УДК 004.056 DOI 10.23683/2311-3103-2017-9-91-103

Ф.Г. Хисамов, А.С. Жук, Р.С. Шерстобитов

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ОЦЕНКИ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА ПРИ ПРОЕКТИРОВАНИИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

Благодаря современным достижениям компьютерных и информационных технологий автоматизированные системы в защищенном исполнении, построенные на основе современных средств вычислительной техники, стали играть существенную роль в обеспечении обороноспособности страны, производства, научных исследованиях и всестороннего развития государства. Проведенные авторами исследования показали, что при проектировании автоматизированных систем в защищенном исполнении накопился ряд противоречий, обусловленных отсутствием научно-методического аппарата и единой методики оценки защищенности информации в условиях повышении информационно-технического воздействия. Целью проведенного исследования является повышение защищенности информации при проектировании автоматизированных систем в защищенном исполнении в условиях развития цифровой экономики, глобального информационного пространства и роста угроз безопасности информации. Задачей исследования является разработка количественных показателей защищенности информации, которые позволят на этапах проектирования автоматизированных систем в защищенном исполнении оценить и оптимизировать вероятность ущерба от несанкционированного доступа. В результате проведенных исследований авторами получены показатели защищенности вероятностного типа, которые позволяют на этапах проектирования автоматизированных систем в защищенном исполнении рассчитать верхнюю и нижнюю границы вероятности несанкционированного доступа к информации и оптимизировать вероятность ущерба относительно времени эксплуатации автоматизированной системы, количества и шага реализации угроз безопасности информации, применяемых средств защиты информации, заданного грифа секретности информации. В рамках решения поставленной задачи использовались положения теории защиты информации, системного анализа, методы математической логики, теории вероятности и математической статистики.

Автоматизированная система в защищенном исполнении; несанкционированный доступ; угрозы безопасности информации.

F.G. Khisamov, A.S. Zhuck, R.S. Sherstobitov

MATHEMATICAL MODEL OF EVALUATION OF INFORMATION PROTECTION FROM UNAUTHORIZED ACCESS WHEN DESIGNING AUTOMATED SYSTEMS IN THE PROTECTED IMPLEMENTATION

Thanks to modern achievements in computer and information technologies, automated systems, built on the basis of modern computer facilities in secure implementation, began to play an essential role in ensuring the country's defense capability, production, scientific research and comprehensive development of the state. The research conducted by the authors shows that a number of contradictions have arisen during the design of automated system in secure implementation due to the lack of a scientific and methodical apparatus and a unified methodology for assessing the security of information in conditions of increasing information and technical impact. The purpose of the research is to increase the security of information in the design of automated system in secure implementation in the conditions of development of digital economy, global information space and growth of threats to information security. The task of the research is to develop quantitative indicators of information security that will allow us to assess and optimize the probability of damage from unauthorized access. As a result of the conducted researches, the authors obtained the probabilistic type security indicators that allow to calculate the upper and lower bounds of the probability of unauthorized access to the information and optimize the probability

of damage with respect to the time of operation of the automated system, number and step implementation of threats to information security, information protection means used, given information security class. Within the framework of the solution of the task, the provisions of the theory of information protection, system analysis, methods of mathematical logic, probability theory and mathematical statistics have been used.

Automated system in secure execution; unauthorized access; information security threats.

Введение. В условиях активного внедрения новейших информационных технологий, расширения глобальной сети интернет, резко обострились проблемы защиты объектов критической информационной инфраструктуры РФ от кибернетического оружия [15, 18], что позволило сформировать актуальность исследования, которая имеет место в соответствии с основными документами РФ по безопасности - Стратегии национальной безопасности и Доктрины информационной безопасности РФ. В соответствии с которыми «основными угрозами государственной и общественной безопасности являются … нарушение безопасности и устойчивости функционирования критической информационной инфраструктуры Российской Федерации» [12]. В связи с этим, для безопасного функционирования автоматизированных систем в защищенном исполнении (АСЗИ), необходимо, в условиях «…наращивания рядом зарубежных стран возможностей информационно-технического воздействия на информационную инфраструктуру в военных целях», «…совершенствовать систему обеспечения информационной безопасности…» [13]. Президент России Путин В.В. на выступлении в рамках Петербургского международного экономического форума 2 июня 2017 года призвал развивать цифровую экономику для достижения экономического роста и технологического лидерства. "При этом все решения должны приниматься с учетом обеспечения информационной безопасности государства, бизнеса и граждан", – подчеркнул глава государства [4]. На этом фоне по данным Совета Безопасности РФ, в 2016 году было совершено более 50 миллионов кибератак на российские информационные ресурсы, причем 60 % атак велось из-за рубежа [5]. Для внедрения цифровых технологий во все сферы жизни необходимо сформировать соответствующую нормативную базу.

Для обеспечения требуемого уровня защищенности информации при проектировании АСЗИ реализуются организационные, технические и организационно-технические меры защиты информации. Организационные меры предназначены для руководящего состава, органов по защите информации, других пользователей и заключаются в организации, упорядочении, контролю деятельности по защите информации в организации. Технические и организационно-технические меры защиты информации предусматривают применение технических средств, которые объединяются в комплексы средств защиты информации (КСЗИ) и являются составной частью АСЗИ [14, 16]. Степень реализации мер по защите информации оценивается в процессе проектирования АСЗИ и зависит от оптимального комплектования КСЗИ средствами защиты информации (СрЗИ) и эффективностью функционирования КСЗИ в целом [2, 3].

1. Постановка задачи. При проектировании АСЗИ в условиях внедрения цифровой экономики и развития глобального информационного пространства накопился ряд противоречий, обуславливающих отсутствием научно-методического аппарата и единой методики оценки защищенности информации при проектировании АСЗИ [19, 20]. Это обусловлено:

- значительной неопределенностью из-за отсутствия статистических данных о функционировании множества средств защиты информации в условиях роста угроз безопасности информации и информационно-технических атак;

- сложностью учета и формализации многих существенных для количественной оценки защищенности АСЗИ факторов (например, разнообразием информационных технологий, программного обеспечения, технических средств).

Вместе с тем необходимость количественных оценок защищенности в связи с ростом количества УБ, а также сложности объектов анализа становится весьма актуальной [2].

Известно, что на реализацию несанкционированного доступа (НСД) к информации, приводящих к нарушению нормального функционирования АСЗИ, конфиденциальности, целостности и доступности информации, нарушитель всегда будет затрачивать время $T_{нсд}$, необходимое для образования канала реализации угрозы безопасности информации, то есть, указанное время характеризует временной интервал:

$$T_{нсд} = \sum_{i=1}^{4} T_i.$$

где T_1 – выявление уязвимостей программного (аппаратного) обеспечения; T_2 – оценка возможности эксплуатации уязвимости с учетом существующей системы защиты информации предполагаемого объекта воздействия (носителя информации); T_3 – выбора способа реализации НСД; T_4 – осуществление НСД .

Исходя из этого, путем увеличения T_i всегда можно было бы управлять защищенностью информации в АСЗИ. То есть T_i можно было бы принять в качестве критерия для оценки защищенности информации в АСЗИ. Тогда путем задания при проектировании АСЗИ порогового значения $T_{доп\ нсд}$ и обеспечив выполнение условия $T_{нсд} \le T_{допнсд}$, можно было бы реализовать допустимую защиту информации ограниченного доступа в АСЗИ.

Однако, такой подход не будет отражать реальную картину, так как время T_i – это случайная величина, закон распределения которой сложно вычислить, так как он будет меняться в зависимости от возможностей нарушителя. Кроме того, здесь не учитываются основные факторы эксплуатации, такие как: различные угрозы безопасности информации в АСЗИ, время эксплуатации АСЗИ, характеристики используемых СрЗИ, от которых также может зависеть НСД к информации.

Поэтому для повышения объективности контроля своевременности, достоверности, полноты и непрерывности защищенности информации, проектируемых АСЗИ целесообразно разработать математическую модель вероятности НСД к циркулирующей информации с учетом условий эксплуатации и состава КСЗИ. На базе найденной модели сформулировать качественные и количественные критерии повышения защищенности информации при проектировании АСЗИ.

2. Описание подхода. Известно, что классическая постановка задачи разработки КСЗИ для обеспечения максимальной эффективности функционирования АСЗИ в условиях НСД будет иметь вид:

$$\begin{matrix} U_{\Sigma} \to \min \\ C = C_{opt} \end{matrix}, \qquad (1)$$

где U_{Σ} – суммарный наносимый ущерб; C – затраты на проектирование КСЗИ.

или

$$\begin{matrix} E_3 \to \max, & \delta_3 \to \max, \\ C = C_{opt} & C = C_{opt}. \end{matrix} \qquad (2)$$

где E_3 – эффективность функционирования АСЗИ; δ_3 – относительная эффективность функционирования АСЗИ.

Несмотря на кажущуюся простоту классической постановки задачи, на практике воспользоваться приведенными результатами удается редко. Это объясняется сложностью математического описания снижения возможного НСД от затрат на проектирование КСЗИ. Если зависимость защищенности от стоимости средств защиты можно получить, имея технические и стоимостные характеристики доступных на рынке средств защиты, но оценить реальный ущерб от НСД чрезвычайно трудно [14], так как этот ущерб также зависит от множества факторов, влияющих на вероятность ущерба.

Например, ущерб будет зависеть от: количества подразделений, включенных в АСЗИ, характеристик СрЗИ, количества возможных к реализации УБ в АСЗИ, квалификации нарушителя и количества попыток реализации УБ, последствий несанкционированного доступа и т.д.

Вместе с тем проектирование КСЗИ для АСЗИ объектов критической информационной инфраструктуры, связанных, например, с управлением атомными электростанциями, для которых НСД к информационным ресурсам может привести к катастрофическим последствиям, выбор СрЗИ осуществляется с наилучшими показателями и поэтому, влиянием стоимости средств защиты на эффективность можно пренебречь, то есть если $C << U$, то:

$$U_{\Sigma} = \frac{U}{f(C)}. \tag{3}$$

В этом случае (1) и (2) принимают вид:

$$\begin{aligned} &U_{\Sigma} \to \min, \\ &C \le C_{доп}. \end{aligned} \tag{4}$$

Или

$$\begin{aligned} &E_3 \to \max, \qquad \delta_3 \to \max, \\ &C \le C_{доп}, \qquad C \le C_{доп}, \end{aligned} \tag{5}$$

где $C_{доп}$ – допустимые расходы на защиту.

Таким образом, НСД к информации в АСЗИ, будет зависеть от применяемых СрЗИ, от количества угроз безопасности информации, степени защищенности и времени эксплуатации АСЗИ.

В соответствии с ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения» целью защиты информации является предотвращение ущерба обладателю информации в связи с возможным НСД к информации, нарушением нормального функционирования АСЗИ, хищения, модификации или уничтожения информации [6].

Очевидно максимальный ущерб может быть нанесен тогда, когда информация в АСЗИ скомпрометирована полностью. Такая ситуация может возникнуть при следующих условиях: либо при захвате АСЗИ противником, либо при ситуации, когда суммарные информационно-технические атаки противника позволяют ему обеспечить НСД к защищаемой информации, циркулирующих по всем защищенным каналам АСЗИ.

Если реализована одна УБ, то при моделировании будем считать, что это приводит к минимальному ущербу.

Сформулируем задачу и найдем выражение для вероятности НСД к информации, циркулирующей в АСЗИ.

Пусть проектируется АСЗИ, содержащая *k* подразделений, в каждом из которых возможна реализация $N_i, i = 1,2,...,k$ угроз безопасности информации. Всего же АСЗИ содержит *S* возможных к реализации УБ, причем

$S = N_1 + N_2 + ... + N_k = \sum_{i=1}^{k} N_i$, Парирование УБ осуществляется СрЗИ, включенных в КСЗИ. СрЗИ обладают различными функциональными возможностями по обеспечению защиты, в зависимости от характеристик, реализуемым механизмам защиты, техническим требованиям, совместимостью с другими средствами защиты, экономическими и эргономическими характеристиками.

Для различения КСЗИ (СрЗИ) целесообразно ввести весовые коэффициенты M_i, $i = 1, 2, .., k$. Чем выше гриф секретности обрабатываемой информации, жестче требования к защите и выше ТТХ, тем большее значение должно быть присвоено коэффициенту M_i и наоборот.

Предположим, что возможный НСД к информации при реализации хотя бы одной УБ происходит с вероятностью P_x, а вероятность НСД к информации при реализации всех УБ P_y.

Напомним, что рассматриваемая АСЗИ содержит *S* возможных к реализации УБ. Предположим, что все угрозы являются случайными с равновероятным законом распределения. Тогда, вероятность НСД к информации при реализации одной конкретной УБ без относительного места ее реализации и защищенности КСЗИ от НСД определяется как:

$$P_S = \frac{1}{S}. \tag{6}$$

Для того, чтобы учесть уязвимости АСЗИ подразделения, наличие которых является обязательным условием для образования канала реализации УБ [17], необходимо в (6) ввести весовой коэффициент M_i, учитывающий характеристики использованных СрЗИ для данного *i*-го подразделения. Если M_i ввести в знаменатель выражения (6), то полученное выражение будет отражать физику процесса НСД к информации при реализации одной УБ *i*-го подразделения, т.е. получим:

$$P_{iS} = \frac{1}{M_i + S}. \tag{7}$$

Действительно, если $M_i = 0$, что соответствует отсутствию защиты, то (7) превращается в (6). А если M_i будет возрастать, то вероятность НСД к информации будет уменьшаться, что правильно отражает физику явления.

Существуют различные методы определения точной количественной оценки M_i, например, при помощи экспертных оценок, описанных и реализованных в работах Т. Саати, М. Эддоуса, Р. Стэнсфилда, О.И. Ларичева, В.Б. Коробова [7–11]. Общим свойством всех методом является возможность варьировать значения в необходимых для задачи пределах, например, в пределах от 1 до 10 или в пределах больших значений. Такое «взвешивание» СрЗИ при помощи коэффициента M_i позволяет правильно отражать качественную картину процесса НСД к информации и, следовательно, позволит пользоваться (7) для выработки качественных рекомендаций.

Напомним, что АСЗИ произвольного *i*-го подразделения содержит N_i возможных к реализации УБ. Следовательно, для вероятности НСД к информации U_i при реализации хотя бы одной УБ из N_i возможных угроз *i*-го подразделения будет справедливо выражение:

$$U_i = 1 - \left(1 - P_{iS}\right)^{N_i}. \quad (8)$$

Однотипные УБ имеются в k подразделениях, где также могут образовывать каналы реализации угроз. Поэтому для вероятности НСД к информации при реализации хотя бы одной УБ, с учетом всех k подразделений, будет справедливо выражение, определяемое формулой для расчета полной вероятности событий:

$$P_x = \sum_{i=1}^{k} \eta_i U_i = \sum_{i=1}^{k} \frac{N_i}{S}\left[1 - \left(1 - P_{iS}\right)^{N_i}\right], \quad (9)$$

где значение η_i определяется соотношением $\eta_i = \frac{N_i}{S}$

Значение P_x обозначает вероятность НСД к информации хотя бы в одном подразделении при реализации хотя бы одной УБ, то есть вероятность НСД к информации при реализации хотя бы одной из S угроз.

В случае, если в подразделениях одинаковое количество возможных к реализации УБ, т.е.

$$N_1 = N_2 = ... = N_k, \qquad S = N_1 + N_2 + ... + N_k = k \cdot N_i,$$

следовательно

$$\eta_i = \frac{N_i}{S} = \frac{N_i}{k \cdot N_i} = \frac{1}{k},$$

тогда формула (4) принимает следующий вид:

$$P_x = \sum_{i=1}^{k} \eta_i U_i = \frac{1}{k} \sum_{i=1}^{k}\left[1 - \left(1 - P_{iS}\right)^{N_i}\right]. \quad (9.1)$$

Заметим, что формула (9 и 9.1) определяет вероятность НСД к информации при реализации хотя бы одной из возможных УБ для всех подразделений в АСЗИ. Справедливо полагать, что в этом случае общий причиняемый ущерб будет минимально возможным. С другой стороны вероятность НСД к информации при реализации хотя бы одной УБ как характеристика защищенности будет принимать максимальное возможное значение, т.е. верхнюю граничную оценку вероятности НСД к информации в АСЗИ.

Далее введем следующую оценку защищенности информации, определяемую как вероятность НСД к информации при реализации всех возможных к реализации УБ одновременно.

Максимальный ущерб возникает тогда, когда, как было указано выше, при реализации всех возможных к реализации УБ, то есть:

$$P_y = \prod_{i=1}^{k} P_{iS}^{N_i}. \quad (10)$$

Таким образом, приведены две оценки защищенности АСЗИ P_x и P_y дают верхнюю и нижнюю границы вероятности НСД к информации, что соответствует наилучшему и наихудшему случаю причинения ущерба АСЗИ в целом.

Тем не менее, очевидно, что выражения (9) и (10) справедливы только для одной попытки реализации УБ.

Теоретически в течение времени эксплуатации АСЗИ таких попыток может быть бесчисленное множество. Количественно оценить число попыток реализации УБ практически невозможно. Однако можно задать априори шаг указанных попыток во времени. При этом интервал времени, в течение которого может осуществляться одна попытка реализации УБ $\left(T_p\right)$ может задаваться с учетом реальных

условий эксплуатации и социально-политической, военной обстановки. Например, шаг реализации УБ в мирное время можно приравнять одному месяцу, неделе, а во время боевых действий нескольким суткам, 24 часам и т.д. Для заданного значения интервала T_p можно определить количество возможных попыток реализации УБ R за время эксплуатации АСЗИ объекта T:

$$R = \frac{T}{T_p}, \tag{11}$$

где T – время эксплуатации, а T_p – шаг реализации УБ.

Зная количество попыток можно оценить вероятность НСД к защищаемой информации при реализации всех или хотя бы одной УБ за время эксплуатации T:

$$P(t) = 1 - (1 - P_к)^R, \tag{12}$$

где значение $P_к$ – это некоторая оценка, которая характеризует вероятность одной успешной попытки реализации УБ, а $t = T$.

Заметим, что ранее нами были приведены два метода расчета оценки $P_к$: P_x и P_y для наилучшего и наихудшего случая соответственно.

Следовательно, если необходимо рассчитать вероятность того, что за период времени T будет осуществлен НСД к информации при реализации хотя бы одной УБ, в выражение (12) необходимо подставить значение $P_к = P_x$.

С другой стороны необходимо рассчитать вероятность наихудшего для системы случая, то есть НСД при реализации всех возможных УБ АСЗИ одновременно. Тогда в выражение (12) в качестве $P_к$ необходимо подставить значение P_y.

3. Эксперимент. С использованием разработанной математической модели проведем имитационное моделирование для оценки защищенности и степени влияния эксплуатационных показателей для различных АСЗИ.

Следует подчеркнуть, что выражение (12) можно использовать как по всему перечню УБ для конкретной АСЗИ, так и выборочно, для угроз, составляющих определенную направленность. В частности, можно выделить УБ, при реализации которых нарушается конфиденциальность информации, ее целостность или доступность. Для разных АСЗИ ущерб от реализации УБ различной направленности может существенно отличаться. Это связано с разнообразием АСЗИ по выполняемым функциям. Например, угрозы конфиденциальности информации для АСЗИ информационного характера актуальнее чем угрозы, направленные на нарушение доступности информации. С другой стороны для АСЗИ управления критически важного объекта угрозы нарушения доступности и целостности информации играют главную роль, в связи с возможными последствиями из-за нарушения работоспособности системы. Такой полиморфизм выражения (12) является его важным достоинством, так как нет необходимости корректировки методов расчета оценки защищенности информации в зависимости от состава УБ в АСЗИ.

Полученные количественные результаты имитационного моделирования можно представить в табличной или графической форме. При этом следует подчеркнуть, что выражение (12) дает верхнюю границу для вероятности НСД к информации в АСЗИ, то есть для наихудшего случая, что является особенно важным показателем при проектировании АСЗИ.

В табл. 1 и 2 показано, как численно различаются оценки защищенности P_x и P_y для АСЗИ с разными исходными параметрами.

В табл. 3 приведены значения вероятности НСД к информации при реализации как минимум одной УБ и для случая реализации всех УБ одновременно с учетом количества попыток реализации УБ для АСЗИ 2 и АСЗИ 7 из табл. 1 и 2.

Таблица 1

Оценка защищенности информации для АСЗИ

	АСЗИ 1	АСЗИ 2	АСЗИ 3	АСЗИ 4	АСЗИ 5
S	18	20	12	15	30
k	3	3	3	3	3
N_1	5	4	3	5	10
N_2	6	6	4	5	10
N_3	7	10	5	5	10
M_1	9	5	3	3	3
M_2	3	2	4	3	3
M_3	6	9	2	3	3
P_1	0,037037	0,04	0,066667	0,055555	0,030303
P_2	0,047619	0,045455	0,0625	0,055555	0,030303
P_3	0,04166	0,034483	0,071429	0,055555	0,030303
U_1	0,171966	0,150653	0,186963	0,248581	0,264876
U_2	0,253784	0,243551	0,227524	0,248581	0,264876
U_3	0,257637	0,295955	0,309638	0,248581	0,264876
P_x	0,232555	0,251174	0,251598	0,248581	0,264876
P_y	1,77E-25	5,37E-29	8,41E-15	1,48E-19	2,78E-46

Таблица 2

Оценка защищенности информации для АСЗИ

	АСЗИ 6	АСЗИ 7	АСЗИ 8	АСЗИ 9	АСЗИ 10
S	40	40	40	40	40
k	4	4	4	4	4
N_1	10	10	20	10	10
N_2	10	10	5	10	10
N_3	10	10	7	10	10
N_4	10	10	8	10	10
M_1	6	1	1	6	4
M_2	5	1	1	6	3
M_3	4	1	1	6	9

	АСЗИ 6	АСЗИ 7	АСЗИ 8	АСЗИ 9	АСЗИ 10
M_4	2	1	1	6	8
P_1	0,021739	0,02439	0,02439	0,021739	0,022727
P_2	0,022222	0,02439	0,02439	0,021739	0,023256
P_3	0,022727	0,02439	0,02439	0,021739	0,020408
P_4	0,02381	0,02439	0,02439	0,021739	0,020833
U_1	0,197312	0,218802	0,389729	0,197312	0,205383
U_2	0,201267	0,218802	0,116146	0,197312	0,20967
U_3	0,205383	0,218802	0,158735	0,197312	0,186324
U_4	0,214139	0,218802	0,179253	0,197312	0,189849
P_x	0,204525	0,218802	0,273012	0,197312	0,197806
P_y	1,49E-66	3,08E-65	3,08E-65	3,09E-67	3,28E-67

Таблица 3

Оценка защищенности информации в АСЗИ в зависимости от *R*

R	АСЗИ 2		АСЗИ 7	
	P_x	P_y	P_x	P_y
	0,251174	5,37E-29	0,218802	3,08E-65
1	0,251174	5,37E-29	0,218802	3,08E-65
2	0,439259	7,29E-27	0,389729	2,45E-62
3	0,580102	2,64E-25	0,523257	6,37E-60
4	0,685569	1,25E-24	0,627569	4,25E-57
5	0,764546	9,83E-21	0,709058	7,67E-53
6	0,823686	5,37E-20	0,772716	2,92E-51
0,5	0,134652	5,48E-30	0,116146	4,67E-67
0,33333333	0,091914	1,26E-32	0,079012	7,585E-69
0,25	0,069759	8,25E-32	0,059865	4,74E-70
0,2	0,056208	3,29E-34	0,048186	6,36E-73
0,16666667	0,047064	4,37E-36	0,040319	5,29E-75

Заключение. Проанализируем зависимость количественной оценки вероятности НСД к информации при реализации хотя бы одной УБ P_x от параметров эксплуатации АСЗИ.

Так в табл. 1 наибольшее значение P_x = 0,264876 принимает в АСЗИ № 5 при количестве УБ *S*=30. При меньших значениях *S*, величина P_x будет уменьшаться: P_x=0,232555 при количестве *S*=18 в АСЗИ № 1, P_x=0,251174 при количестве *S*=20 в АСЗИ № 2, P_x=0,251598 при количестве *S*=12 в АСЗИ № 3, P_x=0,248581 при количестве *S*=15 в АСЗИ № 4.

Установлено, что наименьшее значение P_x=0,232555 принимает в АСЗИ № 1, где весовые коэффициенты КСЗИ по подразделениям имеют наибольшие значения (9,3,6). В других АСЗИ при меньших весовых коэффициентах КСЗИ

(АСЗИ № 2 – 5,2,9; АСЗИ № 3 – 3,4,2; АСЗИ № 4 – 3,3,3; АСЗИ № 5 – 3,3,3) величина P_x принимает меньшие значения (0,251174; 0,251598; 0,248581; 0,264876 соответственно).

Вызывает интерес тот факт, что в случае, когда весовые коэффициенты КСЗИ равномерны во всех подразделениях одной АСЗИ, вероятность реализации хотя бы одной УБ ниже, чем в другой АСЗИ с подразделениями, имеющими различные весовые коэффициенты КСЗИ. Причем общий весовой коэффициент КСЗИ всех подразделений обоих АСЗИ одинаков. Так в АСЗИ № 9 и АСЗИ № 10 (таблице 2) равное количество S=40, одинаковое количество подразделений K=4 и одинаковое распределение УБ между подразделениями – по 10 УБ в каждом K. Однако, весовые коэффициенты КСЗИ по подразделениям различны: АСЗИ № 9 (6,6,6,6), АСЗИ № 10 (4,3,9,8). Общий весовой коэффициент в обоих АСЗИ равен 24. В тоже время, P_x=0,197312 для АСЗИ № 9 меньше чем, P_x=0,197806 для АСЗИ № 10.

Проанализировав табл. 3, можно сделать вывод, что P_x существенно увеличивается с ростом попыток реализации УБ. Так для АСЗИ № 2 P_x при одной попытке равна 0,251174. При осуществлении нарушителем пяти попыток такая вероятность достигнет значения 0,764546.

Таким образом, разработанные аналитические оценки позволяют на этапах проектирования АСЗИ рассчитать верхнюю и нижнюю границы вероятности НСД к информации, что имеет исключительно важное значение для проектирования АСЗИ. Так как дает возможность при проектировании оптимизировать вероятность возникновения ущерба относительно времени эксплуатации, количества УБ, применяемых средств защиты информации, заданного грифа секретности информации и количества попыток реализации УБ.

Учитывая, предпочтительность в использовании вероятностно-временных показателей защищенности в дальнейших исследованиях предполагается разработка математической модели оценки временных показателей защищенности АСЗИ в зависимости от возможностей нарушителя.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Язов Ю.К.* Проектирование защищенных информационно-телекоммуникационных систем: учеб. пособие. – Воронеж: ФГБОУ ВПО «Воронежский государственный технический университет», 2014. – 636 с.
2. *Герасименко В.А.* Защита информации в автоматизированных системах обработки данных. В 2-х кн. – М.: Энергоиздат, 1994. – 302 с.
3. *Завгородний В.И.* Комплексная защита информации в компьютерных системах. – М.: Логос, ПБОЮЛ Егоров Н.А., 2001. – 264 с.
4. Российская газета. 02.06.2017 г. О чем рассказал Владимир Путин на пленарном заседании ПМЭФ. Электронный документ. – Режим доступа: URL:https://rg.ru/2017/06/02/reg-szfo/o-chem-rasskazal-vladimir-putin-na-plenarnom-zasedanii-pmef.html.
5. Российская газета. 15.02.2017 г. Совбез: Число кибератак на РФ за 2016 год выросло втрое. Электронный документ. – Режим доступа: URL:https://rg.ru/2017/02/15/sovbez-chislo-kiberatak-na-rf-za-2016-god-vyroslo-vtroe.html.
6. ГОСТ Р 50922-2006. Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения. – М.: Стандартинформ, 2008. – 8 с.
7. *Саати Т.* Принятие решений. Метод анализ иерархий: пер. с англ. – М.: Радио и связь, 1993. – 278 с.
8. *Саати Т., Кернс К.* Аналитическое планирование. Организация систем. – М.: Радио и связь, 1991. – 224 с.
9. *Эддоус М., Стэнсфилд Р.* Методы принятия решения: пер. с англ. – М.: Аудит, ЮНИТИ, 1997.

10. *Коробов В.Б.* Сравнительный анализ методов определения весовых коэффициентов «влияющих факторов» // Социология. – 2005. – № 20. – С. 12-20.
11. *Ларичев О.И.* Теория и методы принятия решений, а также Хроника событий в Волшебных странах: учебник. – 2-е изд., перераб. и доп. – М.: Логос, 2002. – 392 с.
12. Стратегия национальной безопасности, утверждена Указом Президента Российской Федерации от 31.12.2015 г. № 683.
13. Доктрина информационной безопасности РФ, утверждена Указом Президента Российской Федерации от 05.12.2016 г. № 646.
14. *Грибунин В.Г., Чудовский В.В.* Комплексная система защиты информации на предприятии: учеб. пособие. – М.: ИЦ Академия, 2009. – 416 с.
15. Проблемы защиты от информационного оружия в условиях глобальной информатизации общественных формаций // Специальная связь и безопасность информации (ССБИ-2012): Сб. трудов международного симпозиума. НЧОУ ВПО «Кубанский институт информзащиты». – Краснодар: Экоинвест, 2012. – С. 296.
16. *Малюк А.А., Пазизин С.В., Погожий Н.С.* Введение в защиту информации в автоматизированных системах. – М.: Горячая линия – Телеком, 2004. – 147 с.
17. *Новиков А.А., Устинов Г.Н.* Уязвимость и информационная безопасность телекоммуникационных технологий: учеб. пособие для вузов. – М.: Радио и связь, 2003. – № 6. – С. 46-48.
18. Positive Research 2016. Сборник исследований по практической безопасности. Электронный документ. – Режим доступа: URL: www.ptsecurity.com/upload/ptru/analytics/Positive-Research-2016-rus.pdf/.
19. *Домарев В.В.* Безопасность информационных технологий. Методология создания систем защиты. – К.: ДиаСофт, 2002. – 688 с.
20. *Щеглов А.Ю.* Защита компьютерной информации от несанкционированного доступа. – М.: Наука и техника, 2004. – 384 с.

REFERENCES

1. *Yazov Yu.K.* Proektirovanie zashchishchennykh informatsionno-telekommunikatsionnykh sistem: ucheb. Posobie [The design of the protected information and telecommunication systems: a tutorial]. Voronezh: FGBOU VPO «Voronezhskiy gosudarstvennyy tekhnicheskiy universitet», 2014, 636 p.
2. *Gerasimenko V.A.* Zashchita informatsii v avtomatizirovannykh sistemakh obrabotki dan-nykh [. V 2-kh kn. – M.: Energoizdat, 1994. – 302 s.
3. *Gerasimenko V.A.* Zashchita informatsii v avtomatizirovannykh sistemakh obrabotki dannykh [Protection of information in automated data processing systems]. In 2 book. Moscow: Energoizdat, 1994, 302 p.
4. *Zavgorodniy V.I.* Kompleksnaya zashchita informatsii v komp'yuternykh sistemakh [Comprehensive protection of information in computer systems]. Moscow: Logos, PBOYuL Egorov N.A., 2001, 264 p.
5. Rossiyskaya gazeta. 02.06.2017 g. O chem rasskazal Vladimir Putin na plenarnom zasedanii PMEF. Elektronnyy document [Russian newspaper. 02.06.2017 what said Vladimir Putin at the plenary session of SPIEF. Electronic document]. Available at: https://rg.ru/2017/06/02/reg-szfo/o-chem-rasskazal-vladimir-putin-na-plenarnom-zasedanii-pmef.html.
6. Rossiyskaya gazeta. 15.02.2017 g. Sovbez: Chislo kiberatak na RF za 2016 god vyroslo vtroe. Elektronnyy dokument [Russian newspaper. 15.02.2017 g. security Council: Number of cyber attacks on Russia for 2016 has tripled. Electronic document]. Available at: https://rg.ru/2017/02/15/sovbez-chislo-kiberatak-na-rf-za-2016-god-vyroslo-vtroe.html.
7. GOST R 50922-2006. Natsional'nyy standart Rossiyskoy Federatsii. Zashchita informatsii. Osnovnye terminy i opredeleniya [National standard of the Russian Federation. Basic terms and definitions]. Moscow: Standartinform, 2008, 8 p.
8. *Saati T.* Prinyatie resheniy. Metod analiz ierarkhiy [Decision-making. Method the analysis of hierarchies]: translation from English. Moscow: Radio i svyaz', 1993, 278 c.
9. *Eddous M., Stensfild R.* Metody prinyatiya resheniya [The methods of decision making]: transl. from english. Moscow: Audit, YuNITI, 1997.

10. *Korobov V.B.* Sravnitel'nyy analiz metodov opredeleniya vesovykh koeffitsientov «vliyayushchikh faktorov» [Comparative analysis of methods for the determination of the weighting factors "influencing factors"], *Sotsiologiya* [Sociology], 2005, No. 20, pp. 12-20.
11. *Larichev O.I.* Teoriya i metody prinyatiya resheniy, a takzhe Khronika sobytiy v Volshebnykh stranakh: uchebnik [Theory and methods of decision-making, and also Chronicle of events in Magic countries: textbook]. 2nd ed. Moscow: Logos, 2002, 392 p.
12. Strategiya natsional'noy bezopasnosti, utverzhdena Ukazom Prezidenta Rossiyskoy Federatsii ot 31.12.2015 g. № 683 [National security strategy, approved by the decree of the President of the Russian Federation dated 31.12.2015, No. 683].
13. Doktrina informatsionnoy bezopasnosti RF, utverzhdena Ukazom Prezidenta Rossiyskoy Federatsii ot 05.12.2016 g. № 646 [The information security doctrine of the Russian Federation, approved by decree of the President of the Russian Federation from 05.12.2016, No. 646].
14. *Gribunin V.G., Chudovskiy V.V.* Kompleksnaya sistema zashchity informatsii na predpriyatii: ucheb. posobie [A complex system of information protection at the enterprise: textbook]. Moscow: ITs Akademiya, 2009, 416 p.
15. Problemy zashchity ot informatsionnogo oruzhiya v usloviyakh global'noy informatizatsii obshchestvennykh formatsiy [Problems of protection from information weapons in conditions of global Informatization of the social formations], *Spetsial'naya svyaz' i bezopasnost' informatsii (SSBI-2012): Cb. trudov mezhdunarodnogo simpoziuma. NChOU VPO «Kubanskiy institut informzashchity»* [Special communications and information security (SSBI-2012): proceedings of the international Symposium. NCHOU VPO "Kuban Institute InfoSec"]. Krasnodar: Ekoinvest, 2012, pp. 296.
16. *Malyuk A.A., Pazizin S.V., Pogozhiy N.S.* Vvedenie v zashchitu informatsii v avtomatizirovannykh sistemakh [Introduction to the protection of information in automated systems]. Moscow: Goryachaya liniya – Telekom, 2004, 147 p.
17. *Novikov A.A., Ustinov G.N.* Uyazvimost' i informatsionnaya bezopasnost' telekommunikatsionnykh tekhnologiy: ucheb. posobie dlya vuzov [Vulnerability and information security of telecommunication technologies: textbook for universities]. Moscow: Radio i svyaz', 2003, No. 6, pp. 46-48.
18. Positive Research 2016. Sbornik issledovaniy po prakticheskoy bezopasnosti. Elektronnyy document [Positive Research 2016. A collection of studies on practical security. Electronic documen]. Available at: www.ptsecurity.com/upload/ptru/analytics/Positive-Research-2016-rus.pdf/.
19. *Domarev V.V.* Bezopasnost' informatsionnykh tekhnologiy. Metodologiya sozdaniya sistem zashchity [Security of information technologies. Methodology of creation of systems of protection]. Kiev: DiaSoft, 2002, 688 p.
20. *Shcheglov A.Yu.* Zashchita komp'yuternoy informatsii ot nesanktsionirovannogo dostupa [Protection of computer information from unauthorized access]. Moscow: Nauka i tekhnika, 2004, 384 p.

Статью рекомендовал к опубликованию д.т.н. Г.А. Аршинов.

Хисамов Франгиз Гильфанетдинович – Краснодарское высшее военное училище; e-mail: kiiz@rambler.ru; Краснодар, Центральный микрорайон, ул. Красина, 4; тел.: 89183998526; д.т.н.; профессор.

Жук Арсений Сергеевич – e-mail: arseniyzhuck@mail.ru; тел.: 89384754442; преподаватель.

Шерстобитов Роман Сергеевич – e-mail: indexxx1922rambler.ru; тел.: 89604934985; адъюнкт.

Khisamov Frangiz Gilfanetdinovich – Krasnodar high military academy; e-mail: kiiz@rambler.ru; 4, Krasina, stret, Central district, Krasnodar, Russia; phone: +79183998526; dr. of eng. sc.; professor.

Zhuck Arseniy Sergeevich – e-mail: arseniyzhuck@mail.ru; phone: +79384754442; lecturer.

Sherstobitov Roman Sergeevich – e-mail: indexxx1922rambler.ru; phone: +79604934985; postgraduate student.