Разработан алгоритм совмещения оцифрованных документов и попиксельного сравнения соответствующих изображений документов и разработан программный продукт, который реализирует эти алгоритмы с целью определения достоверности контролируемого документа. Эффективность разработанного программного продукта была доказана с помощью проведенных экспериментов, которые описаны в статье.
Ключевые слова: *идентификация печатных документов, коэффициент PSNR, информация на материальных носителях, графические методы защиты.*

Dronjuk I.M., Nazarkevych M.A., Opotiak Yu.V. Determination of the printed documents reliability by the per-pixel comparing
Abstract. *The paper presents a method of determining authenticity of a printed document, based on the signal-to-noise ratio criteria, which is calculated from pixel by pixel comparison of controlled and reference document images. The algorithm combines digitized documents and pixel by pixel identity checking of the appropriate document images, and processes the software tool that implements these algorithms on purpose to determine authenticity of the controlled document. Effectiveness of the software product was proved on the basis of experiments described in this paper.*
Key words: *authenticity of a printed document, coefficient PSNR, high-security printing.*

Отримано *16 січня 2013 року*, затверджено редколегією *20 лютого 2013 року*

ОПРЕДЕЛЕНИЕ ВЕРОЯТНОСТНОЙ НАДЕЖНОСТИ ЕДИНИЧНОЙ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ ИЗ РЕАЛЬНЫХ ПОПЫТОК ВЗЛОМА

Борис Журиленко

Национальный авиационный університет, Україна

ЖУРИЛЕНКО Борис Евгеньевич, к.ф.-м.н., доцент, с.н.с.

Год и место рождения: 1946 год, г. Чугуев Харьковской области, Украина.
Образование: Киевский государственный университет им.Т.Г.Шевченко, 1974 год.
Должность: доцент кафедры методов защиты информации с 2003 года.
Научный интерес: методы съема и методы технической защиты информации.
Публикации: более 80 научных статей и патентов на изобретения.
E-mail: zhurilenko@mail. ru

Аннотация. *В результате проведенной работы предложен метод для определения вероятностной надежности технической защиты информации на основании реальных попыток взлома. Предложенный метод позволяет оценить вероятностную надежность единичных систем защиты, а при установке ее на нескольких объектах предсказать не только попытку, но и время, при которых вероятен взлом на других объектах.*

Ключевые слова: *защита информации, надежность, вероятность взлома, комплекс технической защиты информации.*

Введение

Современный этап выбора, исследования, проектирования, создания и эксплуатации комплекса технической защиты информации (КТЗИ) требует использования данных, ориентированных на специально проведенные экспериментальные исследования или на реальные результаты взлома используемых защит. Такой подход позволит сэкономить финансовые ресурсы, провести исследования КТЗИ, выработать рекомендации для его модернизации или новые требования для его разработки. Основными трудностями, связанными с реальными результатами взлома используемых защит, является необходимость взлома защиты и, естественно, невозможность сбора статистических данных о результатах взлома, так как такая защита после взлома не может использоваться в дальнейшем. Проведение специальных экспериментальных исследований – это фактически проведение попыток взлома, которые требуют соответствующего уровня секретности сохранения методов и результатов исследований, что не всегда может быть обеспечено с помощью

организационных мер защиты и малых финансовых затрат на эту защиту.

С другой стороны, если создать метод или методологию, с помощью которой по отдельным взломам или результатам попыток взлома определять вероятность надежности комплекса технической защиты информации (КТЗИ) и ее эффективность, то можно было бы исследовать, проектировать, создавать и эксплуатировать КТЗИ, опираясь на объективные практические результаты.

Целью данной работы является создание метода и методологии для определения вероятностной надежности КТЗИ из отдельных попыток взлома или результатов попыток взлома во времени.

Анализ существующих исследований

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

Системный подход [1] имеет как минимум 140 параметров – вопросов по организуемой системе защиты информации, на которые необходимо дать экспертные ответы. В то же время эти ответы не исчерпывают вопросы по организуемой защите. Решение проблемы защиты с помощью данного подхода идет по пути увеличения количества параметров – вопросов, что усложняет анализ КТЗИ или комплексной системы защиты информации (КСЗИ), и не дает однозначного ответа.

Использование экспертных оценок аналитиков [2-3], в принципе, дает субъективный анализ технической защиты информации (ТЗИ), так как оценки экспертов основываются на методологии, которая не имеет количественных оценок, и на опыте экспертов, которые занимаются защитой информации. Если методология оценок ошибочна, то и результаты оценок будут соответствующие.

Построение ТЗИ на основе теории игр [4] основывается на определении самого слабого звена в защите, на котором и строятся все теоретические расчеты. На практике, если известно слабое звено, то его защиту обычно усиливают. В результате получается, что при использовании теории игр для построения ТЗИ необходимо создавать слабое звено в защите. С другой стороны определить слабое звено в защите можно было бы, если использовать статистику результатов взломов. В ТЗИ статистику набрать трудно, так как после взлома данная защита более не используется. Она либо меняется, либо модернизируется.

Предлагаемая в данной работе методология определения вероятностных параметров КТЗИ на основе вероятностной модели КТЗИ [5] позволит количественно, из экспериментальных или реальных параметров попыток взлома, оценить характеристики той или иной системы ТЗИ. Эти количественные результаты позволят оценить, модернизировать или проанализировать возможности КТЗИ или КСЗИ, уменьшить или оценить самые необходимые из 140 параметров–вопросов. В случае экспертных оценок количественные вероятностные результаты помогут оценить и проанализировать правильность методологии построения ТЗИ, и добавят уверенности в выборе экспертов и их оценок. И в случае использования теории игр количественные результаты оценок ТЗИ позволят правильно определить слабое звено в защите, основываясь на результатах экспериментальных данных.

Основная часть исследований

Для создания методологии для определения вероятности надежности КТЗИ из отдельных реальных попыток взлома или результатов попыток взлома во времени проведем дополнительный анализ выражения вероятности взлома во времени для одной защиты, полученного в [6].

В работе [6] было получено выражение распределения вероятности попыток взлома, которое подчиняется геометрическому закону распределения вероятностей.

Плотность вероятности взлома на m – той попытке во времени может быть записана как

$$P(t) = [(\frac{t_0}{t_0 + t})^{m-1}(\frac{t}{t_0 + t})]^{\gamma}, \quad (1)$$

где t_0 – параметр, присущий данной системе защиты, и который может быть определен только из реальных результатов взлома защиты; t – текущая координата времени; m – текущая попытка взлома; γ – определяет эффективность защиты во времени.

В работах [5,6] предполагалось, что t_0 является постоянной величиной. Параметр t_0 в результате вывода выражения (1) определяет максимум в распределении плотности вероятности взлома и связывает количество попыток взлома m и время этой попытки взлома t

$$t_0 = (m-1) \cdot t \,. \quad (2)$$

Выражение (2) определяет связь между попытками взлома m и временем этой попытки t. Используя (2) в (1) получим выражение для максимумов вероятности взлома во времени

$$P(t) = [(\frac{t_0}{t_0 + t})^{\frac{t_0}{t}}(\frac{t}{t_0 + t})]^{\gamma} \,. \quad (3)$$

Рассмотрим возможность определения вероятностной надежности для единичной защиты информации из реальных попыток взлома.

Вероятность взлома защиты информации на m – той попытке будет определяться выражением

$$P(m) = \frac{1}{m}. \quad (4)$$

С другой стороны вероятность взлома во времени (3) будет определяться вероятностью взлома за счет самих попыток взлома, то есть

$$P(t) = P(m). \quad (5)$$

Учитывая выражение (2) для t_0, подставляя его в выражение (3), приравнивая к (4) и считая, что взлом произошел на m – той попытке, получим выражение

$$(\frac{m-1}{m})^{m-1}(\frac{1}{m})]^{\gamma} = \frac{1}{m}. \quad (6)$$

Из выражения (6) можно определить эффективность γ единичной защиты информации. Для этого возьмем логарифм выражения (6) и определим γ. Получим

$$\gamma = \frac{\lg(m)}{m \cdot \lg(m) - (m-1) \cdot \lg(m-1)}. \quad (7)$$

На рис.1 представлен график зависимости для эффективности защиты единичной ТЗИ от попыток взлома. Из графика видно, что в реальных условиях, если произошел взлом защиты, то всегда $\gamma < 1$. При $\gamma = 1$ взлом возможен только при $m = \infty$, а при $\gamma > 1$ теоретически гарантируется защита информации. Эти результаты согласуются с выводами работы [6].

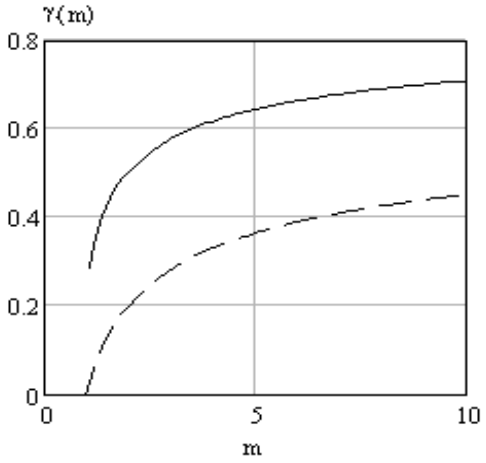

Рис.1. Зависимость эффективности единичной технической защиты информации от попыток взлома. Сплошная линия -расчет по формуле (7), пунктирная линия - расчет с учетом реальных попыток взлома для $m_1=1$, $t_1=0$, $m_2=5$, $t_2=6$

Рассмотрим следующую ситуацию. Имеем единичную техническую защиту информации на нескольких объектах. Например, некоторая антивирусная программа на нескольких компьютерах с одинаковым обновлением. В этом случае для всех компьютеров будет использоваться ТЗИ с одинаковой эффективностью защиты, но на некоторых компьютерах работа антивирусной защиты может нарушаться, то есть другими словами происходить взлом ТЗИ. По этому одному взлому можно предсказать на какой попытке и в какое время возможен взлом на других компьютерах, если не было обновления системы защиты.

Предположим, что на одном из компьютеров произошел взлом антивирусной программы на $m=9$ попытке и во времени при $t=2$. Время принято в условных единицах, так как для теоретических исследований размерность времени не имеет значения.

Из графика рис.1 или с помощью формулы (7) определяем эффективность ТЗИ. Для выбранного случая $\gamma = 0,7$. По формуле (2) по попытке и времени взлома определяем $t_0=16$.

По формулам (3), (4) и по левой части выражения (6) построим поверхности вероятностей взлома в зависимости от количества m и времени t попыток.

На рис.2 представлены поверхности расчетов вероятностей взлома по формулам (3) – $P(t)$ – поверхность средне серого цвета, (4) - $P(m)$ - поверхность белого цвета и по левой части выражения (6) - поверхность темно серого цвета.

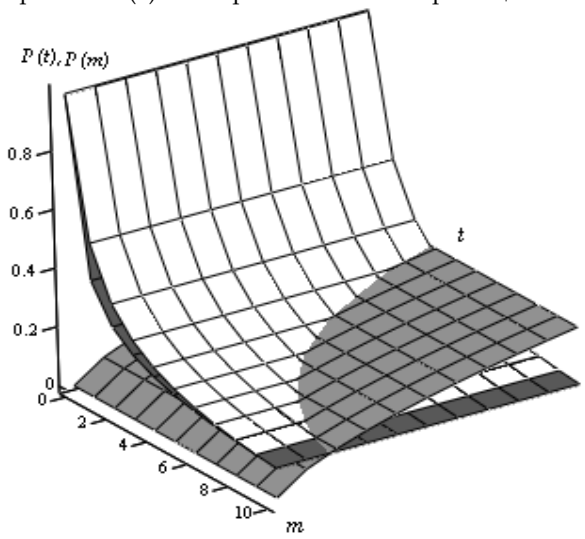

Рис.2. Поверхности расчетов вероятностей взлома по формулам: (3) – $P(t)$ – поверхность средне серого цвета, (4) - $P(m)$ - поверхность белого цвета и по левой части выражения (6) - поверхность темно серого цвета

Координаты точки пересечения всех трех поверхностей соответствуют реальным параметрам происшедшего взлома защиты информации, а именно: вероятности $P(t)=P(m)$, времени $t=2$ и попытки $m=9$ взлома.

Таким образом, взлом антивирусной программы на одном компьютере позволит определить вероятность взлома на других. Ведь количество попыток атак на компьютеры распределено неравномерно во времени, а программы антивирусной защиты до обновления везде одинаковы. На рис.2 линия пересечения белой поверхности со светло - серой дает возможность определить, на какой попытке и в какое время возможен взлом на другом компьютере. Таким образом, те компьютеры, на которых все попытки взлома с координатами, находящимися в области поверхности белого цвета, имеют некоторую вероятность защищенности. Причем лимит защищенности

будет определяться координатами границ между белой, темной и средне - серой поверхностями. Так, если во времени было мало попыток взлома на компьютере, например, четыре попытки проникновения, то есть вероятность взлома защиты при пятой попытке на шестой условной единице времени.

С другой стороны, если не было взлома защиты, а также при разработке системы защиты информации, можно определить вероятностную надежность разрабатываемой защиты, возможного количества попыток взлома и времени взлома. Как видно из рис.2, чем больше попыток взлома, тем меньшее время будет существовать защита и наоборот.

Далее рассмотрим ситуацию, когда нет статистики по попыткам взлома защиты информации, но есть одна или две попытки, не приведшие к взлому ТЗИ.

В ранее рассмотренном случае предполагалось, что $t_0=const$, следовательно, из всего множества возможных значений m и t выбирались только те значения, которые удовлетворяли выражение (2). Связь между количеством попыток взлома m и временем t этой же попытки взлома при $t_0=const$ представлена на рис.3 обратно пропорциональными кривыми.

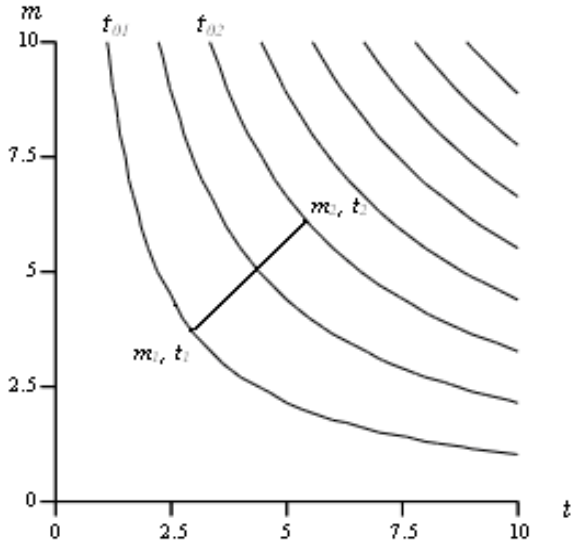

Рис.3. Связь между количеством попыток взлома m и временем t этой же попытки взлома при $t_0=const$

Из рис.3 видно, что каждому значению постоянной величины t_{01} и t_{02} соответствуют жестко связанные по обратно пропорциональному закону значения m и t.

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 (2) значение t_0 должно возрастать. На рис.3 и рис.4 этот факт представлен прямой линией между двумя значениями t_{01} и t_{02} и координатами m_1, t_1 и m_2, t_2.

Если принять m и t независимыми, то получим поверхность всевозможных значений t_0, которые являются решениями выражения (1), (2) и (3), и соответствуют реальным условиям попыток взлома.

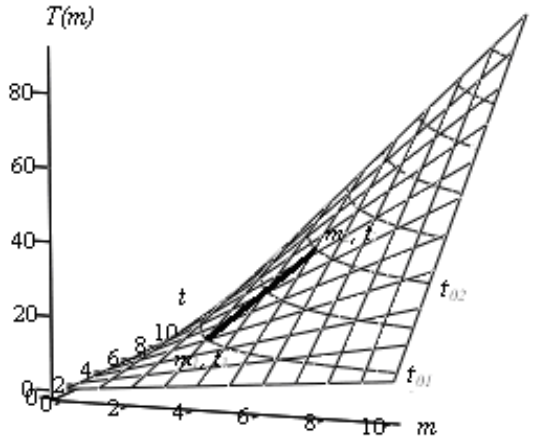

Рис.4. Вид поверхности t_0 в случае независимости между количеством попыток взлома m и временем пытки взлома t

С другой стороны в реальных условиях при удачных попытках взлома, когда взлом защиты произошел, или неудачных, когда взлом защиты на остальных компьютерах не произошел, всегда можно зафиксировать очередную попытку взлома и время, когда эта попытка произошла.

Предположим, что имеем две попытки взлома со значениями m_1, t_1 и m_2, t_2 не приведшие к взлому защиты. Причем одну из попыток можно взять из начальных условий $m_1=1$, $t_1=0$. Необходимо по значениям m_1, t_1 и m_2, t_2 построить прямую линию на поверхности рис.4. Для этого проанализируем выражение (2), у которого t_0 представляет собой линейную зависимость отдельно от $(m-1)$ и от t. Поскольку при выводе выражения (1) и (3) t_0 было постоянной величиной и не зависело от времени, то, не нарушая требований к выводу уравнения (1) и (3), можно ввести линейную зависимость t_0 от $(m-1)$ через две имеющиеся точки попыток взлома [7]. Запишем (2) в виде системы уравнений

$$\begin{aligned} a + b\cdot(m_1 - 1) &= (m_1 - 1)\cdot t_1 \\ a + b\cdot(m_2 - 1) &= (m_2 - 1)\cdot t_2 \end{aligned}. \qquad (8)$$

Найдем решение уравнения (3) относительно неизвестных a и b, которые при решении системы уравнений (8), будут иметь вид

$$a = \frac{(m_1 - 1)\cdot(m_2 - 1)\cdot(t_1 - t_2)}{m_2 - m_1}, \qquad (9)$$

$$b = \frac{(m_2 - 1)\cdot t_2 - (m_1 - 1)\cdot t_1}{m_2 - m_1}. \qquad (10)$$

Получим значение $(m-1)$, которое обозначим через $M(m)$ и которое пропорционально зависит только от количества попыток взлома m и соответствует прямой линии

$$M(m) = a + b\cdot(m). \qquad (11)$$

Эта прямая принадлежит поверхности рис.2, которая соответствует реальным значениям попыток взлома.

Из прямой рис.4 в координатной плоскости m, t получим связь между попыткой взлома и временем этой же попытки

$$T(t) = (m-1)\cdot\frac{t_2 - t_1}{m_2 - m_1}. \qquad (12)$$

Таким образом, из выражений (6) и (7) получим $t_0=T_0(m)$

$$T_0(m) = M(m)\cdot T(t). \qquad (13)$$

Подставив выражение $M(m)$ (11) в выражение (6) вместо m, получим вероятности попыток взлома во времени для одной защиты из реальных параметров взлома m_1, t_1 и m_2, t_2.

$$P(m) = [(\frac{M(m)-1}{M(m)})^{M(m)-1}(\frac{1}{M(m)})]^{\gamma} = \frac{1}{m}. \qquad (14)$$

Приравнивая это выражение вероятности происшедшего взлома на одном из компьютеров, определяем эффективность γ единичной защиты информации, как и в случае (7).

На рис.1 пунктирной линией представлен график зависимости для эффективности защиты единичной ТЗИ от попыток взлома для произвольного случая, взятого с "потолка".
Параметры a и b определены для $m_1=1$, $t_1=0$, начальных условий одинаковых для всех случаев, и $m_2=5$, $t_2=6$, взятых произвольно.

Для примера возьмем эффективность ТЗИ $\gamma=0,4$ и построим графики правой и левой части выражения (14), которые представлены на рис.5.

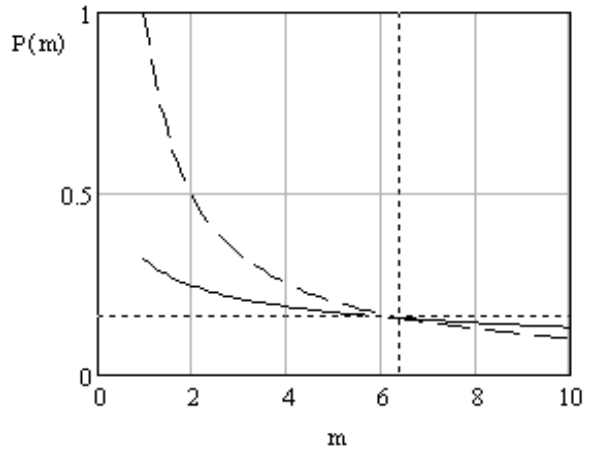

Рис.5. Зависимость вероятности единичной технической защиты информации из реальных попыток взлома для $\gamma=0,4$, $m_1=1$, $t_1=0$, $m_2=5$, $t_2=6$

Сплошная линия вероятности взлома, построенная из реальных попыток взлома. Штрихпунктирная линия соответствует вероятности, связанной с реальным взломом и рассчитана по формуле (4). Мелкая пунктирная линия указывает на точку совпадения вероятностей и указывает на попытку, на которой возможен взлом защиты, если он еще не произошел

Из рис.5 видно, что при $\gamma=0,4$, $m_1=1$, $t_1=0$, $m_2=5$, $t_2=6$ точка пересечения будет на попытке взлома $m_{в3}=6,3$, то есть на седьмой. В соответствии с (12) время взлома произойдет на $t_{в3}=7,95$ условной единице.

Зная время и попытку взлома по формуле (13) определяем $T_0(m)$. По полученным данным, по аналогии с рис.2, можно построить поверхность вероятностной защищенности единичной ТЗИ с учетом реальных попыток взлома. Для этого, вычитая из единицы вероятности взлома по попыткам и времени, соответственно получим поверхности защищенности ТЗИ. Эти поверхности представлены на рис.6.

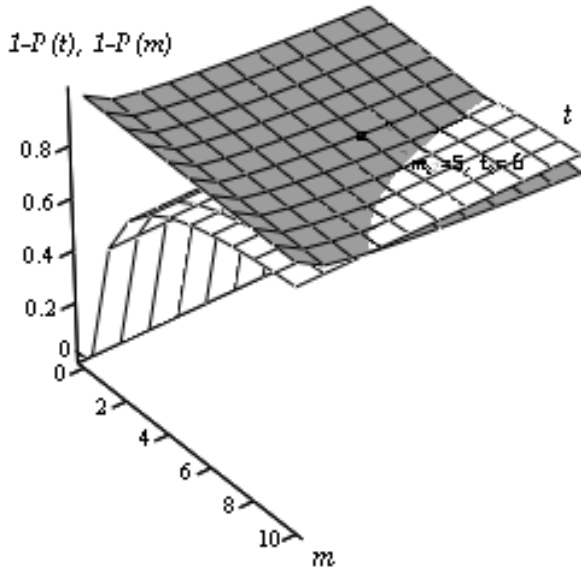

Рис.6. Поверхности определяющие вероятностную защищенность единичной ТЗИ с учетом реальных попыток взлома. *1-P(t)* – поверхность серого цвета с учетом $t_0=T_0(m)$ и черной точкой попытки взлома с координатами $m_2=5$, $t_2=6$, которые определяют вероятность защищенности используемой ТЗИ; *1-P(m)* - поверхность белого цвета, определяет вероятность защищенности от попыток взлома

Из рис.6 видно, если координаты точки попытки взлома находятся в области серой поверхности, то еще существует вероятность защищенности объекта или программного обеспечения, а в области белой поверхности уже нет. Граница между белой и серой поверхностями указывает на то, что лимит защиты данной единичной ТЗИ уже исчерпан.

Выводы

В результате проведенной работы предложен метод для определения вероятностной надежности технической защиты информации на основании реальных попыток взлома. Данный метод позволяет оценить вероятностную надежность единичных систем защиты и при установке ее на нескольких объектах, например, установке антивирусной программы на нескольких компьютерах, позволяет предсказать не только попытку, но и время, при которых вероятен взлом на других компьютерах.

Приведенные расчеты учитывают частоту попыток взлома во времени. Согласно выражению

(12), чем больше попыток взлома, тем меньшее время обеспечивается защищенность, и чем большее время тратится на попытки взлома, тем дольше сохраняется защищенность системы.

Предложенный метод позволяет по одной или по двум другим попыткам взлома, построить поверхности вероятностной надежности ТЗИ. В качестве одной из попыток могут быть взяты начальные условия, которые всегда известны - $m_1=1$, $t_1=0$.

Таким образом, возможности определения вероятностной надежности ТЗИ из реальных попыток взлома позволят сэкономить финансовые ресурсы при проектировании защиты. Провести исследования комплекса технической защиты информации, выработать рекомендации для ее модернизации или новые требования для ее разработки.

Недостатком данного метода для определения вероятности взлома защиты является необходимость знания эффективности используемой ТЗИ, которая в данном методе получается из реальной попытки взлома. Для исследования и модернизации ТЗИ, а также в случаях, когда ТЗИ используется для защиты нескольких систем, такой подход возможен. С другой стороны в работе [6] предусмотрена возможность вычисления эффективности использования ТЗИ по известной вероятности взлома на данной попытке.

И, в то же время, определение эффективности используемой ТЗИ без ее взлома требует дополнительных исследований.

Литература

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

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

[3] Архіпов О.Є. Оцінювання якості роботи експертів за даними багатооб'єктної експертизи / О.Є. Архіпов, С.А. Архіпова// 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/ Р.В.Грищук. - Житомир : Рута, 2010. – 280 с.

[5] Журиленко Б.Е. Математическая модель вероятностной надежности комплекса технической защиты информации / Б.Е. Журиленко // Безпека інформації: науково – практичний журнал - К. : НАУ, 2012. №2 (18). – С. 61-65.

[6] Журиленко Б.Е. Оценка стойкости технической защиты информации во времени / Б.Е. Журиленко, Н.К. Николаева, Н.С. Пелих // Захист інформації: науково-технічний журнал. – К.: НАУ, 2012. №1(54). С. 104-108.

[7] Ефимов Н.В. Краткий курс аналитической геометрии / Н.В. Ефи мов // М.: Госуд. Узд. Технико-теоретической литературы, 1956. – 256 с.

УДК 004.056.5 (045)

Журиленко Б.Є. Визначення вірогідної надійності одиничного технічного захисту інформації з реальних спроб злому

Анотація. *В результаті проведеної роботи запропонований метод для визначення вірогідної надійності технічного захисту інформації на підставі реальних спроб злому. Запропонований метод дозволяє оцінити вірогідну надійність одиничних систем захисту, а при установці її на декількох об'єктах передбачити не тільки спробу, але і час, при якому вірогідний злом на інших об'єктах.*

Ключові слова*: захист інформації, надійність, вірогідність злому, технічний захист інформації.*

Zhurilenko B.E. Definition of reliable reliability of single technical information security from the real attack attempts

Abstract. *The as a result conducted work the offered method for determination of reliable reliability of technical defence of information on the basis of the real attempts of breaking in. The offered method allows to estimate reliable reliability of the single systems of defence, and during setting of her on a few objects to foresee not only an attempt but also time at which reliable breaking in on other objects.*

Key words: *defence of information, reliability, probability of breaking in, technical defence of information.*

Отримано *12 лютого 2013 року*, затверджено редколегією *18 березня 2013 року*