МЕТОДИЧЕСКИЙ ПОДХОД К КОМПЛЕКСНОМУ ОПИСАНИЮ ОБЪЕКТА ИНФОРМАЦИОННОЙ ЗАЩИТЫ

Кругликов С.В.[1], Касанин С.Н.[2], Кулешов Ю.В.[3]

Аннотация

Цель статьи: *на основе анализа комплексного подхода к оценке угроз безопасности информации обосновать методический подход к комплексному описанию объекта информационной защиты с оценкой его рисков. Предложить инструмент для построения частных моделей и системы управления информационной безопасности.*

Метод исследования: *использование частного интегрального показателя защищенности, который отражает средний риск нанесения ущерба при реализации угрозы определенного вида и характеризует степень ее опасности. Анализ архитектуры объекта оценки в приложении по отношению к возможным нарушениям информационной безопасности, оценка риска угроз безопасности информации с использованием аппарата теории нечетких множеств при рассмотрении методического подхода к комплексному описанию объекта информационной защиты с оценкой его рисков.*

Полученный результат: *предложен комплексный подход к оценке угроз безопасности информации. Оценка состояния объекта защиты при нарушении безопасности проводится с помощью частного интегрального показателя защищенности, характеризующего возможности по нанесению ущерба при ее реализации, по которому производится ранжирование. На основании этого обоснован методический подход к комплексному описанию объекта информационной защиты с оценкой его рисков, используя анализ архитектуры объекта в приложении к возможным нарушениям информационной безопасности, а также производить оценку риска с использованием аппарата теории нечетких множеств. Данный методический подход является формальным инструментом для построения частных моделей и системы управления информационной безопасности в целом. На основании этих моделей можно разработать: методики количественной оценки защищенности; методы и подходы к описанию факторов, влияющих на защищенность; методики оценки защищенности операционных систем с использованием методологического подхода к безопасности информационных систем.*

Ключевые слова: *информационная безопасность, информационная система, защита информации, угроза информационной безопасности, объект информационной защиты, объект оценки, киберпространство.*

DOI:10.21681/2311-3456-2022-4-39-51

Введение

Анализ современных аналитических публикаций показывает, что в настоящее время средства информационного воздействия и защиты развиваются наиболее динамично [1-28]. Это, прежде всего, объясняется такими свойствами инфосферы, как неисчерпаемость и восполняемость инфоресурсов, возможность их быстрого копирования, перемещения практически без потерь на огромные расстояния с высокой скоростью и степенью достоверности, компактность источников и носителей информации, мгновенная реакция (отклик) инфосферы на трудно идентифицируемое в отношении источников информационное воздействие.

Военное руководство Соединенных Штатов рассматривает киберпространство как одну из сред проведения военных операций наряду с наземной, морской, воздушной и космической. В 2015 году Пентагон разработал «Стратегию действий министерства обороны США в киберпространстве», которая определила основные направления развития киберпотенциала вооруженных сил и предъявляемые к нему требова-

1 Кругликов Сергей Владимирович, доктор военных наук, генеральный директор государственного научного учреждения «Объединенный институт проблем информатики Национальной академии наук Белоруссии», Минск, Белоруссия. E-mail: secretary_od@newman.bas-net.by

2 Касанин Сергей Николаевич, кандидат технических наук, доцент, заместитель генерального директора по научной работе государственного научного учреждения «Объединенный институт проблем информатики Национальной академии наук Белоруссии», Минск, Белоруссия. E-mail: kas.sv40@rambltr.ru

3 Кулешов Юрий Владимирович, кандидат военных наук, доцент, начальник военного факультета в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Белоруссия. E-mail: prcom@bsuir.by

ния. В качестве основных противников Соединенных Штатов в киберпространстве названы Россия, Китай, Северная Корея и Иран. В соответствии с положениями новой стратегии США должны использовать все имеющиеся возможности для отражения любой угрожающей интересам страны кибератаки. Содержание «Стратегии действий министерства обороны США в киберпространстве» свидетельствует о намерении военного ведомства играть главную роль в обеспечении национальной кибербезопасности, а также о стремлении обладать возможностями для ведения масштабных разведывательных, наступательных и оборонительных кибероперациий. При этом важное значение придается взаимодействию с союзниками и партнерами [1].

Разработка и внедрение передовых технологий военного назначения является главным направлением деятельности управления перспективных исследований МО США (DARPA). Объём финансирования DARPA в этом направлении составляет около 400 млн долл. США в год. Развитие средств и способов ведения наступательных и оборонительных действий в киберпространстве DARPA предполагает продолжить в рамках начатого в 2018 году проекта «Комплексные кибероперации» (Symbiotic Cyber Operations). Значительные усилия DARPA в области киберразведки в настоящее время сконцентрированы на повышении точности и оперативности определения конкретных источников деструктивных действий в киберпространстве [2].

В своей работе [3] известный американский журналист Шейн Харрис подробно описывает историю создания военно-сетевого комплекса США и сегодняшние тенденции его развития. Военные США рассматривают киберпространство как пятый театр военных действий (наряду с наземным, морским, воздушным и космическим), в котором участвуют Министерство обороны, АНБ, ЦРУ, независимые группы хакеров – все, кто может создавать и использовать компьютерные вирусы для нанесения удара по врагу. Изложена роль кибервойн в иракской войне, о коллаборации госструктур с такими сетевыми гигантами, как Facebook и Google, в целях сбора информации о пользователях [3].

В развитых странах мира обосновывается необходимость формирования нового вида Вооруженных Сил, предназначенного для ведения военных действий в киберпространстве. С этой целью ведется разработка моделей современного боя с применением кибератак [4, 5]. Прорабатываются основные цели «техносферной войны» и способы их достижения, порядок проведения операций в киберпространстве, которые становятся одной из перспективных форм применения вооруженных сил [6, 7].

Современные информационно-коммуникационные онлайн-технологий, применятся для дестабилизации национальных политических режимов, включая технологии массовой политической пропаганды и манипуляции общественным сознанием в интернет-пространстве. Рассматривается вероятность использования кибероружия в ходе военных действий для провоцирования техногенных катастроф на промышленных предприятиях и энергетических объектах, приводящих к жертвам среди мирного населения и серьезному ущербу экономике [8-10].

В целях минимизации последствий применения средств информационного воздействия создаются системы, способные осуществлять предупреждение и заблаговременное пресечение компьютерных атак на критически важные информационные ресурсы. Разрабатываются подходы к аналитическому моделированию кибератак, организации защиты информации в информационных системах от несанкционированного доступа, а также теоретико-методологические подходы к решению задачи формирования перечня актуальных для защищаемой автоматизированной системы компьютерных атак [11-15]. Совершенствуются методы тестирования информационных систем на проникновение, теоретически и практически прорабатываются подходы к аудиту информационной безопасности критической информационной инфраструктуры, проводиться анализ защищенности информационных ресурсов [16-22].

Наличие «информационного общества» в ведущих экономически развитых западных странах не смогло способствовать устойчивому экономическому росту. В ряде случаев современные Интернет-сети привели к ряду государственных переворотов, принесли несчастье многим публичным людям, так как пользователи социальных сетей фактически не несут никакой ответственности за свои высказывания. В связи с этим возникла необходимость правового регулирования информационной безопасности в законодательствах стран мира, незамедлительное создание механизмов международного управления, одним из которых могут стать Правила поведения государств в информационном пространстве, обеспечение международной информационной безопасности, формирования под эгидой ООН режима контроля над вооружениями, основанными на информационно-коммуникационных технологиях [23-26].

В [27] был выработан и предложен методический подход к оценке вероятностей реализации угроз безопасности информации (УБИ). Как было указано,

проблематика исследований в данной предметной области связана со сложностью оценки эффективности обеспечения безопасности информации. Это обусловлено неопределенностью режимов и характера эксплуатации объектов информационных технологий (ОИТ) и средств защиты информации (СЗИ) по причине отсутствия полной информации обо всех режимах их функционирования, а также появлением различных видов угроз, бурным развитием современных технических средств воздействия на информационные ресурсы потенциальным нарушителем и возможностью по_явления новых способов и средств нарушения информации (новых угроз).

Теоретический анализ

Рассуждая и вырабатывая концептуальные подходы к комплексной оценке УБИ, отметим следующее. На наш взгляд, для построения комплексной защиты информации необходимо выявить в первую очередь УБИ и оценить их последствия, а именно опасность

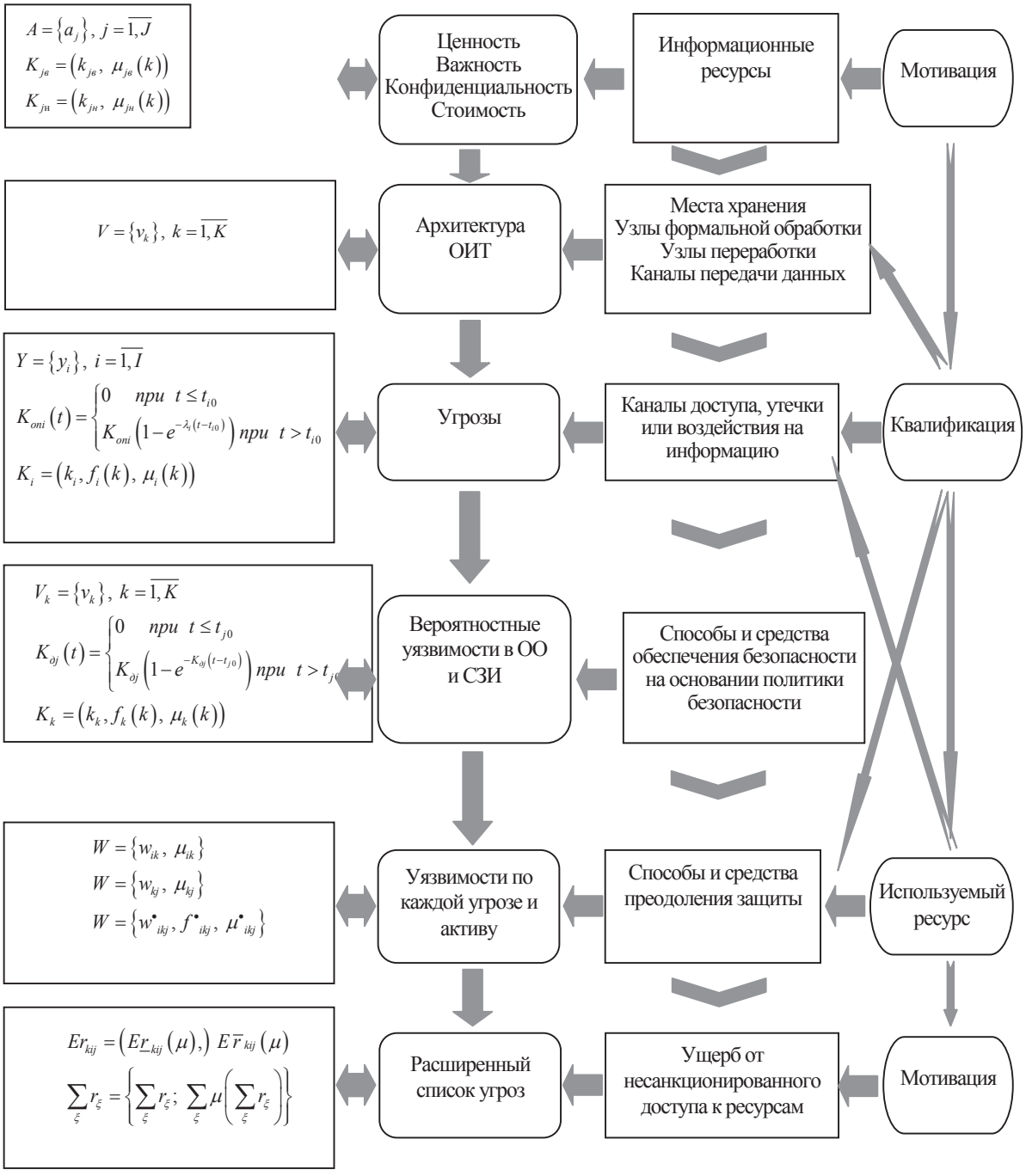

Рис. 1. Порядок оценки и ранжирования угроз безопасности

каждой угрозы. Предлагается формирование методологии выявления УБИ осуществлять по следующим направлениям:

- систематизация и статистическая оценка атак и попыток несанкционированного доступа к объектам информации;
- экспериментальное тестирование информационных систем (ИС) на предмет обнаружения уязвимых мест, использование которых возможно для реализации угроз;
- создание аналитических и имитационных моделей процессов функционирования ИС, угроз безопасности и генераторов атак;
- экспертный анализ и экспертные оценки с привлечением специалистов – системных администраторов, администраторов безопасности, аудиторов информационной безопасности и других специалистов в области информационной безопасности.

При этом оценка УБИ является одним из основных этапов процесса анализа и управления рисками при создании и эксплуатации ИС. Она должна включать априорную оценку на этапе разработки, уточненную периодическую оценку в процессе эксплуатации с учетом информации мониторинга, выявления нарушений информационной безопасности (ИБ) и динамического управления рисками. В этом случае оценку следует проводить с использованием моделей общей оценки угроз, которые являются основой оценки как самих УБИ, так и потерь, которые могут иметь место при их проявлении. Модели данного типа важны еще и тем, что именно на них в основном выявлены те условия, при которых такие оценки могут быть адекватны реальным процессам защиты информации. К настоящему времени разработаны различные табличные, диаграммные, формализованные, имитационные модели УБИ.

Следует отметить, что, несмотря на достоинства этих моделей, ни одна из них не позволяет одновременно учесть три основных параметра – уязвимость, активизируемую атакой, метод ее реализации и возможные последствия. Другими словами, возникает противоречие между теорией и практикой информационной защиты из-за неразрешенности вопросов в подходах к комплексности оценки УБИ. Предлагаемый авторами статьи порядок комплексной оценки и ранжирования УБИ приведен на рис. 1.

Для определения потенциала УБИ в этом случае целесообразно использовать частный интегральный показатель защищенности:

$$R_{\text{cpi}} = \sum_k \sum_j r_{ikj} P_i = \sum_j r_{ij} P_i, \quad j = \overline{1, J} \qquad (1)$$

Он отражает средний риск нанесения ущерба при реализации угрозы определенного вида и характеризует степень ее опасности. В зависимости от априорного описания оценки показатель может быть в т. ч. нечетким статистическим и нечетким.

В первом случае для определения элементов множества рисков используются вероятностные оценки нечеткого случайного события:

- вероятность

$$p\left(r_{ikj}\right) = \int_{-\infty}^{\infty} f\left(r_{ikj}\right) \mu\left(r_{ikj}\right) dr_{ikj}; \qquad (2)$$

- математическое ожидание

$$Er_{kji} = \left(E\underline{r}_{ikj}(\mu), E\bar{r}_{ikj}(\mu)\right); \qquad (3)$$

- дисперсия

$$Dr_{ikj} = 0{,}5\int_0^1 \left[\left(\underline{r}_{ikj}(\mu) - E\underline{r}_{ikj}(\mu)\right)^2 + \left(\bar{r}_{ikj}(\mu) - E\bar{r}_{ikj}(\mu)\right)^2\right] d\mu, \qquad (4)$$

где $\underline{r}, \bar{r}$ – соответствующие ветви функции принадлежности при обратном отображении $\mu = \left(\underline{\mu}, \bar{\mu}\right)$, $0 \le \mu \le 1$.

Для определения потенциала атаки используются формулы теории вероятностей, поскольку в данном случае кроме нечеткости по Заде используются дополнительные операции, такие как включение, алгебраическая сумма и алгебраическое произведение по Бандлеру и Кохоуту, эквивалентность.

При втором подходе для определения потенциала атаки операция суммирования определяется выражением

$$\sum_\xi r_\xi = \left\{\sum_\xi \mathrm{r}_{¾}; \sum_\xi \mu\left(\sum_\xi \mathrm{r}_{¾}\right)\right\}, \qquad (5)$$

в котором суммирование элементов носителей является скалярным, а значение функции принадлежности вычисляется согласно правилу центра тяжести, используемого в операции дефазификации

$$\sum_\xi \mu\left(\sum_\xi \mathrm{r}_{¾}\right) = \frac{\sum_\xi \mathrm{r}_{¾}\mu\left(\mathrm{r}_{¾}\right)}{\sum_\xi \mathrm{r}_{¾}}. \qquad (6)$$

Таким образом, предложенный комплексный подход к оценке и ранжированию УБИ предусматривает

использование частного интегрального показателя защищенности, характеризующего возможности по нанесению ущерба при ее реализации, по которому и производится ранжирование.

Рассуждая далее, выработаем подход к оценке состояний объекта оценки (ОО) при нарушении безопасности (рис. 2).

Внешняя среда характеризуется нечетким множеством угроз активам

$$Y = \{y_i, \mu(y_i)\}, \; i = \overline{1,I} \qquad (7)$$

элементы которого определяются нечетким случайным коэффициентом опасности в качестве его динамической характеристики. В общем случае данный коэффициент можно описать выражением

$$x_i(t) = \begin{cases} 0 & \text{при} \quad t \le t_{i0} \\ K_i\left(1 - e^{-\lambda_i (t - t_{i0})}\right) & \text{при} \quad t > t_{i0}, \end{cases} \qquad (8)$$

где $K_i = \prod_{\xi_1=1}^{\Xi_1} k_{i\xi_1}$, $\lambda_i = \prod_{\xi_2=1}^{\Xi_2} \lambda_{i\xi_2}$, t_{i0} – параметры угрозы.

ОО характеризуется двумя множествами:

уязвимостей $V = \{v_k\}, \; k = \overline{1,K}$ (9)

и активов (информации или ресурсов)

$$A = \{a_j\}, \; j = \overline{1,J}. \qquad (10)$$

Уязвимости предлагается характеризовать коэффициентом доступности, который является их динамической характеристикой и в общем случае определяется выражением

$$v_k(t) = \begin{cases} 0 & \text{при} \quad t \le t_{k0} \\ K_k\left(1 - e^{-K_k (t - t_{k0})}\right) & \text{при} \quad t > t_{k0}, \end{cases} \qquad (11)$$

где $K_j = \prod_{\varsigma=1}^{\Sigma_1} K_{j\varsigma}$, t_{ij0} – параметры уязвимости.

Коэффициенты K_i, K_k являются нечеткими случайными величинами

$$K_i = (k_i, f_i(k), \mu_i(k)) \qquad (12)$$
$$K_k = (k_k, f_k(k), \mu_k(k))',$$

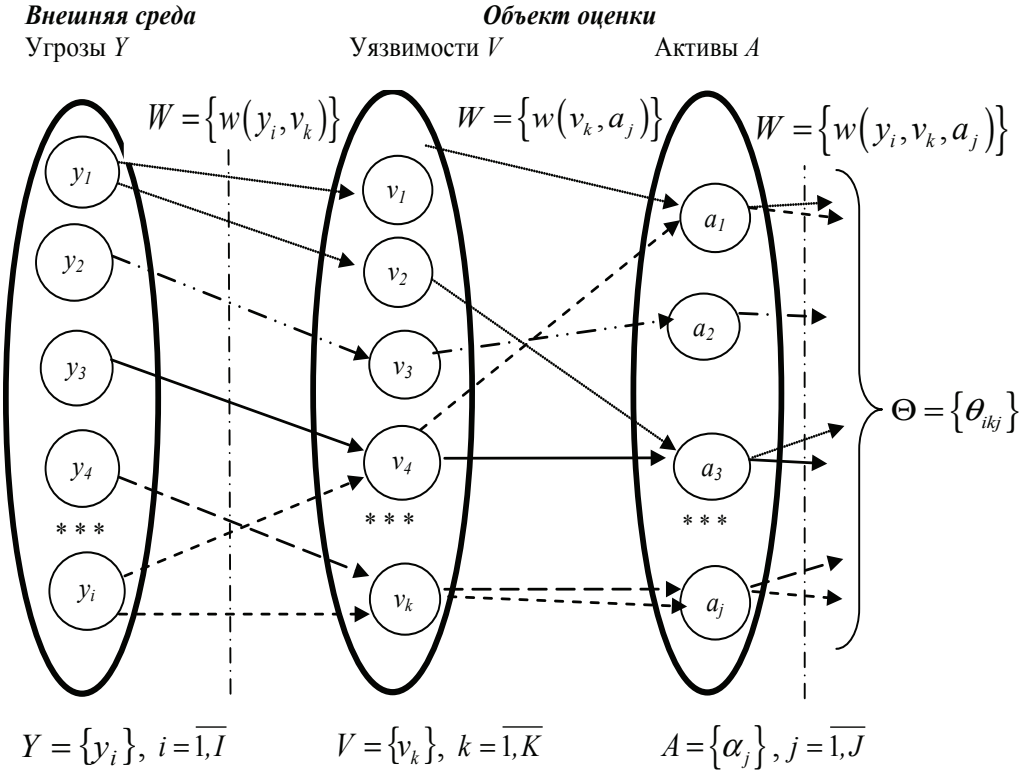

Рис. 2. Граф состояний объекта оценки

где k_η – оценочное значение соответствующего коэффициента (среднее значение), $f_\eta(k)$, $\mu_\eta(k)$ – случайная и нечеткая составляющие нечеткой случайной величины.

Активы характеризуются нечетким коэффициентом ценности $K_{j=} = \left(k_{j=},\ \mu_{j=}(k)\right)$ со стороны нарушителей (важность, ценность и степень заинтересованности в их получении) и коэффициентом ценности $K_{j2} = \left(k_{j2},\ \mu_{j2}(k)\right)$ со стороны их владельцев (важность, стоимость, влияние на организацию, возможность восстановления и др.).

Между угрозами безопасности и уязвимостями ОО существует однозначная связь, образующая 2-дольный *H*-вершинный граф:

$$G = \left(Y, V, E_H\right), \quad (13)$$

где $E_H = \left\{e_h\right\} = \left\{e_{ij}\right\}, h = \overline{1,H}, H < I \times J$ – множество ребер графа G;

$$e_h = \left(y_i, v_k\right) = \{0,1\}.$$

Ребро $e_h = 1$, если угроза y_i может быть реализована через уязвимость v_k, т.е.

$$\left(\exists\, y_i \in Y\right)\left(\exists\, v_k \in V\right)\ \ \left(\exists\, e_{ik}\right)\left(e_{ik} = 1\right). \quad (14)$$

Каждому ребру $e_{ik} = \left(y_i, v_k\right)$ приписан вес w_{ik}, являющийся элементом нечеткого множества

$$W = \left\{w_{ik}, f_{ik},\ \mu_{ik}\right\}, \quad (15)$$

где $w_{ik} = k_{ik}$ – элемент-носитель, означающий коэффициент опасности определенной угрозы при ее реализации через определенную уязвимость;

f_{ik}, μ_{ik} – совместные плотность распределения и функция принадлежности, соответственно.

Уязвимости и активы также образуют 2-дольный *D*-вершинный граф

$$G = \left(V, A, E_d\right), \quad (16)$$

где $E_d = \left\{e_d\right\} = \left\{e_{kj}\right\}, d = \overline{1,D}, D < K \cdot J$ – множество ребер графа G;

$e_d = \left(v_k, a_j\right), e_d = \{0,1\}$ – ребро графа G, удовлетворяющее условию

$$\left(\exists\, v_k \in V\right)\left(\exists\, a_j \in A\right)\ \ \left(\exists_{kj}\right)\left(e_{kj} = 1\right).$$

Каждому ребру $e_{kj} = \left(v_k, a_j\right)$ приписан вес w_{kj}, являющийся элементом нечеткого множества

$$W = \left\{w_{kj},\ \mu_{kj}\right\}, \quad (17)$$

где $w_{kj} = k_{kj}$ – коэффициент опасности данной уязвимости для данного актива;

μ_{kj} – совместная функция принадлежности.

Объединение графов $G = \left(Y, V, E_H\right)$ и $G = \left(V, A, E_D\right)$ приводит к 3-дольному $L = H \times D$ -вершинному графу

$$G = \left(Y, V, A, E_L\right). \quad (18)$$

Результирующее открытое ребро $e_{ikj} = \left(y_i, v_k, a_j\right) = \{0,\ 1\}$ множества ребер $E_L = \left\{e_l\right\} = \left\{e_{ikj}\right\},\ l = \overline{1,L}$ графа G удовлетворяет условию

$$\left(\exists y_i \in Y\right)\left(\exists\, v_k \in V\right)\left(\exists\, a_j \in A\right)\ \ \left(\exists\, e_{ikj}\right)\left(e_{ikj} = 1\right). \quad (19)$$

Каждому ребру $e_{ikj} = \left(y_i, v_k, a_j\right)$ приписан вес w_{ikj}, являющийся элементом случайного нечеткого множества

$$W = \left\{w_{ikj}, f_{ikj},\ \mu_{ikj}\right\}, \quad (20)$$

где $w_{ikj} = k_{ikj}$ – коэффициент возможности принятия ОО состояния нарушения ИБ (ikj), характеризующий возможность реализации угрозы через определенную уязвимость на определенный актив,

μ_{ikj} – функция принадлежности элемента $w_{ikj} = k_{ikj}$ нечеткому множеству $W = \left\{w_{ikj},\ \mu_{ikj}\right\}$.

Граф $G = \left(Y, V, A, E_L\right)$ представляет собой граф состояний ОИТ с позиций ИБ. Он характеризует множество состояний ОО $\Theta = \left\{\theta_{ikj}\right\}$ при нарушении ИБ с учетом заинтересованности нарушителя ИБ, характеризуемой коэффициентом ценности активов $K_{jh} = \left(k_{jh},\ \mu_{jh}(k)\right)$.

Для определения взаимосвязи между элементами множеств $Y = \left\{y_i\right\}$, $i = \overline{1,I}$, $V = \left\{v_k\right\}$, $k = \overline{1,K}$ и $A = \left\{a_j\right\}$, $j = \overline{1,J}$ можно использовать базовые положения о сотрудничестве, конфликте и безразличии между подсистемами $\Im_1$ и $\Im_2$, входящими в окружение некоторой системы $\Im = \left\{\Im_1, \Im_2, \ldots, \Im_n\right\}$, суть которых заключается в следующем:

$$\begin{gathered} q\left(\Im_i, \Im_j\right) < q\left(\Im_i, \overline{\Im_j}\right), \\ \text{если}\ \ q\left(\Im_i, \Im_j\right) > q\left(\Im_i, \overline{\Im_j}\right), \\ q\left(\Im_i, \Im_j\right) = q\left(\Im_i, \overline{\Im_j}\right), \\ \Im_j \Re\left(\overline{\Im_j}\right) \Im_j,\ \text{кофликт между}\ \Im_j \text{ и } \Im_i \\ \Im_j \overline{\Re}_c\left(\overline{\Im_j}\right) \Im_i,\ \text{сотрудничество между}\ \Im_j \text{ и } \Im_i \\ \Im_j \overline{\Re}_l\left(\overline{\Im_j}\right) \Im_i,\ \text{безразличие между}\ \Im_j \text{ и } \Im_i \end{gathered} \quad (21)$$

где q – функция полезности системы; $\overline{\Im}_j = \varnothing$. Мера структурного взаимодействия, которая при $\Im_j = 2$ определяется соотношением

$$\mu_{ij}\left(\overline{\Im}_j\right)=q\left(\Im_i,\Im_j\right)-q\left(\Im_i,\overline{\Im}_j\right)=\frac{\partial q\left(\Im_i,\overline{\Im}_j\right)}{2\partial\Im_j}\Im_j \quad (22)$$

Таким образом, рассмотренный комплексный подход к оценке угроз безопасности информации с оценкой состояния объекта защиты при нарушении безопасности показал отсутствие механизмов достоверного подтверждения качества и достаточности средств защиты и недостаточной проработки вопросов моделей системы защиты, системы показателей и критериев безопасности ИТ.

Это обусловливает необходимость развития нормативно-методической базы, методик и моделей оценки защищенности на основе системного подхода. Первостепенным направлением можно назвать разработку моделей систем безопасности, критериев и показателей защищенности, методов их оценки и оценки элементов безопасности, методик оценки защищенности на всех

Рис. 3. Содержание процесса комплексного обследования и описания объекта оценки

этапах жизненного цикла ОИТ. Также важна динамическая оценка рисков на основе системного подхода. В данном случае первостепенное значение имеют только те свойства элементов защиты, которые определяют взаимодействие друг с другом, оказывают влияние на систему в целом и на достижение поставленной цели.

На наш взгляд для комплексного обследования и описания ОО прежде всего, необходимо определиться с исходными данными. Можно утверждать, что исходными данными будет являться политика безопасности организации, которая определяет: цели и задачи организации; активы, подлежащие защите и их ценность; классы угроз, от которых требуется защита; общие требования безопасности; категории нарушителей; требования защиты по классам угроз; метод анализа и управления рисками.

Исходя из перечисленного, предлагается содержание процесса комплексного обследования и описания ОО проводить по схеме, представленной на рис. 3.

В результате проведения анализа по предложенной авторами схеме, можно сформировать выходные данные, которые могут включать: активы, подлежащие защите; общие угрозы безопасности для анализируемого объекта оценки; уязвимые места объекта оценки; требования защиты.

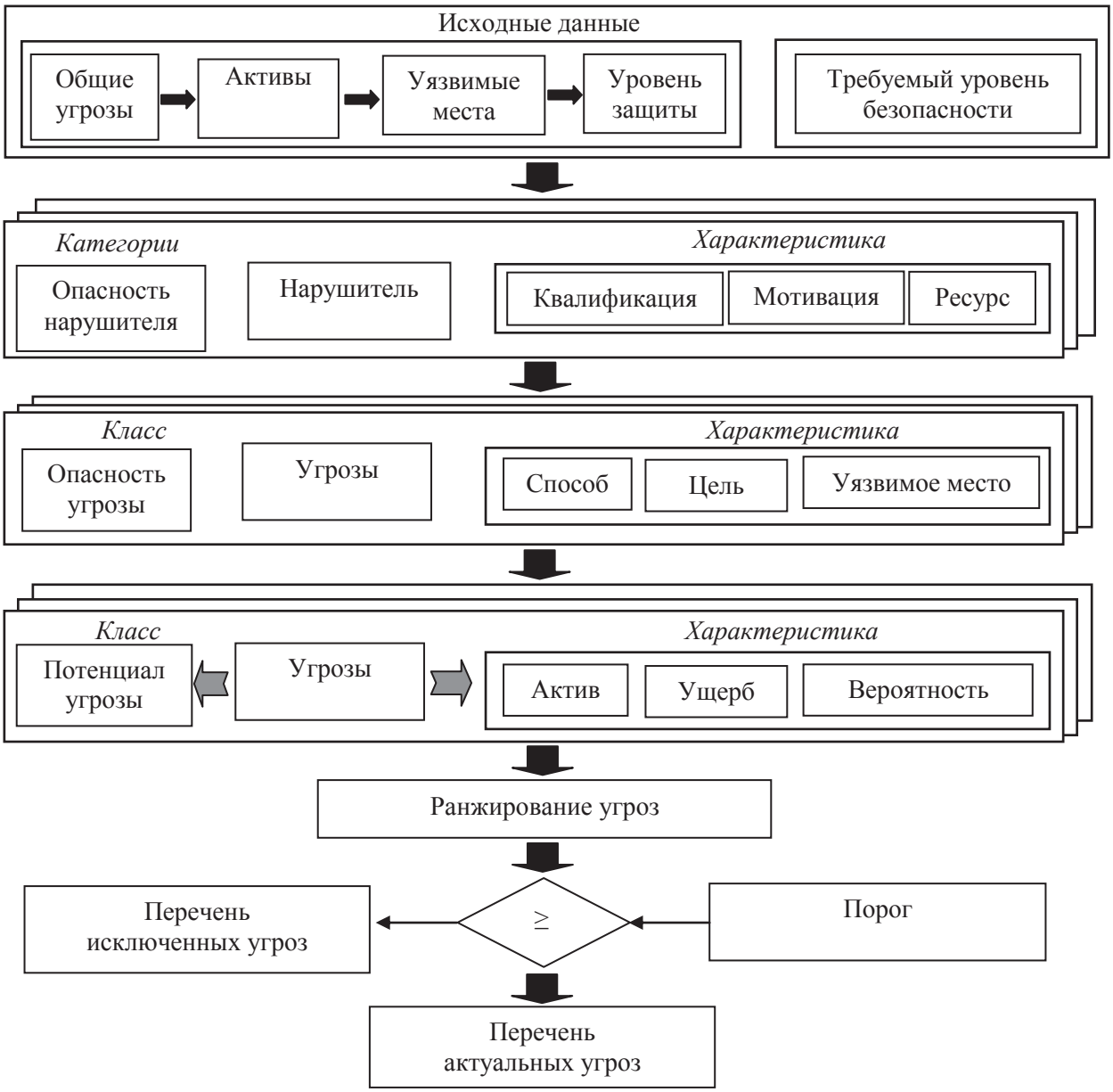

Рис. 4. Процесс определения перечня актуальных угроз

Эти выходные данные процесса анализа объекта оценки являются исходными данными для определения перечня актуальных угроз. Дополнительными исходными данными являются требуемый уровень безопасности и метод оценки рисков. Формирование перечня актуальных для ОО угроз проводится на основании их ранжирования и сравнения с некоторым допустимым пороговым значением. Ранжирование угроз безопасности выполняется на основании оценочного значения потенциала угрозы, который определяется категориями опасности нарушителя безопасности и опасности угрозы.

Для оценки опасности нарушителя целесообразно использовать его персональные характеристики: квалификация, мотивация и используемый ресурс. Для оценки опасности угрозы предлагается использовать ее характеристики, такие как способ реализации, цели реализации угрозы и используемое уязвимое место.

Далее необходимо оценить потенциал угроз безопасности. Потенциал угроз безопасности можно оценить на основании оценочных значений следующих факторов безопасности: актив, ущерб, вероятность реализации угрозы.

Путем сравнения рассчитанных потенциалов угроз с некоторым пороговым значением формируются перечни исключенных угроз и актуальных угроз для данного объекта оценки (рис. 4).

Проводя рассуждения далее, выработаем подход к оценке риска с использованием аппарата теории нечетких множеств.

Величину возможных потерь можно оценить по следующей формуле:

$$\textit{ЦЕНА ПОТЕРИ} = P_н \times \textit{УЩЕРБ}, \quad (23)$$

где под ущербом понимается материальная стоимость актива, Рн – мера, характеризующая возможность перехода в состояние нарушения ИБ. Она определяется через параметры и характеристики угроз безопасности, уязвимостей ОО и активов.

При оценке состояний объекта оценки при нарушении ИБ с использованием нечетких множеств элементы множеств угроз безопасности $Y = \{y_i, \mu(y_i)\}$, $i = \overline{1,I}$, уязвимостей $V = \{v_k, \mu(v_k)\}$, $k = \overline{1,K}$ и активов (информации и/или ресурсов) $A = \{a_j, \mu(a_j)\}$, $j = \overline{1,J}$, характеризующих взаимодействие ОО с внешней средой, описываются нечеткими величинами $k = (k,\ \mu(k))$, где $k \in [0;1]$ – оценочное среднее значение соответствующего нечеткого коэффициента k, $\mu(k) \in [0;1]$ – функция принадлежности нечеткой величины k.

Величина риска

$$r_{ikj}\left(r^{\bullet}_{ikj}, \mu^{\bullet}_{ikj}\right) = y_i \cdot v_k \cdot a_j \quad (24)$$

будет определяться с использованием выражений

$$r^{\bullet}_{ikj} = y_i \cdot v_k \cdot a_j,\ \ \mu^{\bullet}_{ikj} = \min\left(\mu_i, \mu_k, \mu_j\right). \quad (25)$$

Ущерб j-му активу описывается формулой

$$U_j = \sum_{i,k} r_{ikj} \cdot s_j, \quad (26)$$

а суммарный ущерб

$$U = \sum_{i,k,j} r_{ikj} \cdot s_j, \quad (27)$$

где s_j – материальная ценность j-го актива.

Степень опасности угрозы y_i, оценивается по нескольким параметрам и рассчитываются по формулам:

$$y_i\left(y_i, \mu_i\right) = \prod_{l=1}^{L} y_{il} = \left(\prod_{l=1}^{L} y_{il}, \min_{l}\left(\mu_{il}\right)\right), \quad (28)$$

где $y_{il} \in [0;1]$ – оценочное среднее значение l-го параметра i-й угрозы; $\mu_{il} \in [0;1]$ – степень принадлежности нечеткой величины y_{il} – l-го параметра i-й угрозы; L – количество параметров угрозы.

Степень опасности уязвимости v_k и значимость актива a_j оцениваются аналогично. Следует отметить, что параметры угроз, уязвимостей и активов не обязательно должны оцениваться по шкале от 0 до 1. В случае, если используется другая шкала оценки параметров, необходимо провести нормировку.

Все параметры угроз, уязвимостей и активов (за исключением материальной стоимости актива) оцениваются в соответствии с приведенными выше бальными шкалами и представляются в виде нечетких величин с L=5 термами на множестве-носителе [0; 1]. Функции принадлежности значения параметра k_i терму j представляют собой колоколообразные функции с максимумом в точках 0; 0,25; 0,5; 0,75; 1 для 1-го ... 5-го термов соответственно и могут быть рассчитаны по формуле:

$$\mu_i^j\left(k_i\right) = \frac{1}{\left(1 + \left(k_i \cdot (L-1) - i + 1\right)^2\right)^{\beta}}, \quad (29)$$

$$L = \overline{1,5}\ .$$

Для теоретической проработки подхода рассмотрим особенности реализации операции умножения нечетких величин (рис. 5).

Выполнение операции умножения с использованием максминной композиции над большим количеством переменных ведет быстрому росту пар $(k,\ \mu(k))$, задающих нечеткую величину. Так, в

нашем случае в зависимости от источника угроз риск оценивается по 8 или 9 параметрам, каждый из которых после преобразования в нечеткую величину (фаззификации) описывается пятью парами $\left(k,\ \mu\left(k\right)\right)$. Риск, в таком случае, будет содержать до двух миллионов таких пар, что явно избыточно и требует больших вычислительных затрат.

Основываясь на принципе обобщения, максминная композиция реализуется двумя процедурами. Первая выполняется по формуле:

$$\mu_i^j\left(k_i\right)=\frac{1}{\left(1+\left(k_i\cdot\left(L-1\right)-i+1\right)^2\right)^\beta},$$
$$=\bigcup_{i=1}^{n}\bigcup_{j=1}^{m}\left(\left(\mu_x\left(x_i\right)\wedge\mu_{\ y}\left(y_j\right)\right)/\ x_i\cdot y_j\right) \quad (30)$$

Во второй процедуре осуществляется поглощение нескольких компонентов $\mu_z\left(z_k\right)/\ z_k, k=\overline{1,}$ (r-количество компонентов с равнозначными носителями) одним $\mu_z\left(z_s\right)/\ z_s$; $\mu_z\left(z_s\right)=\max\left(\mu_z\left(z_k\right)\right)$. Результат первой процедуры можно увидеть на рисунке 5в.

Вторая процедура несколько уменьшает количество полученных точек, однако оно все равно остается велико, при этом все равно остаются точки, степень принадлежности которых заметно ниже, чем у ближайших соседей, т.е. функция принадлежности результирующего числа имеет множество провалов. Наличие этих провалов практически не влияет на конечный результат, и их можно отбросить, заменив функцию принадлежности огибающей (рисунок 5г). В результате количество пар $\left(k,\ \mu\left(k\right)\right)$ может быть уменьшено

Получить огибающую можно, производя операцию умножения с помощью α-уровневого принципа обобщения. Суть его заключается в следующем. Исходные числа урезаются по уровню α (т.е. из всех a_i, b_j остаются только те, для которых степень принадлежности не меньше α), вычисляются значения $a_i \times b_j$ и для всех $\min(a_i b_j) \le z \le \max(a_i b_j)$ степень принадлежности принимается равной α. Проделав эту операцию для множества α от 0 до 1 (в MatLab используется 101 значение α = 0:1 с шагом 0,01) и объединив полученные результаты как во второй процедуре максминной композиции, получим искомую огибающую, значение которой с помощью интерполяции можно рассчитать для любых значений множества-носителя.

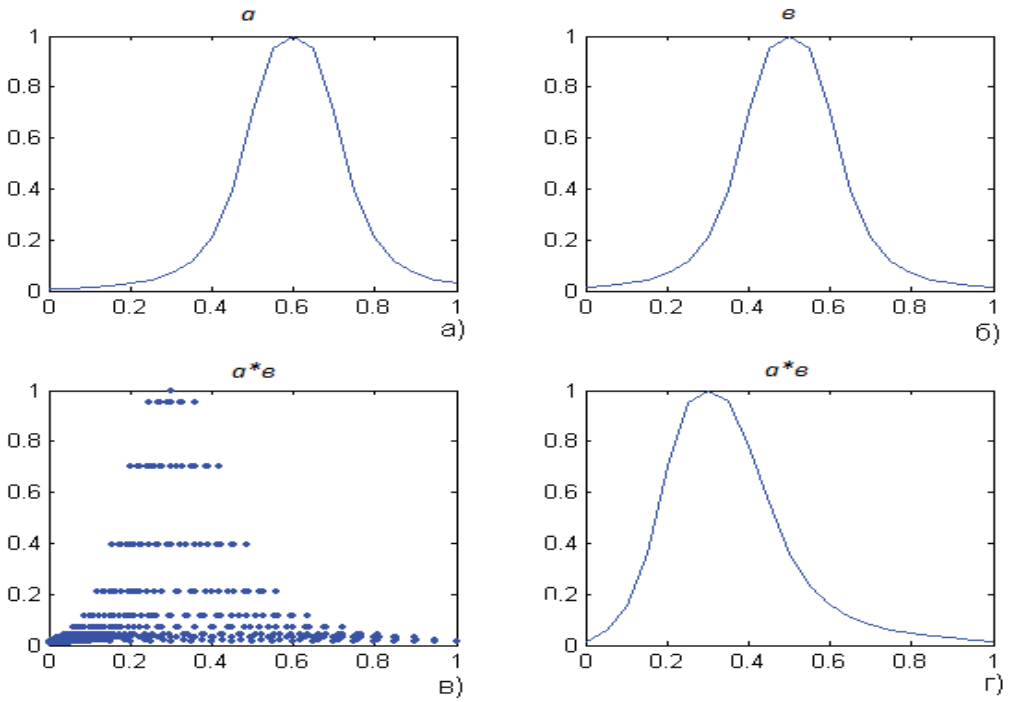

Рис. 5. Выполнение операции умножения

а, б – нечеткие числа a и b; в – результат первой процедуры максминной композиции при умножении чисел a×b; г – результат умножения a×b полученный с помощью α-уровневого принципа обобщения

Заключение

Таким образом, предложенный методический подход позволяет построить результат на любом выходном множестве-носителе с любым желаемым числом компонентов и получить огибающую, производя операцию умножения с помощью α-уровневого принципа обобщения.

На основании изложенных принципов целесообразно разработать программу в среде MatLab, производящую анализ рисков при различных значениях входных переменных.

Разработанный методический подход, представляющий собой содержание и взаимосвязь процедур управления ИБ на всех этапах жизненного цикла ОО, является формальным инструментом для построения частных моделей и системы управления ИБ в целом. Предложенные модели позволяют разработать: методики количественной оценки защищенности; методы и подходы к описанию факторов, влияющих на защищенность; методики оценки защищенности операционных систем с использованием методологического подхода к безопасности ИС. Проведенные исследования показали необходимость продолжения работ в данном направлении.

Литература

1. Колосков, С. Стратегия действий министерства обороны США в киберпространстве / С. Колосков // Зарубежное военное обозрение. - 2016. - № 10. - С. 3-7.
2. Баташов, В. Деятельность министерства обороны США по развитию новых технологий в сфере кибербезопасности / В. Баташов // Зарубежное военное обозрение. - 2018. - № 10. - С. 10-13.
3. Харрис Ш. Кибер войн@. Пятый театр военных действий – М.: Альпина нон-фикшн, 2016. - 390 с.
4. Стародубцев Ю.И., Закалкин П.В., Иванов С.А. Многовекторный конфликт в киберпространстве как предпосылка формирования нового вида Вооруженных Сил // Военная мысль. 2021. № 12. С.126-135.
5. Бойко А.А. Боевая эффективность кибератак: аналитическое моделирование современного боя. Системы управления, связи и безопасности. 2020. N 4. С. 101-133.
6. Стародубцев Ю.И., Закалкин П.В., Иванов С.А. Техносферная война как основной способ разрешения конфликтов в условиях глобализации // Военная мысль. 2020. № 10. С.16-21.
7. Тумар В.А., Левчук Н.Н. Киберпространство как среда противоборства: военный аспект и Белорусский опыт нормотворчества // Вестник Академии военных наук. 2020. № 3 (72). С.43-49.
8. Володенков С.В. Интернет-коммуникации в глобальном пространстве современного политического управления. – М.: Издательство Московского университета; Проспект, 2018. 272 с., ил.
9. Дурнев Р.А., Крюков К.Ю., Дедученко Ф.М. Предупреждение техногенных катастроф, провоцируемых в ходе военных действий // Военная мысль. 2019. № 10. С. 41-48.
10. Зарудницкий В.Б. Характер и содержание военных конфликтов в современных условиях и обозримой перспективе // Военная мысль. 2021. № 1. С.34-44.
11. Бирюков Д.Н., Ломако А.Г., Петренко С.А. Порождение сценариев предупреждения компьютерных атак. Защита информации. Инсайд. 2017. N 4 (76). С. 70-79.
12. Дроботун Е.Б. Теоретические основы построения систем защиты от компьютерных атак для автоматизированных систем управления. Монография. – СПб.: Наукоемкие технологии, 2017. – 120 с., ил. ISBN 978-5-9909412-2-9.
13. Марков А.С. Технические решения по реализации подсистем ГосСОПКА. В книге: Управление информационной безопасностью в современном обществе. Сборник научных трудов V Международной научно-практической конференции. 2017. С. 85-96.
14. Лаута О.С., Коцыняк М.А., Иванов Д.А., Гудков М.А. Моделирование компьютерных атак на основе метода преобразования стохастических сетей. В сборнике: Радиолокация, навигация, связь. Сборник трудов XXIV Международной научно-технической конференции. В 5-и томах. 2018. С. 137-146.
15. Язов Ю.К. Организация защиты информации в информационных системах от несанкционированного доступа: монография / Ю.К. Язов, С.В. Соловьев. Воронеж: Кварта, 2018. – 588 с.
16. Бегаев А.Н., Бегаев С.Н., Федотов В.А. Тестирование на проникновение. СПб.: Университет ИТМО, 2018. – 45 с.
17. Дорофеев А.В., Лемберская Е.Х., Рауткин Ю.В. Анализ защищенности: нормативная база, методологии и инструменты. Защита информации. Инсайд. 2018. N 4 (82). С. 63-69.
18. Макаренко С.И. Аудит безопасности критической инфраструктуры специальными информационными воздействиями. Монография. – СПб.: Наукоемкие технологии, 2018.– 122 с.
19. Коцыняк М.А., Лаута О.С., Иванов Д.А. Математическая модель таргетированной компьютерной атаки. Наукоемкие технологии в космических исследованиях Земли. 2019. Т. 11. N 2. С. 73–81. DOI: 24411/2409-5419-2018-10261.
20. Дергунов И.Ю., Зима В.М., Глыбовский П.А., Мажников П.В. Модель процесса интеллектуального тестирования АС на проникновение с учетом временных параметров. Защита информации. Инсайд. 2020. N 5 (95). С. 64-67.
21. Жиленков А.А., Черный С.Г. Система безаварийного управления критически важными объектами в условиях кибернетических атак // Вопросы кибербезопасности. 2020. № 2 (36). С. 58-66. DOI:10.21681/2311-3456-2020-2-58-66.
22. Котенко И.В., Крибель А.М., Лаута О.С., Саенко И.Б. Анализ процесса самоподобия сетевого трафика как подход к обнаружению кибератак на компьютерные сети // Электросвязь. 2020. № 12. С.54-59. DOI:10.34832/ELSV.2020.13.12.008.
23. Бочков С.И., Макаренко Г.И., Федичев А.В. Об окинавской хартии глобального информационного общества и задачах развития российских систем коммуникации // Правовая информатика. 2018. № 1. С. 4-14. DOI: 10.21681/1994-1404-2018-1-04-14
24. Ромашкина Н.П. Глобальные военно-политические проблемы международной информационной безопасности: тенденции, угрозы, перспективы // Вопросы кибербезопасности. 2019. № 1(29). С. 2-8. DOI: 10.21681/2311-3456-2019-1-2-9.

25. Карцхия А.А., Макаренко Г.И., Сергин М.Ю. Современные тренды киберугроз и трансформация понятия кибербезопасности в условиях цифровизации системы права // Вопросы кибербезопасности. 2019. № 3 (31). С. 18-23. DOI: 10.21681/2311-3456-2019-3-18-23.
26. Ромашкина Н.П., Марков А.С., Стефанович Д.В. Международная безопасность, стратегическая стабильность и информационные технологии: Монография / Н.П. Ромашкина, А.С. Марков, Д.В. Стефанович. – Москва, 2020. Сер. Библиотека Национального исследовательского института мировой экономики и международных отношений имени Е.М. Примакова. – 98 с. ил.
27. Кулешов, Ю.Е., Паскробка, С.И., Сергиенко, В.А., Касанин, С.Н. Методический подход к оценке вероятностей реализации угроз безопасности информации/ Ю.Е. Кулешов, С.И. Паскробка, В.А. Сергиенко, С.Н. Касанин // Научно-производственный журнал «Веснік сувязі». - 2017. - №5. - С. 56-59.

METHODICAL APPROACH TO THE COMPLEX DESCRIPTION OF INFORMATION PROTECTION OBJECT

Kruglikov S.V.[4], Kasanin S.N.[5], Kuleshov Y.E.[6]

Abstract

Purpose: *on the basis of analysis of a comprehensive approach to the assessment of threats to information security to substantiate a methodological approach to a comprehensive description of the object of information protection with an assessment of its risks. Offer a tool for building private models and information security management system.*

Research method: *use of partial integral index of security, which reflects the average risk of damage during the implementation of a threat of a certain type and characterizes the degree of danger. Analysis of the architecture of the object of assessment in relation to possible violations of information security, information security risk assessment using the apparatus of the theory of fuzzy sets when considering the methodological approach to a comprehensive description of the object of information security with an assessment of its risks.*

Result: *proposed a comprehensive approach to assessing threats to the security of information. The assessment of the state of the protection object in case of violation of security is carried out with the help of particular integral index of security, which characterizes the possibility of inflicting damage in its implementation, according to which the ranking is made. On the basis of this methodical approach to complex description of the object of information protection with an assessment of its risks, using analysis of architecture of the object in application to possible violations of information security, and also making an assessment of risk using the apparatus of the theory of fuzzy sets is substantiated. This methodical approach is a formal tool for building private models and information security management system as a whole. On the basis of these models, it is possible to develop: methods of quantitative estimation of security; methods and approaches to the description of the factors influencing security; methods of security estimation of operating systems with use of the methodological approach to information systems security.*

Keywords: *information security, information system, information protection, information security threat, information protection object, assessment object, cyberspace.*

References

1. Koloskov, S. Strategija dejstvij ministerstva oborony SShA v kiberprostranstve / S. Koloskov // Zarubezhnoe voennoe obozrenie. - 2016. - № 10. - S. 3-7.
2. Batashov, V. Dejatel'nost' ministerstva oborony SShA po razvitiju novyh tehnologij v sfere kiberbezopasnosti / V.Batashov // Zarubezhnoe voennoe obozrenie. - 2018. - № 10. - S. 10-13.
3. Harris Sh. Kiber vojn@. Pjatyj teatr voennyh dejstvij – M.: Al'pina non-fikshn, 2016. - 390 s.

4 Sergey V. Kruglikov, Dr.Sc. (in Military), Director General of the State Scientific Institution "United Institute of Informatics Problems of the National Academy of Sciences of Belarus", Minsk, Belarus. E-mail: secretary_od@newman.bas-net.by

5 Sergey N. Kasanin, Ph.D. (in Tech.), Associate Professor, Deputy General Director for Research of the State Scientific Institution «United Institute of Informatics Problems of the National Academy of Sciences of Belarus», Minsk, Belarus. E-mail: kas.sv40@rambltr.ru

6 Yuri V. Kuleshov, Ph.D. (in Military), Associate Professor, Head of the Military Faculty at the Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus. E-mail: prcom@bsuir.by

4. Starodubcev Ju.I., Zakalkin P.V., Ivanov S.A. Mnogovektornyj konflikt v kiberprostranstve kak predposylka formirovanija novogo vida Vooruzhennyh Sil // Voennaja mysl'. 2021. № 12. S.126-135.
5. Bojko A.A. Boevaja jeffektivnost' kiberatak: analiticheskoe modelirovanie sovremennogo boja. Sistemy upravlenija, svjazi i bezopasnosti. 2020. N 4. S. 101-133.
6. Starodubcev Ju.I., Zakalkin P.V., Ivanov S.A. Tehnosfernaja vojna kak osnovnoj sposob razreshenija konfliktov v uslovijah globalizacii // Voennaja mysl'. 2020. № 10. S.16-21.
7. Tumar V.A., Levchuk N.N. Kiberprostranstvo kak sreda protivoborstva: voennyj aspekt i Belorusskij opyt normotvorchestva // Vestnik Akademii voennyh nauk. 2020. № 3 (72). S.43-49.
8. Volodenkov S.V. Internet-kommunikacii v global'nom prostranstve sovremennogo politicheskogo upravlenija. – M.: Izdatel'stvo Moskovskogo universiteta; Prospekt, 2018. 272 s., il.
9. Durnev R.A., Krjukov K.Ju., Deduchenko F.M. Preduprezhdenie tehnogennyh katastrof, provociruemyh v hode voennyh dejstvij // Voennaja mysl'. 2019. № 10. S. 41-48.
10. Zarudnickij V.B. Harakter i soderzhanie voennyh konfliktov v sovremennyh uslovijah i obozrimoj perspektive // Voennaja mysl'. 2021. № 1. S.34-44.
11. Birjukov D.N., Lomako A.G., Petrenko S.A. Porozhdenie scenariev preduprezhdenija komp'juternyh atak.Zashhita informacii. Insajd. 2017. N 4 (76). S. 70-79.
12. Drobotun E.B. Teoreticheskie osnovy postroenija sistem zashhity ot komp'juternyh atak dlja avtomatizirovannyh sistem upravlenija. Monografija. – SPb.: Naukoemkie tehnologii, 2017. – 120 s., il. ISBN 978-5-9909412-2-9.
13. Markov A.S. Tehnicheskie reshenija po realizacii podsistem GosSOPKA. V knige: Upravlenie informacionnoj bezopasnost'ju v sovremennom obshhestve. Sbornik nauchnyh trudov V Mezhdunarodnoj nauchno-prakticheskoj konferencii. 2017. S. 85-96.
14. Lauta O.S., Kocynjak M.A., Ivanov D.A., Gudkov M.A. Modelirovanie komp'juternyh atak na osnove metoda preobrazovanija stohasticheskih setej. V sbornike: Radiolokacija, navigacija, svjaz'. Sbornik trudov XXIV Mezhdunarodnoj nauchno-tehnicheskoj konferencii. V 5-i tomah. 2018. S. 137-146.
15. Jazov Ju.K. Organizacija zashhity informacii v informacionnyh sistemah ot nesankcionirovannogo dostupa: monografija / Ju.K. Jazov, S.V. Solov'ev. Voronezh: Kvarta, 2018. – 588 s.
16. Begaev A.N., Begaev S.N., Fedotov V.A. Testirovanie na proniknovenie. SPb.: Universitet ITMO, 2018. – 45 s.
17. Dorofeev A.V., Lemberskaja E.H., Rautkin Ju.V. Analiz zashhishhennosti: normativnaja baza, metodologii i instrumenty.Zashhita informacii. Insajd. 2018. N 4 (82). S. 63-69.
18. Makarenko S.I. Audit bezopasnosti kriticheskoj infrastruktury special'nymi informacionnymi vozdejstvijami. Monografija. – SPb.: Naukoemkie tehnologii, 2018. – 122 s.
19. Kocynjak M.A., Lauta O.S., Ivanov D.A. Matematicheskaja model' targetirovannoj komp'juternoj ataki.Naukoemkie tehnologii v kosmicheskih issledovanijah Zemli. 2019. T. 11. N 2. S. 73–81. DOI: 24411/2409-5419-2018-10261.
20. Dergunov I.Ju., Zima V.M., Glybovskij P.A., Mazhnikov P.V. Model' processa intellektual'nogo testirovanija AS na proniknovenie s uchetom vremennyh parametrov.Zashhita informacii. Insajd. 2020. N 5 (95). S. 64-67.
21. Zhilenkov A.A., Chernyj S.G. Sistema bezavarijnogo upravlenija kriticheski vazhnymi ob#ektami v uslovijah kiberneticheskih atak // Voprosy kiberbezopasnosti. 2020. № 2 (36). S. 58-66. DOI:10.21681/2311-3456-2020-2-58-66.
22. Kotenko I.V., Kribel' A.M., Lauta O.S., Saenko I.B. Analiz processa samopodobija setevogo trafika kak podhod k obnaruzheniju kiberatak na komp'juternye seti // Jelektrosvjaz'. 2020. № 12. S.54-59. DOI:10.34832/ELSV.2020.13.12.008.
23. Bochkov S.I., Makarenko G.I., Fedichev A.V. Ob okinavskoj hartii global'nogo informacionnogo obshhestva i zadachah razvitija rossijskih sistem kommunikacii // Pravovaja informatika. 2018. № 1. S. 4-14. DOI: 10.21681/1994-1404-2018-1-04-14
24. Romashkina N.P. Global'nye voenno-politicheskie problemy mezhdunarodnoj informacionnoj bezopasnosti: tendencii, ugrozy, perspektivy // Voprosy kiberbezopasnosti. 2019. № 1(29). S. 2-8. DOI: 10.21681/2311-3456-2019-1-2-9.
25. Karchija A.A., Makarenko G.I., Sergin M.Ju. Sovremennye trendy kiberugroz i transformacija ponjatija kiberbezopasnosti v uslovijah cifrovizacii sistemy prava // Voprosy kiberbezopasnosti. 2019. № 3 (31). S. 18-23. DOI: 10.21681/2311-3456- 2019-3-18-23.
26. Romashkina N.P., Markov A.S., Stefanovich D.V. Mezhdunarodnaja bezopasnost', strategicheskaja stabil'nost' i informacionnye tehnologii: Monografija / N.P. Romashkina, A.S. Markov, D.V. Stefanovich. – Moskva, 2020. Ser. Biblioteka Nacional'nogo issledovatel'skogo instituta mirovoj jekonomiki i mezhdunarodnyh otnoshenij imeni E.M. Primakova. – 98 s. il.
27. Kuleshov, Ju.E., Paskrobka, S.I., Sergienko, V.A., Kasanin, S.N. Metodicheskij podhod k ocenke verojatnostej realizacii ugroz bezopasnosti informacii/ Ju.E. Kuleshov, S.I. Paskrobka, V.A. Sergienko, S.N. Kasanin // Nauchno-proizvodstvennyj zhurnal «Vesnik suvjazi». - 2017. - №5. - S. 56-59.