ТЕОРЕТИЧЕСКОЕ ОБОСНОВАНИЕ МЕТОДИКИ ПРОЕКТИРОВАНИЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ В ВИРТУАЛЬНЫХ СРЕДАХ И ОБЛАЧНЫХ ПЛАТФОРМАХ

Нащекин П.А.[1]

Цель статьи: *повышение эффективности систем защиты информации в условиях высокой неопределенности исходных данных.*

Метод: *моделирование систем защиты информации методами теории нечетких множеств, теории возможностей и теоретической информатики.*

Полученный результат: *показано, что существующие модели и методы проектирования систем защиты информации недостаточно полно отражают специфику систем защиты информации как сложных организационно-технических систем. Поведение таких систем отражает динамику слабоструктурированных процессов, характеризующихся высокой степенью неопределенности вследствие нестационарности, неточности и недостаточности наблюдений, нечеткости и нестабильности тенденций. При несомненных достоинствах и широком признании статистического (вероятностного) подхода применение его ограничено в процессах создания систем защиты информации таких систем. Обоснована актуальность научной задачи разработки методики проектирования систем защиты информации в виртуальных средах и облачных платформах в условиях высокой неопределенности. Предлагаемое теоретическое обоснование абстрагировано от конкретных видов облачных сервисов и моделей их размещения. Исследована модель системы защиты, представленная иерархией уровней защиты сопоставленной архитектуре информационной системы, реализующей облачные сервисы: композиции иерархически взаимосвязанных уровней виртуальных устройств обработки, хранения и/или передачи данных, аппаратных и/или программных средств, необходимых для их работы. С использованием основных положений теоретической информатики показано, что параметры оценки эффективности механизмов защиты применимы и как параметры для оценки нейтрализуемых угроз безопасности информации. Теоретическое обоснование методики проектирования систем защиты информации в виртуальных средах и облачных платформах позволило предложить процедуру вычисления семантического порога предпочтения при выборе механизмов защиты, нейтрализующих определенные в «Модели угроз и потенциального нарушителя информационной безопасности» угрозы, разработать и практически применить в процессах проектирования государственных информационных систем метод выбора предпочтительных механизмов защиты, нейтрализующих угрозы безопасности информации на уровнях защиты в общей архитектуре таких систем.*

Ключевые слова: *механизмы защиты, угрозы безопасности информации, уровни защиты, нечеткие множества, нечеткие числа, лингвистическая переменная, возможность, неопределенность, риски, ущерб.*

DOI:10.21681/2311-3456-2020-06-14-22

Введение

Перспективы развития государственных информационных систем (ГИС) связаны с реализацией виртуальных сред и облачных платформ, предоставляющим пользователям возможность доступа к информационным ресурсам из сети Интернет, больший по сравнению с традиционными системами спектр услуг в плане многопользовательской структуры и обеспечивающих удобство и легкость в работе. Важным аспектом является экономичность облачных вычислений и доступность электронных информационных ресурсов для различных слоев населения.

Согласно проекту ГОСТ «Требования по защите информации, обрабатываемой с использованием технологии облачных вычислений» защищаемая ГИС, реализующая облачные технологии, представляет собой многоуровневую систему[2]: уровень оборудования, уровень виртуализации, уровень управления и уровень оркестровки.

Система защиты информации (СЗИ) таких систем должна обеспечивать защиту от актуальных угроз безопасности информации (БИ) как традиционных средств вычислительной техники (СВТ), нейтрализация которых осуществляется также на нескольких уровнях защиты: BIOS (Basicinput-outputsystem – базовая система ввода-вывода), аппаратный, операционная система (ОС), сетевой, система управления базами данных (СУБД), функциональное (прикладное) программное обеспе-

2 Проект ГОСТ Р Защита информации. Требования по защите информации, обрабатываемой с использованием технологий «Облачных вычислений». Основные положения.
URL: http://docs.cntd.ru/document/1200102839

1 Нащекин Павел Александрович, директор НТЦ «Система», Москва, Россия. E-mail:npa@systema.ru

чение, так и актуальных угроз БИ, характерных для конкретной облачной платформы в соответствии с «Моделью угроз и потенциального нарушителя информационной безопасности в ГИС, реализующей облачные технологии» (далее – модель угроз и нарушителя – МУН) [3,4].

Практика применения средств виртуализации и облачных платформ в ГИС показывает, что для защиты информации недостаточно уже имеющихся механизмов защиты (МЗ), реализующих функции защиты, рассчитанных на применение в традиционных СВТ и поэтому в настоящее время активно разрабатываются новые, в частности, криптографические МЗ [1].

Методика проектирования СЗИ в виртуальных средах и облачных платформах предполагает использование уже имеющихся МЗ на перечисленных ранее уровнях и включает в себя метод (процедуру) выбора предпочтительных МЗ, которые наиболее эффективно нейтрализуют актуальные угрозы БИ на уровнях защиты. Методика должна учитывать множественные теоретико-семантические аспекты организации комплексной системы защиты ГИС [2,3]

СЗИ представляет собой сложную организационно-техническую систему, поведение которой отражает динамику слабоструктурированных процессов (систем) [4] и характеризуется высокой степенью неопределенности вследствие нестационарности, неточности и недостаточности наблюдений, нечеткости и нестабильности тенденций. Рассматриваемое качество не имеет статистической природы: невозможно получить выборки статистически однородных событий из их генеральной совокупности, наблюдаемых в неизменных внешних условиях наблюдения. То есть классически понимаемой статистики не существует [5].

Практика работы со случайными величинами убедительно доказывает, что вероятностные методы применимы ограниченно при моделировании сложных недетерминированных процессов, причём к этим процессам можно смело отнести и действия по несанкционированному доступу к облачным сервисам. В работах [6,7] показано, что теория вероятностей является частным случаем теории возможностей. В свою очередь математической основой последней является интервальный анализ и теория нечетких множеств (НМ). В качестве подхода к решению проблемы высокой неопределенности в процессе разработки методики проектирования СЗИ в виртуальных средах и облачных платформах будем использовать методы теории НМ [8,9], теории возможностей [10] и теоретической информатики [11].

Согласно стандарту международного союза электросвязи (ITU-T) Е.408 [ITU-T. Recommendation E.408. Te lecommunicationNetworkSecurityRequirement, 2004] количественная оценка риска угрозы ИБ в сети связи, определяется двумя характеристиками – вероятностью угрозы и последствием от реализации этой угрозы (т.е. ущербом) [12]. Что касается первой характеристики, то здесь целесообразно оценивать не вероятность, а возможность реализации угроз БИ имеющимися МЗ с использованием экспертных оценок. Экспертные оценки касаются, в частности, определения рейтингов потенциала нападения и стойкости МЗ, соотношение которых и определяет возможность реализации угрозы БИ или возможность ее нейтрализации. Считается, что потенциал нападения зависит от уровня мотивации злоумышленника, его квалификации и имеющихся ресурсов. Мотивация влияет на выделяемое на атаки время и, возможно, на привлекаемые ресурсы и подбор нападающих.

Неопределенность обусловлена также оценками параметров эффективности МЗ, таких как стоимость МЗ, средневзвешенное количества угроз, нейтрализуемых МЗ, величина предотвращаемого риска, степень доверия и совместимости средств защиты, возможность применения МЗ в виртуальных средах и облачных платформах.

Таким образом, особую актуальность приобретает научная задача разработки методики проектирования СЗИ в виртуальных средах и облачных платформах в условиях высокой неопределенности. Актуальность задачи подтверждается и критериями социальной, политической, экономической, экологической значимости и значимости объектов социально-экономических отраслей для обеспечения обороны страны, безопасности государства и правопорядка.

Для повышения эффективности СЗИ необходимо обеспечить адекватность применяемых моделей и методов путем перехода от статистической (вероятностной) концепции к концепции создания методического базиса но основе методов теории НМ, теории возможностей и математической информатики, которые как нельзя лучше подходят для описания и решения задач с высокой степенью неопределенности.

1. Постановка задачи

В рамках методики проектирования СЗИ в виртуальных средах и облачных платформах исследуем модель СЗИ с распределением МЗ по нейтрализуемым угрозам БИ на уровнях защиты, предложенную в работе [13] и уточняющую более общую модель защиты с полным перекрытием. При построении данной модели в качестве исходной взята естественная посылка, состоящая в том, что в СЗИ как для традиционных СВТ, так и для виртуальных сред и облачных платформ должен содержаться по крайней мере один МЗ для нейтрализации любой потенциально возможной угрозы БИ.

Представим модель СЗИ в виде кортежа $MOD_{СЗИ} = <\{UR\},\{UG\},\{MZ\},\{PR\},\{TR\}>$.

Здесь

$ur_u \in UR$ – уровни защиты в СЗИ, $u = \overline{1,U}$, U – количество уровней защиты;

$ug_n \in UG$ – множество актуальных угроз БИ для ГИС, $n = \overline{1,N}$, N – количество актуальных угроз;

$MZ = \{mz_k\} = \bigcup_{u=\overline{1,U}} MZ_u = \{mz_{k \in K_u, u}\}$, где MZ_u – подмножество МЗ уровня защиты $ur_u \in UR$, $k \in K_u$ – подмножество индексов $k = \overline{1,K}$ МЗ на этом уровне, $\bigcup_u K_u = K$, $\bigcap_u K_u = \varnothing$;

3 ГОСТ Р 56938-2016. Защита информации при использовании технологий виртуализации. Общие положения. URL: https://files.stroyinf.ru/Data2/1/4293754/4293754619.pdf

4 Всё по ГОСТу. Защита информации при использовании технологий виртуализации URL: https://habr.com/ru/company/cloud4y/blog/352178/

$pr_j \in PR, j = \overline{1, J}$, множество параметров оценки эффективности МЗ;

$tr_{mz_{ku}} \in TR$– множество требований к МЗ: $tr_{mz_{ku}} = \{rsk^{don}_{mz_{ku}}, st^{\max}_{mz_{ku}}\}$, где $rsk^{don}_{mz_{ku}}$– допустимый уровень риска от реализации угрозы, $st^{\max}_{mz_{ku}}$ – максимально допустимые затраты на средства защиты (для класса функционально-однотипных МЗ).

Угрозу ug_n представим в виде вектора $ug_n = \{p^{ug_n}, uch^{ug_n}, rsk^{ug_n} = p^{ug_n} \times uch^{ug_n}\}$ [14], где p^{ug_n} – оценка возможности реализации угрозы ug_n, uch^{ug_n} – ущерб от реализации угрозы ug_n, rsk^{ug_n}– риск от реализации угрозы ug_n.

Требуется сформировать структуру СЗИ путем распределения $mz_{ku} \in MZ$ по множеству актуальных угроз БИ $ug_n \in UG$ на уровнях защиты $ur_u \in UR$:

$$M_{СЗИ} = \cup_n M_n = \{mz_{k_1} \mid \max_{k \in K_1} poss(mz_{k1}, ug_n); ...,$$

$$\max_{k \in K_U} poss(mz_{ku}, ug_n)\}.$$

Здесь $mz_{ku} \mid \max_{k \in K_u} poss(mz_{ku}, ug_n)$ – механизм защиты mz_{ku} с индексом $k \in K_u$ выбранный на уровне защиты $ur_u \in UR$ и обеспечивающий максимальную возможность нейтрализации актуальной угрозы $ug_n \in UG$.

Ограничение рассматриваемой модели СЗИ заключается в точечных оценках возможностей нейтрализации актуальной угрозы БИ определенным МЗ и в точечных оценках в виде значений соответствующих функций принадлежности параметров эффективности МЗ.

Согласно «Общей методологии оценки безопасности информационных технологий»[5] потенциал нападения оценивается в общем и целом по той же схеме, что и степень риска от наличия уязвимостей, но с некоторыми отличиями (например, из нескольких сценариев нападения выбирается наихудший, с наибольшим потенциалом). Считается, что он является функцией уровня мотивации злоумышленника, его квалификации и имеющихся ресурсов. Мотивация влияет на выделяемое на атаки время и, возможно, на привлекаемые ресурсы и подбор нападающих [15].

Тогда возможность $poss(mz_k, ug_i) = \mu_{ug_i}(mz_k)$ нейтрализации угрозы ug_i функцией защиты mz_k можно определить следующим образом:

$$m_{ugi}(mz_k) = \begin{cases} 1, & если\ r_c \geq r_н; \\ \dfrac{r_c}{r_н}, & если\ если\ r_c < r_н \end{cases}$$

. Здесь $r_н$– рейтинг потенциала нападения, r_c- рейтинг стойкости функции защиты. Полагаем, что для любой угрозы существует функция защиты такая, что $r_c \geq r_н$: $\forall ug_i\ \exists mz_k \mid r_c \geq r_н$ – любая угроза нейтрализуется хотя бы одной функцией защиты. Величина $\mu_{ug_i}(mz_k)$ представляет собой точечную оценку. Преодолеть указанное выше ограничение можно путем оценки рейтингов нападения и стойкости МЗ с использованием нечетких чисел (НЧ). Такое решение обосновывается тем обстоятельством, что диапазоны рейтингов, характеризующих стойкость МЗ и потенциал нападения, представимы лингвистическими значениями [15]: диапазоны рейтингов стойкости МЗ – базовая (диапазон 10 – 17), средняя (диапазон 18 – 24), высокая (диапазон > 24) и потенциал нападения – низкий (диапазон < 10),умеренный (диапазон 10 – 17), высокий (диапазон 18 – 24) и нереально высокий (диапазон > 24). Лингвистические значения можно интерпретировать как НЧ, определенное на заданном диапазоне.

Набор операций над НЧ сводится к алгебраическим операциям с обычными числами при задании определенного интервала достоверности (уровня принадлежности), называемых мягкими вычислениями [16,17].

2. Представление качественных выражений и оценок S- нечеткими множествами

Важным для практических приложений в плане представления качественных выражений и оценок человека в процессе решения задач является случай S нечетких множеств [18], задаваемых парой (X, μ), где $(\mu : X \to S)$ отображение из X в линейно упорядоченное множество S.

В том случае, когда набор НМ $\tilde{A}_i, i = \overline{1, I}$, в X соответствует I свойствам рассматриваемого объекта, каждый элемент $x \in X$ характеризуется вектором значений принадлежности $((\mu_1(x), ..., \mu_I(x))$ выражающим степень удовлетворения этим свойством. Таким образом, строится функция $\mu : X \to [0,1]^i$, где $[0,1]^i$ - полная решетка [11,18]. Векторозначное НМ представляется отображением: $\mu : X \to S_1 \times ... \times S_I$, где S_i– ограниченные линейно упорядоченные множества. Примеры конечного линейно упорядоченного множества – набор лингвистических значений лингвистической переменной «Рейтинг нападения» = {низкий, умеренный, высокий, нереально высокий}, «Рейтинг стойкости МЗ» = {базовый, средний, высокий}.[6]

3. Операции над нечеткими числами

Для практических вычислений удобно работать с НЧ специального вида: треугольными и трапециевидными. Трапециевидное число имеет функцию принадлежности, задаваемую формулой

$$\mu_{\tilde{A}}(x) = \begin{cases} 0, & x < a_1 \text{ или } x > a_1, \\ \dfrac{x - a_1}{a_2 - a_1}, & a_1 \leq x < a_2, \\ 1, & a_2 \leq x \leq a_3, \\ \dfrac{a_1 - x}{a_4 - a_3}, & a_3 < x \leq a_4, \end{cases} \quad (1)$$

где $a_1 \leq a_2 \leq a_3 \leq a_4$.

5 Опубликована в августе 1999г (Common Methodology for Information Technology Security Evaluation) с целью унификации процедуры сертификации по «Общим критериям» (Международный стандарт ISO/IEC 15408:1999 Common Criteria for IT Security Evaluation, Национальный стандарт ГОСТ Р ИСО/МЭК 15408:2002 Критерии оценки безопасности информационных технологий (КОБИТ) и Руководящий документ Гостехкомиссии Росии «Безопасность информационных технологий. Критериоценкибезопасностиинформационныхтехнологий»)

6 Лингвистическая переменная – это переменная, значениями которой могут быть не только числовые значения, но и слова и словосочетания естественного или искусственного языка. Смысл каждого лингвистического значения выражается в виде нечеткого подмножества универсального множества X

Оно обычно обозначается как $\tilde{A} = (a_1, a_2, a_3, a_4)$. В случае $a_2 = a_3$, получается треугольное число $\tilde{A} = (a_1, a_2, a_4)$.

Имея в виду принцип расширения НМ и применяя его к арифметическим операциям и трапециевидным НЧ получают следующие правила сложения и вычитания [16]:

$$(a_1, a_2, a_3, a_4) + (b_1, b_2, b_3, b_4) = (a_1 + b_1, a_2 + b_2, a_3 + b_3, a_4 + b_4), \quad (2)$$
$$(a_1, a_2, a_3, a_4) - (b_1, b_2, b_3, b_4) = (a_1 - b_4, a_2 - b_3, a_3 + b_2, a_4 + b_1). \quad (3)$$

Произведение и частное от деления трапециевидных чисел уже не будут трапециевидными, но будут криволинейно трапециевидными. В данном случае можно написать приближённые равенства:

$$(a_1, a_2, a_3, a_4) \cdot (b_1, b_2, b_3, b_4) \approx (a_1 \cdot b_1, a_2 \cdot b_2, a_3 \cdot b_3, a_4 \cdot b_4), \quad (4)$$
$$(a_1, a_2, a_3, a_4) / (b_1, b_2, b_3, b_4) \approx (a_1 / b_4, a_2 / b_3, a_3 / b_2, a_4 / b_1). \quad (5)$$

Предполагается, что НЧ положительны, т.е. $a_1 > 0$ и $b_1 > 0$. Точность вычислений по формулам (2-5) зависит от учитываемого количества α-срезов.

Снижение объема вычислений при операциях над НЧ достигается применением чисел (L-R)-типа. Функции принадлежности НЧ (L-R)-типа задаются с помощью невозрастающих на множестве неотрицательных действительных чисел функций действительного переменного $L(x)$ и $R(x)$ [16].

С нечётким трапециевидным числом $\tilde{A} = (a_1, a_2, a_3, a_4)$ связывают две числовые характеристики: среднее значение и дисперсию, – вычисляемые по формулам [16]:

$$E(\tilde{A}) = \frac{a_1 + 2a_2 + 2a_3 + a_4}{6},$$
$$Var(\tilde{A}) = \frac{(a_4 - a_1)^2 + 2(a_4 - a_1)(a_3 - a_2) + 3(a_3 - a_2)^2}{24}.$$

4. Семантика информационных описаний МЗ и угроз БИ

Согласно основным положениям теоретической информатики [11] под информационным описанием $\Delta(mz)$ любого МЗ будем понимать структурированную совокупность сведений вида $(p)A(mz)$: $\Delta(mz) = \{(p_i)A_i\}(mz), i = \overline{1, N}$.

Здесь сведения $\{(p_i)A_i\}(mz)$ интерпретируются как «механизм защиты mz из MZ характеризуется возможностью (семантической достоверностью) p_i нейтрализациии угрозы БИ $ug_n \in A_i$», A_i– подмножество угроз БИ ug_n из UG, которыемогут быть нейтрализованы МЗ mz , $A_i \subset UG$. Другими словами, возможность нейтрализации механизмом защиты mz_k угрозы БИ ug_n можно записать в виде $poss(mz_k, ug_n) = \mu_{ug_i}(mz_k) = \tilde{p}_{kn}$, $\tilde{p}_{kn}$ представляет собой НЧ, значение которого $\mu_{ug_i}(mz_k)$ показывает правдоподобность того, что действительное значение величины ug_i равно $\mu_{ug_i}(mz_k)$.

Формальное определение информационного описания $\Delta(mz)$ механизмов защиты позволяет сделать вывод о том, что параметры оценки эффективности МЗ применимы и к оценке нейтрализуемых угроз БИ.Следовательно, применительно к нейтрализуемым угрозам БИ можно оценить стоимость нейтрализации угрозы БИ, средневзвешенное количество МЗ, нейтрализующих угрозу, величину предотвращаемого риска, степень доверия и совместимость средств защиты при нейтрализации угрозы, степень применимости МЗ при нейтрализации конкретной угрозы в виртуальных средах и облачных платформах.

5. Параметры эффективности механизмов защиты

На множествах актуальных угроз $ug_n \in UG$ и МЗ $mz_k \in MZ$ определено нечеткое отношение $M\tilde{U}$. В нашем случае $poss(mz_k, ug_n) = \tilde{p}_{kn}$ – оценка возможности нейтрализации функцией защиты mz_k актуальной угрозы ug_n. В предельном (классическом) случае $\mu_{MU}(ug_n, mz_k) = \chi_{MU}(ug_n, mz_k) = 1$, если угроза ug_n однозначно нейтрализуется средством защиты mz_k и $\mu_{MU}(ug_n, mz_k) = \chi_{MU}(ug_n, mz_k) = 0$ – если угроза не нейтрализуется.

Оценку эффективности МЗ будем вычислять с использованием параметров, представленным ниже. Полагаем, что количественные оценки значений параметров представимы НЧ, определенными на соответствующих шкалах (универсальных множествах). Значения параметров зафиксированы на момент времени оценки МЗ.

1. Параметр pr_1.

Стоимость механизмов защиты. Количественную оценку параметра можно определить в виде НЧ $mz_{ku}(p\tilde{r}_1)$ на универсальной шкале стоимостей.

Стоимость нейтрализации актуальной угрозы. Обозначим через $mz_{ku}(p\tilde{r}_1)$ значение параметра $p\tilde{r}_1$ для средства защиты mz_{ku}. Тогда значение $ug_n(p\tilde{r}_1)$ параметра $p\tilde{r}_1$ для угрозы ug_n можно определить следующим образом:

$$ug_n(p\tilde{r}_1) = \max_u \{\min_{k \in K_u} \{mz_{ku}(p\tilde{r}_1) \mid \tilde{p}_{kn,u} > 0\}\}.$$

Здесь $\min_{k \in K_u} \{mz_{ku}(p\tilde{r}_1) \mid \tilde{p}_{kn,u} > 0\}$ – минимальное значение параметра $p\tilde{r}_1$ для mz_{ku}, нейтрализующих угрозу ug_n на уровне $ur_u \in UR$, $ug_n(p\tilde{r}_1)$ – максимальная стоимость нейтрализации актуальной угрозы имеющимися функциями защиты. На каждом уровне защиты выбираются МЗ с минимальной стоимостью, а для нейтрализации угрозы по всем уровням системы защиты рассматривается наихудший вариант – применяется функция защиты с максимальной стоимостью.

2. Параметр $p\tilde{r}_2$.

Оценка средневзвешенного количества угроз, нейтрализуемых функцией защиты mz_{ku}:

$$p\tilde{r}_2 = \left(\frac{|UG_k| - sm^{mz_{ku}}}{\max_{ku}(|UG_k| - sm^{mz_{ku}})} \right),$$

где $UG_k = \{ug_n \mid \tilde{p}_{kn,u} > 0\}$ – множество угроз, нейтрализуемых функцией защиты mz_{ku}, $sm^{mz_{ku}} = \sum_{n=1}^{N} \tilde{p}_{kn,u}$ – сумма оценок возможностей нейтрализации угроз средством защиты mz_{ku}, $\max_{ku}(|UG_k| - sm^{mz_{ku}})$– максимальная разница между количеством угроз и суммой оценок возможностей нейтрализации угроз средствами защиты mz_{ku} на u-ом уровне.

Оценка средневзвешенного количества МЗ, нейтрализующих актуальную угрозу ug_n:

$$ug_n(p\tilde{r}_2) = \min_u\{\max_{k\in K_u}\{mz_{ku}(p\tilde{r}_2) \mid \tilde{p}_{kn,u} > 0\}\}.$$

По уровням защиты выбираются МЗ с максимальной оценкой средневзвешенного количества нейтрализуемых угроз. Для оценки нейтрализации угрозы на всех уровнях защиты рассматривается вариант применения функций защиты с минимальной средневзвешенной оценкой количества нейтрализуемых угроз.

3. Параметр $p\tilde{r}_3$.

Величина предотвращаемого функцией защиты mz_{ku} *риска от реализации актуальных угроз.*

Риск от реализации угрозы ранее был определен как $rsk^{ug_n} = p^{ug_n} \times uch^{ug_n}$. Тогда $rsk^{\max}_{mz_{ku}} = \max^N_{n=1} rsk^{ugn} \times (1 - \tilde{p}_{kn,u}))$ - максимальный риск от реализации угроз, которые не были нейтрализованы функцией защиты mz_{ku} на уровне защиты u и значение параметра $p\tilde{r}_3$ для mz_{ku} можно определить следующим образом:

$$p\tilde{r}_3 = \left(\frac{rsk^{\max}_{mz_{ku}}}{rsk^{\partial on}_{mz_{ku}}}\right).$$

Предполагаем, что актуальная угроза нейтрализуется хотя бы одним механизмом защиты.

Величину предотвращаемого риска от реализации угрозы оценим следующим образом

$$ug_n(p\tilde{r}_3) = \min_u\{\max_{k\in K_u}\{mz_{ku}(p\tilde{r}_3) \mid \tilde{p}_{kn,u} > 0\}\}.$$

По уровням защиты выбирается функция защиты, которая может допустить максимальный ущерб от реализации угрозы. В целом по уровням защиты принимается вариант причинения минимального ущерба от реализации угрозы.

4. Параметр $p\tilde{r}_4$

Степень доверия к МЗ

Степень доверия $p\tilde{r}_4 = sd_{mz_k}$ к функции защиты можно определить по методике, представленной в работе [19]. Согласно [19] количественная оценка степени доверия функциизащиты вычисляется с использованием пяти критериев: kr^{sd}_1 – оценка компании-разработчика (наивысшие оценки для российских компаний), kr^{sd}_2 – объем предоставляемых исходных кодов, kr^{sd}_3 – оценка исследований средства защиты по требованиям БИ; kr^{sd}_4 – оценка технологии производства средства защиты; 5) kr^{sd}_5 оценка технической поддержки средства защиты. Критерии kr^{sd}_2 и kr^{sd}_3 позволяют оценить выполнение требований БИ разработчиком, а критерии kr^{sd}_4 и kr^{sd}_5характеризуют степень технологической независимости изготавливаемых МЗ.

Степень доверия к МЗ по отношению к нейтрализуемым угрозам вычисляется как

$$ug_n(p\tilde{r}_4) = \min_u\{\max_{k\in K_u}\{mz_{ku}(p\tilde{r}_4) \mid \tilde{p}_{kn,u} > 0\}\}$$

На уровнях защиты оценка осуществляется по МЗ с максимальной оценкой степени доверия. СЗИ в целом оценивается по МЗ с наименьшими степенями доверия.

5. Параметр $p\tilde{r}_5$.

Степень совместимости механизмов защиты.

На множестве $mz_{ku} \in MZ$ определим отношение SV следующим образом: $\mu_{SV}(mz_{:}, mz_j) = \tilde{p}_{kj}$ – степень совместимости mz_k с mz_j, $\tilde{p}_{kj}$- нечеткое число. Обратное может быть неверным: mz_j может быть несовместим с mz_k. В предельном (классическом) случае $\mu_{SV}(mz_k, mz_j) = \chi_{SV}(mz_k, mz_j) = 1$, если mz_k полностью совместим с mz_j и $\mu_{SV}(mz_k, mz_j) = \chi_{SV}(mz_k, mz_j) = 0$ – если несовместимы.

Степень совместимости mz_k с другими средствами защиты по параметру $p\tilde{r}_5$ определим следующим образом:

$$p\tilde{r}_5 = \left(\frac{(|SV_k| - sm^{SV}_{mz_k})}{|SV_k|}\right),$$

где $SV_k = \{mz_j \mid \tilde{p}_{kj} > 0\}$– множество функций защиты, совместимых с mz_k, $sm^{SV}_{mz_k} = \sum_{j=1}^{K} \tilde{p}_{kj}$ – сумма степеней совместимости mz_j с mz_k.

Оценка степени совместимости механизмов защиты по отношению к нейтрализуемым угрозам:

$$ug_n(p\tilde{r}_5) = \min_u\{\max_{k\in K_u}\{mz_{ku}(p\tilde{r}_5) \mid \tilde{p}_{kj,u} > 0\}\}$$

На уровнях защиты применяются МЗ с максимальной оценкой степени совместимости. Структура СЗИ при нейтрализации угрозы характеризуется наименее совместимыми МЗ.$\tilde{p}_{kj}$

6. Параметр $p\tilde{r}_6$.*Применимость в облачных платформах.* Количественную оценку параметра можно определить в виде НЧ $mz_{ku}(p\tilde{r}_6)$ на универсальной (бальной) шкале.

Применимость по отношению к угрозам ИБ. Обозначим через $mz_{ku}(p\tilde{r}_6)$ значение параметра $p\tilde{r}_6$ для механизма защиты mz_{ku}. Тогда значение $ug_n(p\tilde{r}_6)$ параметра $p\tilde{r}_6$ для угрозы ug_n определим следующим образом:

$A_i \subset UG$.

Здесь $\min_{k\in K_u}\{mz_{ku}(p\tilde{r}_6) \mid \tilde{p}_{kn,u} > 0\}$ – минимальное значение параметра $p\tilde{r}_6$ для mz_{ku}, нейтрализующих угрозу ug_n на уровне $ur_u \in UR$, $ug_n(p\tilde{r}_6)$ – максимальная возможность применения функций защиты для нейтрализации актуальной угрозы БИ. На каждом уровне защиты выбираются МЗ с минимальной возможностью применения, а по всем уровням системы защиты – функциязащиты с максимальной возможностью применения.

6. Метод выбора предпочтительных механизмов защиты в структуре СЗИ

Формирование структуры СЗИ путем выбора предпочтительных МЗ $mz_{ku} \in MZ$ осуществляется на уровнях защиты $ur_u \in UR$ путем их распределения по множеству нейтрализуемых угроз БИ $ug_n \in UG$, обеспечивающего максимальную возможность нейтрализации этих угроз. Для реализации такого распределения необходимо определить решающее правило выбора предпочтительных МЗ, которое связано с формированием семантического порога предпочтения при распределении МЗ по нейтрализуемым угрозам БИ [20].

Ранее мы определили, что возможность нейтрализации механизмом защиты mz_k угрозы БИ ug_n представи-

ма НЧ $\tilde{p}_{kn}$. Это определение можно представить в виде отношения $M\tilde{U}$:

$$M\tilde{U} = \begin{matrix} & \begin{bmatrix} ug_1 & ug_2 & \dots & ug_N \end{bmatrix} \\ \begin{bmatrix} mz_1 \\ mz_2 \\ . \\ . \\ . \\ mz_K \end{bmatrix} & \begin{bmatrix} \tilde{p}_{11} & \tilde{p}_{12} & \dots & \tilde{p}_{1N} \\ \tilde{p}_{21} & \tilde{p}_{22} & \dots & \tilde{p}_{2N} \\ . & . & & . \\ . & . & & . \\ . & . & & . \\ \tilde{p}_{k1} & \tilde{p}_{k2} & \dots & \tilde{p}_{kN} \end{bmatrix} \end{matrix}$$

В нечетких множествах $\tilde{A}_1, \tilde{A}_2, \dots, \tilde{A}_N$ представлены возможности $\tilde{p}_{kn}$ нейтрализации угроз $\tilde{A}_1, \tilde{A}_2, \dots, \tilde{A}_N$, $n = \overline{1, N}$, функциями защиты mz_k: $\mu_{\tilde{A}_1}(\tilde{p}_{k1}), \mu_{\tilde{A}_2}(\tilde{p}_{k2}), \dots, \mu_{\tilde{A}_N}(\tilde{p}_{kN})$.

Вычислим значение $p\tilde{g}'$следующим образом:

$$p\tilde{g}' = \min(\max(\tilde{A}_1(\tilde{p}_{k1}) \min_k \tilde{A}_2(\tilde{p}_{k2})), (\tilde{A}_1(\tilde{p}_{k1}) \min_k \tilde{A}_3(\tilde{p}_{k3})), \dots,$$

$$(\tilde{A}_1(\tilde{p}_{k1}) \min_k \tilde{A}_N(\tilde{p}_{kN})), (\tilde{A}_2(\tilde{p}_{k2}) \min_k \tilde{A}_3(\tilde{p}_{k3})), \dots, (\tilde{A}_{N-1} \min_k \tilde{A}_N)))$$

В этом случае порог предпочтения $p\tilde{g}$ при выборе МЗ для нейтрализации угроз БИ заключатся в поиске в отношении $M\tilde{U}$ такого наибольшего значения, которое меньше $p\tilde{g}'$:

$p\tilde{g} = \min\{p_{kn}\} \mid p_{kn} > p\tilde{g}'\}$.

На множествах MZ и параметров эффективности PR определим отношение $M\tilde{R}$ - $\mu_{M\tilde{R}} : MZ \times PR \to [m\tilde{r}_{rj}]$. Здесь $m\tilde{r}_{kj}$- НЧ, отражающее оценку возможного значения параметра эффективности $pr_j \in PR$ для $mz_k \in MZ$.

Отношение $M\tilde{R}$ представим в матричной форме:

$$M\tilde{R} = \begin{matrix} & \begin{bmatrix} pr_1 & pr_2 & \dots & pr_J \end{bmatrix} \\ \begin{bmatrix} mz_1 \\ mz_2 \\ . \\ . \\ . \\ mz_K \end{bmatrix} & \begin{bmatrix} m\tilde{r}_{11} & m\tilde{r}_{12} & \dots & m\tilde{r}_{1J} \\ m\tilde{r}_{21} & m\tilde{r}_{22} & \dots & m\tilde{r}_{2J} \\ . & . & . & . \\ . & . & . & . \\ . & . & . & . \\ m\tilde{r}_{K1} & m\tilde{r}_{K2} & \dots & m\tilde{r}_{KJ} \end{bmatrix} \end{matrix}$$

На множествах параметров PR и актуальных угроз UG сформируем отношения $K\tilde{G}$– $\mu_{K\tilde{G}} : PR \times UG \to [k\tilde{g}_{jn}]$. Для всех $pr_j \in PR$и всех $ug_n \in UG$ $k\tilde{g}_{jn}$– оценка угрозы ug_n по параметру pr_j, определяемая необходимостью нейтрализации угрозы ug_n механизмами защиты mz_k. Оценки $k\tilde{g}_{jn}$ в виде НЧ вычисляются в порядке, представленном в разделе 5.

В матричной форме отношение принимает вид

$$K\tilde{G} = \begin{matrix} & \begin{bmatrix} ug_1 & ug_2 & \dots & ug_N \end{bmatrix} \\ \begin{bmatrix} pr_1 \\ pr_2 \\ . \\ . \\ . \\ pr_J \end{bmatrix} & \begin{bmatrix} k\tilde{g}_{11} & k\tilde{g}_{12} & \dots & k\tilde{g}_{1N} \\ k\tilde{g}_{21} & k\tilde{g}_{22} & \dots & k\tilde{g}_{2N} \\ . & . & . & . \\ . & . & . & . \\ . & . & . & . \\ k\tilde{g}_{j1} & k\tilde{g}_{j2} & \dots & k\tilde{g}_{jN} \end{bmatrix} \end{matrix}$$

Тогда на базе отношений $M\tilde{R}$ и $K\tilde{G}$ можно сформировать отношение $M\tilde{G}$, представленное ниже:

$$M\tilde{G} = \begin{matrix} & \begin{bmatrix} ug_1 & ug_2 & \dots & ug_N \end{bmatrix} \\ \begin{bmatrix} mz_1 \\ mz_2 \\ . \\ . \\ . \\ mz_K \end{bmatrix} & \begin{bmatrix} \mu_{\tilde{A}_1}(m\tilde{g}_{11}) & \mu_{\tilde{A}_2}(m\tilde{g}_{12}) \dots & \mu_{\tilde{A}_N}(m\tilde{g}_{1N}) \\ \mu_{\tilde{A}_1}(m\tilde{g}_{21}) & \mu_{\tilde{A}_2}(m\tilde{g}_{22}) \dots & \mu_{\tilde{A}_N}(m\tilde{g}_{2N}) \\ . & . & . \\ . & . & . \\ . & . & . \\ \mu_{\tilde{A}_1}(m\tilde{g}_{K1}) & \mu_{\tilde{A}_2}(m\tilde{g}_{K2}) \dots & \mu_{\tilde{A}_N}(m\tilde{g}_{KN}) \end{bmatrix} \end{matrix}$$

Элементы в матрице определим следующим образом:

$$\mu_{\tilde{A}_n}(m\tilde{g}_{kn}) = \frac{\sum_j m\tilde{r}_{kj} \times k\tilde{g}_{jn}}{\sum_j m\tilde{r}_{kj}},$$ для всех $mz_k \in MZ$, $pr_j \in KR$, $ug_n \in UG$.

Сумма $\sum_j m\tilde{r}_{kj}$интерпретируется как количество значимых параметров pr, характеризующих mz_k, а $\mu_{\tilde{A}_n}(m\tilde{g}_{kn})$ представляет собой *взвешенную оценку возможности нейтрализации актуальной угрозы* ug_n механизмом защиты mz_k (степень предпочтения при выборе механизма защиты mz_k для нейтрализации актуальной угрозы ug_n).

Отметим, что и ранее определенные значения $\mu_{\tilde{A}_1}(\tilde{p}_{k1}), \mu_{\tilde{A}_2}(\tilde{p}_{k2}), \dots, \mu_{\tilde{A}_N}(\tilde{p}_{kN})$ $\mu_{\tilde{A}_i}(mz_k)$(отношение $M\tilde{U}$)и вычисленные значения $\mu_{\tilde{A}_1}(m\tilde{g}_{K1})$, $\mu_{\tilde{A}_2}(m\tilde{g}_{K2}), \dots,$ $\mu_{\tilde{A}_N}(m\tilde{g}_{KN})$ отражают оценки возможностей нейтрализации угрозы ug_i функцией защиты mz_k. Но при определении значения $\mu_{\tilde{A}_i}(\tilde{p}_{ki})$ не делаются предположения относительно корректности *реализации МЗ или, проще говоря, не учитываются их параметры эффективности: степень доверия*, параметры стоимости, средневзвешенное количество нейтрализуемых угроз и т.д. Значения критериев эффективности функций защиты учтены в вычисленных значениях $\mu_{\tilde{A}_n}(m\tilde{g}_{kn})$.

Согласно принятому подходу формируется матрица $\tilde{W}$:

$$\tilde{W} = \begin{bmatrix} \mu_{\tilde{A}_1}(m\tilde{g}_{11}) \min \mu_{\tilde{A}_2}(m\tilde{g}_{12}), \dots, \mu_{\tilde{A}_{N-1}}(m\tilde{g}_{1N-1}) \min \mu_{\tilde{A}_N}(m\tilde{g}_{1N}) \\ \mu_{\tilde{A}_1}(m\tilde{g}_{21}) \min \mu_{\tilde{A}_2}(m\tilde{g}_{22}), \dots, \mu_{\tilde{A}_{N-1}}(m\tilde{g}_{2N-1}) \min \mu_{\tilde{A}_N}(m\tilde{g}_{2N}) \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ \mu_{\tilde{A}_1}(m\tilde{g}_{k1}) \min \mu_{\tilde{A}_2}(m\tilde{g}_{k2}), \dots, \mu_{\tilde{A}_{N-1}}(m\tilde{g}_{kN-1}) \cap \mu_{\tilde{A}_N}(m\tilde{g}_{N}) \end{bmatrix}$$

Семантический порог предпочтения МЗ относительно нейтрализуемых угроз определим из условия:

$$p\tilde{g} = \min\{\mu_{\tilde{A}_n}(m\tilde{g}_{kn})\} \mid \mu_{\tilde{A}_n}(m\tilde{g}_{kn}) >$$

$$\max(\mu_{\tilde{A}_1}(m\tilde{g}_{k1}) \min_k \mu_{\tilde{A}_2}(m\tilde{g}_{k2})), \dots, (\mu_{\tilde{A}_{N-1}}(m\tilde{g}_{kN-1}) \min_k \mu_{\tilde{A}_N}(m\tilde{g}_{kN}))\}$$

Семантический порог предпочтения применим для выбора МЗ, наиболее эффективно нейтрализующих угрозы $ug_n \in UG$ по уровням защиты и в структуре СЗИ в целом.

$M_n = \{mz_{ku} \mid \mu_{\tilde{A}_n}(mz_{ku}, ug_n) \geq p\tilde{g}\}$ - множество механизмов защиты mz_{ku}, которые нейтрализуют угрозу ug_n на уровне защиты $ur_u \in UR$ с возможностью, превышающей вычисленный семантический порог предпочтения.

Теоретическое обоснование методики проектирования СЗИ в виртуальных средах м облачных платформах позволило разработать и практически применить в процессах проектирования ГИС метода выбора предпочтительных МЗ, нейтрализующих угрозы БИ в соответствии с МУН с оценкой возможности, превышающей вычисленный семантический порог предпочтения.

Заключение

1. Существующие методики, модели и методы проектирования систем защиты информации как традиционных средств вычислительной техники, так и виртуальных сред и облачных платформ недостаточно полно отражают специфику систем защиты информации как сложных организационно-технических систем. Поведение таких систем отражает динамику слабоструктурированных процессов, характеризующихся высокой степенью неопределенности вследствие нестационарности, неточности и недостаточности наблюдений, нечеткости и нестабильности тенденций. Обоснована актуальность научной задачи разработки методики проектирования систем защиты информации в виртуальных средах и облачных платформах в условиях высокой неопределенности.

2. Возможность нейтрализации угроз безопасности информации известными механизмами защиты определяется по соотношению рейтингов стойкости механизмов защиты и потенциала нападения. Эти рейтинги представлены в нормативных документах значениями лингвистических переменных, определенными экспертами на бальных шкалах в виде диапазонов (интервалов). Значения лингвистических переменных предложено интерпретировать (формализовать) как нечеткие числа, представляющих собой частный случай нечетких множеств, определенных на конечных шкалах действительных чисел.

3. Исследована формальная модель многоуровневой системы защиты информации, в которой качественные выражения и оценки представлены S- нечеткими множествами, где значения функций являются нечеткими числами. В предложенной модели для механизмов защиты определены параметры эффективности, такие как стоимость механизмов защиты, средневзвешенное количество угроз, нейтрализуемых механизмом защиты, величина предотвращаемого механизмом защиты риска от реализации актуальных угроз, степень доверия к механизмам защиты, возможность совместимости механизмов защиты и применимость в облачных платформах. Количественные оценки значений параметров представимы нечеткими НЧ, определенными на соответствующих шкалах (универсальных множествах).

4. Исследовано формальное представление семантики информационных описаний механизмов защиты и угроз безопасности информации, по результатам которого сделан вывод о том, что параметры оценки эффективности механизмов защиты распространяются и на нейтрализуемые ими угрозы безопасности информации. Применительно к нейтрализуемым угрозам предложены оценки стоимости нейтрализации угроз, средневзвешенное количество механизмов защиты, нейтрализующих угрозу, величина предотвращаемого риска, степени доверия и возможности совместимости механизмов защиты при нейтрализации угрозы и возможности применимости механизмов защиты при нейтрализации конкретной угрозы в виртуальных средах и облачных платформах.

5. Предложен метод выбора предпочтительных механизмов защиты для проектируемой структуры системы защиты информации.Выбор связан с вычислением семантического порога предпочтения путем обработки нечетких отношений, значения в которых представлены нечеткими числами и которые через параметры эффективности связывают множества МЗ и актуальных угроз БИ.

6. Определен семантический порог предпочтения, применяемый в процедуре выбора механизмов защиты, характеризующихся наибольшей возможностью нейтрализации угроз на уровнях защиты.

7. Теоретическое обоснование методики проектирования систем защиты информации в виртуальных средах и облачных платформах абстрагировано от видов предоставляемых государственными информационными системами облачных сервисов и от моделей размещения и позволило разработать и практически применить в процессах проектирования систем защиты информации метод выбора предпочтительных механизмов защиты, наиболее эффективно нейтрализующих угрозы безопасности информации в соответствии с моделью угроз и нарушителя. Выбор основан на сравнении оценок возможностей нейтрализации имеющимися механизмами защиты угроз безопасности информации с вычисленным семантическим порогом предпочтения.

Литература:

1. Минаков С.С.Основные криптографические механизмы защиты данных, передаваемых в облачные сервисы и сети хранения данных// Вопросы кибербезопасности, 2020. № 3(37) С. 66-75. DOI:10 21681/2311-3456-2020-03-66-75
2. Бутусов И.В., Нащекин П.А., Романов А.А. Теоретико-семантические аспекты организации комплексной системы защиты информационных систем // Вопросы кибербезопасности, 2016. №1(14). С. 9-16. DOI:10 21681/2311-3456-2016-01-09-16
3. Ряполова Е.И., Шрейдер М.Ю., Боровский А.С.Метод обработки информации для поддержки принятия решений в управлении облачным сервисом// Вопросы кибербезопасности №3(27). 2018. С. 39-46. DOI:10.21681/2311-3456-2018-3-39-46
4. Simon H. The Structure of Ill-structured Problems / H. Simon // Artificial Intelligence. 1973. Vol. 4. P. 181-202.

5. Щербаков Е.С., Корчагин П.В. Применение методов теории возможностей при моделировании систем защиты информации // Вопросыкибербезопасности, №1(19). 2017. С. 2-5. DOI: 10.21681/2311-3456-2017-1-2-5
6. Yager R. A foundation for a theory of possibility // J. of Cybernetics, 1980. Vol. 10. №. 1–3. P. 177–209.
7. Пытьев Ю. П. Возможность. Элементы теории и применения, Эдиториал УРСС, 2000. 237 с.
8. Zadeh L.A. Fuzzy Sets. Information and Control. 8 (1965). pp. 338-353
9. Zadeh L.A. PRUF - A Meaning Representation Language for Natural Language // Intern J. of Man-Machine Studies, 1978. Vol.10. N4. P.395-399,451-460
10. Дюбуа Д. Теория возможностей: приложения к представлению знаний в информатике / Д. Дюбуа, А. Прад/ М.: Радио и связь, 1990.
11. Чечкин А.В. Математическая информатика. М.: Наука. Гл. ред. физ.-мат. лит. 1991. 416 с.
12. Бельфер Р.А.,КалюжныйД.А., Тарасова Д.В.Анализ зависимости уровня риска информационной безопасности сетей связи от экспертных данных при расчетах с использованием модели нечетких множеств // Вопросы кибербезопасности, №1(2). 2014. С. 33-39
13. Мурзин А.П., Бутусов И.В., Романов А.А. Адаптация системы защиты информации автоматизированных систем управления к нейтрализуемым угрозам // Приборы и системы. Управление, контроль, диагностика. Автоматизированные системы управления, 2017. №10. С. 1-7
14. Оладько В.С. Модель выбора рационального состава средств защиты в системе электронной коммерции // Вопросы кибербезопасности, 2016. №1 (14). С. 17-23
15. Комплексная защита информации. Анализ уязвимостей и оценка стойкости функций безопасности. URL: http://rpcnix.blogspot.ru/2012/04/1999.html
16. Сапкина Н. В. Свойства операций над нечеткими числами // Вестник ВГУ, серия: системный анализ и информационные технологии, 2013. № 1. С. 23-28
17. Аньшин В.М., Демкин И.В., Царьков И.Н., Никонов И.М. Применение теории нечётких множеств к задаче формирования портфеля проектов (теория возможностей). URL: https://www.hse.ru/data/620/907/1224/Publ2_Anshin.pdf
18. Нечеткие множества в моделях управления и искусственного интеллекта / Под ред. Д. А. Поспелова. М.: Наука. Гл. ред. физ.-мат. лит., 1986. 312 с. (Проблемы искусственного интеллекта).
19. Захаренков А.И., Бутусов И.В., Романов А.А. Метод количественной оценки степени доверенности программно-аппаратных средств // Приборы и системы. Управление, контроль, диагностика. Автоматизированные системы управления, 2017. С.34-39
20. Нащекин П.А. Перспективы информатизации основных видов деятельности в государственной системе правовой информации // Приборы и системы. Управление, контроль, диагностика. Автоматизированные системы управления. 2020. № 5. с. 1-6.

THEORETICAL JUSTIFICATION OF THE METHOD DESIGN OF INFORMATION SECURITY SYSTEMS IN VIRTUAL ENVIRONMENTS AND CLOUD PLATFORMS

Naschekin P. A.[7]

The purpose of the article *is to improve the efficiency of information security systems in conditions of high uncertainty of source data.*

Method: *modeling of information security systems using fuzzy set theory, possibility theory, and theoretical computer science.*

The result: *it is shown that the existing models and methods of designing information security systems do not fully reflect the specifics of information security systems as complex organizational and technical systems. The behavior of such systems reflects the dynamics of weakly structured processes characterized by a high degree of uncertainty due to unsteadiness, inaccuracy and insufficiency of observations, indistinctness and instability of trends. While the statistical (probabilistic) approach has obvious advantages and is widely recognized, its application is limited in the process of creating information security systems for such systems. The relevance of the scientific task of developing a methodology for designing information security systems in virtual environments and cloud platforms under conditions of high uncertainty is justified. The proposed theoretical justification is abstracted from specific types of cloud services and their placement models. The model of the security system is studied, which is represented by a hierarchy of security levels compared to the architecture of an information system that implements cloud services:*

7 Pavel Nashchokin, Director of the Federal state unitary enterprise “Sistema” of the FSO of Russia, Moscow, Russia. E-mail: pavel-vivos@yandex.ru

a composition of hierarchically interconnected levels of virtual devices for processing, storing and/or transmitting data, hardware and/or software necessary for their operation. Using the main provisions of theoretical computer science, it is shown that the parameters for evaluating the effectiveness of security mechanisms are also applicable as parameters for evaluating neutralizable threats to information security. Theoretical substantiation of methods of designing of systems of information protection in virtualized environments and cloud platforms made it possible to offer calculation procedure of the semantic threshold preferences when choosing protection mechanisms, defined in neutralizing "a threat Model and a potential intruder information security" threats, to develop and apply in the process of designing public information systems the method of choice preferred defense mechanisms, neutralizing security threats information on security levels in the overall architecture of such systems.

Keywords: *security mechanisms, information security threats, security levels, fuzzy sets, fuzzy numbers, linguistic variable, opportunity, uncertainty, risks, damage.*

References:

1. Minakov S.S. osnovnÿe kriptograficheskie mekhanizmÿ zashchitÿ dannÿkh, peredavaemÿkh v oblachnÿe servisÿ i seti khraneniya dannÿkh // Voprosy kiberbezopasnosty, 2020. № 3(37) P. 66-75. DOI:10.21681/2311-3456-2020-03-66-75
2. Butusov I.,V., Nashchekin P.A., Romanov A.A. Teoretiko-semanticheskie aspekty organizatsii kompleksnoy sisitemy zashchity informatsionnykh system // Voprosy kiberbezopasnosty, 2016. №1(14). pp. 9-16
3. Ryapolova E.I., Shreĭder M.Yu., Borovskiĭ A.S. Metod obrabotki informatsii dlya podderzhki prinyatiya reshenĭi v upravlenii oblachnÿmi servisami // Voprosy kiberbezopasnosty, №3(27). 2018. P. 39-46. DOI:10.21681/2311-3456-2018-3-39-46
4. Simon, H. The Structure of Ill-structured Problems / H. Simon // Artificial Intelligence. 1973. Vol. 4. P. 181-202.
5. Shcherbakov E.S., Korchagin P.V. Primenenie metodov teorii vozmozhnosteĭ pri modelirovanii sistem zashchitÿ informatsii // Voprosy kiberbezopasnosty, 2017. №1(19). pp. 2-5. DOI: 10.21681/2311-3456-2017-1-2-5
6. Yager R. A foundation for a theory of possibility // J. of Cybernetics, 1980. Vol. 10. №. 1–3. P. 177–209.
7. Pÿt'ev Yu. M. Vozmozhnost': élementÿ trorii i primeneniya. M.:URSS, 2000.
8. Zadeh L.A. Fuzzy Sets. Information and Control. 8 (1965). pp. 338-353.
9. Zadeh L.A. PRUF - A Meaning Representation Language for Natural Language//Intern.J. of Man-Machine Studies,1978. Vol.10. N4. P.395-399, 451-460.
10. Dyubua D., Prad A. Teoriya Vozmozhnostei: prilozheniya k predstavleniyu znanii v informatike. M.: Radio I svyaz', 1990.
11. Chechkin A.V. Matematicheskaya informatika. M.: Nauka. Gl. red. fiz.-mat. lit. 1991. 416 p.
12. Bel'fer R.A., Kalyuzhnÿĭ D.A., Tarasova D.V. Analiz zavisimosti urovnya riska informatsionnoĭ bezopasnosti seteĭ svyazi ot ékspertnÿkh dannÿkh pri raschëtakh s ispol'zovaniem modeli nechetkikh mnozhestv // Voprosy kiberbezopasnosty, №1(2). 2014. P. 33-39.
13. Murzin A.P., Butusov I.V., Romanov A.A. Adaptatsiya sistemÿ zashchitÿ informatsii avtomatizirovannÿkh system upravlrniya k neĭtralizuemÿm ugrozam // Priborÿ i sistemÿ. Upravlenie, rontrol', diagnostika. Avtomatizirovannÿe systemÿ upravlrniya. 2017. №10. pp. 1–7.
14. Olad`ko V.,S. Model' vÿbora ratsional'nogo sostava sredstv zashchity v sisteme elektronnoĭ kommertsii // Voprosÿ kiberbezopasnosti, 2016. №1 (14). pp. 17-23.
15. Kompleksnaya zashchita informatsii. Analiz uyazvimosteĭ i otsenka stoĭkosti funktsiĭ bezopasnosti. Adres dostupa: URL: http://rpcnix.blogspot.ru/2012/04/1999.html
16. Sapkina N. V. Svoistva operatsii nad nechetkimi chislami // Vestnik VGU, seriya: sistemnÿi analiz I informatsionnÿe tekhnologii, 2013. № 1. P. 23-28.
17. An'shin V.M., Demin I.V., Tsar'kov I.N., Nikonov I.M. Primenenie teorii nechetkikh mnozhestv k zadache formirovaniya portfelya proektov (teoriya vozmozhnostei). URL: https://www.hse.ru/data/620/907/1224/Publ2_Anshin.pdf
18. Nechetkie mnozhestva v modelyakh upravleniya I iskustvennogo intellekta/pod red. D.A.Pospelova/ M.: Nauka. Gl. red. fiz.-mat. lit. 1986. 312 p. (Problemÿ iskustvennogo intellekta).
19. Zakharenkov A.I., Butusov I.,V., Romanov A.A. Metod kolichestvennoy otsenki stepeni doverennosti programmno-apparatnykh sredstv // Pribory i sistemy. Upravlenie, control`, diagnostika. Avtomatizirovannye sistemy upravleniya. 2017. №8. P. 34-39.
20. Nashekin P.A. Perspektivÿ informatizatsii osnovnÿkh vidov deyatelnosti v gosudarstvennoi sisteme pravovoi informatsii // Pribory i sistemy. Upravlenie, control`, diagnostika. Avtomatizirovannye sistemy upravleniya. 2020. № 5. P. 1-6.