.

[14] Zhurilenko B.E. Nikolaev K.I/.: Sequential two-level information protection with probability reliability. *Zahist Information*, vol 22, 2020. - pp. 21-26.

[15] Журиленко Б.Е. Математическая модель физического процесса взлома технической защиты

информации/ Б.Е. Журиленко, К.И. Николаев, Л.В. Рябова // *Захист інформації*, том.23, №3, 2021. - с.167-176.

ASSESSMENT OF DESIGNED AND OPERATING TECHNICAL PROTECTION OF INFORMATION USING A MATHEMATICAL MODEL OF THE REAL PHYSICAL PROCESS OF HACKING PROTECTION

This paper shows the possibility of assessing the designed and operating technical information security (TIS) using a mathematical model of the real physical process of breaking the protection according to the experimentally obtained attempts and the time of these attempts to break. Evaluation of multi-level operating technical information protection is carried out through an equivalent single-level protection, which can be compared with the equivalent projected multi-level protection and determine its effectiveness. To obtain all the parameters of an effective single-level mathematical model of the real process of breaking TIS, at least three real attempts and their time of breaking the protection are required. Usually protection after hacking is not used, but the hacking parameters become known. If we obtain the data of three attempts to hack TIS with the same parameters of the used information protection, then it is possible to calculate all the necessary parameters of the equivalent one-level protection determined by the mathematical model of the real physical process of hacking. Since, in the open press, there are no experimental results of the study of the process of cracking technical protection, the following model was used to determine the parameters of the investigated TIS. We calculated the probability of hacking with known initial hacking parameters and built a one-level protection, from which we determined three attempts and their time of hacking, the direction of the hacking process, the intensity of hacking attempts and other data that can be determined from the real hacking process. With the help of these data, the inverse problem was solved and all unknown parameters of the investigated TIS were obtained, with a sufficiently high accuracy, coinciding with the initial data laid down in the model when designing the protection.

Key words: technical information security, hacking probability distribution, mathematical model of a real physical process of security cracking, Poisson distribution, probability distribution of possible hacking, real hacking process, hacking direction line.

ОЦІНКА ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ, ЩО ПРОЕКТУЄТЬСЯ ТА ПРАЦЮЄ, ЗА ДОПОМОГОЮ МАТЕМАТИЧНОЇ МОДЕЛІ РЕАЛЬНОГО ФІЗИЧНОГО ПРОЦЕСУ ЗЛАМУ ЗАХИСТУ

У даній роботі показана можливість оцінки проектованого та працюючого технічного захисту інформації (ТЗІ) за допомогою математичної моделі реального фізичного процесу зламу захисту за експериментально отриманими спробами та часом цих спроб зламу. Оцінка багаторівневого працюючого технічного захисту інформації здійснюється через еквівалентний їй однорівневий захист, який може порівнюватися з еквівалентним проектованим багаторівневим захистом і визначати його ефективність. Для отримання всіх параметрів ефективної однорівневої математичної моделі реального процесу зламу ТЗІ необхідно, як мінімум, три реальні спроби та їх час зламу захисту. Зазвичай захист після зламу не використовується, але параметри зламу стають відомими. Якщо отримати дані трьох спроб зламу ТЗІ з однаковими параметрами захисту інформації, то можна обчислити всі необхідні параметри еквівалентного однорівневого захисту, що визначаються математичною моделлю реального фізичного процесу зламу. Оскільки, у відкритій пресі, немає експериментальних результатів дослідження процесу зламу технічних захистів, то для визначення параметрів досліджуваної ТЗІ скористалися наступною моделлю. Виконали розрахунок ймовірності зламу з відомими вихідними параметрами зламу та побудували однорівневий захист, з нього визначили три спроби та їх час зламу, напрямок процесу зламу, інтенсивність спроб зламу та інші дані, які можуть бути визначені з реального процесу зламу. За допомогою цих даних було вирішено обернене завдання і були отримані всі невідомі параметри досліджуваної ТЗІ, з досить високою точністю, що збігаються з вихідними даними, закладеними в моделі при проектуванні захисту.

Ключові слова: технічний захист інформації, розподіл ймовірності зламу, математична модель реального фізичного процесу зламу захисту, розподіл Пуассона, розподіл ймовірності можливого зламу, реальний процес зламу, лінія напряму зламу.

Журиленко Борис Евгеньевич, кандидат физико-математических наук, доцент кафедры автоматизации и энергоменеджмента Национального авиационного университета.
E-mail: zhurylenko@gmail.com.
Orcid ID: 0000-0003-2980-5630.
Журиленко Борис Євгенович, кандидат фізико-математичних наук, доцент кафедри автоматизації та енергоменеджменту Національного авіаційного університету.
Zhurilenko Boris, Candidate of Physical and Mathematical Sciences, assistant professor of automation and energy management Department of the National Aviation University.