© Zhurilenko B. Simulation of hacking and operation condition analysis for technical information security // Ukrainian Scientific Journal of Information Security, 2016, vol. 22, issue 1, p. 26-31.

ЗАХИСТ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ОБЛАДНАННЯ / SOFTWARE & HARDWARE ARCHITECTURE SECURITY

МОДЕЛИРОВАНИЕ ПРОЦЕССА ВЗЛОМА И АНАЛИЗА РАБОЧЕГО СОСТОЯНИЯ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Борис Журиленко

Национальный авиационный университет, Украина

ЖУРИЛЕНКО Борис Евгеньевич, к.ф.-м.н.

Год и место рождения: 1946 год, г. Чугуев Харьковской области, Украина.
Образование: Киевский государственный университет им. Т.Г.Шевченко, 1974 год.
Должность: доцент кафедры автоматизации и энергоменеджмента с 2014 года.
Научный интерес: методы съема и методы технической защиты информации.
Публикации: 98 научных статей и патентов на изобретения.
E-mail: zhurilenko@mail.ru

Аннотация. *В данной работе рассмотрен процесс моделирования взлома технической защиты информации путем генерации серий подбора числового кода и времени очередных попыток взлома. На основании смоделированных данных по направлению и статистики серий взлома предложена методология для проведения анализа текущего рабочего состояния защиты информации. Показаны возможности моделирования процесса взлома ТЗИ и оценки таких важных в защите параметров, как вероятность взлома, вложенные финансовые затраты, эффективность защиты, возможные попытка и ее время взлома, которые позволят вовремя выполнить корректировку отработанной ТЗИ. Оценка параметров защиты информации основывается на статистике известных, на данный момент, параметрах взлома. Поскольку в процессе эксплуатации ТЗИ появляются дополнительные сведения о попытках взлома (направлении взлома и параметрах дополнительных серий попыток взлома), то в этом случае параметры и состояние защиты необходимо будет все время уточнять. После оценки состояния и определения параметров защиты информации их можно сравнить с проектируемыми параметрами. Если параметры работающей технической защиты на данный момент близки к параметрам проектируемой или состояние параметров ТЗИ близко к взлому, то проектировщик может провести модернизацию или ее замену.*

Ключевые слова: *моделирование процесса взлома, техническая защита информации, направление взлома защиты, попытка взлома, время попытки взлома, вероятность взлома, анализ рабочего состояния защиты.*

Введение

Проектирование и разработка системы технической защиты информации (ТЗИ), в общем-то, требует экспериментальных проверок и исследований по определению возможностей защиты информации спроектированных и разработанных ТЗИ. В настоящее время экспериментальные исследования в большинстве случаев проводятся только при сертификации защиты. Причем, оценка возможностей защиты представляет собой достаточно сложную задачу. Трудности экспериментальных проверок ТЗИ заключаются в том, что реальные результаты взлома защиты становятся известны только после ее реального взлома. Для того, чтобы сделать сравнительные исследования и заключения по возможностям той или иной защиты информации, необходимо провести реальный взлом ТЗИ и одновременно получить ее количественную оценку, например, ее вероятность взлома. Естественно, рабочую защиту могут попытаться взломать при ее сертификации и не факт, что при этом защита будет реально взломана.

С другой стороны, разработчику защиты важно знать вероятность взлома защиты информации на каждом этапе ее работы и, желательно, из реальных попыток взлома. 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. Такие результаты помогут разработчику принять решение о замене используемой ТЗИ или ее модернизации, что позволит сэкономить финансовые и материальные ресурсы, вкладываемые в защиту информации. Проверить возможности ТЗИ и провести экспериментальные исследования той или иной защиты можно, если смоделировать процесс взлома соответствующий реальным физическим условиям. В связи с этими задачами, целью данной работы является разработка методологии экспериментальных исследований и оценки вероятности взлома или защиты ТЗИ по параметрам, которые моделируются в соответствие с реальными физическими условиями процесса взлома.

Основная часть исследований

Рассмотрим процесс взлома технической системы, защита которой осуществляется цифровым *n*–размерным кодом. В этом случае реальный процесс взлома происходит следующим образом. Для защиты информации выбирается любое случайное *n*–размерное кодовое число. Злоумышленник последовательным или случайным перебором чисел пытается угадать *n*–размерный цифровой код. Если код был угадан, то взлом произошел, и процесс взлома ТЗИ на этом закончен.

Таким образом, в процессе взлома служба защиты информации будет обладать такими реальными параметрами взлома, как количество попыток взлома, время этих попыток взлома и *n*–размерный цифровой код.

Причем знание *n*–размерного цифрового кода может принести пользу для защиты информации только в том случае, если его подбор ведется последовательным перебором чисел и служба защиты информации сможет успеть изменить код. В иных случаях знание n–размерного цифрового кода для службы защиты является бесполезной информацией.

Смоделировать такой процесс взлома ТЗИ для проведения исследований и анализа ее надежности можно следующим образом. Возьмем два генератора случайных чисел, один из которых генерирует n–размерный цифровой код с возможностью изменения размера, второй – случайным образом генерирует временной интервал между моделируемыми взломами. В программе моделирующей процесс взлома ко времени предыдущей попытки взлома добавлялось сгенерированное время последующей попытки.

Главное окно программы моделирования процесса взлома представлено на рис. 1:

– первая колонка цифр рис. 1 определяет очередную попытку взлома;

– вторая – генерируемый код, третья – время очередной попытки взлома.

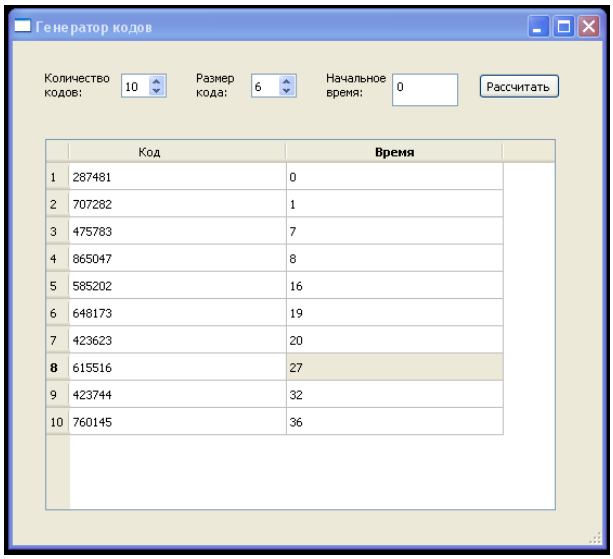

Рис. 1 Главное окно программы моделирования процесса взлома

В работе были исследованы 24 серии генерации кодов, и в каждой серии генерировалось по 10 кодов. Причем экспериментальная генерация кодов осуществлялась по 12 серий в разное время с выключением генератора, но с одними и теми же настройками параметров генератора кода. В ходе моделирования в каждой серии фиксировались попытки взлома (первая колонка рис. 1) и время этой попытки взлома (соответствующая попытке третья колонка Рис. 1). Совпадение выбранного и генерируемого кодов в процессе моделирования взлома ТЗИ не наблюдалось (вторая колонка Рис. 1).

В данной работе изменение временного интервала генерировалось от нуля до девяти просто для удобства проводимых исследований моделирования процесса взлома и чтобы суммарный временной параметр не был слишком большим при построении графиков и оценки результатов исследования.

Генерируемый код выбирался шестизначным, чтобы вероятность выбранного кода была малой, и он не мог быть угадан при небольшом количестве выборок.

На Рис. 2 представлены результаты генерации попыток и времени этих попыток взлома первых четырех серий. Тонкие прерывистые линии первой серии - *t1, t2* – второй серии, *t3* – третьей серии, *t4* – четвертой серии. Толстая пунктирная линия t_{c1} представляет собой среднее значение попыток и времени взлома этих четырех серий. Сплошная толстая линия t_c является средним значением всех 24 серий генерации кодов.

Анализируя результаты исследований моделирования процесса взлома ТЗИ можно сделать выводы, что с увеличением количества серий генерации кодов, средние значения будут приближаться к прямой линии, которая будет указывать направление процесса взлома ТЗИ [1]. Исследования показали, что даже для одной серии направление взлома близко к среднему значению 24 серий с относительной ошибкой,

которая зависит от частоты попыток взлома и уменьшается с увеличением их количества. Частота попыток взлома ТЗИ в данном случае определяется как направление процесса взлома

$$\omega = \frac{m_2 - m_1}{t_2 - t_1} = \frac{\Delta m}{\Delta t}\ , \qquad (1)$$

где Δm и Δt – приращение попыток взлома к соответствующим приращениям времени этих попыток взлома. Более подробные результаты исследования модели процесса взлома ТЗИ будут опубликованы позже.

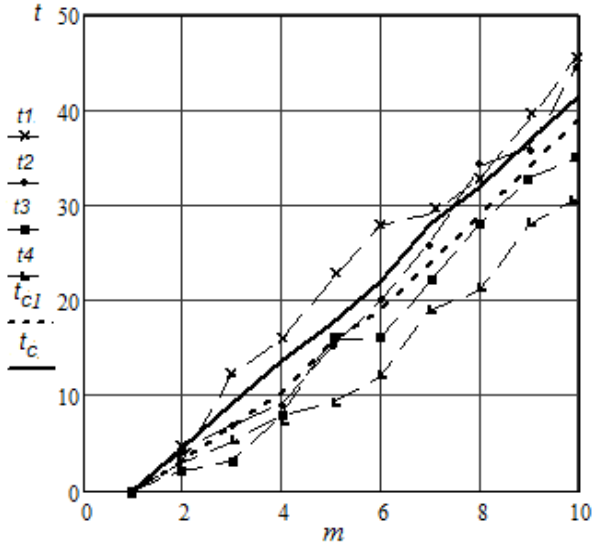

Рис. 2 Представлены результаты генерации попыток и времени этих попыток взлома первых четырех серий. *t1* - первой серии , *t2* – второй серии, *t3* – третьей серии, *t4* – четвертой серии. Толстая пунктирная линия t_{c1} - среднее значение этих четырех серий. Сплошная толстая линия t_c является средним значением всех 24 серий генерации кодов

Рассмотрим возможности оценки вероятности взлома или защиты ТЗИ по параметрам, которые определяются реальными физическими условиями процесса взлома. В данном случае воспользуемся результатами моделирования взлома, которые представлены на рис. 2.

Выражение распределения для максимумов вероятностей взлома комплекса технической защиты информации (КТЗИ), полученное в работах Б. Журиленко [2-4], может быть представлено в виде

$$P_{взлКТЗИ} = \prod_{i=1}^{n} [P_{взлi}(X_i) \cdot P_{взлi}(m,t)]^{\alpha_i}\ , \qquad (2)$$

где $P_{взлi}(X_i)$ – выражение максимумов вероятности взлома защиты от вложенного финансирования, приведенное к возможным финансовым потерям в случае отсутствия защиты

$$P_{взлi}(X_i) = \frac{X_i^{X_i}}{(1+X_i)^{1+X_i}}\ , \text{ и } X_i = \frac{x_i}{H_i} = (m_c\text{-}1)\ , \qquad (3)$$

где x_i – финансовые затраты на создание одиночной технической защиты информации (ОТЗИ); H_i – первоначальные финансовые потери в случае взлома при отсутствии защиты; m_c – выбранная попытка взлома для финансовых затрат [4]. $P_{взлi}(m,\ t)$ – распределение максимумов вероятностей взлома в зависимости от попыток взлома m и времени этих попыток взлома t для ОТЗИ; a_i – коэффициент эффективности i–той защиты (КЭЗ); n – количество защит; i – индекс параметра текущей одиночной защиты.

Распределение максимумов вероятностей взлома в зависимости от попыток взлома и времени взлома этих попыток для ОТЗИ, согласно [3], может быть представлено в виде

$$P_{взлi}(m,t) = \left(\frac{f_i(m,t)}{f_i(m,t)+t}\right)^{\frac{f_i(m,t)}{t}} \cdot \left(\frac{t}{f_i(m,t)+t}\right), \qquad (4)$$

и

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

где $f_i(m,t)$ – функция, присущая данной i–той системе защиты, определяющая направление взлома и ее защитные свойства; $m_1,\ t_1,\ m_2,\ t_2$ – параметры, которые выбираются в направлении взлома и соответствуют проектируемым, реальным или моделируемым попыткам взлома; $m,\ t$ – текущие значение попытки и времени взлома; $m_1=1,\ t_1=0$ – тривиальные начальные или исходные условия процесса взлома.

Взлом на m–той попытке позволяет определить вероятность процесса взлома ТЗИ.

Вероятность взлома любой защиты информации (ОТЗИ или КТЗИ) на m–той попытке будет

$$P(m) = \frac{1}{m}\ . \qquad (6)$$

В работе [5] рассмотрены случаи определения возможных конкретных попыток и времени этих попыток взлома при наличии некоторых исходных данных, которые известны.

Рассмотрим теперь случай, когда начальные условия и другие параметры ТЗИ абсолютно неизвестны, а известно только направление взлома, которое можно получить из результатов моделирования Рис. 2 или результатов реального процесса взлома. Если были бы известны вероятности некоторых попыток взлома, то с этими известными параметрами $m_1,\ t_1,\ m_2,\ t_2$ и вероятностями для этих попыток взлома $P1=P1_{взлОТЗИi}(m_1,\ t_1)$ и $P2=P2_{взлОТЗИi}(m_2,\ t_2)$, в соответствии с рассмотренным в работе [5] случаем, можно было бы определить все параметры используемой ТЗИ. Следовательно, необходимо по направлению взлома определить в точках $m_1,\ t_1,\ m_2,\ t_2$ вероятности $P1=P1_{взлОТЗИi}(m_1,\ t_1)$ и $P2=P2_{взлОТЗИi}(m_2,\ t_2)$. Причем любой КТЗИ можно представить как ОТЗИ с некоторыми усредненными параметрами эквивалентными КТЗИ.

Как уже указывалось, определить все усредненные эквивалентные параметры ТЗИ можно, если известны вероятности соответствующих попыток и времени этих попыток взлома. Из Рис. 2 получить значения этих вероятностей практически невозможно. Однако из Рис. 2 можно приближенно

определить вероятности взлома и как следствие оценить все параметры ТЗИ, которые с каждыми последующими попытками вновь оцениваются, и вводится коррекция параметров ТЗИ.

Чтобы приближенно определить вероятности взлома для известных серий попыток взлома, рассмотрим следующее утверждение.

Утверждение: если одна и та же ТЗИ подвергается воздействию взломов нескольких злоумышленников (использующих разные способы взлома) и после всех попыток равных $m_{1\Sigma}$ (где $m_{1\Sigma}$ - все попытки взлома всех злоумышленников до конкретной попытки m_1) взлом не произошел, то для конкретной попытки m_1 вероятность взлома ТЗИ будет не больше единицы деленной на $m_{1\Sigma}$. Если используются одинаковые способы взлома, то все они рассматриваются как один способ и в общую сумму попыток включаются как одна серия.

Данное утверждение не требует особого доказательства, так как если взлом на $m_{1\Sigma}$ попытке не произошел, то максимальная вероятность взлома на данный момент будет определяться выражением (6), где $m=m_{1\Sigma}$. Следовательно, можем определить максимальную вероятность взлома на данный момент как

$$P1 = \frac{1}{m_{1\Sigma}}. \qquad (7)$$

Аналогично определяется максимальная вероятность взлома $P2$ для последующей выбранной точки взлома.

Для обоснования методологии анализа рабочего состояния ТЗИ считаем, что взлом защиты проходит в направлении (1) по известным точкам взлома m_1, t_1, m_2, t_2, как и все реальные процессы. Для каждой известной или выбранной точки взлома запишем распределение максимумов вероятностей взлома в зависимости от попыток взлома для ОТЗИ, приравняв их к значениям вероятности взлома в этих точках. Получим систему уравнений

$$\begin{cases} P1 = [P_{взлi}(\mathrm{X_i}) \cdot P1(m_1)]^{\alpha_i} \\ P2 = [P_{взлi}(\mathrm{X_i}) \cdot P2(m_2)]^{\alpha_i} \end{cases}, \qquad (8)$$

где введены обозначения вероятностей в соответствующих точках взлома и времени

$$P1(m_1) = P_{взлi}(m_1,t_1) = \left(\frac{f_1(m_1,t_1)}{f_1(m_1,t_1)+t(m_1)}\right)^{\frac{f_1(m_1,t_1)}{t(m_1)}} \times$$

$$\times\left(\frac{t(m_1)}{f_1(m_1,t_1)+t(m_1)}\right),$$

$$f_1(m_1,t_1) = t_1 \cdot (m_1 - 1),$$

$$t(m_1) = \frac{\sqrt{A^2 + \frac{4}{\omega}\cdot f_1(m_1,t_1)} - A}{2}, \qquad (9)$$

$$P2(m_2) = P_{взлi}(m_2,t_2) = \left(\frac{f_2(m_2,t_2)}{f_2(m_2,t_2)+t(m_2)}\right)^{\frac{f_2(m_2,t_2)}{t(m_2)}} \times$$

$$\times\left(\frac{t(m_2)}{f_2(m_2,t_2)+t(m_2)}\right),$$

$$f_2(m_2,t_2) = t_2 \cdot (m_2 - 1),$$

$$t(m_2) = \frac{\sqrt{A^2 + \frac{4}{\omega}\cdot f_2(m_2,t_2)} - A}{2}.$$

В системе уравнений два неизвестных $P_{взлi}(X_i)$ и a_i. Так как оба уравнения описывают одну и ту же кривую, решаем их совместно путем деления первого уравнения на второе. Получим

$$\left(\frac{P1(m_1)}{P2(m_2)}\right)^{\alpha_i} = \frac{P1}{P2}. \qquad (10)$$

Путем логарифмирования выражения (10) находим КЭЗ a_i

$$\alpha_i = \frac{\ln P1 - \ln P2}{\ln P1(m_1) - \ln P2(m_2)}. \qquad (11)$$

С известным параметром a_i из одного уравнения (8) получим вероятность приведенных затрат на ТЗИ

$$P_{взлi}(\mathrm{X_i}) = \exp\left[\frac{\ln P1}{\alpha_i} - \ln P(m_1)\right]. \qquad (12)$$

По вычисленным $P_{взлi}(X_i)$ и a_i, известным параметрам некоторых попыток и времени этих попыток взлома, можно построить поверхность распределения максимумов вероятностей взломов по формуле (2). Пересечение этой поверхности с поверхностью вероятности взлома (6) даст линию возможного взлома ТЗИ с этими параметрами. Пересечение этих поверхностей дает линию взлома, которая описывается уравнением

$$[P_{взлi}(\mathrm{X_i}) \cdot P_{взлi}(m,t)]^{\alpha_i} = \frac{1}{m}. \qquad (13)$$

Определяем время попытки взлома по попытке взлома и направлению процесса взлома путем решения уравнения (13), подставив найденное значение $m_{взл}$ в выражение (9), получим

$$t(m_{взл}) = \frac{\sqrt{A^2 + \frac{4}{\omega}\cdot f(m_{взл},t)} - A}{2}, \qquad (14)$$

где $f(m_{взл},t) = [t_1 + \frac{t_2 - t_1}{m_2 - m_1}\cdot(m_{взл} - m_1)]\cdot(m_{взл} - 1)$,

$$A = -t_1 + \frac{m_1 - 1}{\omega}.$$

Определим все параметры ТЗИ по результатам моделирования процесса взлома, которые представлены на Рис. 2. Из Рис. 2 возьмем параметры попыток и времени этих попыток взлома для нескольких случаев, которые представлены в таблице столбцами m_1, m_2, t_{c1}, t_{c2}. Значения временных параметров t_{c1}, t_{c2} для точек m_1, m_2 соответствуют значениям сплошной толстой линии Рис. 2. Поскольку в процессе моделирования код

защиты не был сгенерирован, то считаем, что взлом защиты не произошел. Параметры $m_{1\Sigma}$, $m_{2\Sigma}$ определялись путем подсчета количества попыток взлома до выбранных точек m_1, m_2 . В данном случае в соответствие с Рис. 2, количество серий равное 4 умножалось на значения выбранных точек m_1, m_2 . Остальные параметры ТЗИ рассчитывались по формулам (7) - (14) в следующем порядке: *P1*, *P2* – по формуле (7), a_i – по формуле (11), $P_{взлі}(X_i)$ – по формуле (12). $m_{взл}$ - являлось решением уравнения (13), $t_{взл}$ – вычислялось по формуле (14).

Результаты расчетов параметров представлены в табл. 1. В таблице использовались обозначения параметров соответствующие обозначениям в формулах статьи. Из анализа результатов вычисления параметров ТЗИ, представленных в таблице, видно, что с увеличением учета общего количества ($m_{1\Sigma}$+$m_{2\Sigma}$) попыток взлома в данном направлении, попытка, при которой возможен взлом ТЗИ, резко возрастает (на девять порядков) и, следовательно, вероятность взлома резко падает. В данном случае суммарное количество взломов в первом случае из таблицы составляет 20 попыток, а в пятом – 76, то есть произошло изменение количества попыток взлома в 3,8 раза. Одновременно незначительно увеличивается коэффициент эффективности защиты ТЗИ в 1,22 раза и вложенные финансовые затраты в защиту изменились в 1,92 раза. Все результаты рассчитаны для одного направления взлома, которое было запрограммировано при моделировании данного процесса взлома.

Таблица 1

Результаты расчетов параметров

Количество случаев	m_1	m_2	$m_{1\Sigma}$	$m_{2\Sigma}$	t_{c1}	t_{c2}	$P1$	$P2$	$P_{взлі}(X_i)$	a_i	$P_{взлКТЗИі}(m, t)$	$m_{взл}$	$t_{взл}$
1	2	3	8	12	4,3	9,17	0,125	0,083	0,273	0,775	$3{,}68\text{x}10^{-4}$	2718	$1{,}323\text{x}10^{4}$
2	3	4	12	16	9,17	13,48	0,083	0,0625	0,359	0,847	$1{,}394\text{x}10^{-5}$	71750	$3{,}092\text{x}10^{5}$
3	4	5	16	20	13,48	17,5	0,0625	0,05	0,411	0,883	$6{,}261\text{x}10^{-7}$	1597261	$6{,}421\text{x}10^{6}$
4	3	10	12	40	9,17	41,5	0,083	0.025	0,424	0,898	$8{,}356\text{x}10^{-8}$	11967418	$5{,}527\text{x}10^{7}$
5	9	10	36	40	36,9	41.5	0,028	0.025	0,523	0,946	$2{,}487\text{x}10^{-13}$	4023981594398	$1{,}851\text{x}10^{13}$

Выводы

В результате выполненной работы можно сделать следующие выводы.

Показана возможность моделирования процесса взлома ТЗИ в простейшем случае и методология анализа рабочего состояния ТЗИ, которая позволяет по направлению и статистики серий данных взлома провести анализ состояния ТЗИ. Если направление взлома и параметры серии попыток взлома будут меняться в процессе эксплуатации ТЗИ, то ее параметры и состояние защиты можно будет корректировать.

После анализа состояния и определения параметров защиты информации возникает возможность сравнения параметров проектируемой ТЗИ и ее рабочего состояния по результатам анализа попыток взлома. Если по результатам выполненного анализа состояние ТЗИ на данный момент близко к параметрам проектируемого или возможности взлома, то проектировщик может провести модернизацию или ее замену.

Результаты исследования моделирования процесса взлома могут быть использованы и злоумышленником для анализа состояния защиты. По полученным параметрам взлома ТЗИ злоумышленник может сориентироваться в правильном ли направлении идет процесс взлома и при каких условиях будет достигнут нужный для него результат. Однако следует заметить, что проектируемые параметры ТЗИ злоумышленник знать не будет. При необходимости он может изменить направление взлома для достижения оптимального направления и, следовательно, нужного результата, но это не значит, что взлом идет в правильном направлении, заложенном организатором защиты информации.

С точки зрения защиты информации организатор защиты тоже может и должен знать результаты направления взлома и анализа состояния работающей ТЗИ, которые можно сравнить с реальными исходными планируемыми параметрами ТЗИ и в случае необходимости вовремя провести модернизацию защиты в нужном направлении. Таким образом, организатор защиты может контролировать ее состояние в процессе работы ТЗИ.

С другой стороны, если злоумышленник после анализа состояния работающей ТЗИ может увидеть, что для ее взлома понадобится много времени и финансовых затрат, то он может отказаться от взлома данной ТЗИ.

Литература

[1] Журиленко Б.Е. Определение направления взлома технической защиты информации по его параметрам/ Б.Е. Журиленко, Н.К. Николаева// Матеріали ІІІ Міжнародної науково-практичної конференції «Інформаційні управляючі системи та технології» (ІУСТ-ОДЕСА-2014), 23-25 вересня 2014 року. – С. 168-171.

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

[3] Журиленко Б.Е. Метод проектирования единичной системы технической защиты

информации с вероятностной надежностью и заданными параметрами взлома / Б.Е. Журиленко // Безпека інформації. – 2014. – №1 (20). – С. 36-42.

[4] Журиленко Б.Е. Методология построения и анализа состояния комплекса технической защиты информации с вероятностной надежностью и учетом временных попыток взлома/ Б.Е. Журиленко // Захист інформації. – 2015. – №3 (17). – С. 196-204.

[5] Журиленко Б.Е. Визначення коефіцієнта ефективності технічного захисту інформації по її параметрах / Б.Е. Журиленко, Н.К. Николаева // Безпека інформації. – 2015. – №3 (21). – С. 245-250.

УДК 004.056.5 (045)

Журиленко Б.Є. Моделювання процесу злому і аналізу робочого стану технічного захисту інформації

Анотація. *У даній роботі розглянуто процес моделювання злому технічного захисту інформації шляхом генерації серій підбору числового коду і часу чергових спроб злому. На підставі змодельованих даних по напрямку і статистики серії злому запропонована методологія для проведення аналізу поточного робочого стану захисту інформації. Показані можливості моделювання процесу злому технічного захисту інформації і оцінки таких важливих в захисті параметрів, як вірогідність злому, вкладені фінансові витрати, ефективність захисту, можливі спроби і її час злому, які дозволять вчасно виконати коригування відпрацьованого технічного захисту інформації. Оцінка параметрів захисту інформації грунтується на статистиці відомих, на даний момент, параметрах злому. Оскільки в процесі експлуатації технічного захисту інформації з'являються додаткові відомості про спроби злому (напрями злому і параметрах додаткових серій спроб злому), то в цьому випадку параметри і стан захисту необхідно буде увесь час уточнювати. Після оцінки стану і визначення параметрів захисту інформації їх можна порівняти з проектованими параметрами. Якщо технічний захист інформації на даний момент близький до раніше проектованого або злому, то проектувальник може провести модернізацію або його заміну.*

Ключові слова: *моделювання процесу злому, технічний захист інформації, напрям злому захисту, спроба злому, час спроби злому, вірогідність злому, аналіз робочого стану захисту.*

Zhurilenko B. Simulation of hacking and operation condition analysis for technical information security

Abstract. *This paper describes the simulation of technical information security hacking by generating a series of numeric code selection and next hacking attempts time. Based on simulated data direction and statistical series of hacking proposed methodology for the analysis of the current information security operating conditions. Demonstrates the possibility of modelling process for technical information security hacking and evaluation of such important security parameters, hacking probability, financial investments, security efficiency, hacking time and attempts for technical information security and in time correction of checked technical information security. The evaluation of information security parameters is based on well-known at the time hacking parameters. In operation technical information security process new information about hacking attempts is generated (hacking directions and also parameters of additional hacking attempts) and in this case parameters and security conditions must be corrected in process. After conditions evaluation and information security parameters defining its can be compared with projected parameters. If technical information security in the time is approximated to projected conditions or hacking projector can improve or change it.*

Key words: *hacking process simulation, technical information security, hacking direction, hacking attempt, hacking attempt time, hacking probability, analysis of security operating conditions.*

Отримано *16 лютого 2016 року*, затверджено редколегією *11 березня 2016 року*