DOI: 10.18372/2410-7840.20.13424
УДК 004.056.5(045)

ОЦЕНИВАНИЕ ФИНАНСОВЫХ ЗАТРАТ НА ПОСТРОЕНИЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Борис Журиленко

В данной работе предпринята попытка разработки методологии оценивания финансовых затрат на построение системы защиты информации (СЗИ) по известным параметрам. Такими параметрами могут быть: вероятность взлома защиты в зависимости от величины вложенного финансирования в защиту и возможных финансовых потерь без защиты; риски потерь от вложенного финансирования в защиту; риски полных финансовых потерь и эффективность построенной защиты. Все оценки СЗИ проводились для максимальных значений вероятности взлома и максимальных рисков потерь. В данной работе получены конкретные выражения для оценки эффективности защиты информации, оптимизации рисков финансовых потерь при проектировании, сертификации и оценки рабочего состояния в зависимости от финансовых вложений в защиту информации и рисков их потерь. Предложено теоретическое определение эффективности защиты через риски вложенного финансирования в защиту и риски полных финансовых потерь. Коэффициент эффективности защищенности одиночной или одноуровневой защиты будет изменяться от нуля (при отсутствии финансирования в защиту) до единицы (при бесконечном финансировании в построении защиты). Полученные выражения на этапе проектирования позволят сравнить между собой и оценить выбранную СЗИ до процесса ее внедрения. Экспериментальные данные исследований отличий между практическим и теоретическим параметром эффективности защиты позволят исследовать и подобрать наиболее оптимальную и эффективную защиту. Приведены выражения, позволяющие по экспериментальной вероятности взлома определить фактическую эффективность защищенности. Теоретически подтверждена более высокая надежность многоуровневой защиты по сравнению с одноуровневой. Показано, что при одних и тех же финансовых затратах на одноуровневую и многоуровневую защиты вероятность взлома защиты и риски финансовых потерь многоуровневой защиты значительно ниже. Следовательно, с помощью многоуровневой системы защиты можно создать требуемый уровень защиты с меньшими финансовыми затратами. Таким образом, данная работа может быть полезна для оценки эффективности защиты информации, оптимизации рисков финансовых потерь при проектировании, сертификации и оценки рабочего состояния.

Ключевые слова: *система защиты информации, вероятность взлома защиты, риски потерь от вложенного финансирования в защиту, риски полных финансовых потерь, эффективность защиты, одноуровневая защита, многоуровневая защита.*

Введение. Для защиты секретной и конфиденциальной информации от утечки по техническим каналам необходимо создавать систему защиты информации (СЗИ). Различные фирмы и предприятия, для которых будет создаваться СЗИ, в первую очередь, будет интересовать 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 вложенных потерь и вероятности взлома защиты. Как и в работе [1], 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.

В открытой литературе [2-5] 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 СЗИ, оптимизация финансовых потерь в случае взлома системы защиты информации, критериев необходимости дополнительных затрат на восстановление СЗИ до необходимого технического уровня защиты и, соответственно, оптимизации финансовых потерь.

Актуальность данной работы заключается в разработке новых конкретных расчетов, соответствующих реальным условиям работы СЗИ, для оценки эффективности защиты информации, оптимизации рисков финансовых потерь при проектировании, сертификации и оценки рабочего состояния.

Научная новизна заключается в разработке нового подхода к проектированию, анализу рабочего состояния работающей СЗИ с целью экономии финансовых затрат, вкладываемых в защиту.

Из открытых источников неизвестны защиты, которые разрабатывались бы по нормативным документам и которые позволяли бы оценивать вероятность взлома, риски финансовых потерь, эффективность защиты по вложенному в защиту

финансированию. Существует публикация [1], в которой сделана попытка определить оптимальные финансовые затраты и основные критерии построения или модернизации СЗИ. Однако в этой работе отсутствует более полное и строгое исследование влияния финансовых затрат на защиту информации.

Целью данной работы была попытка определения возможности оптимизации расходов на построение СЗИ и оптимизации финансовых потерь в случае взлома СЗИ с требуемой вероятностью взлома.

Теоретическое обоснование оценивания финансовых затрат на построение системы защиты информации

Как и в работе [1], рассмотрим соотношение, которое представляет собой величину рисков финансовых потерь [6].

При затратах на один вариант защиты информации можем записать величину рисков финансовых потерь как

$$(H + x) \cdot p_x = f(x), \quad (1)$$

где H – первоначальные финансовые потери при отсутствии защиты; x – финансирование, затраченное на организацию защиты с вероятностью взлома p_x; p_x – вероятность взлома при финансовых затратах на защиту равную x; $f(x)$ – функция величины риска полных финансовых потерь;.

В данной работе под попыткой взлома понимается очередная возможность получения информации в одном определенном способе защиты информации.

С математической точки зрения величина рисков финансовых потерь может определяться любой функцией $f(x)$, которая может быть выражена с помощью полинома [7]

$$f(x) = \alpha + \beta \cdot x + \gamma \cdot x^2 + \dots, \quad (2)$$

где a, β, γ – постоянные числа. Сама функция должна быть $f(x) \geq 0$, так как левая часть уравнения (1) не может быть отрицательной.

Если возьмем первое приближение по x, то $f(x) = a + \beta \cdot x$. В этом случае (1) будет иметь вид

$$(H + x) \cdot p_x = \alpha + \beta \cdot x. \quad (3)$$

Рассмотрим поведение вероятности взлома p_x в зависимости от вложенного финансирования x на организацию защиты информации

$$p_x = \frac{\alpha + \beta \cdot x}{H + x} \quad (4)$$

и найдем предел вероятности взлома при бесконечном вкладе финансирования на организацию защиты информации. Получим

$$\lim_{x \to \infty} p_x = \beta. \quad (5)$$

Поскольку $1 \geq \beta > 0$ (вероятность не может быть больше единицы или отрицательной), то вкладываемое финансирование в защиту неэффективно, так как при бесконечном вкладе финансирования в защиту информации существует вероятность ее взлома. Функциональная зависимость в (3) и (1) с $\beta > 0$ приведет к возрастанию функции $f(x)$ в зависимости от вложенного финансирования в ее защиту, что будет указывать на рост рисков финансовых потерь и, следовательно, на необходимость замены выбранного типа защиты на другой более эффективный способ.

При $\beta = 0$ и других коэффициентах степенного ряда (2) равных нулю, кроме a, вкладываемое финансирование в защиту является пропорциональным, то есть выполняется принцип достаточности между вкладываемым финансированием и вероятностью взлома.

Таким образом, функция $f(x)$ в выражении (1) определяет величину рисков финансовых потерь и, естественно, нет смысла разрабатывать систему защиты информации и тратить на нее деньги, если она с повышением уровня затрат будет увеличивать величину рисков потерь (случай $\beta > 0$). На практике, как минимум, удовлетворила бы пропорциональная защита, которая, хотя бы не увеличивала величину рисков потерь (случай $\beta = 0$). Таким образом, одним из критериев оптимального вклада финансирования в техническую защиту информации будет условие

$$f(x) \leq f(0), \quad (6)$$

то есть величина рисков потерь должна быть, как минимум, постоянной (пропорциональный вклад в защиту) либо уменьшать величину рисков (более эффективная защита) с увеличением финансирования на техническую защиту.

Рассмотрим случай пропорциональной защиты с $\beta = 0$. Согласно (3) при $\beta = 0$ получим

$$(H + x) \cdot p_x = \alpha, \quad (7)$$

где a – некоторая постоянная величина.

Из (7) определим вероятность взлома защиты p_x в зависимости от затрат на защиту

$$p_x = \frac{\alpha}{H + x}. \quad (8)$$

Определим a при начальных условиях $x = 0$, когда нет затрат на организацию защиты и когда защита отсутствует, в этом случае $p_x = p_0 = 1$. Отсюда

$$p_0 = \frac{\alpha}{H} = 1, \text{ или } \alpha = H. \quad (9)$$

Следовательно, вероятность взлома в зависимости от вложенного финансирования на защиту можем переписать в виде

$$p_x = \frac{H}{H+x}. \quad (10)$$

Анализируя выражение (10), можем сказать, что вероятность взлома в зависимости от вложенных финансовых затрат на СЗИ, уменьшается и стремится к нулю при затратах на защиту, стремящихся к бесконечности.

Предположим, что попытки проникновения через защиту ведутся до взлома. Причем вероятность первого взлома при каждой последующей попытке не зависит от результатов предыдущих попыток и сохраняет свое постоянное первоначальное значение. Число произведенных попыток взлома обозначим через m раз.

Выбираем независимость вероятности взлома от результатов предыдущих попыток, основываясь на том факте, что злоумышленник может не знать, какую систему защиты взламывает и как ее взломать, и если он ее с очередной попытки не взломал, то вероятность взлома используемой системы защиты остается той же.

Такое распределение попыток взлома будет подчиняться геометрическому закону распределения вероятностей [8].

Вероятность события до взлома на m попытке может быть записана как

$$P(x) = (p_{xз})^{m-1} \cdot p_x = (\frac{x}{H+x})^{m-1} \cdot \frac{H}{H+x}, \quad (12)$$

где m – означает ту попытку, на которой произошел взлом, и вероятность защищенности $p_{xз}$ будет определяться выражением

$$p_{xз} = 1 - \frac{H}{H+x} = \frac{x}{H+x}.$$

Вероятность защищенности имеет обратную тенденцию, когда нет финансовых затрат на защиту, то защищенность равна нулю и стремится к единице при стремлении затрат к бесконечности.

Как и в работе [1], анализируя выражение (12), видим, что при $x=0$ и при x стремящимся к бесконечности, если $m>1$, $P(x)=0$. Следовательно, выражение (12) имеет экстремум, который будет зависеть от вложенного на защиту финансирования и попыток взлома. Исследуем (12) на экстремум по x, учитывая, что m не зависит от вложенного в защиту финансирования. Значение m, то есть рассчитываемое количество взломов может выбираться при организации СЗИ.

Исследования на экстремум показали, что при

$$x = (m-1) \cdot H \quad (13)$$

или для приведенных значений финансовых затрат X к финансовым потерям при отсутствии защиты H

$$X = \frac{x}{H} = (\text{m-1}), \quad (13а)$$

выражение (12) будет иметь максимум, то есть определять максимальную вероятность взлома при данном финансировании на защиту и попытками взлома.

В этом случае финансовые затраты на защиту будут зависеть от величины финансовых потерь H без защиты и количества попыток взлома m, если используется только одна система защиты. Если защита информации не обеспечивается (x=0**)**, то при первой же попытке взлома (m=1) возможны финансовые потери, равные H. При взломе защиты на второй попытке (m=2) необходимо затратить на СЗИ финансирование равное $x = H$. В этом случае общие потери при использовании только одного типа защиты будут составлять $2H$. Повышение уровня защищенности до взлома на m попытке, при использовании только одного типа защиты, будет приводить к общим финансовым потерям, равным mH. Таким образом, будем считать, что выражения (13) и (13а) определяют максимум вероятности взлома и пропорциональный вклад вложенного финансирования в защиту в зависимости от попытки взлома $(m-1)$ и финансовых потерь при отсутствии защиты H.

На рис. 1 представлена поверхность распределения вероятности взлома в зависимости от приведенного вложенного финансирования в защиту X и попытки, на которой произошел взлом $(m-1)$.

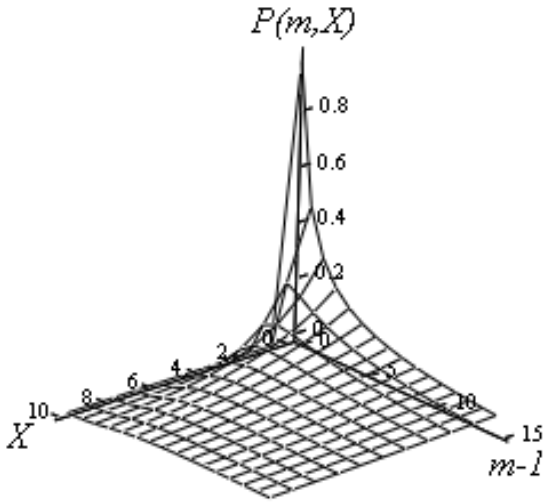


Рис. 1. Распределение максимумов вероятности взлома в зависимости от вложенного финансирования в защиту и попытки, на которой произошел взлом

На рисунке видно, что на поверхности значения вероятности взлома распределены неравномерно. Максимальные значения наблюдаются при выполнении соотношения (13а) или (13). При несоблюдении этого соотношения вероятность взлома уменьшается. Причем, от величины вложенного в защиту финансирования вероятность взлома уменьшается больше, чем от попытки взлома. Из рисунка также видно, что чем большее финансирование вкладывается в защиту информации, тем меньше вероятность ее взлома. Этот факт необходимо учитывать при проектировании технической защиты информации.

Из теории вероятности известно, что событие взлома возможно по всей поверхности распределения максимумов вероятности взлома (рис. 1.), однако достоверность события взлома по всей поверхности будет разным. В данной работе считается, что взлом возможен в любой точке поверхности, а достоверность этого события не учитывается.

Если экстремальные значения (13) подставить в (12), то получим выражение, которое определяет распределение максимальной вероятности $P(x)$ в зависимости от попыток взлома m.

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

Распределение максимальной вероятности $P(X)$ в зависимости от приведенных значений финансовых затрат X с учетом выражения (13а) будет иметь вид

$$P_m(X)=\frac{X^{X}}{(1+X)^{1+X}}. \qquad (14а)$$

На рис. 2 представлены результаты расчета максимума вероятности события проникновения через защиту $P(x)$ по формуле (12) или (14), (14а) (толстая сплошная линия). В расчетах кривые $P_m(X)$ и $P(m)$ полностью совпадают.

Объясним смысл $P(m)$, используя кривую 4 рис. 2 (тонкую сплошную линию). Поскольку кривая 4 рассчитана с затратами на возможность взлома с четвертой попытки, то и максимум вероятности взлома приходится для затрат $x = 3H$, согласно выражения (13). Очевидно, что при таких затратах, вероятность взлома с первой попытки минимальна по сравнению со второй (точка в, рис. 2) и третьей (точка б, рис. 2) попытками, для которых вероятность взлома будет увеличиваться. С другой стороны, если затраты на защиту информации будут больше оптимально необходимых затрат для взлома с четвертой попытки (точка а, рис. 2), то вероятность взлома будет уменьшаться. Это соответствует кривой, находящейся после максимума ($x = 4H$) в направлении увеличения X. В этом случае вероятность взлома защиты с четвертой попытки будет уменьшаться в зависимости от вложенного финансирования. Данные выводы подтверждаются результатами расчетов, представленными на рис. 1.

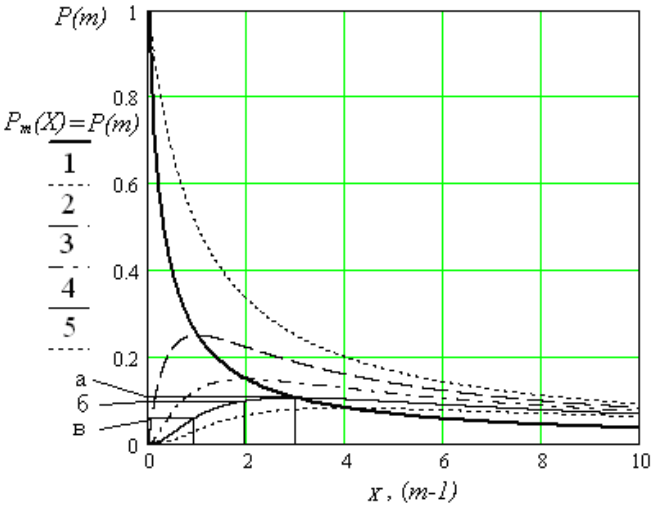


Рис. 2. Расчет максимума вероятности события проникновения $P(m)$ через защиту в зависимости от попыток взлома m: 1 – при $m = 1$; 2 – при $m = 2$; 3 – при $m = 3$; 4 – при $m = 4$; 5 – при $m=5$; $X = x/H$ – приведенные значения финансовых затрат; H – финансовые потери при отсутствии защиты, x – финансовые затраты на организацию защиты информации; $P_m(X)$ - кривая, определяющая максимальные значения вероятности проникновения через защиту в зависимости от уровня финансовых затрат на защиту информации x; а, б, в - значения вероятности проникновения с 4, 3, 2 попыток при затратах финансирования на защиту для взлома с 4 попытки

Определим величину рисков при потере информации и при затратах на СЗИ, которые соответствуют следующим выражениям:

$$R_{общ}(x)=P_m(X)\cdot(H+x) \qquad (15)$$

- соответствует величине рисков полных финансовых потерь в случае взлома защиты;

$$R^*_{общ}(m)=R^*_{общ}(X)=\frac{R_{общ}(x)}{H}=P_m(X)\cdot(1+X) \qquad (15а)$$

- соответствует величине приведенных рисков полных финансовых потерь в случае взлома защиты;

$$R_{вл}(x)=P_m(X)\cdot x \qquad (16)$$

- соответствует величине рисков финансовых потерь, вложенных в построение СЗИ;

$$R^*_{вл}(m)=R^*_{вл}(X)=\frac{R_{вл}(x)}{H}=P_m(X)\cdot X \qquad (16а)$$

- соответствует величине приведенных рисков финансовых потерь, вложенных в построение СЗИ.

Результаты расчетов максимумов величин приведенных рисков представлены на рис. 3 при пропорциональном вкладе финансирования в защиту информации, то есть при соответствии формулам (13) или (13а).

Определим пределы, к которым стремятся максимумы величины приведенных рисков полных финансовых потерь (15а) и величины приведенных рисков вложенных финансовых потерь (16а), при стремлении попыток взлома m к бесконечности. Для этого вместо X в выражения (15а) и (16а) подставим условие экстремума (13а). Получим

$$\lim_{m\to\infty} R^{*}_{общ}(m) = \lim_{m\to\infty} \frac{(m-1)^{m-1}\cdot m}{m^{m}} = \frac{1}{e} \approx 0{,}37\,, \quad (17)$$

$$\lim_{m\to\infty} R^{*}_{вл}(m) = \lim_{m\to\infty} \frac{(m-1)^{m-1}\cdot (m-1)}{m^{m}} = \frac{1}{e} \approx 0{,}37\,. \quad (18)$$

Отсюда видно, что величины максимумов приведенных рисков полных потерь и потерь финансирования, вложенных в построение одноуровневой СЗИ, то есть одного способа защиты информации, при бесконечных попытках взлома и, следовательно, бесконечного финансирования, имеют предельное значение величины рисков, равное $1/e \approx 0{,}37$ (рис. 3 прямая сплошная линия). В выражениях (15) и (16) величины рисков будут равны $\approx 0{,}37H$, то есть минимальные величины рисков полных потерь и максимальные величины рисков потерь вложенного финансирования при бесконечных попытках взлома и бесконечном финансировании для одной СЗИ будут $\approx 0{,}37H$. Следовательно, одноуровневая защита даже при бесконечном финансировании в защиту имеет 37% рисков полных потерь вложенного финансирования. В этом случае при планировании взлома с 5, 6 или последующих попыток вкладываемое в защиту информации финансирование больше работает на уменьшение рисков вкладываемых финансовых потерь, чем на риски полных финансовых потерь.

Рассмотрим зависимости рисков потерь от вложенного в защиту финансирования и попыток, на которых возможен взлом информации. На рис. 4 представлены расчеты по формулам (16а) рис. 4а и (15а) для рис. 4б. На рисунках построены прямолинейные поверхности, соответствующие уровню приблизительно 0,37 для приведенных рисков потерь, как на рис. 3. На рис. 4а видно, что приведенные риски финансовых затрат на защиту ни при каких значениях x и m-1 не могут пересечь поверхность с уровнем равным приблизительно 0,37. В то же время поверхность рисков полных финансовых потерь (рис. 4б) пересекает прямолинейную поверхность, которая определяется частью области максимальных значений вероятности взлома.

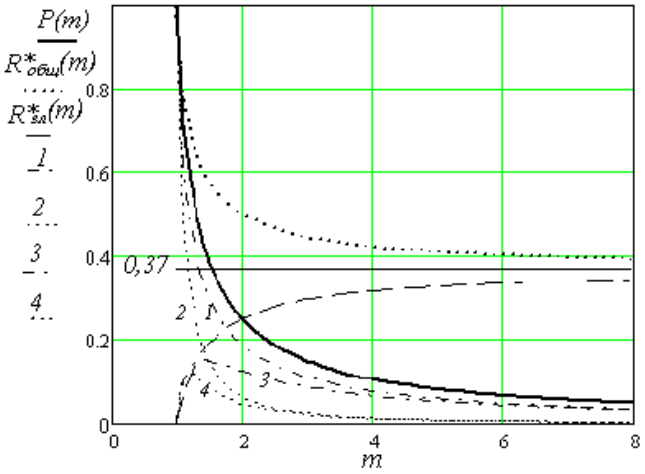


Рис. 3. Расчет величины рисков потерь; *P (m)* - кривая, определяющая максимальные значения вероятности проникновения через защиту в зависимости от попыток взлома $m \geq 1$; $R^{*}_{общ}(m)$ – величина приведенных рисков полных финансовых потерь в случае взлома защиты; $R^{*}_{вл}(m)$ – величина приведенных рисков финансовых потерь, вложенных в построение СЗИ; 1 – величина приведенных рисков полных финансовых потерь в случае взлома двухуровневой защиты $P^{*}_{\Sigma общ}(m_1, m_2)$; 2 – величина приведенных рисков полных финансовых потерь в случае взлома трехуровневой защиты $P^{*}_{\Sigma общ}(m_1, m_2, m_3)$; 3 - величина приведенных рисков финансовых потерь, вложенных в построение двухуровневой СЗИ $P^{*}_{\Sigma вл}(m_1, m_2)$, 4 - величина приведенных рисков финансовых потерь, вложенных в построение трехуровневой СЗИ $P^{*}_{\Sigma вл}(m_1, m_2, m_n)$

В соответствие с расчетами (14), (14а) и рис. 3 область максимальных значений рисков полных финансовых потерь достигнет прямолинейной поверхности сверху только при бесконечных значениях x и m-1. Из рис. 4б видно, что при больших вкладах финансирования риски полных финансовых потерь уменьшаются, а также уменьшаются при больших попытках возможного взлома при малом финансировании защиты информации.

В реальных условиях бесконечные затраты финансирования на защиту информации при рисках общих потерь в 37% мало кого устроят, поэтому исследуем возможности уменьшения финансирования защиты и уменьшения рисков потерь путем использования многоуровневой защиты, то есть использования нескольких разных способов защит информации на один и тот же объект носителя информации.

Рассмотрим многоуровневую защиту, состоящую из n- пропорциональных защит $P(m_1)$, …,

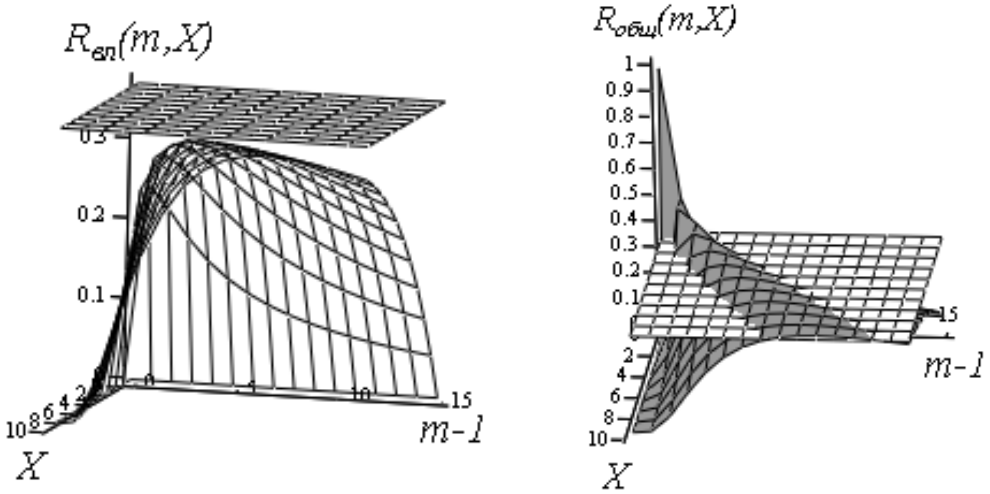
$P(m_n)$ (14), где $m_1 \dots m_n$ – означают попытки взлома, которые произошли на первом или n –том уровне защиты. То есть происходит последовательный взлом одиночных способов защит на пути к объекту носителя информации. Считаем, что события взлома каждого уровня многоуровневой системы защиты являются независимыми друг от друга, тогда вероятность взлома многоуровневой защиты можно представить в виде

$$P_{\Sigma}(m_1, \dots, m_n) = \prod_{j=1}^{n} P(m_j), \qquad (19)$$

где m_j – попытка, при которой происходит взлом в j – й защите, n – количество пропорциональных последовательных защит.

Как и в работе [1], определим предельные значения величины рисков полных финансовых потерь для многоуровневой системы защиты $R^*_{\Sigma общ}(m_1, \dots m_n)$ при стремлении попыток взлома к бесконечности.

$$R^*_{\Sigma\text{общ}}(m_1, \dots, m_n) = \lim_{m_1,\dots,m_n \to \infty} \frac{(m_1-1)^{m_1-1}}{{m_1}^{m_1}} \times \dots \times \frac{(m_n-1)^{m_n-1}}{{m_n}^{n}} \times (m_1 + \dots + m_n - n + 1) = \frac{m_1+\dots+m_n-n+1}{e^n \cdot \prod_{j=1}^{n}(m_j)} = 0. \qquad (20)$$



а б

Рис. 4. Поверхности величин рисков финансовых потерь: а – вложенных в защиту; б – полных потерь; плоские поверхности ограничивают уровень рисков, равный приблизительно 0,37

Аналогично определяем предельные значения величины рисков вложенных финансовых потерь для многоуровневой системы защиты при стремлении попыток взлома к бесконечности

$$R^*_{\Sigma\text{вл}}(m_1, \dots, m_n) = \lim_{m_1,\dots,m_n \to \infty} \frac{(m_1-1)^{m_1-1}}{{m_1}^{m_1}} \times \dots \times \frac{(m_n-1)^{m_n-1}}{{m_n}^{n}} \times (m_1 + \dots + m_n - n) = \frac{m_1+\dots+m_n-n}{e^n \cdot \prod_{j=1}^{n}(m_j)} = 0. \qquad (21)$$

Результаты расчетов величин рисков для двух и трехуровневых защит по формулам (20) и (21) представлены на рис. 3 кривыми 1, 2, 3, 4. Из расчетов (20) и (21) видно, что риски потерь, в отличие от одноуровневой защиты, стремятся к нулю с увеличением финансовых вложений в защиту информации.

Рассмотрим, как меняются вероятности взлома и риски финансовых вложений одноуровневой и многоуровневой защит при одних и тех же финансовых затратах на защиту информации.

Результаты расчетов представлены в табл. 1.

Таблица 1

Приведены величины вероятностей, рисков вложенных и полных финансовых потерь для одно-, двух- и трехуровневых систем защиты информации

№ п/п	Число уровней защиты n	Максимум попытки взлома m	$P(m)$	$P^n(m)$	$R^*_{\Sigma вл}(m)$	$R^*_{\Sigma общ}(m)$
1	$n=1$	$m=3$	0,148	0,148	0,236	0,444
2	$n=2$	$m=2$	0,25	0,063	0,125	0,188
3	$n=3$	$m=1,6667$	0,326	0,035	0,069	0,104

Расчеты выполнялись при условии финансовых вложений равных *2Н* или общих финансовых потерь равных *3Н*, то есть при взломе в каждом случае с третьей попытки. Также считалось, что максимумы вероятностей взлома составляющих защит одинаковы. Были рассмотрены три случая защит разного уровня. Первый случай – рассчитана одноуровневая защита с максимумом вероятности взлома на третьей попытке и с вложенным в защиту финансированием равным *2Н* или приведенным вложением равным *2*. Второй случай - рассчитана двухуровневая защита с максимумом вероятности взлома составляющих защит на второй попытке и взломом общей защиты на третьей попытке. И третий случай - рассчитана трехуровневая защита с максимумом вероятности взлома между второй и третьей попыток и взломом на третьей попытке. Из результатов исследований можно сделать вывод, что использование многоуровневой защиты при одинаковых финансовых затратах на защиту информации уменьшает вероятность взлома защиты и риски финансовых потерь, хотя вероятность взлома одиночных защит меньше. Например, сравнивая одноуровневую и трехуровневую защиты, можно увидеть, что, хотя максимумы вероятности взлома составляющих трехуровневых защит приблизительно в 2,2 больше, вероятность взлома системы трехуровневой защиты будет в 4,2 раза меньше одноуровневой защиты. Кроме того, риски суммарных финансовых потерь вложений в создание защиты уменьшаются в 3,4 раза, а риски полных суммарных потерь уменьшаются приблизительно в 4,3 раза. Следовательно, с помощью многоуровневой системы защиты можно создать требуемый уровень защиты с меньшими финансовыми затратами.

Введем понятие коэффициента эффективности защищенности (КЭЗ) информации, как отношение рисков потерь вложенного в защиту информации финансирования к рискам полных финансовых потерь

$$\gamma = \frac{R_{\text{вл}}}{R_{\text{общ}}} = \frac{P(x)\cdot x}{P(x)\cdot(x+H)} = \frac{x}{x+H} = \frac{X}{X+1} = \frac{m-1}{m}. \quad (22)$$

Из анализа выражения (22), видно, что коэффициент эффективности защиты γ изменяется от $\gamma=0$, когда $x=0$ или $m=1$ - нет финансовых вложений в защиту информации, и до $\gamma=1$, когда $x=\infty$ или $m=\infty$, то есть при бесконечном финансировании в защиту. Следует заметить, что расчетные значения КЭЗ через попытки взлома фактически будут определяться максимальными значениями вероятности взлома по формуле (13а).

Важными и необходимыми параметрами при построении технической защиты информации являются вероятность взлома от вложенного финансирования (12) и эффективность защиты (22). Определить реальную функцию вероятности взлома от вложенного финансирования можно, только построив экспериментальную зависимость вероятности взлома от вложенного финансирования по всей оси значений x, что практически невозможно из-за отсутствия необходимого количества экспериментальных данных. С другой стороны, можно теоретически оценить вероятность взлома защиты, ориентируясь на наиболее возможные события – на максимальные вероятности взлома, определяемые выражениями (14) или (14а). Построить теоретическую функцию вероятности взлома от вложенного финансирования можно основываясь на том факте, что с уменьшением вложенного финансирования в защиту, вероятность взлома защиты увеличивается. Из выражений (14) и (14а) видно, что при отсутствии финансирования максимум вероятности взлома может быть равен единице и при бесконечном финансировании стремится к нулю. Влияние вложенного финансирования на вероятность взлома можно осуществить через КЭЗ.

В реальных условиях, сохраняя тенденцию поведения кривой вероятности взлома от вложенного финансирования и учитывая эффективность вложенного финансирования, можно построить или аппроксимировать кривую максимумов вероятности взлома по трем точкам для реально построенной системы защиты. В этом случае кривая вероятности взлома защиты должна проходить как минимум по трем известным точкам: $P_m(X_1) = 1$ при $X_1=0$ $(m_1=1)$; $P_m(X)= 0$ при $X=\infty$ $(m=\infty)$; $P_m(X_2)$ при $X=X_2$ $(m=m_2)$. Точка $P_m(X_2)$ при $X=X_2$ берется из реальных условий построения технической защиты, где X_2 – приведенные финансовые затраты на построение защиты, $P_m(X_2)$ – полученная экспериментально вероятность взлома этой реально построенной защиты.

Всем перечисленным требованиям соответствует выражение максимумов вероятности взлома, с помощью которого можно аппроксимировать реальную вероятность взлома, риски общих и вложенных финансовых потерь

$$P_m(X) = \left[\frac{X^X}{(1+X)^{1+X}}\right]^{\gamma}, \quad (23)$$

где γ – определяет эффективность защиты от вложенного финансирования на ее построение. Анализируя выражение (23), можно сказать, что при

γ=1 получим выражение для расчета вероятности взлома и рисков потерь с пропорциональным вложением для бесконечного финансирования, при γ<1, как видно из (22), финансирование защиты будет иметь конечные размеры. Теоретические и реальные КЭЗ могут отличаться, что будет являться поводом для исследования эффективности построенной защиты.

Чтобы определить γ и получить выражение для расчета величины рисков потерь в реальной защите, возьмем известные точки вероятностей взлома и соответствующее им вложенное в защиту финансирование, и подставим в выражение (23).

В результате этого получим $P_m(X_2)$ при приведенных затратах $X=X_2$

$$P_m(X_2)=\left[\frac{X_2^{X_2}}{(1+X_2)^{1+X_2}}\right]^{\gamma}.$$

Возьмем логарифм этого выражения и определим γ как

$$\gamma=\frac{\lg P_m(X_2)}{lg[\frac{X_2^{X_2}}{(1+X_2)^{1+X_2}}]}. \qquad (24)$$

Подставляя полученное значение γ в выражение (23) и умножая на полные финансовые потери, получим формулу для определения приведенных величин рисков полных финансовых потерь

$$R*_{Sобщ}(X)=\left[\frac{X^X}{(1+X)^{1+X}}\right]^{\gamma}\cdot(1+X). \qquad (25)$$

Аналогичным образом получим формулу для определения приведенных величин рисков вложенных финансовых потерь.

Выводы. В данной работе предпринята попытка разработки методологии оценивания финансовых затрат на построение СЗИ по вероятности взлома защиты в зависимости от величины вложенного финансирования в защиту и возможных финансовых потерь без защиты; рискам потерь от вложенного финансирования в защиту; рискам полных финансовых потерь и эффективности построенной защиты. Все оценки СЗИ проводились для максимальных значений вероятности взлома и максимальных рисков потерь. В данной работе получены конкретные выражения для оценки эффективности защиты информации, оптимизации рисков финансовых потерь при проектировании, сертификации и оценки рабочего состояния в зависимости от финансовых вложений в защиту информации и рисков их потерь. Предложено теоретическое определение эффективности защиты через риски вложенного финансирования в защиту и риски полных финансовых потерь. Полученные выражения на этапе проектирования позволят сравнить между собой и оценить выбранную СЗИ до процесса ее внедрения. Предложенное определение коэффициента эффективности защищенности одиночной или одноуровневой защиты будет изменяться от нуля (при отсутствии финансирования защиты) до единицы (при бесконечном финансировании в построение защиты). Экспериментальные данные исследований отличий между практическим и теоретическим параметрами эффективности защиты позволят исследовать и подобрать наиболее оптимальную и эффективную защиту. Приведены выражения, позволяющие по реальной или экспериментальной вероятности взлома определить фактическую эффективность защищенности. Теоретически подтверждена более высокая надежность многоуровневой защиты по сравнению с одноуровневой защитой. Показано, что при одних и тех же финансовых затратах на одноуровневую и многоуровневую защиты вероятность взлома защиты и риски финансовых потерь многоуровневой защиты значительно ниже. Следовательно, с помощью многоуровневой системы защиты можно создать требуемый уровень защиты с меньшими финансовыми затратами. Таким образом, данная работа может быть полезна для оценки эффективности защиты информации, оптимизации рисков финансовых потерь при проектировании, сертификации и оценки рабочего состояния.

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]. В. Колемаев, *Математическая экономика: учебник для вузов* Колемаев В.А. М.: ЮНИТИ-ДАНА, 2002. 399 с.

[3]. А. Шапкин, *Экономические и финансовые риски. Оценка, управление, портфель инвестиций*, М.: Издательско-торговая корпорация «Данков и К°», 2003. 544 с.

[4]. В. Кравченко, Є. Левченко, "Використання теорії нечітких множин для визначення втрат на захист інформації", *Захист інформації*, №1, С. 85-90, 2011.

[5]. В. Домарев, *Безопасность информационных технологий. Системный подход*, К.:ООО «ТИД «ДС», 2004. 992 с.

[6]. І. Сахарцева, О. Шляга, *Ризики економічної діагностики підприємства*, МОН. К.: Кондор, 2008, 380 с.

[7]. Андре Анго *Математика для электро- и радиоинженеров*, М.: Из-во «Наука», 1964, 772 с.

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

ОЦІНЮВАННЯ ФІНАНСОВИХ ВИТРАТ НА ПОБУДОВУ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

У даній роботі зроблено спробу розробки методології оцінювання фінансових витрат на побудову системи захисту інформації (СЗІ) по відомим параметрам. Такими параметрами можуть бути: ймовірність злому захисту в залежності від величини вкладеного фінансування в захист і можливих фінансових втрат без захисту; ризики втрат від вкладеного фінансування в захист; ризики повних фінансових втрат і ефективність побудованого захисту. Всі оцінки СЗІ проводилися для максимальних значень ймовірності злому і максимальних ризиків втрат. У даній роботі отримані конкретні вирази для оцінки ефективності захисту інформації, оптимізації ризиків фінансових втрат при проектуванні, сертифікації та оцінки робочого стану в залежності від фінансових вкладень в захист інформації та ризиків їх втрат. Запропоновано теоретичне визначення ефективності захисту через ризики вкладеного фінансування в захист і ризики повних фінансових втрат. Коефіцієнт ефективності захищеності одиночного або однорівневого захисту буде змінюватися від нуля (при відсутності фінансування на захист) до одиниці (при нескінченному фінансуванні побудови захисту). Отримані вирази на етапі проектування дозволять порівняти між собою і оцінити обрану СЗІ до процесу її впровадження. Експериментальні дані досліджень відмінностей між практичним і теоретичним параметром ефективності захисту дозволять досліджувати і підібрати найбільш оптимальний і ефективний захист. Наведено вирази, що дозволяють по експериментальної ймовірності злому визначити фактичну ефективність захищеності. Теоретично підтверджена більш висока надійність багаторівневого захисту в порівнянні з однорівневим захистом. Показано, що при одних і тих же фінансових витратах на однорівневий і багаторівневий захист ймовірність злому захисту і ризики фінансових втрат багаторівневого захисту значно нижче. Отже, за допомогою багаторівневої системи захисту можна створити необхідний рівень захисту з меншими фінансовими витратами. Таким чином, дана робота може бути корисна для оцінки ефективності захисту інформації, оптимізації ризиків фінансових втрат при проектуванні, сертифікації та оцінки робочого стану.

Ключові слова: система захисту інформації, ймовірність злому захисту, ризики втрат від вкладеного фінансування в захист, ризики повних фінансових втрат, ефективність захисту, однорівневий захист, багаторівневий захист.

ESTIMATION OF FINANCIAL COSTS FOR BUILDING OF INFORMATION PROTECTION SYSTEM

In this paper, an attempt has been made to develop a methodology for estimating the financial costs of building a complex of technical information protection (CTIP) using known parameters. Such parameters can be: the likelihood of hacking protection, depending on the amount of funding invested in protection and possible financial losses without protection; risks of losses from invested funding in defense; risks of total financial losses and the effectiveness of the constructed protection. All CTEI assessments were conducted for the maximum values of the likelihood of hacking and the maximum risk of loss. In this paper, specific expressions are obtained for assessing the effectiveness of information protection, optimizing the risks of financial losses in the design, certification and evaluation of the working condition depending on financial investments in information protection and the risks of their losses. A theoretical definition of the effectiveness of protection through the risks of invested funding in defense and the risks of total financial losses are proposed. Coefficient the effectiveness of the protection of a single or single-tier protection will vary from zero (in the absence of funding for protection) to unity (with infinite funding for the construction of protection). The obtained expressions at the design stage will allow you to compare with each other and evaluate the chosen KTPDI before the process of its implementation. Experimental research data on the differences between the practical and theoretical parameters of the effectiveness of protection will allow to investigate and select the most optimal and effective protection. Expressions are given that make it possible to determine the actual effectiveness of security based on the experimental probability of hacking. Theoretically confirmed higher reliability of multi-level protection compared with single-level. It is shown that with the same financial costs for single-level and multi-level protection, the likelihood of hacking protection and risks financial loss of multi-level protection is much lower. Consequently, with the help of a multi-level protection system, you can create the required level of protection with lower financial costs. Thus, this work can be useful for assessing the effectiveness of information protection, optimizing the risks of financial losses in the design, certification and assessment of the working condition.

Keywords: technical information protection complex, probability of protection breaking, risks of losses from invested funding in defense, risks of total financial losses, protection effectiveness, single-level protection, multi-level protection.

Журиленко Борис Евгеньевич, кандидат физико-математических наук, доцент кафедры автоматизации и энергоменеджмента Национального авиационного университета.
E-mail: zhurylenko@gmail.com.
Журиленко Борис Євгенович, кандидат фізико-математичних наук, доцент кафедри автоматизації та енергоменеджменту Національного авіаційного університету.
Zhurilenko Boris Evgenievich, Candidate of Physical and Mathematical Sciences, assistant professor of automation and energy management of the National Aviation University.