DOI: 10.18372/2410-7840.20.13073
УДК 004.056.5(045)

ВЕРОЯТНОСТНАЯ НАДЕЖНОСТЬ ЗАЩИТЫ ИНФОРМАЦИИ В ЗАВИСИМОСТИ ОТ НАПРАВЛЕНИЯ ВЗЛОМА

Борис Журиленко, Надежда Николаева

В данной работе приведено теоретическое исследование предлагаемого нового направления в проектировании, анализе состояния и своевременной модернизации работающей технической защиты информации (ТЗИ) в зависимости от происходящего процесса взлома в направлении взлома. Основываясь на рисках защищенности ТЗИ, получена функция присущая данной технической защите, зависящая от параметров направления процесса взлома и определяющая вероятностную надежность технической защиты в направлении взлома. Показано, что эта функция соответствует физическим требованиям процесса взлома. Из функции направления процесса взлома получено выражение, позволяющее из параметров попытки или времени взлома определить один или другой неизвестный параметр времени или попытки. Например, по известной попытке взлома можно оценить возможное время, когда произойдет взлом ТЗИ или, наоборот, по известному времени определить попытку. В работе получено распределение максимумов вероятности взлома технической защиты для направлений взлома, зависящих от параметров попытки, времени этой попытки взлома и коэффициента эффективности защищенности. Следует заметить, что реальный процесс взлома является случайной величиной, как по попыткам, так и по времени взлома, поэтому направление взлома не отображается прямой линией. В реальных условиях направление взлома может определяться по методологии, как это было предложено в работах Б.Журиленко, по прямой линии. В этом случае направление линии определяется как среднеквадратичное или среднее значение результатов попыток и его времени взлома. В результате проведенных исследований по полученным теоретическим выражениям построены поверхность распределения максимумов вероятностной взлома ТЗИ и вероятность в направлении линии процесса взлома, зависящая от его двух параметров - номера попытки и его времени взлома. Полученные выражения будут иметь большое значение при проектировании, анализе рабочего состояния работающей ТЗИ и модернизации защиты для экономии вложенных финансовых затрат в защиту.

Ключевые слова: *техническая защита информации, коэффициент эффективности защиты, распределение максимума вероятности взлома, попытка взлома, время попытки взлома, линия направления взлома.*

Введение. Техническая защита информации (ТЗИ) в различных странах осуществляется в соответствие со своими нормативными документами и разрабатываемыми методами. В этом случае построенная ТЗИ, в основном, имеет качественную оценку защиты, которая отвечает начальным условиям использования защиты. И только некоторые способы построения ТЗИ дают количественную оценку.

Естественно, разработчику защиты важно знать вероятность взлома защиты информации на каждом этапе ее работы и желательно из реальных попыток взлома. В реальных условиях при взломе защиты информации единственными фактами или параметрами, которые могут быть зафиксированы, являются попытка взлома и ее время. В этом случае, зная в каждый момент времени по исходным данным вероятность взлома работающей ТЗИ, разработчик может оценить вероятность возможного взлома защиты по реальным параметрам попыток взлома, которые можно получить всегда, например, по количеству попыток и времени этих попыток взлома. Эти результаты помогут разработчику принять решение о замене, используемой ТЗИ или ее модернизации, что позволит сэкономить финансовые и материальные ресурсы, вкладываемые в защиту информации.

Актуальность работы заключается в том, чтобы в отличие от нормативных документов разработать новый подход к разработке ТЗИ, опирающийся на реальные физические процессы взлома информации.

Научная новизна заключается в разработке новой методологии в подходе к проектированию, анализу рабочего состояния работающей ТЗИ с целью экономии финансовых затрат, вкладываемых в защиту.

Из открытых источников неизвестны защиты, которые разрабатывались бы по нормативным документам и которые обеспечивали бы контроль их состояния от количества попыток взлома во времени. С другой стороны, контроль количества попыток и времени взлома позволили бы определить интенсивность и направление взлома. Поскольку направление взлома зависит от двух параметров, то вероятностная надежность также должна зависеть от попыток и времени взлома, причем параметры попыток и времени связаны между собой направлением взлома. Существуют публикации Б. Журиленко [1-7], в которых сделана попытка разработать методологию построения защиты, контроля ее состояния в процессе работы, модернизации ТЗИ в зависимости от финансовых вложений на защиту, эффективности создаваемой защиты и направления взлома. Однако в этих работах отсутствует строгое доказательство вероятностной надежности в зависимости от направления взлома.

Целью работы является получение распределений максимума вероятности взлома ТЗИ и вероятности в зависимости от направления взлома, определяемых двумя параметрами – попыткой и временем этой попытки взлома.

Теоретическое обоснование распределения вероятностной надежности ТЗИ в зависимости от направления взлома.

Определим общий вид физических требований необходимых для распределения вероятностной надежности ТЗИ в зависимости от направления взлома. Хотя направление взлома определяется попыткой и временем попытки взлома, процесс этот носит случайный характер. Исходя из здравого смысла, основным требованием для вероятностной надежности должна быть ее зависимость от попыток взлома. Зависимость от времени определяется направлением взлома и носить зависимый характер от попытки взлома. При отсутствии попытки взлома вероятностная надежность не должна изменяться с изменением времени, а изменяться только при наличии попытки взлома. В общем виде распределение вероятностной надежности ТЗИ должно определяться как попыткой, так и временем этой попытки взлома.

Для получения выражения распределения вероятностной надежности ТЗИ примем следующие предположения. Пусть t_0 – некоторый параметр создаваемой ТЗИ, зависящий от направления взлома, и который необходимо определить, t – текущее время, в течение которого осуществляется защита, $p'(t)$ – вероятность защищенности ТЗИ во времени.

Определим риски защищенности ТЗИ во времени, как

$$(t_0 + t) \cdot p'(t) = f(t), \qquad (1)$$

где $f(t)$ - произвольная положительная функция, так как левая часть выражения (1) не может быть отрицательной.

Анализируя выражение (1), можно сказать, что для обеспечения ТЗИ функция рисков защищенности $f(t)$ при увеличении времени t должна быть хотя бы постоянной. Если $f(t)$ со временем будет уменьшаться, то используемая ТЗИ является неэф-фективной и ее необходимо поменять на другую защиту. В случае, если $f(t)$ увеличивается со временем, то такая ТЗИ является более эффективной, так как риски защищенности увеличиваются со временем.

Таким образом, чтобы иметь более эффективную защиту, выбираем:

$$f(t) = \alpha + \beta \cdot t, \qquad (2)$$

в виде степенного многочлена первого порядка в соответствие с левой частью формулы (1) и требованием независимости вероятностной надежности ТЗИ от времени, когда нет попытки взлома. Поскольку $f(t)$ является произвольной положительной функцией, то коэффициенты в выражении (2) должны быть $\alpha \geq 0,\ \beta \geq 0$ при любом значении $t \geq 0$.

Из (1) вероятность защищенности будет

$$p'(t) = \frac{f(t)}{(t_0 + t)}. \qquad (3)$$

Из начальных условий при $t=0$ вероятность защищенности $p'(0)=1$. Отсюда

$$p'(0) = \frac{f(t)}{(t_0)} = 1; f(t) = t_0. \qquad (4)$$

Следовательно, вероятность защищенности ТЗИ будет

$$p'(t) = \frac{f(t)}{f(t)+t} = \frac{\alpha + \beta \cdot t}{\alpha + \beta \cdot t + t}. \qquad (5)$$

Определим вероятность взлома во времени

$$p(t) = 1 - p'(t) = \frac{t}{\alpha + \beta \cdot t + t}. \qquad (6)$$

Считаем независимость вероятности взлома от результатов предыдущих попыток и, если с очередной попытки взлом не произошел, то вероятность взлома используемой защиты остается той же. Такое распределение попыток взлома будет подчиняться геометрическому закону распределения вероятностей [8].

В этом случае вероятность события взлома на m – той попытке может быть записана как

$$P(m,t) = [p'(t)]^{m-1} \cdot p(t) = \left[\frac{\alpha + \beta \cdot t}{\alpha + \beta \cdot t + t}\right]^{m-1} \cdot \left[\frac{t}{\alpha + \beta \cdot t + t}\right]. \qquad (7)$$

Определим экстремум кривой вероятности взлома $P(m,t)$ на m-той попытке по времени. Для чего возьмем первую производную выражения (7) по времени и приравняем ее нулю. В результате получим:

$$\alpha + \beta \cdot t = (m-1) \cdot t, \quad \text{или} \quad f(t) = (m-1) \cdot t = f(m,t). \qquad (8)$$

Поскольку $\alpha \geq 0, \beta \geq 0$, то вторая производная по времени будет больше нуля, что соответствует максимуму вероятности взлома (7) при значении функции (8). Сравнивая (8) с (2) получим $\alpha = 0$, $\beta = (m-1)$.

Таким образом, максимумы вероятностей взлома $P(m,t)$ на m – той попытке будут описываться выражением

$$P(m,t) = \left[\frac{f(m,t)}{f(m,t)+t}\right]^{m-1} \cdot \left[\frac{t}{f(m,t)+t}\right] = \left[\frac{(m-1)\cdot t}{(m-1)\cdot t + t}\right]^{m-1} \cdot \left[\frac{t}{(m-1)\cdot t + t}\right], \qquad (9)$$

или поверхность максимумов вероятностей взлома $P(m,t)$ от любых попыток и времени взлома:

$$P(m,t) = \left[\frac{f(m,t)}{f(m,t)+t}\right]^{\frac{f(m,t)}{t}} \cdot \left[\frac{t}{f(m,t)+t}\right]. \quad (10)$$

Выражение (9) соответствует выбранному физическому требованию зависимости вероятностной надежности $P(m,t)$ от попыток взлома и независимости от времени взлома, когда нет попыток взлома. Для доказательства этого запишем выражение (9) в виде

$$\lim_{t\to\infty} P(m,t) = \lim_{t\to\infty}\left\{\left[\frac{(m-1)\cdot t}{(m-1)\cdot t+t}\right]^{m-1} \cdot \left[\frac{t}{(m-1)\cdot t+t}\right]\right\} = \lim_{t\to\infty}\left[\frac{(m-1)^{(m-1)}}{(m)^{(m)}}\right] = const. \quad (11)$$

В этом случае, если нет последующей попытки взлома, то независимо от текущего времени (вплоть до бесконечного времени) вероятность взлома остается постоянной в соответствие с предыдущей попыткой, так как в выражении (11) время в числителе и знаменателе сокращается. С другой стороны, если попытка возможного взлома стремится к бесконечности, то вероятность взлома будет определяться выражением

$$\lim_{m\to\infty} P(m,t) = \lim_{m\to\infty}\left[\frac{(m-1)^{(m-1)}}{(m)^{(m)}}\right] = \lim_{m\to\infty}\left[\left(\frac{m-1}{m}\right)^{m-1} \cdot \frac{1}{m}\right] = \lim_{m\to\infty}\left[\frac{1}{e\cdot m}\right] = 0. \quad (12)$$

Таким образом, если попытка взлома происходит на бесконечности, то вероятность взлома будет равна нулю.

Функция $f(m,t)$, присущая данной технической защите, определяет ее защитные свойства и направление взлома. Эта функция, которая определяет поверхность максимумов вероятностей взлома $P(m,t)$ и зависит от координат m и t точки взлома. Соотношение между координатами m и t точки взлома при постоянных значениях функции представлены на рис. 1 линиями 1, 2, 3, 4. С возрастанием номера линии от 1 до 4 значение функции будет меняться соответственно 1, 10. 20. 40. Линии 5, 6 дают направление взлома, которое определяется двумя точками взлома. Причем, одна из точек может определяться началом координат, то есть $m\text{-}1=0$ и $t=0$. Таким образом, пересечение линий постоянства функции и направления взлома даст значение максимума вероятности взлома в каждой точке пересечения с данной попыткой взлома.

В реальных условиях каждой определенной попытке взлома соответствуют значения m_1, t_1 и m_2, t_2. Причем каждая последующая попытка взлома будет иметь значения $m_2 > m_1$, $t_2 > t_1$ и, следовательно, согласно выражению (8) значение $f(m,t)$ должно возрастать. На рис. 1 этот факт представлен прямой линией направления взлома (линия 5) между двумя значениями $f(m_1,t_1)$ и $f(m_2,t_2)$ и координатами m_1, t_1 и m_2, t_2.

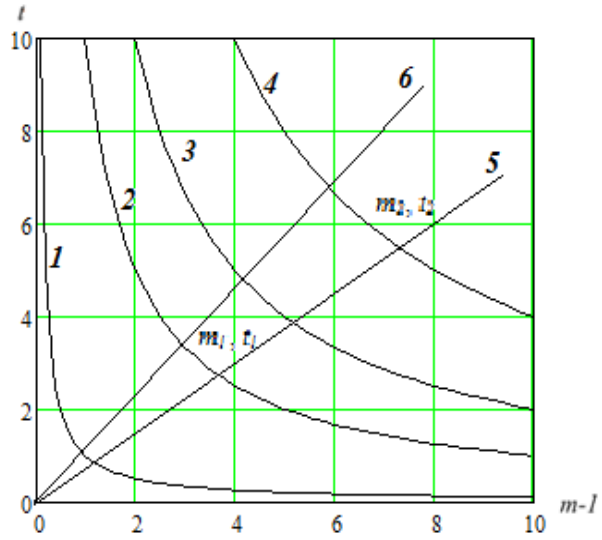

Рис. 1 Соотношение между координатами m и t точки взлома при постоянных значениях функции $f(m,t)$ и линии направления взлома. Линия 1 соответствует $f(m,t) = 1$, линия 2 - $f(m,t) = 10$, линия 3 - $f(m,t) = 20$, линия 4 - $f(m,t) = 40$, линии – 5, 6 дают направления взлома.

Функцию $f(m,t)$ в направлении взлома в зависимости от изменения одной из координат можно представить в виде: времени

$$f(t) = \left[(m_1 - 1) + \frac{m_2-m_1}{t_2-t_1}\cdot(t-t_1)\right]\cdot t \quad (13)$$

и попытки взлома

$$f(m) = \left[t_1 + \frac{t_2-t_1}{m_2-m_1}\cdot(m-m_1)\right]\cdot(m-1). \quad (14)$$

Значения выражений (8), (13) и (14) равны между собой и дают значение максимума вероятности в точке взлома. Выражение (8) определяет поверхность максимумов вероятности взлома (10), которая описывается двумя координатами m и t точки взлома. Выражение (13) дает кривую максимумов вероятности взлома от одной координаты времени t точки взлома. Выражение (14) дает кривую максимумов вероятности взлома от координаты m точки взлома. Таким образом, можем записать

$$f(m,t) = f(t) = f(m). \quad (15)$$

Введем понятие интенсивности или частоты попыток взлома

$$\omega = \frac{m_2-m_1}{t_2-t_1}. \quad (16)$$

В процессе построения, контроля или модернизации ТЗИ может возникать необходимость по одному из известных параметров m или t определить другой, используя функцию ТЗИ $f(t)$ или $f(m)$ и направление взлома. Это позволит при оценке качества ТЗИ определить возможную попытку и ее время взлома при постоянной частоте взлома. Учитывая равенство (15), из выражений (13) и (14) находим зависимость времени от попытки взлома

$$t(m) = \frac{\sqrt{A^2+\frac{4}{\omega}\cdot f(m)}}{2} - \frac{A}{2}, \qquad (17)$$

где $A = t_1 + \frac{m_1-1}{\omega}$,и зависимость попытки взлома от времени

$$m(t) = \frac{\sqrt{B^2+4\cdot\omega\cdot f(t)}}{2} - \frac{B}{2} + 1, \qquad (18)$$

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

Следует учитывать, что в (18) при первой попытке взлома $m(t) = 1$, то есть соответствует предстоящей реальной попытке взлома, когда реальное начальное время еще равно нулю.

Функция $f(m,t)$ определяет направление взлома, но не учитывает эффективность защищенности, то есть дает значение максимума вероятности взлома при коэффициенте эффективности защиты (КЭЗ) равном $\gamma = 1$, что соответствует взлому на бесконечной попытке. В реальных условиях взлом происходит на конечной попытке при КЭЗ меньше единицы. В работах [6,7] показано, что коэффициент эффективности защиты может быть вычислен через значения вероятностей двух любых известных попыток взлома и представлен в виде:

$$\gamma = \frac{\ln P1 - \ln P2}{\ln[P(m_1\, t_1)] - [P(m_2\, t_2)]}, \qquad (19)$$

где *P1*, *P2* – реальные известные вероятности в первой и второй точках взлома соответственно, $P(m_1, t_1)$, $P(m_2, t_2)$ – расчетные вероятности в первой и второй точках взлома соответственно.

Учитывая КЭЗ в соответствие с [7], выражение (10) будет иметь вид:

$$P(m,t) = \left\{\left[\frac{f(m,t)}{f(m,t)+t}\right]^{\frac{f(m,t)}{t}} \cdot \left[\frac{t}{f(m,t)+t}\right]\right\}^{\gamma}. \qquad (20)$$

При проектировании ТЗИ параметры взлома закладываются разработчиком и должны соответствовать исходным данным. В этом случае необходимо знать вероятностную надежность ТЗИ в проектируемом направлении взлома и в направлении реального процесса взлома. Чтобы построить проектируемую поверхность для конкретной попытки взлома и времени взлома, выбранной разработчиком защиты, в выражениях (9) или (10) необходимо выразить степень через параметры конкретной попытки взлома, например, $m = m_c$, $t = t_c$. Тогда (9) будет иметь вид

$$P(m,t) = \left\{\left[\frac{f(m,t)}{f(m,t)+t}\right]^{m_c-1} \cdot \left[\frac{t}{f(m,t)+t}\right]\right\}^{\gamma}, \qquad (21)$$

а (10)

$$P(m,t) = \left\{\left[\frac{f(m,t)}{f(m,t)+t}\right]^{\frac{f(m_c,t_c)}{t_c}} \cdot \left[\frac{t}{f(m,t)+t}\right]\right\}^{\gamma} = \left\{\left[\frac{f(m,t)}{f(m,t)+t}\right]^{\frac{f(m_c)}{t_c}} \cdot \left[\frac{t}{f(m,t)+t}\right]\right\}^{\gamma}. \qquad (22)$$

В выражении (14) заменяем m на m_c и получаем $f(m_c)$. Время t_c берется из исходных параметров. Если есть проектируемое направление взлома и задано время взлома, то вместо функции $f(m_c)$ можно использовать $f(t_c)$, заменяя t на t_c в выражении (22).

На рис. 2 построена поверхность максимумов вероятности взлома по формуле (20). По этой формуле каждая точка строится по максимуму вероятности взлома ТЗИ с эффективностью защиты γ =0,7.

Представлена поверхность с выбранным направлением взлома по линии 5, а линия 6 соответствует другому, например, реальному направлению взлома. По линиям 5 и 6 построены вероятности взлома в зависимости от направления взлома. Точки пересечения поверхности с линиями дают координаты вероятности взлома в данном направлении. Для линии 5 эти координаты будут $m_м$ = 9, $t_м$ = 6 с максимумом вероятности взлома в данной точке, а для линии 6 – $m_м$ = 12, $t_м$ = 11.

На рис. 3 представлена поверхность с максимумом вероятности взлома в точке с выбранным направлением взлома по линии 5, например, с максимумом в точке m_c=9, t_c=6. Линия 5 соответствует выбранному направлению, а линия 6 другому реальному направлению взлома, но на поверхности линии 5.

Из рис. 3 видно, что при изменении направления взлома (линия 6) надежность ТЗИ будет меняться и при ее проектировании необходимо это учитывать. На поверхности по координатам m, t видны максимумы значений вероятностей взлома. Точка пересечения обоих максимумов и направления линии дает точку максимума вероятности взлома в данном направлении. Такая точка может быть только одной и на рис. 2 представлена пересечением поверхности с линией направления процесса взлома для линии 5 эти координаты будут $m_м$ = 9, $t_м$ = 6, а для линии 6 – $m_м$ = 12, $t_м$ = 11.

Выводы. Из рисков защищенности ТЗИ получена функция $f(m,t)$, которая присуща данной технической защите, зависит от направления процесса взлома и определяет вероятностную надежность технической защиты в направление взлома. Показано, что эта функция соответствует здравому смыслу и физическим требованиям процесса взлома.

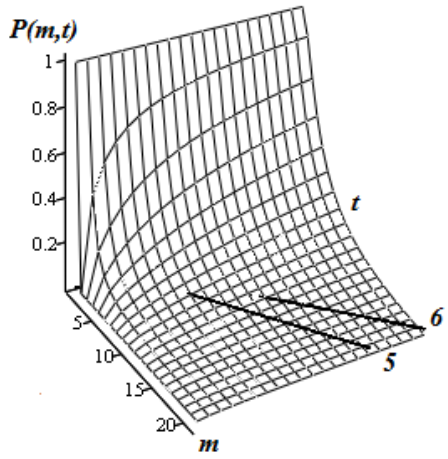

Рис. 2. Поверхность максимумов вероятности взлома, построенная по формуле (20) с эффективностью защиты γ =0,7; 5, 6 – линии взлома, направление которых соответствуют линиям рис. 1. Точки пересечения поверхности с линиями дают координаты максимума вероятности взлома в данном направлении.

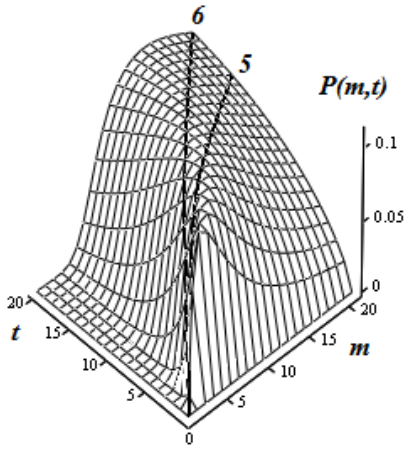

Рис. 3. Поверхность с максимумом вероятности взлома в точке с выбранным направлением взлома по линии 5 с максимумом в точке m_c = 9, t_c = 6. Линия 5 соответствует выбранному направлению, а линия 6 реальному направлению взлома.

Из функции направления процесса взлома получено выражение, позволяющее по одному из параметров m или t, определять другой. Это выражение важно при проектировании, анализе состояния и модернизации ТЗИ, потому что позволит по одному из известных параметров по направлению взлома найти другой. Например, по известной попытке взлома можно оценить возможное время, когда это произойдет.

В данной работе получено распределение максимумов вероятности взлома ТЗИ для направления практического взлома, зависящего от параметров попытки, времени этой попытки взлома и коэффициента эффективности защищенности. Следует заметить, что практический процесс взлома является случайной величиной, как по попыткам, так и времени взлома, и не отображается прямой линией. В реальных условиях направление взлома может определяться по методологии, как это было предложено в работе [6]. При проектировании процесс взлома выбирается в виде прямой линии, которая строится по требуемым исходным данным.

По полученным выражениям построена поверхность максимумов вероятности взлома (рис. 2), по которой в точках пересечения поверхности и линии определяется наиболее вероятное значение взлома и координаты точки взлома. Построено распределение вероятности взлома (рис. 3) по линиям направления взлома (линии 5, 6). Эти выражения важны при оценке ТЗИ по ее вероятностной надежности.

В результате проделанной работы можно представить, как происходит реальный физический процесс взлома.

ЛИТЕРАТУРА

[1]. Б. Журиленко, Н. Николаева, Н. Пелих, "Оптимальные финансовые затраты и основные критерии построения или модернизации комплекса технической защиты информации", *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*, Київ, КПІ НДЦ «Тезіс», випуск 1 (22), С. 33-43, 2011.

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

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

[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, Н. Николаева, "Определение направления взлома технической защиты информации по его параметрам", *Інформаційні управляючі системи та технології: міжнар. наук.-практ. конф., 23-25 вересня 2014 р.: тези доп.*, С. 168-171.

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

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

[8]. Л. Румшинский, *Элементы теории вероятностей*, М.: Изд-во «Наука», Главн. Ред. Физ.-мат. Лит., 1970, 256 с.

PROBABILITY RELIABILITY OF TECHNICAL PROTECTION OF INFORMATION DEPENDING ON BACKGROUND

This paper presents a theoretical study of the proposed new direction in the design, analysis of the state and timely modernization of the operating technical information protection (TZI) depending on the hacking process in the direction of hacking. Based on the risks of protection of TZI, the function inherent in this technical protection is obtained, depending on the parameters of the direction of the hacking process and determining the probabilistic reliability of technical protection in the direction of hacking. It is shown that this function meets the physical requirements of the hacking process. An expression is obtained from the direction function of the hacking process, which allows one or another unknown time or attempt parameter to be determined from the parameters of the attempt or the time of the hacking. For example, by a known hacking attempt, it is possible to estimate the possible time when a TZI hacking will occur, or, conversely, to determine an attempt by a known time. In this paper, the distribution of the maximums of the probability of breaking into technical protection is obtained for directions of breaking depending on the parameters of the attempt, the time of this attempt and the protection effectiveness ratio. It should be noted that the actual process of hacking is a random variable, both in attempts and in the time of hacking, so the direction of hacking is not displayed as a straight line. In real conditions, the direction of hacking can be determined according to the methodology, as proposed in the works of B. Zhurilenko, in a straight line. In this case, the direction of the line is defined as the rms or mean value of the results of the attempts and its hacking time. As a result of the studies carried out according to the obtained theoretical expressions, the distribution surface of the maxima of probabilistic cracking of the CRT and the probability in the direction of the cracking process line, depending on its two parameters - the number of the attempt and its cracking time, are constructed. The resulting expressions will be of great importance in the design, analysis of the working state of the working TZI and modernization of protection to save the invested financial costs in protection.

Keywords: technical protection of information, efficiency coefficient of protection, distribution of the maximum probability of breaking, attempt of breaking, time of attempt of breaking, line of direction of breaking.

ІМОВІРНА НАДІЙНІСТЬ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ В ЗАЛЕЖНОСТІ ВІД НАПРЯМКИ ЗЛОМУ

У даній роботі наведено теоретичне дослідження запропонованого нового напряму в проектуванні, аналізі стану та своєчасної модернізації працюючого технічного захисту інформації (ТЗІ) в залежності від того, як відбувається процес злому в напрямку злому. Ґрунтуючись на ризиках захищеності ТЗІ, отримана функція притаманна даному технічному захисту, яка залежить від параметрів напрямку процесу злому і визначає вірогідність надійності технічного захисту в напрямку злому. Показано, що ця функція відповідає фізичним вимогам процесу злому. З функції напрямку процесу злому отримано вираз, який дозволяє з параметрів спроби або часу злому визначити один або інший невідомий параметр часу або спроби. Наприклад, за відомою спробою злому можна оцінити можливий час, коли відбудеться злом ТЗІ або, навпаки, за відомим часом визначити спробу. В роботі отримано розподіл максимумів ймовірності злому технічного захисту для напрямків злому, які залежать від параметрів спроби, часу цієї спроби злому і коефіцієнта ефективності захищеності. Слід зауважити, що реальний процес злому є випадковою величиною, як по спробах, так і за часом злому, тому напрямок злому не відображається прямою лінією. В реальних умовах напрямок злому можна визначити за методологією, яка була запропонована в роботах Б. Журиленка, по прямій лінії. У цьому випадку напрямок лінії визначається як середньоквадратичне або середнє значення результатів спроб і його часу злому. В результаті проведених досліджень по отриманим теоретичним виразам побудовані поверхня розподілу максимумів ймовірності злому ТЗІ і ймовірність в напрямку лінії процесу злому, що залежить від його двох параметрів - номера спроби і його часу злому. Отримані вирази будуть мати велике значення при проектуванні, аналізі робочого стану працюючої ТЗІ і модернізації захисту для економії вкладених фінансових витрат на захист.

Ключові слова: технічний захист інформації, коефіцієнт ефективності захисту, розподіл максимуму ймовірності злому, спроба злому, час спроби злому, лінія напрямку злому.

Журиленко Борис Евгеньевич, кандидат физико-математических наук, доцент кафедры автоматизации и энергоменеджмента Национального авиационного университета.

Журиленко Борис Євгенович, кандидат фізико-математичних наук, доцент кафедри автоматизації та енергоменеджменту Національного авіаційного університету.

E-mail: zhurylenko@gmail.com.

Zhurilenko Boris, Candidate of Physical and Mathematical Sciences, assistant professor of automation and energy management of the National Aviation University.

Николаева Надежда Константиновна, инженер 1-ой категории кафедры автоматизации и энергоменеджмента Национального авиационного университета.

E-mail: nnikolaeva1717@gmail.com.

Ніколаєва Надія Костянтинівна, інженер 1-ої категорії кафедри автоматизації та енергоменеджменту Національного авіаційного університету.

Nikolaeva Nadezhda, engineer of the 1st category of the Automation and Energy Management Department of the National Aviation Universit