shielded rooms for research. In addition, it is shown how to calculate the spectrum of information leakage signals in the form of white-black stripes, horizontal and vertical blank impulses. The calculations are presented for signals from video cards of personal computer monitors in a simplified two-tone form of a static image, for an infinite analysis time. The creation of test images in the form of 54, 56, 58, 60, 62 white-black stripes and calculations of the spectra of information leakage signals for a monitor screen of 1024 by 768 pixels with a vertical frequency of 60 Hz and test images with 54, 58 and 62 white-black stripes. The scanning of the spectrum of signals of information leakage from the screens of monitors on the crystal structures and statistical processing of the results of measurements of the spectral characteristics of the signals is carried out. A conclusion is made about the consistency of the adopted signal model for further studies of spurious emissions from images on the monitor screen in the form of texts.

Keywords: spurious electromagnetic radiation, monitor screens based on rare crystal structures, Fourier coefficients, SDR - receivers, relative measurement error.

Євграфов Дмитро Вікторович, здобувач наукового ступеня доктор технічних наук Вінницького національного технічного університету.
E-mail: ramgraf@bigmir.net.
Orcid ID: 0000-0001-9651-1558.
Евграфов Дмитрий Викторович, соискатель научной степени доктор технических наук Винницкого национального технического университета.
Yevgrafov Dmutro Viktorovych, applicant for a scientific degree, Doctor of Technical Sciences, Vinnytsia National Technical University.

Яремчук Юрій Євгенович, директор Центру інформаційних технологій та захисту інформації, професор кафедри менеджменту та безпеки інформаційних систем Вінницького національного технічного університету.
E-mail: yurevyar@vntu.edu.ua.
Orcid ID: 0000-0002-6303-7703.
Яремчук Юрий Евгеньевич, директор Центра информационных технологий и защиты информации, профессор кафедры менеджмента и безопасности информационных систем Винницкого национального технического университета.
Yaremchuk Yurii, Director of the Center for Information Technologies and Information Protection, Professor of the Department of Management and Security of Information Systems, Vinnytsia National Technical University.

DOI: 10.18372/2410-7840.23.16405
УДК 004.056.5(045)

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ФИЗИЧЕСКОГО ПРОЦЕССА ВЗЛОМА ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Борис Журиленко, Кирилл Николаев, Любовь Рябова

В данной работе представлена математическая модель физического процесса взлома технической защиты информации (ТЗІІ). Математическая модель базируется на работах Б.Журиленко, в которых используются: вложенное в защиту финансирование, коэффициент эффективности защиты и направление взлома. Математическая модель строилась с учетом распределения Пуассона, используемого в теории массового обслуживания. Распределение Пуассона позволяет учесть вероятность появления той или иной попытки и ее времени взлома защиты информации. Проведенные исследования показали, что, в случае отсутствия финансирования в защиту, вероятность взлома будет определяться только распределением Пуассона и вероятностью взлома применяемой защиты. При наличии финансирования в защиту информации, наблюдаются различия между распределениями вероятности и максимума вероятности взлома, причем распределение вероятности взлома имеет максимальное значение в определенной точке, а распределение максимумов вероятности взлома носит экспоненциальный характер. Кроме того, эти распределения имеют остронаправленный характер с максимальным значением вероятности по направлению линии взлома. Значения вероятностей падают при удалении от линии направления взлома, увеличении координат взлома и времени. В случае отличия реального направления взлома от проектируемого вероятность максимального значения возможного взлома ТЗІІ изменяется. Показано, что в этом случае вероятность возможного взлома падает, так как уменьшается площадь пересекающихся поверхностей вероятностей реального и возможного взломов. В математическую модель физического процесса взлома ТЗІІ введено выражение, определяющее вероятность взлома предполагаемой защиты. Таким образом, в результате выполненной работы получена математическая модель физического процесса взлома ТЗІІ, которая описывается такими параметрами: вложенным в защиту финансированием, эффективностью вложенного в защиту финансирования, направлением попыток взлома и их интенсивностью, вероятностью появления той или иной попытки взлома и вероятностью взлома предполагаемой ТЗІІ.

Ключевые слова: *техническая защита информации, распределение вероятности взлома, распределение максимума вероятности взлома защиты, распределение Пуассона, распределение вероятности возможного взлома, реальный процесс взлома, линия направления проектируемого взлома, линия направления реального взлома.*

ВВЕДЕНИЕ

Развитие информационных технологий и глобального информационного пространства создали принципиально новую структуру – киберпространство, имеющее неограниченный потенциал, играющее все большую роль в экономическом и социальном развитии стран. Создание киберпространства привело к новому типу угроз – киберугрозы. Проблемы кибербезопасности и киберзащиты являются актуальными и приобретают статус ключевых проблем. Поскольку информация циркулирует в достаточно сложных технических и компьютерных системах, то ее утечка будет определяться физическими и техническими взаимодействиями этих систем. Чтобы исключить возможную утечку информации применяют различные системы защит [1-6]. Однако основное количество разрабатываемых защит более ориентированы на качественную оценку защиты, хотя некоторые из них дают и количественную оценку. Следует заметить, что в настоящее время применяемые методы для проектирования и оценки технических защит информации (ТЗИ) не дают представления о физических процессах взлома ТЗИ. В работах Б. Журиленко [7-13] достаточно подробно рассмотрены определенные вопросы физического процесса взлома защиты информации, но не дано полного представления о самом физическом процессе взлома ТЗИ и его математической модели.

ФОРМУЛИРОВАНИЕ ЦЕЛИ ИССЛЕДОВАНИЙ

Целью работы является получение математической модели физического процесса взлома ТЗИ, что позволит исследовать, анализировать, сравнивать различные виды одно- и многоуровневых защит информации при их проектировании и модернизации.

Актуальность работы заключается в том, что создание математической модели физического процесса взлома в отличие от нормативных документов, позволит осуществить новый подход к анализу рабочего состояния и разработке одно- и многоуровневой ТЗИ, опирающийся на реальные физические процессы взлома информации.

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

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

Объект исследования – процесс технической защиты информации. *Предмет исследования* – распределение вероятностной надежности ТЗИ с учетом математической модели физического процесса взлома. *Методы исследования* – основываются на математическом представлении реального процесса взлома защиты информации.

ПОСТАНОВКА И РЕШЕНИЕ ПРОБЛЕМЫ

Исследования, проведенные в работах [7-13], позволили рассмотреть отдельные вопросы физического процесса взлома и получить выражения распределений вероятности и максимума вероятности взлома в зависимости: от вложенного в ТЗИ финансирования (x); от коэффициента эффективности построенной защиты (γ); от направления попыток и времени этих попыток взлома. Выражение для распределения вероятности взлома без учета попыток их возникновения будет иметь вид:

$$P_{взл} = \{ P_m(X) \cdot [\frac{f(m,t)}{f(m,t)+t}]^{\frac{f(m_c,t_c)}{t_c}} \cdot [\frac{t}{f(m,t)+t}] \}^{\gamma}, \quad (1)$$

и выражение для распределения максимума вероятности взлома:

$$P_{взл} = \{ P_m(X) \cdot [\frac{f(m,t)}{f(m,t)+t}]^{\frac{f(m,t)}{t}}, \quad [\frac{t}{f(m,t)+t}]\}^{\gamma}, \qquad (1a)$$

где $f_1(m,t)$, $f_1(m_c,t_c)$ – функции, присущие данной системе защиты, определяющие ее защитные свойства в зависимости от направления взлома m_1, t_1, m_2, t_2 и текущих координат m,t. $X=x/H$ – 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); $P_m(X)$ – вероятность взлома от вложенного в защиту финансирования:

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

Коэффициент эффективности (γ) построенной защиты будет иметь вид:

$$\gamma = \frac{x}{x+H} = \frac{X}{1+X}. \qquad (3)$$

Сами же функции для распределения вероятности взлома в зависимости от направления времени попытки взлома, выраженной через параметры конкретной максимальной попытки взлома, например, максимум взлома в координатах $m=m_c$, $t=t_c$, имеют вид:

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

то же для распределения вероятности взлома в зависимости от направления попытки взлома:

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

и, соответственно, зависимости функции в том же выбранном направлении от текущих координат t и m:

$$f(t) = f(m,t) = [(m_1-1)+\frac{m_2-m_1}{t_2-t_1}\cdot(t-t_1)]\cdot t, \qquad (5)$$

$$f(m) = f(m,t) = [t_1+\frac{t_2-t_1}{m_2-m_1}\cdot(m-m_1)]\cdot(m-1)\cdot \qquad (5a)$$

Связь между координатами попытки взлома m и временем этой попытки взлома t определяется выражениями, если $m_1=1$ и $t_1=0$ (начальные условия, когда начинается первая попытка взлома при нулевом времени), где зависимость времени взлома от ее попытки будет иметь вид:

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

где $A = t_1 + \frac{m_1-1}{\omega}$, $\omega = \frac{m_2-m_1}{t_2-t_1}$ (6)

и зависимость попытки взлома от ее времени

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

где $B = \omega\cdot t_1 - (m_1-1)$. (6a)

Как уже указывалось ранее выражения (1) и (1a), описывают зависимости вероятностей взлома от вложенного в защиту финансирования и ее эффективности, направления взлома, но эти выражения не дают значение вероятности взлома в отсутствии ТЗИ. При отсутствии ТЗИ коэффициент эффективности защиты равен нулю и вероятности взлома становятся равными единице, что указывает на взлом с первой же попытки. В реальных условиях этого не происходит. В этом случае процесс взлома становится случайным событием, и вероятность взлома становится случайной величиной. Следовательно, эти выражения, кроме вышеперечисленных параметров, должны еще учитывать вероятность возникновения самих попыток взлома в зависимости от интенсивности попыток взлома или параметра λ – частоты появления событий взлома, который в теории массового обслуживания называется интенсивностью требований или заявок [14-15]. Интенсивность попыток взлома λ – среднее число событий, поступающих в систему массового обслуживания в единицу времени при взломе ТЗИ, независимо от наличия вложенного в защиту финансирования. Другими словами, в координатах m и t λ указывает на интенсивность идущего реального процесса взлома, в отличие от интенсивности попыток взлома ω (6), которое определяет направление идущего, проектируемого или планируемого процесса взлома. Их значения могут совпадать $\lambda=\omega$, если реальный процесс взлома идет в проектируемом направлении.

Следуя теории массового обслуживания λ можно определить следующим образом:

$$\lambda = \frac{m^*_2 - m^*_1}{t^*_2 - t^*_1}, \qquad (7)$$

где m^*_1, t^*_1, m^*_2, t^*_2 – определяются средним числом случайных событий или реальных попыток взлома.

В нашем случае процесс взлома является стационарным, то есть λ не зависит от времени, но процесс взлома случайный. Поскольку процесс взлома является стационарным, ординарным и без последствий, то такой процесс может быть описан распределением Пуассона, который полностью соответствует реальному физическому процессу взлома ТЗИ.

Поскольку процесс взлома начинается с m=1, то распределение Пуассона для попыток взлома можно записать в виде:

$$P_m(t) = \frac{(\lambda \cdot t)^{m-1}}{(m-1)!} \cdot e^{-\lambda \cdot t}. \qquad (8)$$

Так как процессы событий, описываемые выражениями (1), (1а) и (8), являются независимыми, то сам процесс взлома ТЗИ может быть представлен формулами:

- для распределения вероятности взлома:

$$P_{взл} = \{ P_m(X) \cdot [\frac{f(m,t)}{f(m,t)+t}]^{\frac{f(m_c,t_c)}{t_c}} \cdot [\frac{t}{f(m,t)+t}] \}^{\gamma} \cdot P_m(t), \qquad (9)$$

- для распределения максимума вероятности взлома:

$$P_{взл} = \{ P_m(X) \cdot [\frac{f(m,t)}{f(m,t)+t}]^{\frac{f(m,t)}{t}} \cdot [\frac{t}{f(m,t)+t}] \}^{\gamma} \cdot P_m(t). \qquad (9а)$$

Выражения (9), (9а) являются составляющими математической модели реального процесса взлома и позволяют описать процесс взлома ТЗИ, опираясь на основные параметры, от которых он зависит.

Рассмотрим условие, когда нет вложенного в защиту финансирования. В этом случае, коэффициент эффективности защиты γ (3) будет равен нулю, следовательно, выражения (9) и (9а) в фигурных скобках, равны единице, то есть вероятности (9) и (9а) будут определяться только распределением Пуассона в направлении взлома. Если реальный процесс взлома выбрать с параметрами m_1=1, t_1=0 и m_2=9, t_2=9; ω=0,889, совпадающими с проектируемым направлением, тогда зависимости распределений вероятности и максимума вероятности взлома могут быть представлены одной поверхностью (рис. 1а).

В этом случае направление взлома будет идти с заявками λ=0,889, указывающими на интенсивность идущего реального процесса взлома в проектируемом направлении. Линия 1 на рис. 1 – это направление проектируемого взлома. В данном случае, распределение Пуассона указывает на вероятность возможного появления попытки и ее времени взлома в зависимости от интенсивности заявки идущего реального процесса взлома ТЗИ. Из рисунка (рис. 1а) видно, что вероятность начального состояния при m=1 и t=0, пока нет взлома, будет равна единице. При дальнейших попытках взлома максимум вероятности их появления приходятся на направление реального (в данном случае проектируемого) взлома и спадает по экспоненциальному закону с увеличением попытки и времени.

Вероятность появления попытки взлома и ее времени постепенно уменьшается при удалении от линии 1, направления проектируемого взлома, а область появления повышенного взлома постепенно расширяется и вероятность уменьшается при удалении от начала координат.

На рис. 1б показана темная область, в которой возможен взлом ТЗИ для выбранных условий. Светлая поверхность – поверхность вероятности реального процесса взлома, которая определяется выражением:

$$P_{взл} = 1/m. \qquad (10)$$

Область, где темная поверхность превышает светлую, является областью с наиболее вероятным взломом ТЗИ. Минимальные параметры попытки взлома в реальных условиях с выбранными исходными данными будут - $m_в$=5, $t_в$=4÷5, в первой точке пересечения темной и светлой поверхностей и линии направления взлома.

Рассмотрим случай, когда в защиту вложено X=0,1 приведенного финансирования, то есть 10% от возможных потерь без защиты. Для этого выбираем то же направление взлома, что и для предыдущего случая: m_1=1, t_1=0; m_2=9, t_2=9;

ω=0,889 и получаем дополнительные параметры: *P(X)*=0,715; γ=0,091; λ=0,889. Проведем расчет по формуле (9), которая описывает распределение проектируемой вероятности взлома ТЗИ, и расчет по формуле (9а), описывающей распределение максимумов вероятности взлома.

На рис. 2а представлена поверхность распределения вероятности взлома проектируемой ТЗИ с параметрами для выбранного случая, а на рис. 2б представлена поверхность распределения максимумов вероятности взлома. Линия 1 идет в направлении и по максимуму вероятности взлома. Из рис. 2а видно, что максимум в распределении вероятности взлома будет в точке с параметрами $m_в$=2, $t_в$=1, $P_{взл}$=0,16, а для распределения максимума вероятности взлома (рис. 2б) в точке $m_в$=1, $t_в$=0 с вероятностью для этого случая $P_{взл}$=0,96, вместо $P_{взл}$=1 для случая отсутствия финансирования.

В работах [7-13] показано, что при проектировании и анализе состояния работающей ТЗИ, важным параметром в направлении проектируемого и реального взлома является первая точка максимума вероятности взлома – это точка одноместного пересечения поверхностей и линии направления взлома.

Для расчета используем параметры предыдущего случая *X*=0,1; m_1=1, t_1=0; m_2=9, t_2=9; ω=0,889 и полученные дополнительные параметры *P(X)*=0,715; γ=0,091.

Проведем расчет по формулам (9а) и (10). На рис. 3 представлены поверхности распределения вероятности (9) и максимумов вероятности взлома (9а) проектируемой ТЗИ с параметрами для выбранного случая. Также на рис. 3 приведена линия 2 возможного реального процесса взлома, отличающегося от планируемого направления (линия 1).

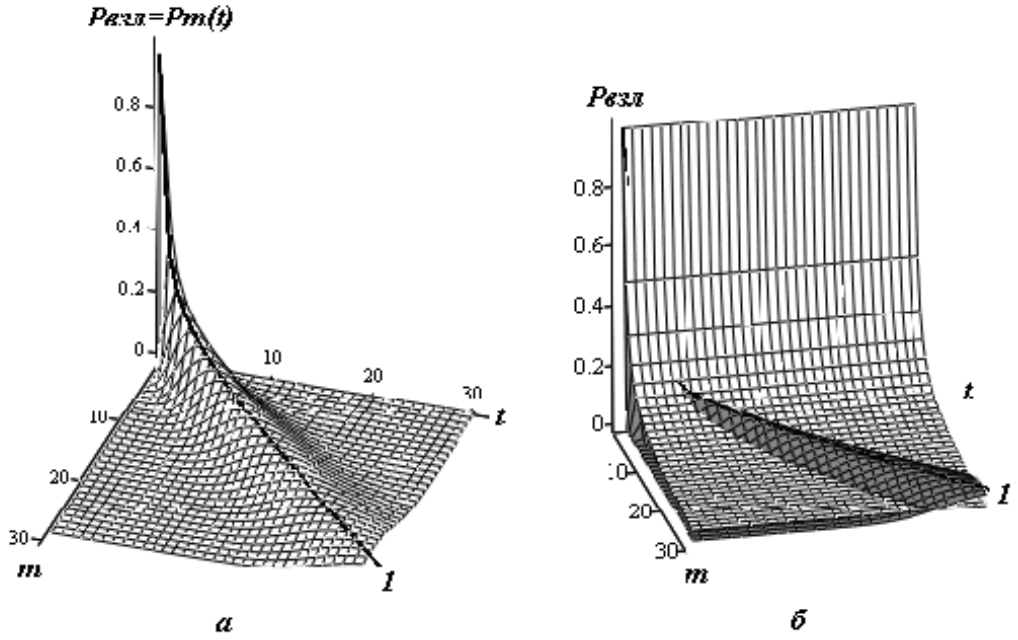

Рис.1 Поверхности распределений вероятности и максимумов вероятности взлома, при отсутствии вложенного в защиту финансирования

На рис. 3а представлена поверхность распределения планируемой вероятности взлома (9) и реального процесса взлома ТЗИ (10). В этом случае взлом возможен при минимальных параметрах $m_в$=11, $t_в$=11.

Координата минимальной точки взлома в этом случае меньше, так как связана с поверхностью, построенной по максимальным значениям вероятности взлома. На рис. 2а значение координаты вероятности реальной точки взлома больше, поскольку поверхность построена по распределению вероятности взлома, максимум которой находится ближе к началу координатных осей ($m_в$=2, $t_в$=1), следовательно, пересечение с поверхностью реального взлома будет происходить при большем значении координат.

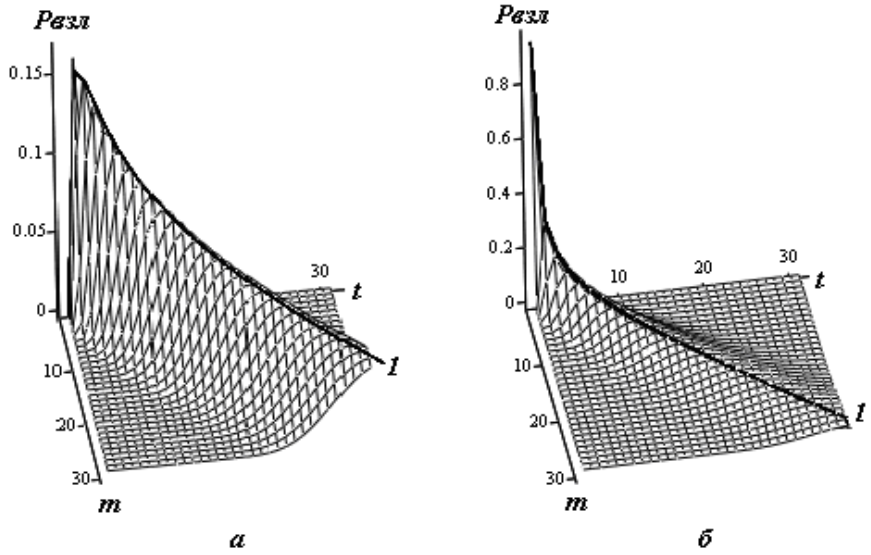

Рис. 2 Поверхности с вложенным в защиту финансированием: ***а*** - распределения вероятности взлома; и ***б*** - распределения максимумов вероятности взлома

Таким образом, на рис. 3 представлены темные области, в которых возможен взлом защиты. Следует заметить, что выбранное и вложенное в защиту финансирование почти в два раза увеличивает минимальные попытку и ее время взлома по сравнению с рис. 1б.

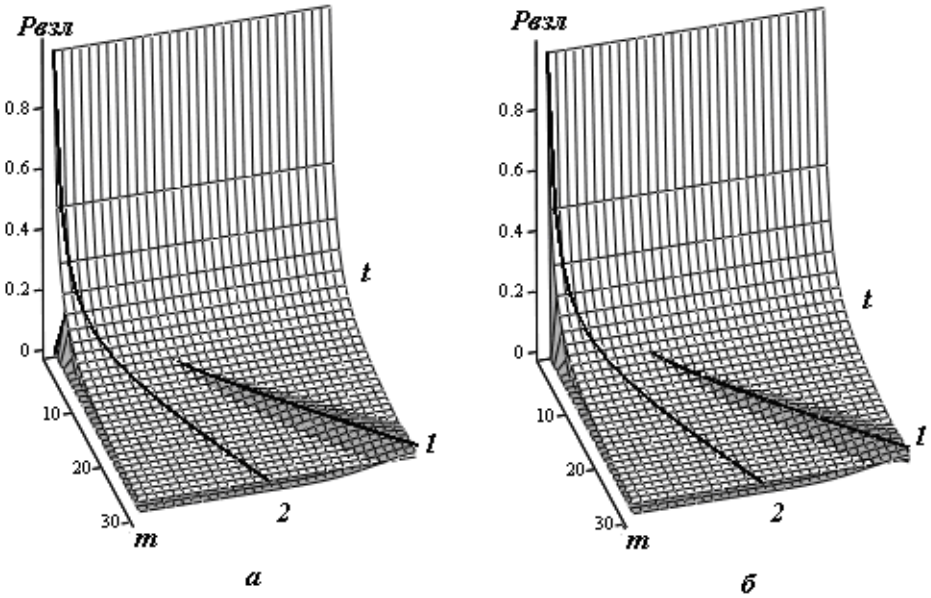

Рис.3 Поверхности: ***а*** **-** распределения вероятности взлома (9), ***б*** – распределение максимумов вероятностей взлома (9а) проектируемой ТЗИ с параметрами для выбранного случая.

Рассмотрим следующий случай, когда при тех же исходных параметрах вероятностей взлома (1), (1а), направление взлома происходит в направлении линии 2 с параметрами m_{21}=1, t_{21}=0; m_{22}=9, t_{22}=4; λ1=2 (7).

В этом случае возникновение попыток взлома и их времени будет описываться распределением Пуассона с заявками λ1:

$$P1_m(t) = \frac{(\lambda 1 \cdot t)^{m-1}}{(m-1)!} \cdot e^{-\lambda 1 \cdot t}, \qquad (11)$$

распределение вероятности и максимумов вероятности взлома произведением выражений (1) на (11) и (1а) на (11) соответственно. Следовательно, вероятности взлома будут определяться соответствующими выражениями:

$$P_{взл}1(m,t) = P_{взл}(m,t) \cdot P1_m(t), \qquad (12)$$

где $P_{взл}(m,t)$ – это выражение либо (1), либо (1а).

Выбор такого распределения (12) связано с тем, что $P_{взл}(m,t)$, в основном, зависит от вложенного в защиту финансирования, ее эффективности, направления попытки и ее времени взлома, то есть зависит от параметров проектируемой технической защиты.

А выражение $P1_m(t)$ описывает возникновение распределений вероятностей той или иной попытки и ее времени в зависимости от реального направления взлома, то есть от интенсивности появления требований попыток взлома λ1. Этим выражение (12) отличается от выражений (9) и (9а), где направление взлома идет в проектируемом направлении $P_m(t)$.

На рис. 4 представлены поверхности, рассчитанные по формулам (1), (1а) множимые на (8) – темные поверхности по линии 1. Поверхности, рассчитанные по формулам (1), (1а) множимые на (11) – темные поверхности по линии 2. Вероятности взлома реального процесса взлома представлены на рис.4 светлой поверхностью.

На рис. 4а представлены распределения вероятностей взлома проектируемого (линия 1) и реального (линия 2) направлений.

На рис. 4б представлены распределения максимумов вероятностей взлома проектируемого (линия 1) и реального (линия 2) направлений.

Из рис. 4 видно, что в рассматриваемых координатах область взлома по проектируемому направлению (темная поверхность по линии 1) более широкая, чем по направлению идущего взлома (темная поверхность по линии 2), следовательно, взлом ТЗИ в проектируемом направлении более вероятен, чем в другом направлении.

Следует заметить, что при реальных попытках взлома, чем ближе будет происходить процесс взлома к координатным осям *m, t*, тем область возможного взлома будет уже. Из рисунка 4 можем определить минимальные координаты по направлению реального процесса взлома (линия 2).

Например, из рис. 4а эти координаты будут: $m_{2взл}$=12, $t_{2взл}$=5. Таким образом, выражение (12) описывает распределение вероятности взлома ТЗИ от параметров: вложенного финансирования, эффективности вложенного в защиту финансирования, направления взлома и ее интенсивности, а также вероятности появления той или иной попытки взлома.

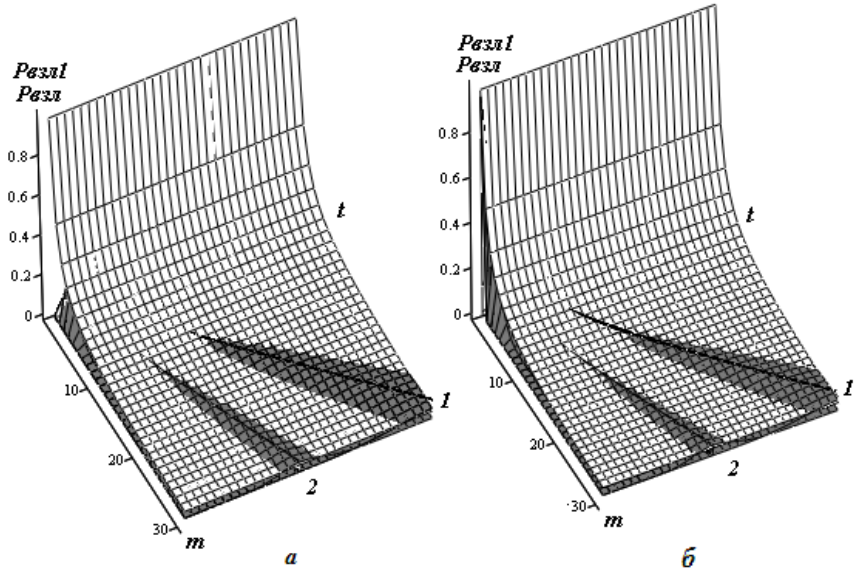

Рис. 4 Поверхности с параметрами для выбранного случая: ***а*** **–** планируемого, возможного направлений взломов (темные поверхности по линиям 1 и 2 соответственно) и реального (светлая поверхность) распределения вероятности взлома; ***б*** **–** те же обозначения для максимумов вероятностей взломов

Чтобы получить математическую модель физического процесса взлома технической защиты информации, необходимо учесть вероятность взлома самой защиты. Если защита определяется цифровым кодом, то необходимо учесть вероятность возникновения этого кода.

Например, чтобы определить количество возможных кодов, воспользуемся формулой количества размещений $A^m_n=n^m$.

В случае, когда из n цифр необходимо выбрать один код, необходимо сделать $A^n_n=n^n$ раз возможных попыток взлома. Вероятность угадать нужный код будет $P(n)=(A^n_n)^{-1}=(n^n)^{-1}$.

Следовательно, математическая модель физического процесса взлома технической защиты информации в проектируемом направлении будет иметь вид:

$$P_{взл}(m,t,n) = P_{взл}(m,t)\cdot P_m(t)\cdot P(n). \qquad (13)$$

Если заменить выражение распределения Пуассона в проектируемом направлении на направление реального взлома, то это выражение математической модели (13) может использоваться для расчета вероятности возможного реального процесса взлома.

В случае, если вероятность взлома самой защиты не определяется кодом $P(n)$, ее необходимо заменить вероятностью взлома, предполагаемой ТЗИ. Введение кода из двух чисел уже существенно повышает вероятность защищенности ТЗИ. В случае отсутствия вложенного в защиту финансирования вероятность взлома ТЗИ будет определяться произведением распределения Пуассона ($P_m(t)$) на вероятность взлома предполагаемой ТЗИ ($P(n)$). Влияние этого параметра на ТЗИ требует дополнительных исследований, которые будут опубликованы позже.

ВЫВОДЫ

Анализ и исследование математической модели физического процесса взлома ТЗИ позволяет сделать следующие выводы. Если нет вложенного в защиту финансирования, то вероятность взлома ТЗИ будет определяться только распределением Пуассона, которое описывает вероятность появления той или иной попытки и ее времени взлома в зависимости от направления реального процесса взлома. Причем, распределения вероятности и максимума вероятности взлома ТЗИ не будут влиять на этот процесс, поскольку коэффициент эффективности защиты при отсутствии финансирования в защиту будет равен нулю.

При наличии вложенного финансирования в ТЗИ наблюдаются различия между распределениями вероятности и максимумов вероятности взлома, при этом, распределение вероятности взлома имеет максимальное значение в определенной точке, а распределение максимумов вероятности взлома носит экспоненциальный характер.

Кроме того, эти распределения имеют остронаправленный характер с максимальным значением вероятности по линии взлома, значение которого падает при удалении от линии направления взлома и увеличении координаты взлома и времени.

В случае отличия реального направления взлома от проектируемого, вероятность максимального значения возможного взлома ТЗИ изменяется. Показано, что в этом случае вероятность возможного взлома падает, так как уменьшается площадь пересекающихся поверхностей вероятностей реального и возможного взломов, что указывает на более высокий уровень защищенности информации.

В выражение вероятности взлома ТЗИ введено выражение, определяющее вероятность взлома предполагаемой ТЗИ. Уже сейчас очевидно существенное влияние этого параметра на ТЗИ, но оценка влияния этого параметра требует дополнительных исследований.

В результате выполненной работы получена математическая модель физического процесса взлома технической защиты информации, которая описывается такими параметрами: вложенным в защиту финансированием, эффективностью вложенного в защиту финансирования, направлением попыток взлома и их интенсивностью, вероятностью появления той или иной попытки взлома и вероятностью взлома, предполагаемой ТЗИ.

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 Pro-tection of Information in Computer Systems. https: // www.google.com/search?q=3.+https%3

A%2F%2Fwww.cl.cam.ac.uk%2Fteaching%2F1011%2FR01%2F75-protec-tion.pdf&rlz=1C1AOHY_ruUA820UA823&oq=3.+https%3A%2F%2Fwww.cl.cam.ac.uk%2Fteaching%2F1011%2FR01%2F75-prote c-tion.pdf&aqs=chrome.69i57.3772j0j8&sourceid =chrome&ie=UTF-8.

[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"*. 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*. 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/9781597495332/02~Chapter_1.pdf.

[6] Pierangela Samarati, Sabrina de Capitani di Vimercati.: *Access Control: Policies, Models, and Mechanisms.*

[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. Ec*ology, 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, 2020. – pp. 838-849.

[14] Смирнов Н.В. *Курс теории вероятностей и математической статистики: для технических приложений/* Н.В.Смирнов, И.В.Дунин-Борковский. – М.: *«Наука»*, 1969. – 512 с.

[15] Солнышкина И.В. *Теория массового обслуживания: учеб. Пособие/* И.В.Солнышкина. – Комсомольск-на-Амуре: ФГБОУ ВПО, «КнАГТУ», 2015. – 76 с.

MATHEMATICAL MODEL OF THE PHYSICAL PROCESS OF HACKING TECHNICAL PROTECTION OF INFORMATION

This paper presents a mathematical model of the physical process of breaking technical information security (TIS). The mathematical model is based on the works of B. Zhurylenko, which use: the funding invested in protection, the coefficient of protection efficiency and the direction of hacking. The mathematical model was built taking into account the Poisson distribution used in the theory of queuing. The Poisson distribution allows us to take into account the probability of a particular attempt and its time of breaking information security. Studies have shown that, in the absence of funding for protection, the probability of breaking will be determined only by the Poisson distribution and the probability of breaking the applied protection. In the presence of funding for information protection, there are differences between the distributions of the probability and the maximum probability of hacking, with the distribution of the probability of hacking having a maximum value at a certain point, and the distribution of the maximum probabilities of hacking is exponential. In addition, these distributions have a highly directional character with the maximum probability value in the direction of the break line. The values of probabilities decrease with distance from the line of the burglary direction, increasing the burglary coordinates and time. If the real direction of hacking differs from the projected one, the probability of the maximum value of a possible hacking of the TIS changes. It is shown that in this case the probability of possible hacking decreases, since the area of intersecting surfaces of probabilities of real and possible hacking decreases. An expression has been introduced into the mathematical model of the physical process of breaking TIS, which determines the probability of breaking the alleged protection. Thus, as a result of the work performed, we obtained a mathematical model of the physical process of hacking TIS, which is described by the following parameters: the funding invested in the protection, the effectiveness of the funding invested in the protection, the direction of the hacking attempts and their intensity, the probability of a particular hacking attempt and the probability of hacking the alleged TIS.

Keywords: technical protection of information, distribution of the probability of breaking, distribution of the maximum probability of breaking the security, Poisson distribution, distribution of the probability of possible breaking, real breaking process, direction line of projected breaking, line of direction of real breaking.

МАТЕМАТИЧНА МОДЕЛЬ ФІЗИЧНОГО ПРОЦЕСУ ЗЛОМУ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

У даній роботі представлена математична модель фізичного процесу злому технічного захисту інформації (ТЗІ). Математична модель базується на роботах Б.Журиленко, в яких використовуються: вкладене в захист фінансування, коефіцієнт ефективності захисту і напрямок злому. Математична модель будувалася з урахуванням розподілу Пуассона, використовуваного в теорії масового обслуговування. Розподіл Пуассона дозволяє врахувати ймовірність появи тієї чи іншої спроби і її часу злому захисту інформації. Проведені дослідження показали, що, в разі відсутності фінансування на захист, ймовірність злому буде визначатися тільки розподілом Пуассона і ймовірністю злому застосовуваного захисту. При наявності фінансування на захист інформації, спостерігаються відмінності між розподілами ймовірності і максимуму ймовірності злому, причому розподіл ймовірності злому має максимальне значення в певній точці, а розподіл максимумів ймовірності злому носить експонентний характер. Крім того, ці розподіли мають гостро направлений характер з максимальним значенням ймовірності у напрямку лінії злому. Значення ймовірностей падають при віддаленні від лінії напряму злому, збільшенні координат злому і часу. Що стосується відхилення реального напрямку злому від проектованого, ймовірність максимального значення можливого злому ТЗІ змінюється. Показано, що в цьому випадку ймовірність можливого злому падає, так як зменшується площа пересічних поверхонь ймовірностей реального і можливого зломів. У математичну модель фізичного процесу злому ТЗІ введено вираз, що визначає ймовірність злому передбачуваного захисту. Таким чином, в результаті виконаної роботи отримано математичну модель фізичного процесу злому ТЗІ, яка описується такими параметрами: вкладеним на захист фінансуванням, ефективністю вкладеного в захист фінансування, напрямком спроб злому і їх інтенсивністю, ймовірністю появи тієї чи іншої спроби злому і ймовірністю злому застосованого ТЗІ .

Ключові слова: технічний захист інформації, розподіл ймовірності злому, розподіл максимуму ймовірності злому захисту, розподіл Пуассона, розподіл ймовірності можливого злому, реальний процес злому, лінія напрямку проектованого злому, лінія напрямку реального злому.

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 of the National Aviation University.

Николаев Кирилл Иванович, агент службы поддержки Ubisoft, Concentrix.
Николаєв Кирило Іванович, агент служби підтримки Ubisoft, Concentrix.
Nikolaev Kirill, Ubisoft gaming support, Concentrix.
E-mail: kyrylo.nikolaiev@gmail.com.
ORCID ID: 0000-0002-2633-6907.

Рябова Любов Володимирівна, асистент кафедри засобів захисту інформації Національного авіаційного університету. Факультет кібербезпеки, компютерної та програмної інженерії.
E-mail: lubanau@ukr.net.
ORCID ID: 0000-0002-9257-6626.
Рябова Любовь Владимировна, ассистент кафедры средств защиты информации Национального авиационного университета. Факультет кибербезопасности, компьютерной и программной инженерии.
Ryabova Lyubov, assistant of Academic Departament of information security means, National Aviation University. Faculty of Cybersecurity, Computer and Software Engineering.