визначення системи відповідних наукових, організаційних та правових заходів, потребує своєї розробки «Концепція розвитку законотворчого процесу», на основі якої необхідно підготувати «Комплексну програму наукового забезпечення законотворчого процесу в Україні».

III Висновки

Законотворчий процес і вся законодавча практика повинні мати творчий, багатоаспектний, науково обґрунтований характер, оскільки він не просто віддзеркалює зміни і розвиток зовнішнього світу, а є складним процесом його цілеспрямованого, концентрованого і нормативно-правового перетворення. Лише завдяки цьому результати законотворчості – закони, отримують силу активного зворотного впливу на навколишній світ. Розвиток наукової, нормативно-правової та організаційної основ інформаційного забезпечення законотворчого процесу сприятиме подальшому динамічному розвитку України як демократичної правової держави, всебічній реалізації прав і свобод її громадян, формуванню в нашій країні сучасного, розвинутого громадянського суспільства.

*Література: **1.** Сіленко А. Інформаційні технології – новий імпульс для пошуку парадигми майбутнього суспільства // Політичний менеджмент. – 2007. - № 3. – с. 98; **2.** Російчук Т. Антиутопія інформаційного суспільства // Соціальна психологія. – 2008. - № 1. – с. 85; **3.** Антощук Л. Д. Законотворчість: організація апарату парламентів світовий досвід // Л. Д. Антощук, заг. ред.: В. П. Кржанівський, Е. Р. Рахімкулов ; Прогр. сприяння парламенту України. - К. : Заповіт, 2007. - с. 67; **4.** Богачова О. Удосконалення законодавства - основна мета законотворчого процесу // Юридична Україна. - 2006. - N5. - с. 12; **5.** Коцюба Р. Принципи юридичної автентичності й архітектоніки в законотворенні України // Вісче. - 2009. - N12. - с. 11; **6.** Маруженко О. П. Роль інформації у законотворчому процесі // Бюлетень Міністерства юстиції України. - 2008. - N3. - с. 100-101; **7.** Конституція України. Науково-практичний коментар / В.Б.Авер'янов, О.В. Батанов, Ю.В.Баулін та ін.: ред. кол. В.Я. Тацій, Ю.П.Битяк, Ю.М. Грошевой та ін.- Харків: Видавництво «Право»; К.: Концерн «Видавничий Дім «Ін Юре», 2003.- с. 655; **8.** Погорєлова А. Передумови розширення доступу громадян до законотворчого процесу // Вісче. - 2007. - N23/24(груд.). - с. 22; **9.** Тертишник В. Забезпечення верховенства права та концептуальні проблеми гармонізації законотворчого процесу // Право України. - 2010. - N12. - с. 75; **10.** Ющенко О. Поняття законотворчого процесу в Україні та його основні елементи // Вісче. - 2010. - N2. - с. 30; **11.** Селиванов А. Проблемні аспекти законотворчого процесу та їх відображення в рішеннях Конституційного Суду України // Право України. – 2004.- № 9.- с. 34.*

УДК 004.056.5(045)

ОПТИМАЛЬНЫЕ ФИНАНСОВЫЕ ЗАТРАТЫ И ОСНОВНЫЕ КРИТЕРИИ ПОСТРОЕНИЯ ИЛИ МОДЕРНИЗАЦИИ КОМПЛЕКСА ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Борис Журиленко, Надежда Николаева, Никита Пелих
Национальный авиационный университет

Аннотация: **В результате теоретических исследований, определены оптимальные финансовые затраты и получены критерии построения и модернизации комплекса технической защиты информации (КТЗИ). Получено выражение для расчета рисков полных финансовых потерь, которые учитывают реальные параметры вероятности взлома многоуровневой защиты, финансовые затраты на ее внедрение и эффективность работы каждой единичной системы защиты, входящей в КТЗИ.**

Summary: **As a result of theoretical researches, optimum financial expenses are determined and criteria of construction and modernization of a complex of technical protection of information (CTPI) are received. Expression for calculation of risks of full financial losses which take into account real parameters of probability of breaking of multilevel protection, financial expenses for its{her} introduction and an overall performance of each individual system of the protection which is included in CTPI is received.**

Ключевые слова: **Комплекс технической защиты информации, вероятность взлома, риски полных финансовых потерь, риски потерь, вложенных в построение технической защиты, многоуровневая защита информации.**

I Введение

Для защиты секретной, конфиденциальной и “ноу-хау” информации от утечки по техническим каналам необходимо создавать комплекс технической защиты информации (КТЗИ). Фирмы и предприятия, которые

будут создавать такой КТЗИ, в первую очередь, будет интересовать экономическая выгода применения того или иного КТЗИ. Из всех возможных параметров, понятных для экономических расчетов, являются величины рисков полных финансовых потерь и величины рисков вложенных потерь. Для расчетов этих рисков исходными параметрами могут быть начальные финансовые потери без защиты, вероятность взлома защиты при определенной попытке взлома и финансовые затраты на выбранную защиту с данной вероятностью взлома.

В открытой литературе [1 – 4] 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 КТЗИ, оптимизация финансовых потерь в случае взлома технической защиты информации (ТЗИ), критериев необходимости дополнительных затрат на восстановление ТЗИ до необходимого технического уровня защиты и, соответственно, оптимизации финансовых потерь.

В связи с этим, целью данной работы были: попытка разработки методики расчета КТЗИ, определение критерия оптимизации расходов на построение КТЗИ и оптимизации финансовых потерь в случае взлома ТЗИ.

II Основная часть

Рассмотрим соотношение, которое представляет собой величину рисков финансовых потерь [5].

Пусть величина затрат на один вариант защиты информации будет x и при этом обеспечивается вероятность взлома p_x с первого раза. Учитывая, что риски потерь при организации защиты для фирмы будут состоять из первоначальных финансовых потерь от утечки информации H и затрат на организацию защиты x, можем записать величину рисков финансовых потерь как

$$(H + x)\cdot p_x = f(x), \tag{1}$$

где H – первоначальные финансовые потери при отсутствии защиты; x – финансирование, потраченное на организацию защиты с вероятностью взлома p_x; $f(x)$ – функция величины риска полных финансовых потерь, полученная в результате перемножения общих финансовых потерь на вероятность взлома; p_x – вероятность взлома при финансовых затратах на защиту, равных x.

С математической точки зрения величина рисков финансовых потерь может определяться любой функцией $f(x)$, которая может быть выражена с помощью степенного ряда [6]

$$\mathrm{f(x)} = \alpha + \beta \cdot \mathrm{x} + \gamma \cdot x^2 + \ldots \ , \tag{2}$$

где α, β, γ – постоянные числа.

Возьмем сначала первое приближение по x $f(x)=\alpha+\beta\cdot x$. Для определения критерия эффективности используемой защиты информации и вероятности взлома от величины затрат на защиту информации важна лишь тенденция поведения функции $f(x)$ в зависимости от x. Поэтому подставив (2) в (1) получим

$$(H + x)\cdot p_x = \alpha + \beta \cdot x\,. \tag{3}$$

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

$$p_x = \frac{\alpha + \beta \cdot x}{H + x} \tag{4}$$

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

$$\lim_{x \to \infty} p_x = \beta\,. \tag{5}$$

Проанализируем выражение (5). Если $\beta > 0$, то вкладываемое финансирование на защиту не эффективно, так как при бесконечном вкладе финансирования на защиту информации существует вероятность ее взлома. Таким образом, функциональная зависимость в (3) и (1) с $\beta > 0$ приведет к возрастанию функции $f(x)$ в зависимости от вложенного финансирования на ее защиту, что будет указывать на необходимость замены выбранного типа защиты на другой более эффективный способ.

Это обстоятельство может быть первым критерием выбора типа защиты и эффективности затрат на ее внедрение.

При $\beta = 0$ вкладываемое финансирование на защиту является пропорциональным, то есть выполняется принцип достаточности между вкладываемым финансированием и вероятностью взлома.

И при $\beta < 0$ “гарантируется” большая защищенность информации по сравнению с $\beta = 0$. В этом случае обеспечивается более эффективная защита информации на единицу вложенного финансирования.

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 $\beta = 0$). В идеале будет случай, когда вклад финансирования в защиту приведет к уменьшению величины рисков потерь (случай $\beta < 0$). Таким образом, одним из критериев оптимального вклада финансирования в техническую защиту информации будет условие

$$f(x) \le f(0), \tag{6}$$

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 два последних случая. Сначала случай пропорциональной защиты с $\beta = 0$. В качестве исходных данных, которые необходимы при разработке одного типа ТЗИ, будем считать вероятность первого проникновения через защиту в начальном состоянии p_0. Вероятность проникновения через ТЗИ, в случае отсутствия защиты, равна единице. Если же в исходном состоянии существовала некоторая защита и ее необходимо улучшить, то $p_0 \le 1$.

Согласно (3) при $\beta = 0$ получим

$$(H + x) \cdot p_x = \alpha, \tag{7}$$

где α – некоторая постоянная величина.

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

$$p_x = \frac{\alpha}{H + x}. \tag{8}$$

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

$$p_0 = \frac{\alpha}{H} = 1, \text{ или } \alpha = H. \tag{9}$$

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

$$p_x = \frac{H}{H + x}. \tag{10}$$

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

Предположим, что попытки проникновения ведутся до полного 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.

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 [7].

Вероятность события до взлома на m попытке может быть записана как

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

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.

Определим условия оптимального вложения финансирования на защиту с числом попыток взлома m. Анализируя выражение (12), видим, что при $x=0$ и при x стремящимся к бесконечности, $P(x)=0$. Следовательно, выражение (12) имеет экстремум, который будет зависеть от вложенного на защиту финансирования и попыток взлома m. Исследуем (12) на экстремум по x, учитывая, что m не зависит от

вложенного на защиту финансирования. Значение m, то есть рассчитываемое количество взломов, может выбираться при организации КТЗИ.

Исследования на экстремум показали, что при

$$x = (m-1)\cdot H \tag{13}$$

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

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

выражение (12) будет иметь максимум, то есть определять оптимальное соотношение между вкладом финансирования 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 ТЗИ 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.

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

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

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

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

На рис.1 представлены результаты расчета вероятности события проникновения через защиту $P(x)$ по формуле (12). В расчетах кривые $P_m(X)$ и $P(m)$ полностью совпадают.

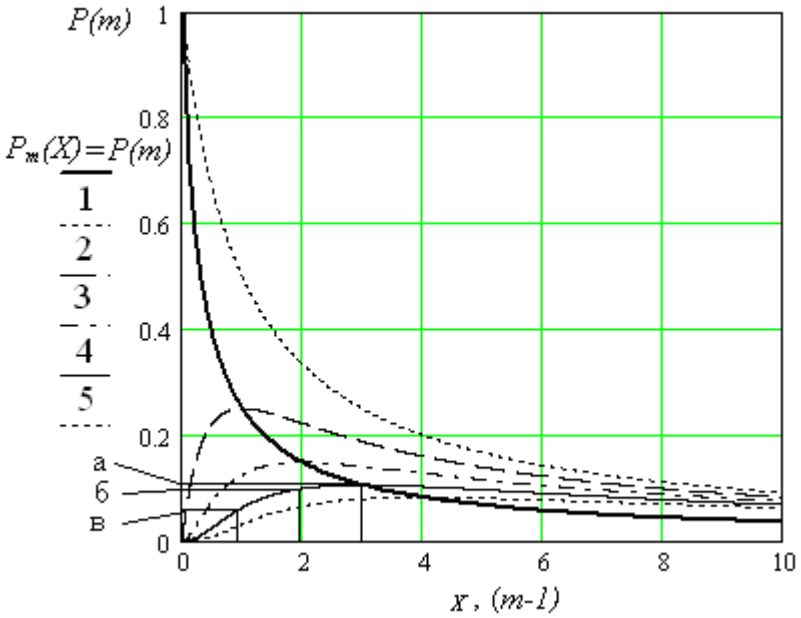

Рисунок 1 - Расчет вероятности события проникновения *P(m)* через защиту в зависимости от попыток взлома *m*: 1 – при *m = 1*; 2 – при *m = 2*; 3 – при *m = 3*; 4 – при *m = 4*; 5 – при *m = 5*; *X = x/H* – приведенные значения финансовых затрат; *H* – финансовые потери при отсутствии защиты, *x* – финансовые 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

Объясним смысл *P(m)*, используя кривую 4 рис. 1 (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 выражению (13). Очевидно, что при таких затратах, вероятность взлома с первой попытки минимальна по сравнению со второй (точка в, рис. 1) и третьей (точка б, рис. 1) попыток, для которых вероятность взлома будет увеличиваться. С другой стороны, если затраты на защиту информации будут больше оптимально необходимых затрат для взлома с четвертой (точка а, рис. 1) попытки, то вероятность взлома будет уменьшаться, согласно 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.

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

$$R_{общ}(x) = P_m(X) \cdot (H + x) \tag{17}$$

соответствует величине рисков полных финансовых потерь в случае взлома защиты;

$$R^*_{общ}(m) = R^*_{общ}(X) = \frac{R_{общ}(x)}{H} = P_m(X) \cdot (1 + X) \tag{17a}$$

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

$$R_{вл}(x) = P_m(X) \cdot x \tag{18}$$

соответствует величине рисков финансовых потерь, вложенных в построение ТЗИ;

$$R^*_{вл}(m) = R^*_{вл}(X) = \frac{R_{вл}(x)}{H} = P_m(X) \cdot X \tag{18a}$$

соответствует величине приведенных рисков финансовых потерь, вложенных в построение ТЗИ.

Результаты расчета величины приведенных рисков представлены на рис. 2.

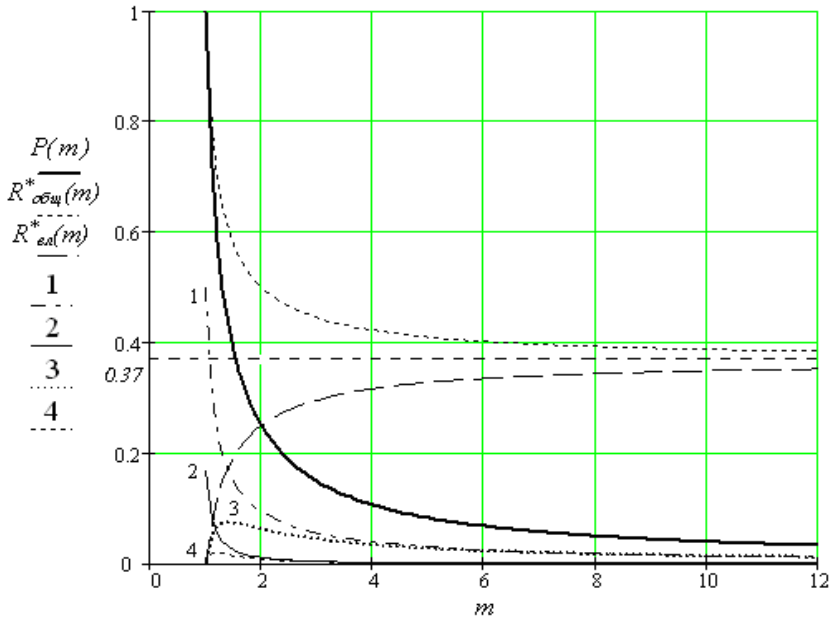

Рисунок 2 – Расчет величины рисков потерь; *P (m)* - кривая, определяющая максимальные значения вероятности проникновения в зависимости от числа попыток взлома $m \geq 1$; $R^*_{общ}(m)$ – величина приведенных рисков полных финансовых потерь в случае взлома защиты; $R^*_{вл}(m)$ – величина приведенных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

Определим пределы, к которым стремятся величины приведенных рисков полных финансовых потерь (17а) и величины приведенных рисков вложенных финансовых потерь (18а), при стремлении попыток взлома m к бесконечности. Для этого вместо X в выражения (17а) и (18а) подставим условие экстремума (13а). Получим

$$\lim_{m\to\infty} R^*_{общ}(m) = \lim_{m\to\infty} \frac{(m-1)^{m-1}\cdot m}{m^m} = \frac{1}{e} \approx 0{,}37\ , \tag{19}$$

$$\lim_{m\to\infty} R^*_{вл}(m) = \lim_{m\to\infty} \frac{(m-1)^{m-1}\cdot (m-1)}{m^m} = \frac{1}{e} \approx 0{,}37\ . \tag{20}$$

Отсюда видно, что величины приведенных рисков полных потерь и потерь финансирования, вложенных в построение одной ТЗИ, при бесконечных попытках взлома и, следовательно, бесконечного финансирования имеют придельное значение величины рисков равное 1/e ≈ 0,37 (рис. 2, прямая пунктирная линия). В выражениях (17) и (18) величины рисков будут равны ≈ 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 ТЗИ будут ≈ 0,37H.

В реальных условиях бесконечные затраты финансирования на защиту мало кого устроят, поэтому для оптимизации финансирования из кривых $R^*_{общ}(m)$ и $R^*_{вл}(m)$ определим процент рисков в зависимости от числа попыток взлома и, следовательно, от величины вложенного в защиту финансирования. Эти результаты представлены в таблице 1.

Таблица 1 – Величины приведенных рисков, проценты величины рисков полных финансовых потерь и проценты величины рисков вложенных финансовых потерь в зависимости от числа попыток взлома

m	$R^*_{вл}(m)$	$R^*_{общ}(m)$	% величины рисков финансовых потерь, вложенных в построение ТЗИ, от числа попыток взлома по отношению к предельно возможному риску 0,37	% величины рисков полных финансовых потерь от числа попыток взлома по отношению к предельно возможному риску 0,37
1	0	1	0	100
2	0,25	0,5	67,6	20,6
3	0,2963	0,4444	80,1	11,8
4	0,3164	0,4219	91,2	8,8
5	0,3277	0,4096	93,7	6,3
6	0,3349	0,4019	94,9	5,1
7	0,34	0,3966	95,8	4,2
8	0,3436	0,3927	96,4	3,6
9	0,3464	0,3897	96,9	3,1
10	0,3487	0,3874	97,2	2,8
11	0,3505	0,3855	97,5	2,5

Из табл. 1 видно, что оптимальные затраты финансирования, вложенного в построение одной ТЗИ, должны рассчитываться на возможность взлома с 3 попытки, то есть вклад финансирования равный 2H или возможным общим потерям – 3H. В этом случае величины рисков полных финансовых потерь уменьшатся на 88,2% по отношению к предельно возможным величинам рисков потерь (0,37, рис. 2). Можно рассчитывать и на возможность взлома с 4 попытки. Однако, начиная с этой попытки и последующих, вкладываемое на защиту информации финансирование, работает больше на уменьшение рисков вкладываемого финансирования, чем на уменьшение рисков общих финансовых потерь. Об этом говорит тот факт, что начиная с 4 попытки, суммарный процент 4-го и 5-го столбцов таблицы 1 дает 100% потерь.

Таким образом, наиболее оптимальное финансирование на защиту информации при использовании одной ТЗИ будет при затратах на защиту с 3 попытки взлома. В этом случае на защиту информации необходимо затратить финансирование, равное 2H, а возможные общие потери – 3H.

Рассмотрим многоуровневую защиту, состоящую из n пропорциональных защит $P(m_1)$, …, $P(m_n)$ (14), где m_1… m_n – означают попытки взлома, на которых произошел взлом на первой или n многоуровневой защите. Взлом этого многоуровневого комплекса технической защиты будет осуществляться при последовательном взломе каждого уровня защиты. В самой первой стадии взлома вероятность взлома любой из n

пропорциональных защит будет равна $\frac{1}{n} P(m_j)$, где j соответствует взламываемой защите. После ее взлома остается (n – 1) не взломанных защит. Вероятность взлома любой из них будет $\frac{1}{n-1} P(m_s)$, где s взламываемая защита. Последняя защита будет иметь вероятность взлома $P(m_k)$, где k последняя взламываемая защита. Все эти вероятности взлома являются независимыми, поэтому вероятность взлома всей многоуровневой технической защиты с учетом количеств взлома $m_j, m_s \ldots m_k$ в каждой защите будет определяться следующей формулой

$$P_{\Sigma}(m_1,\ldots,m_n) = \frac{1}{n!}\prod_{j=1}^{n} P(m_j) \qquad (21),$$

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

Определим предельные значения величины рисков полных финансовых потерь для многоуровневой системы защиты $R^*_{\Sigma общ}(m_1, \ldots m_n)$ при стремлении попыток взлома к бесконечности.

$$R^*_{\Sigma общ}(m_1,\ldots,m_n) = \lim_{(m_1 \ldots m_n)\to\infty}\left[\frac{1}{n!}\times\frac{(m_1-1)^{m_1-1}}{m_1^{m_1}}\times\ldots\times\frac{(m_n-1)^{m_n-1}}{m_n^{m_n}}\times\right. \qquad (22)$$

$$\left.\times(m_1+\ldots+m_n-n+1)\right]=0.$$

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

$$R^*_{\Sigma вл}(m_1,\ldots,m_n) = \lim_{(m_1 \ldots m_n)\to\infty}\left[\frac{1}{n!}\times\frac{(m_1-1)^{m_1-1}}{m_1^{m_1}}\times\ldots\times\frac{(m_n-1)^{m_n-1}}{m_n^{m_n}}\times\right. \qquad (23)$$

$$\left.\times(m_1+\ldots+m_n-n)\right]=0.$$

Результаты расчетов величин рисков для двух и трехуровневых защит по формулам (22) и (23) представлены на рис. 2 кривыми 1, 2, 3, 4 и в таблице 2.

Таблица 2 – Приведенные величины рисков полных и вложенных финансовых потерь для двух и трехуровневых технических систем защиты информации

Число уровней защиты	Приведенные риски	$m_1 = m_2 = m_3$									
		1	2	3	4	5	6	7	8	9	10
2	$R^*_{\Sigma общ}(m_1, m_2)$	0,5	$9{,}4\ 10^{-2}$	$5{,}5\ 10^{-2}$	$3{,}9\ 10^{-2}$	$3{,}0\ 10^{-2}$	$2{,}5\ 10^{-2}$	$2{,}1\ 10^{-2}$	$1{,}8\ 10^{-2}$	$1{,}6\ 10^{-2}$	$1{,}4\ 10^{-2}$
	$R^*_{\Sigma вл}(m_1, m_2)$	0	$6.3\ 10^{-2}$	$4{,}4\ 10^{-2}$	$3{,}3\ 10^{-2}$	$2.7\ 10^{-2}$	$2{,}2\ 10^{-2}$	$1{,}9\ 10^{-2}$	$1{,}7\ 10^{-2}$	$1{,}5\ 10^{-2}$	$1{,}3\ 10^{-2}$
3	$R^*_{\Sigma общ}(m_1, m_2, m_3)$	$1{,}7\ 10^{-1}$	$1{,}0\ 10^{-2}$	$3{,}8\ 10^{-3}$	$2,0\ 10^{-3}$	$1{,}2\ 10^{-3}$	$8{,}0\ 10^{-4}$	$5{,}8\ 10^{-4}$	$4{,}3\ 10^{-4}$	$3{,}4\ 10^{-4}$	$2{,}7\ 10^{-4}$
	$R^*_{\Sigma вл}(m_1, m_2, m_3)$	0	$7{,}8\ 10^{-3}$	$3{,}3\ 10^{-3}$	$1{,}8\ 10^{-3}$	$1.1\ 10^{-3}$	$7{,}5\ 10^{-4}$	$5.5\ 10^{-4}$	$4{,}1\ 10^{-4}$	$3{,}3\ 10^{-4}$	$2{,}6\ 10$

Расчеты выполнялись при условии $m_1=m_2=m_3=2$, то есть при взломе на каждом уровне со второй попытки. Обоснованность такого предположения видна из расчетов в табл. 2 и рис. 2, и связана с тем, что максимальное уменьшение величины полных рисков финансовых потерь приходится с первой на вторую попытку взлома. Отсюда можно предположить, что для многоуровневых систем защиты достаточно рассчитывать возможность взлома со второй попытки для каждого уровня. Использование в расчетах более высоких уровней взлома приводит к малым уменьшениям величины полных рисков финансовых потерь. Максимумы величины рисков вложенных финансовых потерь также находятся между первой и второй попытками взлома.

В отличие от случая с одной пропорциональной защитой приведенные полные и вложенные величины

рисков многоуровневой защиты при бесконечных попытках взлома сходятся к нулю. Следует заметить еще одно отличие – увеличение финансовых затрат на ТЗИ уменьшает не только полные риски потерь, но и риски вложенных потерь.

Отсюда видно, что более эффективно вложить финансирование в защиту и существенно уменьшить величины рисков потерь можно при использовании многоуровневого комплекса технических защит, чем вкладывать финансирование в одну защиту. Например, если для многоуровневой системы использовать две пропорциональные защиты, для которых взлом осуществляется со второй попытки (общие затраты будут *2H*, $m_1=2$, $m_2=2$), приведенные величины рисков полных финансовых потерь будут приблизительно равны 0,094. Используя одну защиту при тех же затратах на защиту *2H* ($m=3$), получим приведенные величины рисков полных финансовых потерь приблизительно равные 0,44. Для трехуровневой технической защиты при тех же условиях, что и для двухуровневой защиты, приведенная величина риска полных финансовых потерь будет 0,01, для одноуровневой защиты – 0,42. Таким образом, с увеличением уровней защиты приведенные величины рисков полных потерь резко падают при одних и тех же расходах на защиту. Для двухуровневой защиты величина риска падает приблизительно в 4,7 раза, а для трехуровневой - приблизительно в 42 раза.

В данном случае при рассмотрении многоуровневой защиты исходили из предположения, что каждая пропорциональная защита участвует в уменьшении величины рисков потерь с долей, равной *H*. Однако можно сэкономить в организации технической защиты и сделать так, чтобы каждая одиночная защита участвовала бы только в малой доле *H*.

Рассмотрим случай многоуровневой системы защиты с долевым распределением финансовых потерь по одиночным защитам. Для этого возьмем двухуровневую защиту. Расчеты для двухуровневой системы защиты по формуле

$$R^*_{\Sigma общ}(m_1, m_2) = \frac{1}{2!} \times \frac{X_1^{X_1}}{(1+X_1)^{1+X_1}} \times \frac{X_2^{X_2}}{(1+X_2)^{1+X_2}} \times (X_1 + X_2 + 1) \qquad (24)$$

представлены в табл. 3, табл. 4, и на рис. 3а и 3б соответственно. В табл. 3 и на рис. 3а представлены результаты расчета при распределении финансовых потерь *H* по половине на защиту. В табл. 4 и рис. 3б затраты на защиту распределены по долям: по оси x_1 – $H_{x_1}=3/4H$, по оси x_2 – $H_{x_2}=1/4H$. На рис.3 видно, что в плоскостях $R^*_{\Sigma общ}(m_1, m_2), x_1$ и $R^*_{\Sigma общ}(m_1, m_2), x_2$ зависимости величины рисков такие же, как и для одноуровневой защиты (на рис. 2, кривая $R^*_{общ}(m)$), а в плоскости x_1, x_2 величина риска обеспечивается обеими защитами. В случае влияния обеих защит величины рисков резко падают и имеют минимум только при одинаковых финансовых затратах на каждую из защит $x_1=x_2$ (табл. 3). Если же финансирование защиты распределено на неравные доли (рис. 3б, табл. 4), то минимум величин общих рисков припадает также на одинаковые финансовые затраты на каждую из защит $x_1=x_2$, но при этом несколько уменьшаются величины рисков общих финансовых потерь.

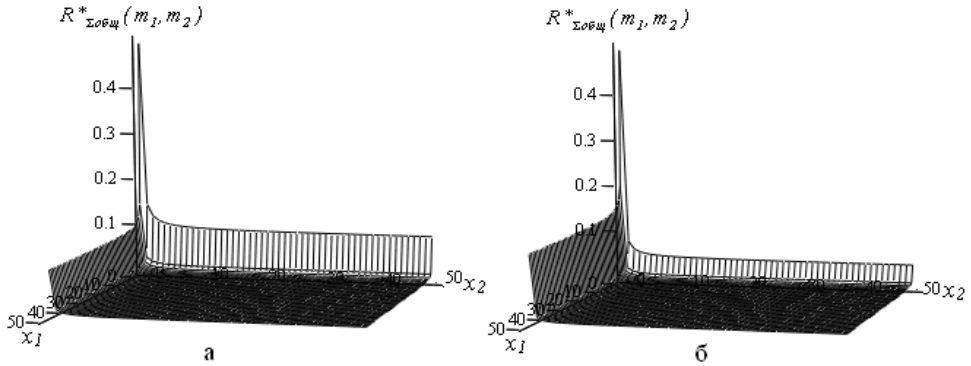

Рисунок 3 – Приведенные величины рисков полных потерь для двухуровневой технической системы защиты информации: а – с равными долевыми вкладами финансирования в одиночные системы защиты информации: по оси x_1 – $H_{x_1}=1/2H$, по оси x_2 – $H_{x_2}=1/2H$; б – с затратами на защиту по долям: по оси x_1 – $H_{x_1}=3/4H$, по оси x_2 – $H_{x_2}=1/4H$. Шкалы по осям x_1 и x_2 имеют одинаковые значения по вкладам финансирования на защиту информации

Это можно объяснить тем, что при одинаковом финансировании на одну защиту с меньшей долей

потребуется больше попыток взлома и, следовательно, она определяет уменьшение минимума общих рисков. С другой стороны для защиты большей доли потерь количество попыток взлома уменьшается. В этом случае общие риски потерь определяются в основном минимальной долей, которая защищена более сильно, чем вторая доля, которая может быть взломана быстрее. Исходя из выше изложенного, чтобы обеспечить более равномерную защиту полных финансовых потерь для двухуровневой защиты, более целесообразно использовать равное деление финансовых потерь на защиты. Однако, следует заметить, что оптимальное долевое деление начальных финансовых потерь при многоуровневой системах технической защиты требует дополнительных исследований.

Таблица 3 – Приведенные величины рисков полных потерь для двухуровневой технической системы защиты информации с равными долевыми вкладами финансирования в одиночные системы защиты информации: по оси x_1 – $H_{x_1}=1/2H$, по оси x_2 – $H_{x_2}=1/2H$**.** Шкалы по осям x_1 и x_2 имеют одинаковые значения по вкладам финансирования на защиту информации.

	0	1	2	3	4	5	6	7	8	9	10
0	0.5	0.148	0.123	0.113	0.108	0.105	0.103	0.102	0.1	0.099	0.099
1	0.148	0.033	0.024	0.021	0.019	0.018	0.017	0.017	0.017	0.016	0.016
2	0.123	0.024	0.017	0.014	0.012	0.011	0.011	0.01	0.01	$9.775\cdot10^{-3}$	$9.556\cdot10^{-3}$
3	0.113	0.021	0.014	0.011	$9.813\cdot10^{-3}$	$8.935\cdot10^{-3}$	$8.339\cdot10^{-3}$	$7.907\cdot10^{-3}$	$7.58\cdot10^{-3}$	$7.324\cdot10^{-3}$	$7.117\cdot10^{-3}$
4	0.108	0.019	0.012	$9.813\cdot10^{-3}$	$8.439\cdot10^{-3}$	$7.589\cdot10^{-3}$	$7.012\cdot10^{-3}$	$6.593\cdot10^{-3}$	$6.277\cdot10^{-3}$	$6.029\cdot10^{-3}$	$5.829\cdot10^{-3}$
5	0.105	0.018	0.011	$8.935\cdot10^{-3}$	$7.589\cdot10^{-3}$	$6.757\cdot10^{-3}$	$6.191\cdot10^{-3}$	$5.781\cdot10^{-3}$	$5.471\cdot10^{-3}$	$5.228\cdot10^{-3}$	$5.032\cdot10^{-3}$
6	0.103	0.017	0.011	$8.339\cdot10^{-3}$	$7.012\cdot10^{-3}$	$6.191\cdot10^{-3}$	$5.633\cdot10^{-3}$	$5.229\cdot10^{-3}$	$4.923\cdot10^{-3}$	$4.684\cdot10^{-3}$	$4.491\cdot10^{-3}$
7	0.102	0.017	0.01	$7.907\cdot10^{-3}$	$6.593\cdot10^{-3}$	$5.781\cdot10^{-3}$	$5.229\cdot10^{-3}$	$4.83\cdot10^{-3}$	$4.527\cdot10^{-3}$	$4.29\cdot10^{-3}$	$4.099\cdot10^{-3}$
8	0.1	0.017	0.01	$7.58\cdot10^{-3}$	$6.277\cdot10^{-3}$	$5.471\cdot10^{-3}$	$4.923\cdot10^{-3}$	$4.527\cdot10^{-3}$	$4.227\cdot10^{-3}$	$3.991\cdot10^{-3}$	$3.802\cdot10^{-3}$
9	0.099	0.016	$9.775\cdot10^{-3}$	$7.324\cdot10^{-3}$	$6.029\cdot10^{-3}$	$5.228\cdot10^{-3}$	$4.684\cdot10^{-3}$	$4.29\cdot10^{-3}$	$3.991\cdot10^{-3}$	$3.757\cdot10^{-3}$	$3.569\cdot10^{-3}$
10	0.099	0.016	$9.556\cdot10^{-3}$	$7.117\cdot10^{-3}$	$5.829\cdot10^{-3}$	$5.032\cdot10^{-3}$	$4.491\cdot10^{-3}$	$4.099\cdot10^{-3}$	$3.802\cdot10^{-3}$	$3.569\cdot10^{-3}$	$3.387\cdot10^{-3}$

Таблица 4 – Приведенные величины рисков полных потерь для двухуровневой технической системы защиты информации с затратами на защиту по долям: по оси x_1 – $H_{x_1}=3/4H$, по оси x_2 – $H_{x_2}=1/4H$. Шкалы по осям x_1 и x_2 имеют одинаковые значения по вкладам финансирования на защиту информации

	0	1	2	3	4	5	6	7	8	9	10
0	0.5	0.082	0.065	0.059	0.056	0.054	0.053	0.052	0.051	0.05	0.05
1	0.203	0.025	0.018	0.015	0.014	0.013	0.012	0.012	0.012	0.011	0.011
2	0.175	0.019	0.013	0.01	$9.105\cdot10^{-3}$	$8.375\cdot10^{-3}$	$7.883\cdot10^{-3}$	$7.53\cdot10^{-3}$	$7.263\cdot10^{-3}$	$7.055\cdot10^{-3}$	$6.888\cdot10^{-3}$
3	0.164	0.017	0.011	$8.441\cdot10^{-3}$	$7.307\cdot10^{-3}$	$6.616\cdot10^{-3}$	$6.151\cdot10^{-3}$	$5.816\cdot10^{-3}$	$5.564\cdot10^{-3}$	$5.367\cdot10^{-3}$	$5.209\cdot10^{-3}$
4	0.158	0.016	$9.57\cdot10^{-3}$	$7.435\cdot10^{-3}$	$6.336\cdot10^{-3}$	$5.666\cdot10^{-3}$	$5.215\cdot10^{-3}$	$4.891\cdot10^{-3}$	$4.646\cdot10^{-3}$	$4.455\cdot10^{-3}$	$4.302\cdot10^{-3}$
5	0.154	0.015	$8.899\cdot10^{-3}$	$6.806\cdot10^{-3}$	$5.728\cdot10^{-3}$	$5.071\cdot10^{-3}$	$4.629\cdot10^{-3}$	$4.311\cdot10^{-3}$	$4.071\cdot10^{-3}$	$3.884\cdot10^{-3}$	$3.733\cdot10^{-3}$
6	0.152	0.014	$8.439\cdot10^{-3}$	$6.374\cdot10^{-3}$	$5.311\cdot10^{-3}$	$4.663\cdot10^{-3}$	$4.227\cdot10^{-3}$	$3.913\cdot10^{-3}$	$3.677\cdot10^{-3}$	$3.492\cdot10^{-3}$	$3.344\cdot10^{-3}$
7	0.15	0.014	$8.104\cdot10^{-3}$	$6.06\cdot10^{-3}$	$5.008\cdot10^{-3}$	$4.366\cdot10^{-3}$	$3.934\cdot10^{-3}$	$3.624\cdot10^{-3}$	$3.389\cdot10^{-3}$	$3.207\cdot10^{-3}$	$3.06\cdot10^{-3}$
8	0.148	0.013	$7.849\cdot10^{-3}$	$5.821\cdot10^{-3}$	$4.777\cdot10^{-3}$	$4.14\cdot10^{-3}$	$3.712\cdot10^{-3}$	$3.403\cdot10^{-3}$	$3.171\cdot10^{-3}$	$2.989\cdot10^{-3}$	$2.844\cdot10^{-3}$
9	0.147	0.013	$7.649\cdot10^{-3}$	$5.633\cdot10^{-3}$	$4.595\cdot10^{-3}$	$3.962\cdot10^{-3}$	$3.536\cdot10^{-3}$	$3.23\cdot10^{-3}$	$2.999\cdot10^{-3}$	$2.819\cdot10^{-3}$	$2.674\cdot10^{-3}$
10	0.146	0.013	$7.487\cdot10^{-3}$	$5.481\cdot10^{-3}$	$4.449\cdot10^{-3}$	$3.819\cdot10^{-3}$	$3.395\cdot10^{-3}$	$3.09\cdot10^{-3}$	$2.86\cdot10^{-3}$	$2.681\cdot10^{-3}$	$2.537\cdot10^{-3}$

Рассмотрим случай более эффективного вложения финансирования в техническую защиту информации при $\beta < 0$. Согласно выражению (4), где используется первое линейное приближение, при значениях $x \geq -\frac{\alpha}{|\beta|} > 0$, $\alpha > 0$, вероятность взлома становится отрицательной, что не соответствует реальной действительности. Следовательно, линейное приближение не может использоваться для расчета реальных полных рисков с более эффективным вложением финансирования в техническую защиту. Выражение (4) может быть преобразовано к виду

$$p_x = \frac{\alpha}{H+x} - \frac{\beta(x)}{H+x},$$

где $\beta(x)$- функция, уточняющая вероятность первичного взлома при пропорциональной защите и

определяющая вклад всех остальных членов приближения выражения (2). Определить функцию $\beta(x)$ можно, только построив реальную зависимость вероятности взлома от вложенного финансирования по всей оси значений *x*, что практически нереально. В реальных условиях можно построить защиту, определить ее вероятность взлома и потраченное финансирование на ее построение по трем точкам, по которым можно определить или аппроксимировать вероятность взлома для реально построенной системы защиты.

Кривая вероятности более эффективной реальной защиты находится между кривой вероятности пропорциональной защиты и осями координат (рис. 1, толстая сплошная кривая) и должна проходить как минимум по трем известным точкам: $P_m(X_1) = 1$ при $X_1=0$; $P_m(X)= 0$ при $X=\infty$; $P_m(X_2)$ при $X=X_2$. 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 вероятность взлома этой реально построенной защиты.

Всем перечисленным требованиям соответствует выражение, с помощью которого можно аппроксимировать реальную вероятность взлома для расчета рисков общих и вложенных потерь

$$P_m(X)=\left[\frac{X^X}{(1+X)^{1+X}}\right]^{\gamma}, \tag{25}$$

где $\gamma>1$ – определяет эффективность защиты от вложенного финансирования на ее построение. Анализируя выражение (25), можно сказать, что при $\gamma=1$ получим выражение для расчета вероятности взлома и рисков потерь с пропорциональным вложением финансирования, при $\gamma<1$ необходимо отказаться от выбранного типа защиты, так как она будет не эффективна в работе. Эти условия являются обобщением критерия (6).

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 (25).

В результате этого получим при $P_m(X_2)$ и 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

$$\gamma=\frac{lg P_m(X_2)}{lg\left[\frac{X_2^{X_2}}{(1+X_2)^{1+X_2}}\right]}. \tag{26}$$

Подставляя полученное значение γ в выражение (25) и умножая на полные финансовые потери, получим формулу для определения приведенных величин полных рисков для более эффективных и других видов защит:

$$R^*_{\Sigma общ}(X)=\left[\frac{X^X}{(1+X)^{1+X}}\right]^{\gamma}\cdot(1+X). \tag{27}$$

Для многоуровневой защиты с долевой потерей *H* расчеты величин рисков могут осуществляться с помощью выражения

$$R^*_{\Sigma общ}(X_1,...,X_n)=\frac{1}{n!}\left\{\prod_{j=1}^{n}\left[\frac{X_j^{X_j}}{(1+X_j)^{1+X_j}}\right]^{\gamma_j}\right\}\times(X_1+...+X_n+1), \tag{28}$$

где *n* - количество защит, $X_1 ... X_n$ – приведенные затраты на защиты, $\gamma_1 ... \gamma_n$ – учитывает эффективность каждой из используемых защит.

III Заключение

В результате выполненной работы предложена методика расчета финансовых затрат при построении или модернизации комплекса технической защиты информации; методика расчета величины рисков общих финансовых потерь КТЗИ; определение критерия оптимизации расходов на построение КТЗИ и оптимизации финансовых потерь в случае взлома ТЗИ.

На основании проделанной работы можно сделать следующие выводы.

Использование одноуровневой защиты (одиночной защиты) абсолютно неэффективно, потому что даже при бесконечном вложении финансирования на защиту или модернизацию нельзя получить достаточный

уровень величин рисков финансовых потерь. Минимальное количество защит, которое может быть использовано для достижения необходимого уровня величины рисков, должно быть не менее двух. Использование многоуровневой защиты позволит более эффективно защитить информацию при одинаковых финансовых затратах.

Получены выражения для расчета вероятности взлома информации, как от величины вложенного финансирования, так и от количества попыток взлома. Определены оптимальные соотношения между числом попыток взлома и вкладываемым в защиту финансированием. Оказалось, что вполне достаточно рассчитывать защищенность до второй или третьей попыток взлома одиночной защиты, но для более существенного уменьшения величины рисков потерь необходимо использовать многоуровневую защиту. В этом случае затраты на разработку или модернизацию КТЗИ будут соответствовать *H* или *2H*.

В многоуровневой защите необходимо при ее разработке или модернизации на каждую из единичных защит вкладывать одинаковое финансирование, что позволит добиться минимальных величин рисков финансовых потерь. Уменьшить вклад финансирования в разработку или модернизацию защиты может позволить долевая защита потерь каждой из защит. Однако, как уже отмечалось, необходимы дополнительные исследования для определения оптимальных условий.

Получены выражения для расчета величин рисков потерь, соответствующих реальным системам защиты, которые получаются при использовании той или иной защиты. При расчете рисков потерь используются реально полученные вероятности взлома каждой защиты $P_m(X_j)$ и реальные для них финансовые затраты X_j. С помощью формулы (26) определяется эффективность применения той или иной единичной защиты, причем формула (26) является обобщенным критерием (6) использования той или иной защиты. Если в результате расчетов $\gamma<1$, то такую защиту необходимо исключить из КТЗИ, как неэффективную. При $\gamma>1$ – защита обеспечит не только более высокий уровень защиты, но и экономию финансовых средств. При $\gamma=1$ защита обеспечивается с пропорциональным вложением финансирования.

Получено выражение (28), с помощью которого можно рассчитать величины рисков полных финансовых потерь любой многоуровневой защиты, определить эффективность не только одноуровневых защит, но и всего КТЗИ, а также использовать реальные параметры единичных защит, таких как вероятность их взлома и затрат на их разработку или модернизацию.

При дальнейших экономических расчетах, зная прибыль от защищенной системы и необходимых затрат на защиту, можно обосновать экономическую выгоду при внедрении КТЗИ.

Литература: ***1.*** *Колемаев В. А. Математическая экономика: учебник для вузов [2-е изд., перераб. и доп.]. / Колемаев В. А. - М.: ЮНИТИ-ДАНА, 2002. 399с.* ***2.*** *Шапкин А. С. Экономические и финансовые риски. Оценка, управление, портфель инвестиций / Шапкин А. С. – М.: Издательско-торговая корпорация «Данков и К°», 2003. 544с. (Монография)* ***3.*** *Кравченко В. І. Використання теорії нечітких множин для визначення втрат на захист інформації / Кравченко В. І., Левченко Є. Г. // Науково-технічний журнал «Захист інформації» - 2011. - №1. - С.85-90.* ***4.*** *Домарев В. В. Безопасность информационных технологий. Системный подход / Домарев В. В. - К.:ООО «ТИД «ДС», 2004. - 992 с.* ***5.*** *Сахарцеа І. І. Ризики економічної діагностики підприємства / Сахарцева І. І., Шляга О. В; МОН. - К.: Кондор, 2008. – 380с.* ***6.*** *Андре Анго. Математика для электро- и радиоинженеров / Андре Анго; [С предисловием Луи де Бройля. Перевод с французского под общей редакцией К. С. Шифрина.]. – М.: Из-во «Наука», 1964, 772 с.* ***7.*** *Румшинский Л. З. Элементы теории вероятностей / Румшинский Л. З. - М.: Изд-во «Наука», Главн. Ред. Физ.-мат. Лит., 1970. 256 с.*

УДК 621.396

СПОСІБ ДОСЛІДЖЕННЯ ПАРАМЕТРІВ ГОМОМОРФНОЇ ФУНКЦІЇ МОВНОГО СИГНАЛУ

Максим Кузнецов

Центр Інформаційно-аналітичних досліджень стратегічних програм

Анотація: **Результат, що висвітлено у статті, є новітнім для галузі дослідження мовних сигналів. Ідеться про отримання залежностей від частоти гомоморфної функції сигналу квантилів варіаційних рядків – порядкових статистик гомоморфної функції мовного сигналу.**

Summary: **The result which presented in this article the newest in speech processing field – the variational series fractals depending on speech signal homomorphic function frequency. This effect was named the order statistics of speech signal homomorphic function.**

Ключові слова: **Мовний сигнал, гомоморфна фільтрація, порядкові статистики, статистичні залежності гомоморфної функції мовного сигналу.**