DOI: 10.18372/2410-7840.21.13950
УДК 004.056.5(045)

МЕТОД ПРОЕКТИРОВАНИЯ И ОЦЕНКА РАБОТАЮЩЕЙ ОДИНОЧНОЙ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ ПО ВЫБРАННОМУ НАПРАВЛЕНИЮ ВЗЛОМА

Борис Журиленко

В данной работе показана альтернативная известным способам возможность проектирования и оценки одиночной технической защиты информации (ТЗИ) по выбранному направлению взлома. А именно, показана возможность построения ТЗИ по выбранным параметрам: направлению и необходимой попытке взлома или по необходимым выбранным попытке взлома и ее времени. С помощью предлагаемого метода проектирования и оценки одиночной ТЗИ по выбранным параметрам взлома можно получить поверхность распределения вероятности взлома защиты и поверхность распределения максимумов вероятности взлома, эффективность выбранной защиты, необходимое финансирование для данного типа защиты, риски потерь вложенного финансирования и риски общих финансовых потерь. Полученные параметры защиты информации можно сравнить с требуемыми проектируемыми параметрами и определить их соответствие заданной ТЗИ. В случае несоответствия требованиям ТЗИ необходимо выбрать другой тип защиты и с помощью данного метода рассчитать ее новые параметры. При оценке работающей ТЗИ по реальному, экспериментально зафиксированному направлению взлома и проектируемой ТЗИ, можно определить вероятностную надежность одиночной работающей защиты, а также при каких попытке и времени возможен ее реальный физический взлом. По полученным результатам анализа состояния работающей ТЗИ принимается решение о продлении работы, замене или модернизации существующей защиты информации. В работе приводится метод расчета с конкретными выбранными параметрами для проектирования и оценки одиночной ТЗИ по выбранному направлению взлома. По конкретным параметрам защиты и взлома построены графики, с помощью которых определены возможные попытка и время этой попытки взлома ТЗИ. С помощью графической иллюстрации показан физический процесс взлома защиты информации.

Ключевые слова: *одиночная техническая защита информации, проектирование защиты, поверхность распределения вероятности взлома защиты, поверхность распределения максимумов вероятности взлома, эффективность выбранной защиты, необходимое финансирование для данного типа защиты, риски потерь вложенного финансирования, риски общих финансовых потерь.*

Введение. Существующие методы проектирования технической защиты информации (ТЗИ) проводятся в соответствие с существующими нормативными документами. Качество разработанной ТЗИ оценивается на момент введения ее в работу, а состояние работающей ТЗИ в процессе ее взлома не оценивается, так как такой методики не существует. При проектировании не учитывается, каким образом будет происходить процесс взлома, то есть не учитывается возможность известного направления взлома и его интенсивность, которые определяются попытками и временем этих попыток взлома. В большинстве случаев спроектированная защита носит качественный характер, мало зависящий от самого физического процесса взлома. Существуют и разрабатываются также другие методы проектирования ТЗИ, но и в этих случаях проектируемая защита обладает, в основном, такими же недостатками, как и при проектировании с нормативными документами.

В настоящее время разрабатывается методология проектирования и оценки, работающей ТЗИ с учетом требований финансовых вкладов в защиту, эффективности защиты и физического процесса взлома, то есть с учетом попыток и времени этих попыток взлома [1-3]. Актуальность данного направления проектирования и оценки, работающей ТЗИ заключается в том, что данный метод и предлагаемая методология позволит по исходным выбранным параметрам проектируемой защиты до ее построения оценить вероятность ее взлома и в процессе эксплуатации защиты оценивать ее деградацию и остаточную вероятность возможного взлома используемой защиты информации. В итоге есть возможность во время до процесса взлома сменить или модернизировать используемую защиту.

Целью данной работы является разработка метода проектирования и оценки, работающей одиночной технической защиты информации по выбранному направлению взлома.

Теоретическое обоснование метода проектирования и оценки работающей одиночной технической защиты информации по выбранному направлению взлома.

Исходными параметрами для проектирования защиты информации является направление или интенсивность взлома ω и выбранная для проектирования попытка m или время t этой попытки взлома.

Согласно работе [4], по направлению или интенсивности взлома определяем «характеристическую» или определяющую вероятность взлома функцию для одноуровневой или одиночной защиты

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

где $\omega = \frac{m_2 - m_1}{t_2 - t_1}$, m_1=1, t_1=0 – начальные условия процесса взлома (первая попытка взлома и ее время), m_2, t_2 – планируемая попытка взлома и ее время, определяющие направление или интенсивность процесса взлома ω. Параметры m_2, t_2 могут выбираться по результатам исследования реальных процессов взлома или по предполагаемому направлению взлома. m_2, t_2 могут выбираться разработчиком из предположения, в каком направлении будет идти процесс взлома разрабатываемой защиты. m – текущая попытка взлома.

В работе [4, 5] получено выражение поверхности распределения для максимумов вероятности взлома с учетом направления взлома, вложенного в защиту финансирования и коэффициента эффективности данной защиты

$$P_{\text{взл}i}(m,\mathrm{t}) = \{P_i(X_i)\cdot\left[\left(\frac{f_i(m,t)}{f_i(m,t)+t}\right)^{\frac{f_i(m,t)}{t}}\cdot\left(\frac{t}{f_i(m,t)+t}\right)\right]\}^{\gamma}, \quad (2)$$

где $P_{\text{взл}i}(m,t)$ – поверхность распределения максимумов вероятности взлома в зависимости от текущих попыток m и текущего времени t попыток взлома, γ - коэффициент эффективности данной защиты, $P_i(X_i) = \frac{X_i^{X_i}}{(1+X_i)^{(1+X_i)}}$ – максимум вероятности взлома защиты от приведенного вложенного финансирования в защиту X_i. Приведенное финансирование определяется, как отношение финансовых затрат в защиту информации x к возможным финансовым потерям без защиты информации H, то есть $X=x/H$. Как показано в работе [6], коэффициент эффективности защиты γ определяется отношением рисков приведенного вложенного финансирования в защиту к рискам приведенных полных финансовых потерь

$$\gamma = \frac{X_i}{1+X_i}. \quad (3)$$

Риски приведенного вложенного финансирования определяются как

$$R_{\text{влi}}(X_i) = P_i(X_i)\cdot X_i \quad (4)$$

и риски приведенных полных финансовых потерь

$$R_{\text{полнi}}(X_i) = P_i(X_i)\cdot(1+X_i). \quad (5)$$

На следующем этапе проектирования ТЗИ определяются необходимые финансовые затраты на защиту, риски финансовых потерь и коэффициент эффективности защиты, которые зависят от выбранной при проектировании попытки взлома $m_{\text{взл}}$. Время взлома можно найти по попытке взлома из проектируемого направления процесса взлома по формуле, подставив вместо текущей попытки взлома проектируемую $m_{\text{взл}}$

$$t(m) = \frac{\sqrt{A^2 + \frac{4}{\omega}\cdot f_i(m,t)}}{2} - \frac{A}{2}, \; A = t_1 + \frac{m_1 - 1}{\omega}. \quad (6)$$

Вероятность взлома любой защиты информации на m-той попытки будет

$$P(m) = \frac{1}{m_{\text{взл}}}. \quad (7)$$

Подставим в уравнение (2) выражение (1) с начальными условиями процесса взлома m_1=1, t_1=0 и параметрами $m_{\text{взл}}$ и $t_{\text{взл}}$. Приравняем уравнение (2) к уравнению (7). Решив равенство относительно выражения для коэффициента эффективности защиты информации, получим

$$\gamma = \frac{-\ln(m_{\text{взл}})}{(m_{\text{взл}}-1)\cdot ln(m_{\text{взл}}-1) - m_{\text{взл}}\cdot ln(m_{\text{взл}}) + X_i\cdot ln(X_i) - (1+X_i)\cdot\ln(1+X_i)} = \frac{X_i}{1+X_i}. \quad (8)$$

Решив уравнение (8) относительно приведенного вложенного финансирования X_i, можно определить, согласно (3), (4) и (5), максимум вероятности взлома от вложенного в защиту финансирования, коэффициент эффективности защиты информации и риски полных и вложенных финансовых потерь. Кроме того, по формуле (2) можно построить поверхность распределения максимумов вероятности взлома проектируемой ТЗИ. Таким образом, по исходным параметрам, а именно по направлению (или интенсивности взлома ω) и выбранной попытке m или времени t этой попытки взлома, получены все необходимые данные проектируемой ТЗИ.

По полученным формулам проведем расчет проектируемой ТЗИ с исходными параметрами с начальными условиями m_1=1, t_1=0 и предполагаемым максимумом процесса взлома и анализ физического процесса взлома $m_{\text{взл}}$ =10 и $t_{\text{взл}}$=5. В этом случае выбранное направление взлома ω=1,8 будет определяться при условии $m_2 = m_{\text{взл}}$ и $t_2 = t_{\text{взл}}$.

Решим уравнение (8) графическим способом при $m_{\text{взл}}$=10. Для чего построим левую и правую части уравнения (8) в зависимости от приведенного вложенного финансирования X_i.

На рис.1 представлены результаты построения графиков левой ***f1(X)*** и правой ***f2(X)*** частей уравнения (8) (сплошные линии) и максимумы вероятности взлома в зависимости от приведенного вложенного финансирования ***P(X)*** (пунктирная линия).

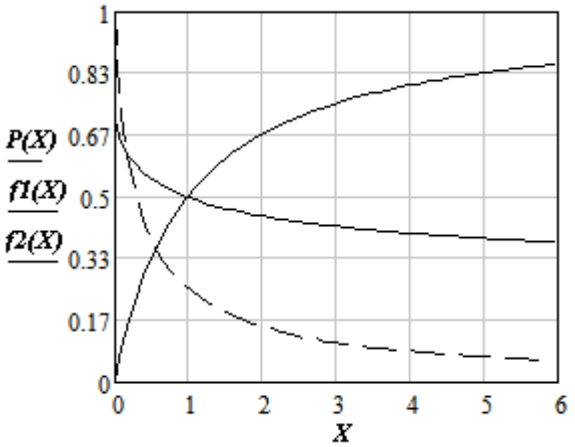


Рис. 1. Результаты построения графиков левой ***f1(X)*** и правой ***f2(X)*** частей уравнения (8) (сплошные линии) и максимумы вероятности взлома в зависимости приведенного вложенного финансирования ***P(X)*** (пунктирная линия)

Из графика можно определить коэффициент эффективности защиты информации $\boldsymbol{\gamma = 0,5}$, приведенное вложенное финансирование $\boldsymbol{X_i}$**=1** и вычислить максимум вероятности взлома $\boldsymbol{P_i(X_i) = 0,25}$ от приведенного вложенного финансирования, риски приведенного вложенного финансирования $\boldsymbol{R_{влi}(X_i) = 0,25}$ и приведенных полных финансовых потерь $\boldsymbol{R_{полнi}(X_i) = 0,5}$.

По формуле (2), с учетом параметров проектируемой защиты $\boldsymbol{\gamma = 0,5}$ и $\boldsymbol{P_i(X_i) = 0,25}$, и по формуле (7) построим поверхности распределения максимумов вероятности взлома ТЗИ (2) и вероятности реального процесса взлома защиты (7).

На рис. 2 представлены поверхности процессов взлома ТЗИ. Серая поверхность соответствует расчету распределения максимума вероятности взлома по формуле (2) с вычисленными параметрами для выбранного проектируемого направления взлома, белая – по формуле (7). Прямая черная линия ***1*** на рисунке указывает направление проектируемого процесса взлома.

Если предположить, что реальный процесс взлома происходит только при максимальной вероятности взлома в каждой точке поверхности проектируемой защиты, то решив равенство $P_{взлi}(m, t) = P(m)$, получим линию с максимально возможной вероятностью взлома проектируемой защиты в виде линии пересечения белой и серой поверхностями (рис. 2). Линия пересечения между белой и серой поверхностями указывает на максимальную вероятность реального и расчетного процесса взлома.

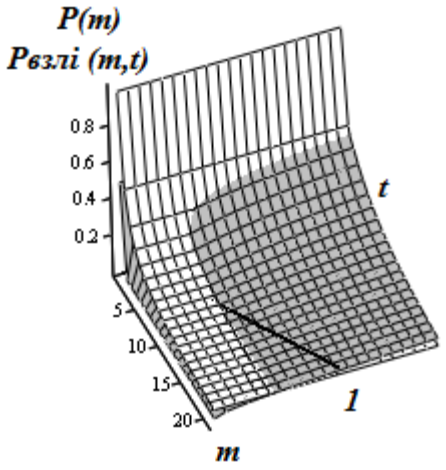


Рис. 2. Поверхности процессов взлома ТЗИ. Серая поверхность соответствует расчету распределения максимума вероятности взлома по формуле (2), белая – по формуле (7). Линия ***1*** указывает направление проектируемого процесса взлома

Пересечение белой, серой поверхностей и черной прямой линии 1 дает максимум вероятности проектируемого процесса взлома в выбранном направлении и попытке взлома.

В реальных условиях процесс взлома не обязательно будет происходить при максимуме вероятности взлома, следовательно, при проектировании ТЗИ необходимо использовать поверхность распределения вероятности взлома проектируемого ТЗИ [7]. Поверхность распределения вероятности взлома проектируемого ТЗИ можно построит с помощью выражения (2) подставив в показатель функции (1) значение проектируемой попытки $m_{взл}$ и вычисленной по формуле (6) времени $t_{взл}=t(m)$ этой попытки взлома. Получим

$$P1_{взлi}(m,t) = \{P_i(X_i) \cdot \left[\left(\frac{f_i(m,t)}{f_i(m,t)+t}\right)^{\frac{f_i(m_{взл},t)}{t(m_{взл})}} \cdot \left(\frac{t}{f_i(m,t)+t}\right)\right]\}^{\gamma}. \quad (9)$$

На рис. 3 представлена поверхность распределения вероятности взлома проектируемой ТЗИ с выбранными и вычисленными исходными параметрами. Линия ***1*** соответствует выбранному проектируемому направлению взлома с максимумом в точке $m_{взл}$ =10 и $t_{взл}$=5. В случае, если реальный процесс взлома (линия ***2***) пошел не по проектируемому направлению, то вероятность взлома проектируемой защиты будет определяться по линии ***2***. Если же злоумышленник с некоторого момента

нападения, по каким-либо причинам, уменьшит интенсивность нападения по времени, то процесс взлома и его вероятность будут определяться линией ***3***, состоящей из точек на рис. 3.

Чтобы определить по каким попыткам и их времени будет проходить максимум попыток взлома по поверхности на рис. 3, построим поверхности выражений (2) и (9). Линия пересечения этих поверхностей даст максимальные значения вероятности взлома проектируемой ТЗИ.

На рис. 4 представлены результаты расчета поверхностей по формулам (2) – белая поверхность и (9) – серая поверхность, линия ***1*** – проектируемое направление взлома, линия ***2*** – реальный процесс взлома, линия ***3*** – реальный процесс взлома, когда злоумышленник уменьшил интенсивность нападения во времени. Из рис. 4а видно (по линии пересечения белой и серой поверхностей) в каких точках при различных направлениях взлома будет максимальная вероятность взлома проектируемой ТЗИ. Также из рис. 4б видно, что если злоумышленник уменьшил интенсивность нападения во времени (линия ***3***), то вероятность взлома защиты меньше максимального значения и со временем для данной защиты максимального значения не достигает. С другой стороны, если бы злоумышленник по каким-либо причинам увеличил количество попыток взлома, то есть уменьшил время между попытками взлома, то направление взлома (линия ***3***) пошло бы параллельно оси *m* и максимальная вероятность была бы достигнута. В этом случае максимальная вероятность взлома могла быть достигнута при меньшем времени взлома.

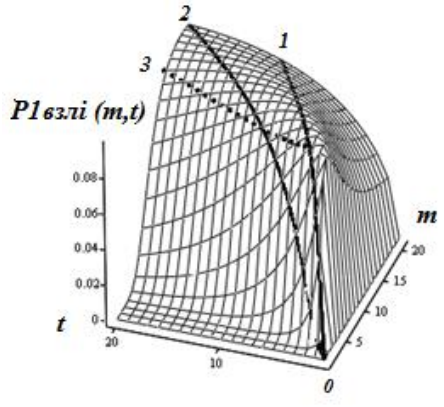
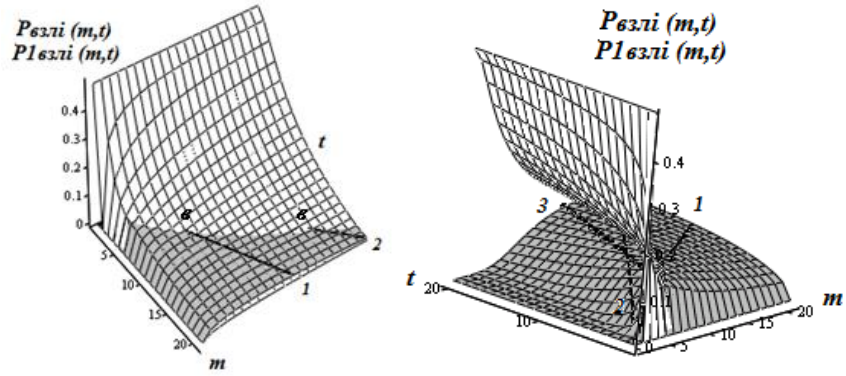


Рис. 3. Поверхность распределения вероятности взлома проектируемой ТЗИ с выбранными и вычисленными исходными параметрами, и максимумом взлома в точке $m_{взл}$ =10 и $t_{взл}$=5. Линия ***1*** соответствует выбранному проектируемому направлению взлома; линия ***2***, когда реальный процесс взлома пошел не по проектируемому направлению; линия ***3***, когда по каким-либо причинам во время нападения направление процесса взлома изменилось с уменьшением интенсивности нападения по времени



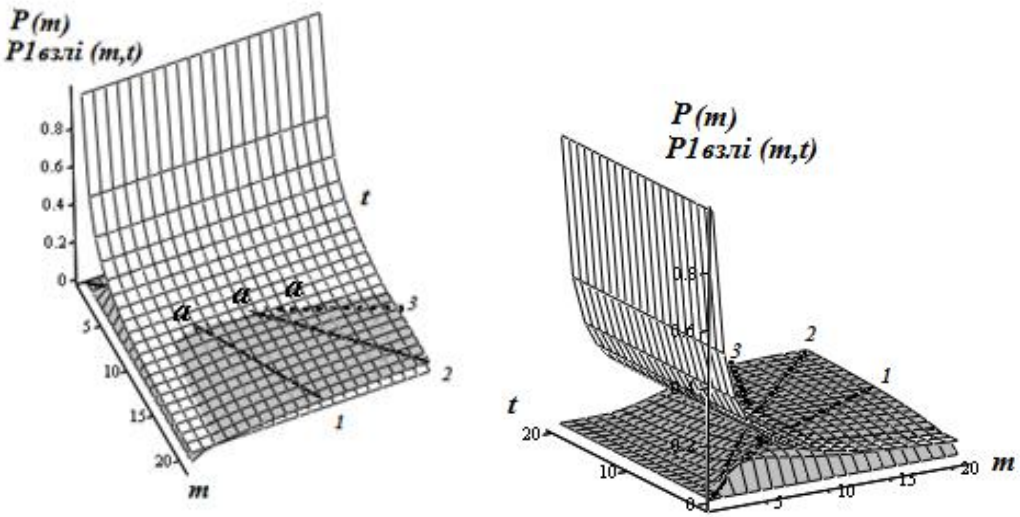
а **б**

Рис. 4. Поверхности распределения максимума вероятности взлома (белая поверхность) и распределения вероятности взлома проектируемой защиты (серая поверхность)

Поскольку реальный процесс взлома проектируемой ТЗИ может происходить не обязательно при максимальных значениях вероятности взлома, то для определения попытки и времени этой попытки взлома, для любого направления взлома необходимо построить поверхности по формулам (7) и (9).

Пересечение этих поверхностей с направлением происходящего процесса взлома даст попытку и время этой попытки взлома.

На рис. 5 построены поверхности по формулам (7) (белая поверхность) и (9) (серая поверхность). Обозначения линий ***1***, ***2***, ***3*** соответствуют предыдущим рисункам.



а б

Рис. 5. Поверхности, построенные по формулам (7) – белая поверхность и (8) – серая поверхность. Линия ***1*** – указывает направление взлома спроектированной защиты; ***2*** – направление происходящего процесса взлома; ***3*** – направление взлома, измененное злоумышленником в процессе нападения

Из рис. 5 видно, что реальный процесс взлома, соответствующий выражению (7), спроектированной защиты будет проходить с вероятностью определяемой линией пересечения белой и серой поверхностями. В данном случае, согласно рис. 4, процесс взлома с расчетным максимальным значением вероятности будет только для направления проектируемой ТЗИ (линия ***1***), а для остальных направлений значение вероятности взлома будет меньше (линии ***2*** и ***3***). Если направление реального процесса взлома близко к проектируемому направлению защиты, то взлом ТЗИ может произойти при значениях близких к проектируемой попытке взлома $m_{взл}$, особенно при небольших увеличениях по времени между попытками взлома. При значительных увеличениях по времени между попытками взлома, взлом ТЗИ возможен не только при большом времени и попытке взлома, но и не произойти совсем. Аналогичная ситуация, когда взлом не произойдет, возможна, если попытки взлома будут следовать очень часто друг за другом.

Анализируя рис. 4 и рис. 5 по направлениям взлома (рис. 6), видно, что при значениях попытки и ее времени (точки, обозначенные буквой ***а***) вероятности попыток проектируемого и реального взлома равны. Максимальные значения вероятностей взлома для проектируемого и реальных направлений взлома обозначены буквой ***в***. Для направлений ***1*** и ***2*** они представлены на рис. 6. Для направления ***3***, как видно из рис. 4, такой точки может и не быть. На рис. 6 крестиками смоделированы возможные координаты реальных попыток взлома: сначала по направлению ***2***, а затем по направлению ***3***, когда злоумышленник изменил тактику взлома.

Следует заметить, что от точки реального взлома - ***а*** до точки максимальной вероятности взлома - ***в***, достоверность вероятности взлома увеличивается. Однако, этот процесс требует дальнейших исследований.

Для того, чтобы определить вероятность взлома некоторое время работающей ТЗИ, необходимо знать процесс взлома, который обозначен крестиками на рис. 6. По крестикам, в соответствие с работой [8], необходимо определить последнее реальное направление взлома (линия ***2*** или ***3***). Затем, по приведенным в статье формулам, строится линия ***2*** или ***3*** по распределению вероятности взлома проектируемой защиты и проводится анализ состояния работающей ТЗИ в соответствие с рис. 5. Проведенный анализ покажет состояние работающей ТЗИ, даст время, попытку и вероятность реального процесса взлома, что будет соответствовать проектируемому процессу взлома и последнему реальному направлению взлома. По полученным результатам анализа принимается решение о продлении работы, замене или модернизации существующей защиты информации.

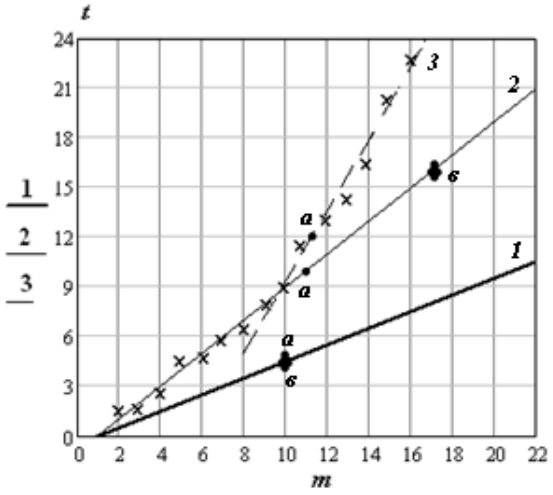


Рис. 6. Направления попыток взлома: проектируемого – линия 1; реального – линия 2; измененного злоумышленником – линия 3; точки: **а** – вероятности проектируемого и реального взлома совпадают (рис. 5); **в** – совпадают максимум вероятности по проектируемому направлению взлома и распределения вероятности проектируемой защиты для выбранного направления взлома (рис. 4)

Выводы. В данной работе показана альтернативная известным способам возможность проектирования и оценки одиночной технической защиты информации (ТЗИ) по выбранному направлению взлома. А именно, показана возможность построения ТЗИ по выбранным параметрам: направлению и необходимой попытке взлома или по необходимым выбранным попытке и ее времени взлома, в данном случае $m_{взл}=10$ и $t_{взл}=5$. С помощью предлагаемого метода проектирования и оценки одиночной ТЗИ по выбранным параметрам взлома были получны: поверхность распределения вероятности взлома защиты (рис. 3) и поверхность распределения максимумов вероятности взлома (рис. 4), эффективность выбранной защиты, необходимое финансирование для данного типа защиты, риски потерь вложенного финансирования и риски общих финансовых потерь. При оценке работающей ТЗИ, по реальному экспериментально зафиксированному направлению взлома (линия ***2*** или линия ***3***) и проектируемой ТЗИ, были определены: вероятностная надежность одиночной работающей защиты, а также при какой попытке и времени (точки ***а*** на рис. 5) возможен ее реальный физический взлом. По полученным результатам анализа состояния работающей ТЗИ принимается решение о продлении работы, замене или модернизации существующей защиты информации.

ЛИТЕРАТУРА

[1]. Б. Журиленко, "Методология построения и анализа состояния комплекса технической защиты информации с вероятностной надежностью и учетом временных попыток взлома", *Захист інформації,* №3(17), С. 196-203, 2015.

[2]. Б. Журиленко, Н. Николаева, "Определение коэффициента эффективности технической защиты информации по ее параметрам", *Безпека інформації*, №3(21), С. 245-250, 2015.

[3]. Б. Журиленко, Н. Николаева, Н. Пелих, "Оценка стойкости технической защиты информации во времени", *Захист інформації*, №1(54), С. 104-108, 2012.

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

[5]. Б. Журиленко, "Определение вероятностной надежности единичной технической защиты информации из реальных попыток взлома", *Безпека інформації,* №1(19), С. 34-39, 2013.

[6]. Б. Журиленко, "Оценивание финансовых затрат на построение системы защиты информации", *Захист інформації*, № 4(20), С. 231-239, 2018. DOI: 10.18372/2410-7840.20.13424.

[7]. Б. Журиленко, Н. Николаева, "Вероятностная надежность защиты информации в зависимости от направления взлома", Захист інформації, №3(20), С. 174-179, 2018. DOI: 10.18372/2410-7840.20.13073.

[8]. Б. Журиленко, Моделирование процесса взлома и анализа рабочего состояния технической защиты информации, *Безпека інформації*, №1(22), С. 26-31, 2016.

DESIGN METHOD AND EVALUATION OF THE WORKING SINGLE TECHNICAL PROTECTION INFORMATION ON THE SELECTED DIRECTION OF HACKING

This paper shows an alternative to the known methods, the ability to design and evaluate a single technical information protection (TZI) in the chosen direction of hacking. Namely, the possibility of constructing a TZI according to the selected parameters: the direction and the necessary attempt to hack or the necessary selected attempt and its time to hack is shown. Using the proposed method for designing and evaluating a single TZI according to the selected parameters of hacking, one can obtain the distribution surface of the probability of breaking into the protection and the distribution surface of the maximums of the probability of breaking, the effectiveness of the chosen protection, the necessary financing for this type of protection, the risks of investment losses and risks of general financial losses. The

obtained parameters of information protection can be compared with the required design parameters and determine their compliance with the specified TZI. In case of non-compliance with the requirements of the technical specifications, it is necessary to choose a different type of protection and use this method to calculate new protection parameters. When assessing a working TZI, according to the real, experimentally recorded, direction of hacking and the designed TZI, it is possible to determine the probabilistic reliability of a single working defense, as well as at what attempt and time its real physical hacking is possible. Based on the results of the analysis of the state of the working TZI, a decision is made to extend the work, replace or modernize the existing information protection. The paper presents a calculation method with specific selected parameters for designing and evaluating a single TZI in the chosen direction of hacking. Charts have been built for specific protection and hacking parameters, with the help of which the possible attempt and time of this attempt to break the TZI have been determined. Using a graphic illustration shows the physical process of hacking information protection.

Keywords: single technical information protection, protection design, probability break-in probability distribution surface, break-in probability maximum distribution surface, selected protection effectiveness, necessary financing for this type of protection, risks of investment losses, risks of general financial losses.

МЕТОД ПРОЕКТУВАННЯ ТА ОЦІНКА ПРАЦЮЮЧОГО ОДИНОЧНОГО ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ ЗА ОБРАНИМ НАПРЯМОМ ЗЛОМУ

У даній роботі показана альтернативна відомим способам можливість проектування і оцінки одиночного технічного захисту інформації (ТЗІ) за обраним напрямом злому. А саме, показана можливість побудови ТЗІ за обраними параметрами: напрямку і необхідної спробі злому або по необхідним обраним спробі злому і її часу. За допомогою запропонованого методу проектування і оцінки одиночної ТЗІ за обраними параметрами злому можна отримати поверхню розподілу ймовірності злому захисту і поверхня розподілу максимумів ймовірності злому, ефективність обраного захисту, необхідне фінансування для даного типу захисту, ризики втрат вкладеного фінансування і ризики загальних фінансових втрат. Отримані параметри захисту інформації можна порівняти з необхідними проектованими параметрами і визначити їх відповідність заданій ТЗІ. У разі невідповідності вимогам ТЗІ необхідно вибрати інший тип захисту і за допомогою даного методу розрахувати нові параметри захисту. При оцінці працює ТЗІ по реальному, експериментально зафіксованому напрямку злому і проектованої ТЗІ, можна визначити вірогідну надійність одиночного працюючого захисту, а також при яких спробі і часі можливий її реальний фізичний злом. За отриманими результатами аналізу стану працюючої ТЗІ приймається рішення про продовження роботи, заміні або модернізації існуючої захисту інформації. У роботі наводиться метод розрахунку з конкретними обраними параметрами для проектування та оцінки одиночної ТЗІ за обраним напрямом злому. За конкретними параметрами захисту та злому побудовані графіки, за допомогою яких визначено можливі спроба і час цієї спроби злому ТЗІ. За допомогою графічної ілюстрації показаний фізичний процес злому захисту інформації.

Ключові слова: одиночний технічний захист інформації, проектування захисту, поверхня розподілу ймовірності злому захисту, поверхня розподілу максимумів ймовірності злому, ефективність обраного захисту, необхідне фінансування для даного типу захисту, ризики втрат вкладеного фінансування, ризики загальних фінансових втрат.

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.