МАТЕМАТИЧЕСКОЕ ПРЕДСТАВЛЕНИЕ ВЕРОЯТНОСТНОЙ НАДЕЖНОСТИ ЗАЩИТЫ ИНФОРМАЦИИ В ЗАВИСИМОСТИ ОТ НАПРАВЛЕНИЯ ВЗЛОМА

Журиленко Б., Николаева Н.

В работе представлено теоретическое исследование для разработки методологии нового подхода к проектированию, анализу состояния и своевременной модернизации работающей технической защиты информации (ТЗИ) в зависимости от направления происходящего процесса взлома. В работе, теоретически более строго получена функция, определяющая вероятностную надежность проектируемой технической защиты, и ее зависимость от параметров направления процесса взлома. Функция позволяет из параметров процесса взлома вычислить один или другой неизвестный параметр времени или попытки. Например, по известной попытке взлома можно получить возможное время, когда произойдет взлом ТЗИ или, наоборот, по известному времени определить попытку. Поскольку реальный процесс взлома является случайной величиной от попыток и времени взлома, поэтому направление взлома не отображается прямой линией.

В этих условиях функция направления линии взлома будет определяться как среднеквадратичное или среднее значение результатов реальных попыток и его времени. Результаты исследования позволяют в случае проектирования ТЗИ по распределению максимумов вероятности взлома определить максимальные вероятности взлома для любых направлений этого процесса. Получено выражение для распределения вероятности взлома. С помощью этого распределения показана возможность определения вероятности, попытки и времени реального процесса взлома ТЗИ, вероятность взлома которого не будет максимально возможной. В этом случае также можно определять вероятность процесса защиты информации во времени, а также анализировать ее реальное состояние, если злоумышленник поменял направление процесса взлома. Результаты проведенных исследований могут иметь большое значение для разработки новой методологии ТЗИ, учитывающей вложенные финансовые затраты в защиту, эффективность защиты и направление процесса взлома.

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

ВВЕДЕНИЕ

В настоящее время в Украине теоретически исследуются защиты информации, в основном, с использованием системного подхода [1], экспертной оценки анализа с помощью нечетких множеств [2-3] и теории игр [4]. Однако при наличии определенных положительных моментов, связанных с разработкой защиты информации этими методами, все они имеют существенные недостатки. Основной

недостаток этих подходов является качественная оценка защиты и невозможность оценки ее состояния в процессе работы.

Техническая защита информации (ТЗИ) в различных странах осуществляется в соответствии со своими нормативными документами и разрабатываемыми методами. Различные фирмы и предприятия, для которых создается ТЗИ, в первую очередь, интересует экономическая выгода применения той или иной защиты. Для технических и экономических расчетов, используемых в проектировании технической защиты из всех возможных параметров, понятных для заказчика и разработчика, являются величины рисков полных финансовых потерь, величины рисков потерь вложенного финансирования и вероятности взлома защиты, как в начальной стадии защиты, так и в процессе ее работы. Как и в работе [5], для расчетов финансовых затрат могут использоваться известные начальные финансовые потери без защиты, риски потерь вложенных финансовых затрат на выбранную защиту с данной вероятностью взлома, риски потерь полных финансовых затрат, вероятность взлома и эффективность выбранной защиты.

ПОСТАНОВКА ПРОБЛЕМЫ

В открытой литературе [2-4,6] приводятся методы расчета рисков, финансовых затрат и оценка эффективности защиты информации. Однако, нет конкретных рекомендаций расчетов, которые определялись бы конкретными параметрами такими как: эффективность финансовых расходов на создание ТЗИ, оптимизация финансовых потерь в случае взлома защиты, критериев необходимости дополнительных затрат на восстановление защиты до необходимого технического уровня и, соответственно, оптимизации финансовых потерь. В рассматриваемых работах построенная ТЗИ, в основном, имеет качественную оценку, которая отвечает начальным условиям использования защиты.

С другой стороны для разработчика при проектировании и эксплуатации ТЗИ важно знать возможную вероятность взлома защиты на каждом этапе ее работы в зависимости от направления процесса взлома. Реальное направление взлома можно определить из попыток и времени этих попыток взлома, хотя этот процесс носит случайный характер. Основным требованием для вероятностной надежности должна быть ее зависимость от параметров попыток взлома. Зависимость вероятностной надежности от времени определяется направлением взлома и носит зависимый характер от попытки взлома. Отсутствие попытки взлома не должно изменять вероятностную надежность с изменением времени, и только при наличии попытки взлома вероятностная надежность должна изменяться. В общем случае распределение вероятностной надежности ТЗИ должно определяться попыткой и временем этой попытки взлома. В реальных условиях при

взломе ТЗИ фиксируемыми фактами или параметрами могут быть попытка взлома и ее время. Зная в каждый момент времени вероятность взлома работающей ТЗИ, разработчик может предсказать попытку и время возможного взлома ТЗИ. Направление взлома можно определить всегда, например, по количеству попыток и времени этих попыток взлома [7]. Таким образом, данный подход к построению ТЗИ позволить получить для нее количественную оценку в виде вероятности и оценить состояние в процессе ее работы. Эти результаты дадут возможность разработчику принять решение о замене используемой ТЗИ или ее модернизации, что позволит сэкономить финансовые и материальные ресурсы, вкладываемые в защиту информации.

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 позволил бы определить интенсивность и направление взлома. Поскольку направление взлома зависит от двух параметров, то вероятностная надежность также должна зависеть от двух этих параметров и должна быть связана между собой направлением взлома. Существуют публикации Б. Журиленко, в которых сделана попытка разработать методологию построения защиты, позволяющей осуществлять контроль ее состояния в процессе работы, давать рекомендации для модернизации ТЗИ в зависимости от финансовых вложений на защиту, эффективности создаваемой защиты и направлению взлома. Однако в этих работах недостаточно строго была показана вероятностная надежность в зависимости от направления взлома.

ФОРМУЛИРОВАНИЕ ЦЕЛИ ИССЛЕДОВАНИЙ

Актуальность работы заключается в том, чтобы в отличие от нормативных документов разработать новый подход к требованиям 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.

Целью работы является получение распределения максимума вероятности взлома ТЗИ и распределение вероятности взлома защиты в зависимости от направления взлома, которые определяются двумя параметрами – попыткой и временем этой попытки взлома.

Задача исследования – разработка методологии и способа получения распределений вероятностей взлома ТЗИ с учетом направления взлома.

Объект исследования – является процесс технической защиты информации.

Предмет исследования – распределение вероятностной надежности ТЗИ в зависимости от направления взлома.

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

ИЗЛОЖЕНИЕ ОСНОВНОГО МАТЕРИАЛА ИССЛЕДОВАНИЙ

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

Для получения выражения распределения вероятностной надежности ТЗИ от направления взлома примем следующие предположения. Пусть t_0 – некоторый параметр создаваемой ТЗИ, зависящий от направления взлома, и вид которого 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), отметим, что для обеспечения защиты информации функция рисков защищенности $f(t)$ с ростом времени t должна быть хотя бы постоянной. Если функция $f(t)$ со временем будет уменьшаться, то используемая защита является неэффективной и ее необходимо заменить на другую более эффективную защиту. Если $f(t)$ увеличивается со временем, то такая защита в процессе эксплуатации более эффективна, так как риски защищенности увеличиваются со временем.

Таким образом, чтобы иметь более эффективную защиту, выбираем в виде степенного многочлена первого порядка [8] в соответствие с левой частью формулы (1) и требованием независимости вероятностной надежности ТЗИ от времени, когда нет попытки взлома.

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

Поскольку $f(t)$ произвольная положительная функция, то коэффициенты в выражении (2) должны быть $\alpha \geq 0$, $\beta \geq 0$ при любом значении $t \geq 0$.

Выражение вероятности защищенности из (1) будет иметь вид

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

Учитывая начальные условия при $t=0$, вероятность защищенности будет полная и $p'(0)=1$. Тогда получим

$$p'(0) = \frac{f(t)}{(t_0)} = 1 \quad : f(t) = t_0 \,. \tag{4}$$

Следовательно, получим вероятность защищенности ТЗИ в виде

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

Определим вероятность взлома во времени

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

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 [9].

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

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

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

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

Поскольку ранее было принято, что $\alpha \geq 0$, $\beta \geq 0$ при любом значении времени $t \geq 0$, 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

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

а поверхность максимумов вероятностей взлома $P(m,t)$ - функцией $f(m,t)$ любых попыток и времени взлома

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

Выражение (9) или (10) должны соответствовать физическому требованию зависимости вероятностной надежности $P(m,t)$ от попыток взлома и независимости от времени, когда нет попыток взлома. Для доказательства этого требования запишем выражение (9) в виде

В результате получим

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

$$= \lim_{t\to\infty}\left[\frac{(m-1)^{(m-1)}}{(m)^{(m)}}\right] = const. \qquad (11)$$

Из выражения (11) видно, что если нет последующей попытки взлома, то независимо от текущего времени (вплоть до бесконечного времени) вероятность взлома остается постоянной в соответствие с предыдущей попыткой. С другой стороны, если попытка возможного взлома стремится к бесконечности, то вероятность взлома будет определяться выражением

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

.

Таким образом, если попытка взлома происходит на бесконечности, то вероятность взлома будет равна нулю, что соответствует физическому требованию вероятностной надежности и здравому смыслу. Функция $f(m,t)$, присущая данной технической защите, определяет ее защитные свойства и направление взлома. Эта функция также определяет поверхность максимумов вероятностей взлома $P(m,t)$ и зависит от координат точек взлома. Соотношение между координатами *m* и *t* точек взлома при постоянных значениях функции $f(m,t)$ представлены на рис.1 линиями 1, 2, 3, 4. С возрастанием номера линии от 1 до 4 значение функции будет возрастать соответственно 1, 10. 20. 40. Линии 5, 6 дают направление взлома, которое определяется двумя точками взлома. В реальных условиях начальная точка взлома может определяться началом координат, то есть *m-1=0* и *t=0*. Таким образом, пересечение линии постоянства функции (гиперболические линии на рис.1) и линии направления взлома дает значение максимума вероятности взлома в каждой точке пересечения с данной попыткой взлома.

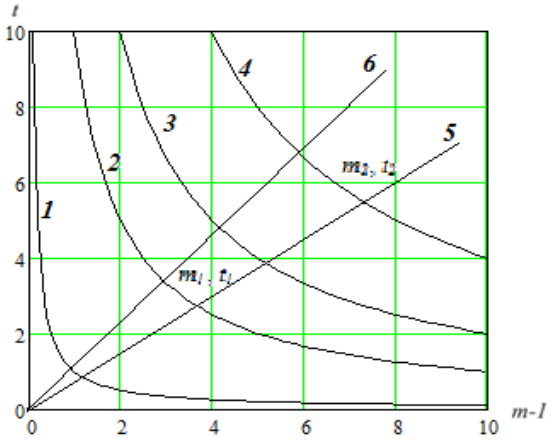

Рис.1– Соотношение между координатами *m* и *t* точки взлома при постоянных значениях функции $f(m,t)$ и линии направления взлома. Линия 1 соответствует функции $f(m,t) = 1$, линия 2 - $f(m,t) = 10$, линия 3 - $f(m,t) = 20$, линия 4 - $f(m,t) = 40$, линии – 5, 6 дают направления взлома.

В реальных не начальных условиях каждой определенной попытке взлома соответствуют значения m_1, t_1 и m_2, t_2. 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 с увеличением времени или попытки взлома. Направление взлома будет определяться линией между координатами взлома. 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. Функцию $f(m,t)$ в направлении линии взлома с изменением одной из координат можно представить в виде функции времени

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

,

и в виде функции попытки взлома

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

При одной и той же попытке взлома выражения (8), (13) и (14) равны между собой и соответствуют максимуму вероятности взлома в данной точке. Выражение (8), отвечающее за параметры защиты, определяет поверхность максимумов вероятности взлома, которая описывается выражением (10) и, следовательно, описывается двумя координатами m и t точки взлома. Выражение (13) описывает кривую максимумов вероятности взлома от одной координаты времени t точки взлома. Выражение (14) описывает кривую максимумов вероятности взлома от координаты m точки взлома. Таким образом, можем записать

$$f(m,t) = f(t) = f(m) \qquad (15)$$

Введем понятие интенсивности или частоты попыток взлома

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

В процессе построения, контроля или модернизации ТЗИ может возникать необходимость по одному из известных параметров m или t определить другой, используя функцию $f(t)$ или $f(m)$ и направление взлома. Это позволит при оценке качества ТЗИ определить возможную попытку и ее время взлома.

Учитывая равенство (15), из выражений (13) и (14) найдем зависимость времени от попытки взлома

$$t(m) = \frac{\sqrt{A^2 + \frac{4}{\omega} \cdot f(m)}}{2} - \frac{A}{2}, \text{ где } A = t_1 + \frac{m_1 - 1}{\omega}, \quad (17)$$

и зависимость попытки взлома от времени

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

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 поверхность максимумов вероятности 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 [5,7,10] показано, что коэффициент эффективности защиты может быть вычислен через значения вероятностей двух любых известных попыток взлома и представлен в виде

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

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 [10], выражение (19)

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

При проектировании технической защиты информации параметры взлома закладываются разработчиком и соответствуют исходным данным. Для разработчика защиты важно знать

вероятностную надежность ТЗИ в проектируемом направлении взлома и в направлении реального процесса взлома. Чтобы построить проектируемую поверхность с выбранными разработчиком параметрами защиты, в выражениях (9) или (10) необходимо выразить степень через параметры конкретной проектируемой 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 попытку взлома и получаем $f(m_c)$. Время t_c время взлома берется из исходных параметров. Если есть проектируемое направление взлома и задано время взлома, то вместо функции $f(m_c)$ используем $f(t_c)$, заменяя t на t_c в выражении (22). На рис.2 построена проектируемая поверхность максимумов вероятности взлома ТЗИ по формуле (20). По этой формуле каждая точка строится по максимуму вероятности взлома ТЗИ с эффективностью защиты $\gamma = 0{,}7$, выбранной для иллюстрации математического представления вероятностной надежности ТЗИ в направлении взлома. На рисунке представлена поверхность с выбранным направлением взлома по линии 5, а линия 6 соответствует другому, например, реальному направлению взлома. Точки пересечения поверхности с линиями дают координаты максимумов вероятности взлома в данном направлении. Для линии 5 это будут, выбранные разработчиком защиты, исходные координаты $m_м = 9$, $t_м = 6$ с максимумом вероятности взлома в данной точке, а для линии 6 – реального направления взлома в точке $m_м = 12$, $t_м = 11$. На рис.3 представлена поверхность распределения вероятности взлома с максимумом в точке с выбранным направлением взлома по линии 5 ($m_c = 9$, $t_c = 6$). Линия 6 соответствует другому реальному направлению взлома, но на поверхности распределения вероятности взлома, которая рассчитана для проектируемого направления взлома по линии 5. Из рис. 3 видно, что при изменении направления взлома (линия 6) надежность ТЗИ будет меняться и при ее проектировании необходимо это учитывать.

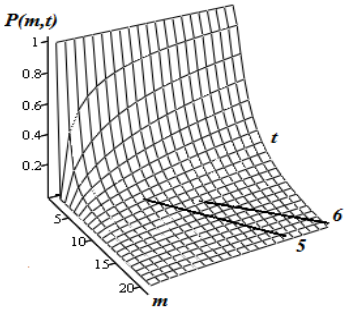

Рис.2 - Поверхность распределения максимумов вероятности взлома

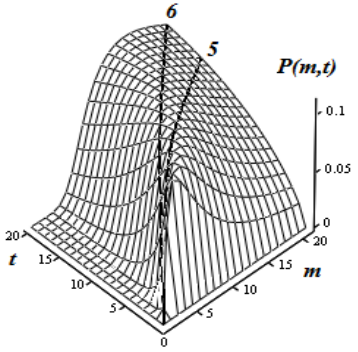

Рис.3 - Поверхность распределения вероятности взлома

Поверхность распределения максимумов вероятности взлома (рис.2), построенная по формуле (20) с эффективностью защиты $\gamma =$ 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.

Поверхность распределения вероятности взлома (рис.3) в точке с выбранным направлением взлома по линии 5 и максимумом в точке $m_c = 9$, $t_c = 6$. Линия 5 соответствует выбранному направлению, а линия 6 реальному направлению взлома

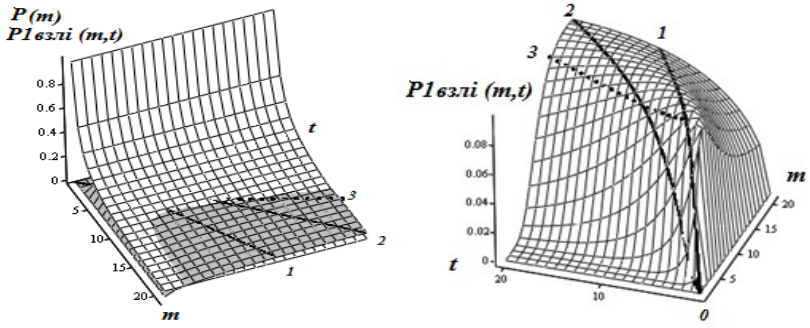

Рис.4 - Распределение вероятности взлома: **а** – с проектируемым направлением взлома по линии 1(серая поверхность); **б** – реальная поверхность взлома (белая поверхность), рассчитываемая по формуле P(m)=1/m

На рис.4а представлена поверхность с максимумом вероятности взлома в точке с другим проектируемым направлением взлома по линии

1, максимум которого в точке $m_c = 10$, $t_c = 5$. Линия 2 соответствует другому реальному направлению взлома, но на поверхности, определяемой направлением взлома по линии 1. Линия 3 дает направление реального взлома, если злоумышленник изменил реальный процесс нападения. 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 на рис.4а представлена пересечением поверхности с линией 1 проектируемого направления процесса взлома с координатами $m_м = 10$, $t_м = 5$, а для линии 2 с $m_м$=12, $t_м = 11$. Из рис.4б видно, что реальный процесс взлома с поверхностью вероятности взлома описываемой выражением ***P(m)=1/m*** (белая поверхность) и поверхностью спроектированной защиты (серая поверхность) будет проходить с вероятностью определяемой линией пересечения белой и серой поверхностей. В данном случае, согласно рис.4б, 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 защиты может не произойти совсем. Аналогичная ситуация, когда взлом не произойдет, возможна, если попытки взлома будут следовать очень часто друг за другом.

ВЫВОДЫ

Из рисков защищенности ТЗИ получена функция $f(m, t)$, зависящая от направления процесса взлома, которая присуща данной технической защите и определяет вероятностную надежность технической защиты в направление взлома.

Из функции направления процесса взлома перспективным является выражение, позволяющее по одному из параметров m или t, определять другой. Это 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 произойдет взлом защиты.

В данной работе получено распределение вероятности взлома ТЗИ для направления проектируемого процесса взлома, зависящего от параметров попытки, времени этой попытки взлома, финансовых вложений в защиту и коэффициента эффективности защищенности. При

проектировании защиты направление взлома выбирается в виде прямой линии, которая строится по требуемым исходным данным. Следует заметить, что реальный процесс взлома является случайной величиной, как по попыткам, так и времени взлома, и не отображается прямой линией. Для анализа состояния работающей технической защиты направление взлома может определяться по методологии, как это было предложено в работе [10].

По полученным в работе 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. Построены поверхности распределения вероятности взлома (рис.3, рис.4а) по линиям проектируемых направлений взлома (линии 5, линия 1). Результаты работы позволяют оценить состояние остаточной вероятности надежности работающей ТЗИ реального процесса взлома в выбранных злоумышленником направлениях нападения.

Проведенные исследования в перспективе позволят создать новую методологию проектирования, модернизации и анализа состояния работающего комплекса технической защиты информации, с учетом вложенного в защиту финансирования, эффективности разработанной защиты и выбранного разработчиком направления взлома.

СПИСОК ЛИТЕРАТУРЫ

[1] Домарев В.В. Безопасность информационных технологий. Системный поход, К.: ООО «ТИД «ДС», 2004. – 992 с.

[2] Корченко А.Г. Построение систем защиты на нечетких множествах. Теория и практические решения, К.: «МК-Пресс», 2006. – 320 с.

[3] Архіпов О.Є. Оцінювання якості роботи експертів за даними багатооб'єктної експертизи // Захист інформації: науково-технічний журнал. - К.: НАУ, 2011. –№4 (53). – С. 45 – 54.

[4] Грищук Р.В. Теоретичні основи моделювання процесів нападу на інформацію методами теорії диференціальних ігор та диференціальних перетворень: Монографія, Житомир : Рута, 2010. – 280 с.

[5] Журиленко Б.Е.Оценивание финансовых затрат на построение системы защиты информации // Науково-технічний журнал «Захист інформації», 2018. – №4(20). – С. 231–239. DOI: 10.18372/2410-7840.20.13424

[6] Кравченко В.І. Використання теорії нечітких множин для визначення втрат на захист інформації // Науково-технічний журнал «Захист інформації», 2011. – №1. – С.85 – 90.

[7] Журиленко Б.Е. Моделирование процесса взлома и анализа рабочего состояния технической защиты информации // Безпека інформації, 2016. – №1(22). – С. 26 – 31.

[8] Андре Анго Математика для электро- и радиоинженеров, М.: Из-во «Наука», 1964. – 772 с.
[9] Румшинский Л.З. Элементы теории вероятностей , М.: Изд-во «Наука», Главн. Ред. Физ.-мат. Лит., 1970. – 256 с.
[10] Журиленко Б.Е.Методология построения и анализа состояния комплекса технической защиты информации с вероятностной надежностью и учетом временных попыток взлома // Науково-технічний журнал «Захист інформації», 2015. – №3(17). – С.196 – 204

MATHEMATICAL REPRESENTATION OF PROBABILISTIC RELIABILITY OF INFORMATION PROTECTION DEPENDING ON HACKING DIRECTION

Zhurilenko B., Nikolaeva N.

In this paper, a theoretical study is presented for further development of methodology of a new approach to designing, analyzing the state and timely modernization of working technical information protection (TIP), depending on the direction of the ongoing hacking process. In the work, there was obtained a theoretically more rigorous function that determines the probabilistic reliability of the designed technical protection, and its dependence on the direction parameters of the hacking process. The function allows one or another unknown parameter, either time or attempt, to be calculated from the parameters of the hacking process. For example, using a known hacking attempt, you can get the possible time when a TIP hacking will occur, or, conversely, using a known time to determine the attempt. Since the real process of hacking is a random variable from the attempts and time of hacking, the direction of the hack is not displayed by a straight line. Under these conditions, the direction function of the cracking line will be determined as the mean square or average value of the results of real attempts and its time. The results of the study allow, in the case of designing a TIP to distribute the maximum probabilities of breaking, to determine the maximum probabilities of breaking for any direction of this process. An expression is obtained for the probability distribution of hacking. Using this distribution, the possibility of determining the probability, attempt and time of a real process is shown for hacking TIP with breaking probability different from maximum possible one. In this case, it is also possible to determine the probability of the process of protecting information over time, as well as analyze its real state if the attacker changed the direction of the hacking process. The results of the research can be of great importance for the development of a new TIP methodology that takes into account the financial investment in defense, the effectiveness of the defense and the direction of the fracture process.

Keywords/ Technical protection of information, protection efficiency coefficient, distribution of the maximum probability of hacking, attempted hacking, time of attempted hacking, line of direction for breaking.