ФОРМАЛИЗОВАННАЯ РИСК-ОРИЕНТИРОВАННАЯ МОДЕЛЬ СИСТЕМЫ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Аносов Р.С.[1], Аносов С.С.[2], Шахалов И.Ю.[3]

Аннотация. *Целью исследования является систематизация принципов построения информационных технологий, существенных с точки зрения оценки информационных рисков, и формирование на этой основе модели, обеспечивающей возможность анализа факторов риска при построении защищенных информационных систем.*

Метод исследования: *использовался теоретический аппарат теории игр и теории множеств.*

Полученный результат. *Предложена модель, ориентированная на учет конфликтного характера взаимодействия информационных технологий и источников угроз безопасности информации.*

Система информационных технологий рассмотрена как взаимосвязанная совокупность технологий противоборствующих сторон, обеспечивающая процессы практической деятельности одной из них, что позволяет на единой методической основе анализировать уязвимости информационных технологий, сценарии реализации угроз, а также выполнять оптимизацию технологических решений по защите информации.

Модель характеризуется высокой степенью обобщения, так как ее основными элементами являются абстрактные сущности: множество используемых сторонами информационных технологий; множества информационных операций, реализуемых отдельными технологиями; информационные и управляющие отношения на множествах технологий и операций. Для использования модели требуется предварительная проработка состава и характеристик этих множеств и отношений применительно к конкретным информационным технологиям.

Ключевые слова: *информационный конфликт, информационные операции, информационный риск, компьютерная архитектура, сетевая архитектура, факторы риска.*

DOI:10.21681/2311-3456-2020-05-69-76

Введение

Система информационных технологий представляет собой сложную систему [1,2], образованную множеством программно-алгоритмических и аппаратно-физических технологий, реализующих обработку информации на различных уровнях абстрагирования – от цифрового до прикладного [3]. Разнообразие и масштабируемость информационных технологий обусловливают высокую сложность задачи оценки информационных рисков, подходом к преодолению которой является построение модели, формализующей отношения между информационными технологиями различных уровней и обеспечивающей единую методическую основу для исследования угроз безопасности информации, с одной стороны, и процессов практической деятельности – с другой (рисунок 1).

Связь модели информационных технологий с моделью угроз обеспечивается на основе формализации уязвимостей технологий различных уровней, уязвимостей среды их функционирования, а также уязвимостей, проявляющихся в сферах организации, менеджмента, персонала автоматизированной системы. Связь модели информационных технологий с моделью практической деятельности осуществляется посредством формальных параметров технологий прикладного уровня, интегрирующих в себе технологии других уровней и обеспечивающих решение практических задач, к числу которых могут быть отнесены:

- непосредственное управление процессами практической деятельности (в автоматизированных системах управления);
- формирование рекомендаций лицу, принимающему решение (в системах поддержки принятия решений, экспертных системах);
- предоставление информационных и телекоммуникационных сервисов (в автоматизированных системах, обеспечивающих операционную деятельность).

Модель системы информационных технологий является, таким образом, средством анализа факторов риска, к числу которых могут быть отнесены информационные активы, их уязвимости, угрозы информационной безопасности и ущерб, связанный с реализацией угроз [4]. Подобные риск-ориентированные модели могут быть построены на основе структурного анализа потоков данных в информационной системе, в процессе которого формализуются факторы риска [5], с применени-

1 Аносов Роман Сергеевич, кандидат технических наук, доцент, Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия имени профессора Н.Е. Жуковского и Ю.А. Гагарина», г. Воронеж, Россия. E-mail: an_rs@list.ru

2 Аносов Сергей Сергеевич, начальник отдела, государственное унитарное предприятие «Научно-технический центр «Заря», г. Москва, Россия. E-mail: serg-anosov@mail.ru

3 Шахалов Игорь Юрьевич, доцент МГТУ им. Н.Э. Баумана, Акционерное общество «Научно-производственное объединение «Эшелон», г. Москва, Россия. E-mail: i-shahalov@npo-echelon.ru

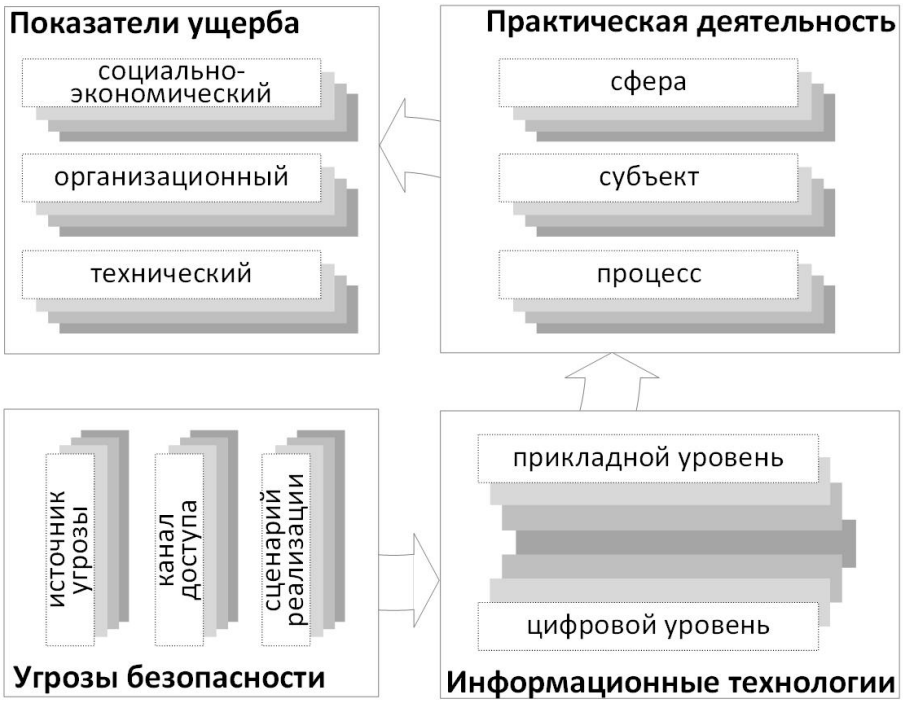

Рис.1. Схема оценки информационного риска

ем методов нейро-нечетких сетей, позволяющего учесть неоднозначность и неполноту информации о факторах риска [6], или методов системной динамики, направленных на исследование поведения сложных систем во времени [7]. К числу классических следует также отнести модели, построенные с применением математического аппарата сетей Петри-Маркова, обеспечивающего учет параллелизма процессов реализации информационных угроз [8], и имитационные модели [9].

В работе [10] рассмотрен комплекс математических моделей, базирующихся на построении вероятностного пространства (Ω, B, P), где Ω – конечное пространство элементарных событий, B – класс всех подмножеств множества Ω, удовлетворяющий свойствам сигма-алгебры, P – вероятностная мера на пространстве элементарных событий. Комбинирование этих элементарных моделей в параллельно-последовательные структуры открывает принципиальную возможность вероятностного моделирования системы произвольной степени сложности и расчета показателей риска в реальном времени. В работе [11] рассмотрен аппаратно-программный комплекс сценарного моделирования развития сложных ситуаций на основе исследования их когнитивных карт. Особенностью метода когнитивного моделирования является использование лингвистических переменных и нечетких алгоритмов для эффективного исследования поведение сложных систем, не поддающихся точному математическому анализу.

Анализ подходов, методов и моделей, разрабатываемых в целях оценки информационных рисков, позволяет, по нашему мнению, выделить следующие актуальные направления исследований в данной области. Во-первых, углубляется горизонт прогнозирования рисков и повышается принимаемый во внимание уровень рефлексии в информационном конфликте «источник угрозы – средство защиты», что ведет к возможности качественного повышения эффективности процессов управления информационной безопасностью. Во-вторых, развиваются методические подходы, ориентированные на оценку рисков в реальном времени и снижение времени реакции системы управления рисками, что позволяет рассматривать в качестве инструмента управления рисками как архитектуру системы защиты информации, так и ее более «подвижные» аспекты – конфигурацию, политики безопасности, режимы работы. В-третьих, наряду с экспертно-эвристическими методами, соответствующими системному характеру задачи оценки рисков, все большее значение приобретают методы математического моделирования, характеризующиеся потенциально значительно более высоким уровнем объективности и точности. Эти направления, внешне являясь самостоятельными, базируются на единой концептуальной основе – детальной структурно-функциональной формализации информационных технологий и их отношений в составе автоматизированных систем различного класса и назначения. Последовательное обобщение таких формальных структурно-функциональных моделей позволяет привести к единой методической основе различные методы, применяемые в практике оценки риска, и увязать их в единую многофункциональную информационно-аналитическую систему оценки рисков.

Поиск такой методической базы, выполняемый на основе построения формализованной риск-ориентированной модели системы информационных технологий, учитывающей конфликтную природу факто-

ров информационного риска [12] и ориентированной на учет технологических принципов обработки информации, является целью настоящей работы.

Основная часть

Субъекты практической деятельности A и нарушители безопасности информации (источники угроз) B образуют в совокупности систему, которая определяется множеством состояний $\boldsymbol{S} = \{\boldsymbol{S}_A, \boldsymbol{S}_B\}$. Состояния системы характеризуются:

- множеством значений показателей назначения $\boldsymbol{S}_A^+$ и показателей ресурсоемкости деятельности $\boldsymbol{S}_A^-$ субъектов A: $\boldsymbol{S}_A = \{\boldsymbol{S}_A^+, \boldsymbol{S}_A^-\}$;
- множеством $\boldsymbol{S}_B$ значений характеристик нарушителей (их возможности, мотивация) и иных источников угроз безопасности информации.

Стратегии сторон A и B заключаются в применении множеств информационных технологий, $\boldsymbol{T}_A$ и $\boldsymbol{T}_B$ соответственно. Цель стороны A – реализовать множество технологий $\boldsymbol{T}_A^*$:

$$\boldsymbol{T}_A^* = arg\left(\max_{\boldsymbol{T}_A} \boldsymbol{S}_A^+(\boldsymbol{T}_A, \boldsymbol{T}_B) \,\&\, \left(\boldsymbol{S}_A^-(\boldsymbol{T}_A, \boldsymbol{T}_B) \subseteq \boldsymbol{S}_{\text{доп}}^-\right)\right)$$

или

$$\boldsymbol{T}_A^* = arg\left(\min_{\boldsymbol{T}_A} \boldsymbol{S}_A^-(\boldsymbol{T}_A, \boldsymbol{T}_B) \,\&\, \left(\boldsymbol{S}_A^+(\boldsymbol{T}_A, \boldsymbol{T}_B) \subseteq \boldsymbol{S}_{\text{доп}}^+\right)\right),$$

где $\boldsymbol{S}_{\text{доп}}^-$ – множество значений показателей $\boldsymbol{S}_A^-$, при которых остаточный риск стороны A не превышает допустимого значения; $\boldsymbol{S}_{\text{доп}}^+$ – множество минимально допустимых (с точки зрения практической деятельности) значений показателей назначения $\boldsymbol{S}_A^+$.

Сторона A использует информационные технологии $\boldsymbol{T}_A^c$ для обеспечения практической деятельности, технологии $\boldsymbol{T}_A^r$ – для выявления (обнаружения) угроз безопасности, технологии $\boldsymbol{T}_A^d$ – для пассивной защиты (снижения риска) и технологии $\boldsymbol{T}_A^a$ – для активной защиты (предупреждения инцидентов): $\boldsymbol{T}_A = \{\boldsymbol{T}_A^c, \boldsymbol{T}_A^r, \boldsymbol{T}_A^d, \boldsymbol{T}_A^a\}$. Сторона B использует информационные технологии $\boldsymbol{T}_B^r$ для исследования (разведки) технологий стороны A и технологии $\boldsymbol{T}_B^a$ – для реализации угроз безопасности (атак) в отношении технологий стороны A: $\boldsymbol{T}_B = \{\boldsymbol{T}_B^r, \boldsymbol{T}_B^a\}$ (рисунок 2). Типовые защитные технологии стороны A приведены в таблице 1.

В рассмотренной постановке задача управления рисками заключается в оптимизации системы технологий стороны A при заданной системе технологий $\boldsymbol{T}_B$. Задача приобретает игровой характер, если сторона B является не пассивным участником, а имеет цель максимизировать ущерб (минимизировать выигрыш) стороны A:

$$\boldsymbol{T}_B^* = arg\left(\max_{\boldsymbol{T}_B} \boldsymbol{S}_A^-(\boldsymbol{T}_A, \boldsymbol{T}_B)\right)$$

или

$$\boldsymbol{T}_B^* = arg\left(min_{\boldsymbol{T}_B} \boldsymbol{S}_A^+(\boldsymbol{T}_A, \boldsymbol{T}_B)\right).$$

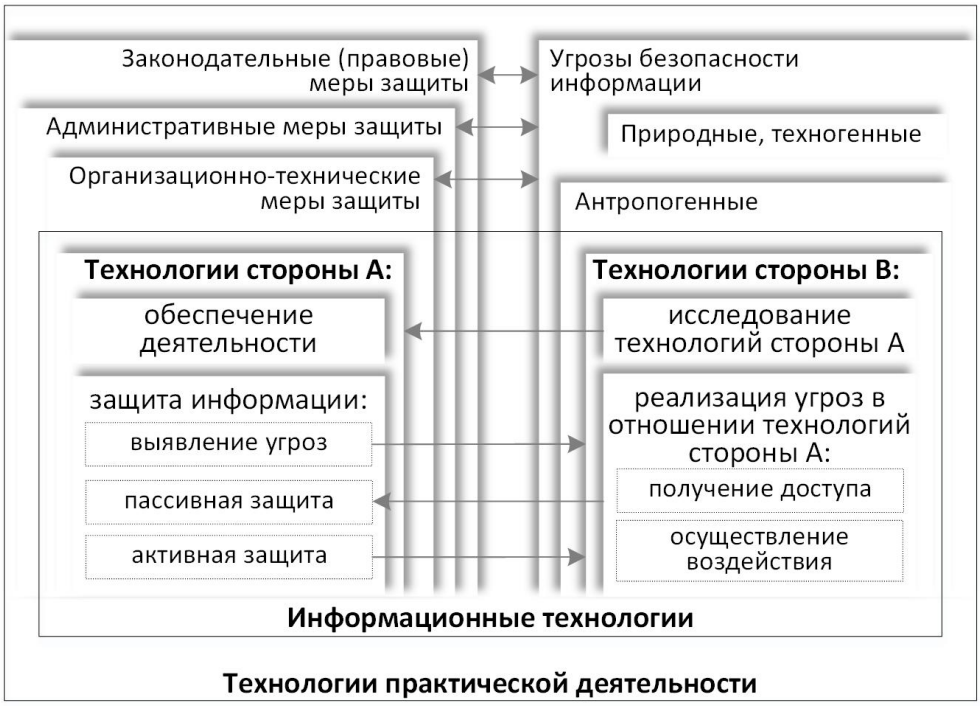

Рис.2. Структура информационного конфликта сторон A и B в контексте практической деятельности

DOI:10.21681/2311-3456-2020-05-69-76

Таблица 1

Система защитных технологий стороны $\{\Sigma_U, \Sigma_R\} \to (S, P)$

Область применения	Вид мер защиты	Типовые меры защиты
Технологии практической деятельности	Законодательные (правовые)	Ограничительные
		Координирующие
	Административные	Политика информационной безопасности
		Управление персоналом
		Управление рисками
	Организационно-технические	Физическая безопасность
		Техническая безопасность
Информационные технологии	Программно-технические	Управление доступом
		Антивирусная защита
		Обнаружение вторжений (целевых атак)
		Управление событиями безопасности
		Предотвращение утечек информации
		Контроль (анализ) защищенности
		Криптографическая защита
		Обеспечение доступности информации

Дальнейшее обобщение этой задачи может осуществляться в направлении формализации процессов управления информационной безопасностью [13] с применением методов теории динамических (многошаговых) игр [14,15].

В результате конфликтного взаимодействия сторон на уровне информационных технологий система практической деятельности переходит в новое состояние, что может быть представлено отображением $\{T_A, T_B\} \to (S, P)$, где P – вероятностная мера на множестве состояний S. Тогда информационный риск R стороны A определяется отображением $(S, P) = (\{\{S_A^+, S_A^-\}, S_B\}, \{P_A^+, P_A^-, P_B\}) \to R = f_R(S_A^-, P_A^-)$, где P_A^+, P_A^-, P_B – вероятностные меры на множествах S_A^+, S_A^-, S_B соответственно, f_R – операция отображения множества значений ресурсоемкости (потенциального ущерба) S_A^- стороны A и вероятностной меры P_A^- на этом множестве в область значений риска R. Связь риска со стратегиями сторон T_A и T_B устанавливается, таким образом, композицией отображений $\{T_A, T_B\} \to (S, P) \to R$. С целью определения структуры отображения $\{T_A, T_B\} \to (S, P)$, являющегося базовым с точки зрения оценки информационных рисков, выполним декомпозицию системы информационных технологий.

1. Понятие технологии связано с понятием уровня абстрагирования компьютерной и сетевой архитектуры: технологию $T_j, j \in \mathbb{N}$, , образует множество информационных операций, реализуемых «внутри» одного уровня абстрагирования (рисунок 3).

Такое определение соответствует принципу построения вычислительных систем, в которых каждый уровень компьютерной архитектуры может быть представлен виртуальной машиной, взаимодействующей с виртуальной машиной соседнего уровня посредством программной или аппаратной интерпретации (трансляции) команд (инструкций). Аналогичный принцип применяется при построении коммуникационных технологий, в которых каждый уровень сетевой архитектуры предоставляет сервисы для вышестоящего уровня посредством стандартизованных интерфейсов (программных или аппаратных). Верхний уровень системы информационных технологий образован прикладными технологиями.

2. Отдельные технологии стороны A, $T_A = \{T_i^A, i = \overline{1, N_A}\}$, и стороны B, $T_B = \{T_i^B, i = \overline{1, N_B}\}$, образуют систему технологий $T_j \in T = \{T_A, T_B\}$ и представляются конечным множеством информационных операций $O_j = \{O_{ji}, i = \overline{1, M_j}\}$ и заданными на этом множестве отношениями (рисунок 4):

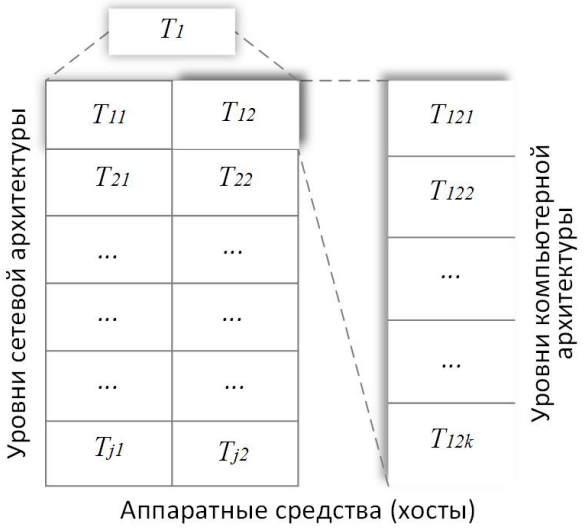

Рис.3. Структура системы информационных технологий (технологии с большей размерностью составного индекса вложены в технологии с меньшей размерностью индекса)

- информационным отношением Ξ_j^O, определяющим порядок передачи данных между последовательно выполняемыми операциями (взаимосвязь операций по входам и выходам);
- управляющим отношением Φ_j^O, определяющим порядок передачи управления от одной операции к другой (зависимость инструкции одной операции от результата выполнения другой).

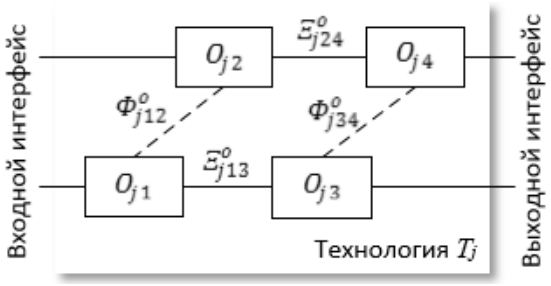

Рис. 4. Пример элементарной информационной технологии

Представление технологий в такой форме, $T_j = \{\boldsymbol{O}_j, \Xi_j^O, \Phi_j^O\}$, отражает функционально-алгоритмический аспект технологий как процессов и методов обработки информации и может быть средством анализа потоков данных в информационной системе.

3. Компьютерная архитектура характеризуется совокупностью преобразований технологий, записанных на языке верхнего уровня (прикладном языке), в технологии, реализованные на языках нижележащих уровней, вплоть до машинного языка. Такие преобразования описываются композицией соответствий (неоднозначных отображений) [16] $F_{i,j}: T_i \to T_j$, в которых мощность множества-образа $\boldsymbol{O}_j$ превышает мощность множества-прообраза $\boldsymbol{O}_i$: $F_{1,k} = F_{1,2} \circ F_{2,3} \circ \ldots \circ F_{k-1,k}$. В обозначениях, принятых на рисунке 3, такая композиция может быть записана в следующей форме: $(T_{121} \to T_{122}) \circ (T_{122} \to T_{123}) \circ \ldots \circ (T_{12k-1} \to T_{12k})$ (рисунок 5). Вид соответствий $F_{i,j}$ и, в частности, мощность множеств $\boldsymbol{O}_i$ и $\boldsymbol{O}_j$, определяется программно-аппаратной архитектурой платформы, на которой реализуются информационные технологии.

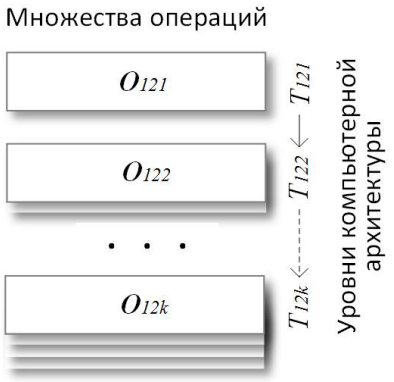

Рис. 5. Преобразование технологий компьютерной архитектуры (обозначения аналогичны рисунку 3)

4. Функциональное взаимодействие отдельных информационных технологий из множества $\boldsymbol{T}$ в рамках системы осуществляется посредством программных и аппаратных интерфейсов, формализуется информационным отношением Ξ^T, заданным на множестве $\boldsymbol{T}$ и определяющим порядок предоставления сервисов (выполнения запросов). Наглядно такое взаимодействие может быть проиллюстрировано на примере модели сетевых протоколов (рисунок 6).

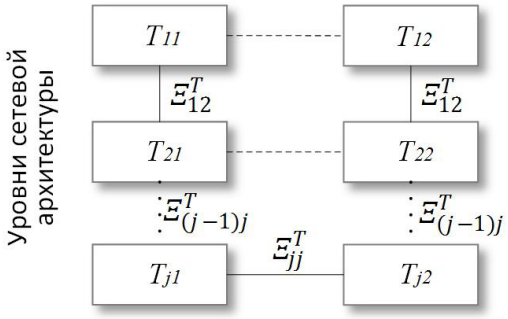

Рис. 6. Схема информационных отношений между технологиями (обозначения технологий аналогичны рисунку 1, штриховыми горизонтальными линиями показаны виртуальные отношения)

5. Множество информационных технологий разбивается на подмножества технологий $\boldsymbol{T} = \{\{T_i, \ldots\}, \ldots, \{T_j, \ldots\}\} = \{\boldsymbol{Tr}_i, i \in \mathbb{N}\}$, использующих общие вычислительные или коммуникационные ресурсы. Характерными примерами совместного использования ресурсов является механизм параллельного выполнения нескольких вычислительных процессов (потоков) на одной аппаратной платформе, передача данных по одному физическому каналу, хранение информации в одной области памяти (на одном носителе). Совместное использование ресурсов приводит к возникновению нефункциональных связей между технологиями, которые формально описываются информационным $\bar{\Xi}_{ij}^O$ и управляющим $\bar{\Phi}_{ij}^O$ отношениями на множествах операций $\boldsymbol{O}_i$ и $\boldsymbol{O}_j$ технологий T_i и T_j из некоторого подмножества $\boldsymbol{Tr}_k$ технологий, использующих общие ресурсы, и информационным отношением $\bar{\Xi}^T$ на этом подмножестве (рисунок 7).

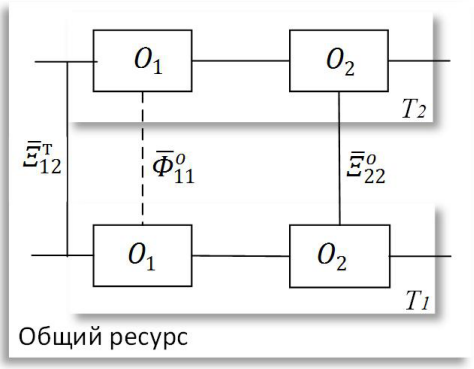

Рис. 7. Нефункциональные отношения между технологиями через общий ресурс

DOI:10.21681/2311-3456-2020-05-69-76

Таким образом, система информационных технологий характеризуется множеством параметров Σ, включающим:

- множество используемых технологий $\boldsymbol{T}$;
- множество операций $\boldsymbol{O_i}$, реализуемых технологией T_i;
- информационное Ξ_j^O и управляющее Φ_j^O отношения на множестве операций $\boldsymbol{O_j}$ технологии T_j;
- соответствие $F_{i,j}$ из множества операций $\boldsymbol{O_i}$ технологии T_i в множество операций $\boldsymbol{O_j}$ технологии T_j, реализуемое в контексте компьютерной архитектуры;
- информационное отношение Ξ^T на множестве технологий системы;
- информационное отношение $\bar{\Xi}^T$ на подмножестве технологий, обусловленное непредусмотренными связями технологий через совместно используемые ресурсы, $\bar{\Xi}^T \bigcap \Xi^T = \varnothing$;
- информационное $\bar{\Xi}_{ij}^O$ и управляющее $\bar{\Phi}_{ij}^O$ отношения на множествах операций $\boldsymbol{O_i}$ и $\boldsymbol{O_j}$, обусловленные непредусмотренными связями технологий T_i и T_j через совместно используемые ресурсы.

Множество $\Sigma = \{\Sigma_U, \Sigma_R\}$ состоит из двух подмножеств, первое из которых, Σ_U, образуют функциональные параметры, обеспечивающие реализацию декларированного стороной A назначения технологий $\boldsymbol{T_A}$, а второе подмножество, Σ_R, образуют факторы риска, включающие:

- элементы множества параметров Σ, непосредственно не связанные с реализацией назначения технологий $\boldsymbol{T_A}$ (нефункциональные параметры);
- элементы множества Σ, относящиеся к технологиям $\boldsymbol{T_B}$ стороны B.

Подмножество факторов риска Σ_R представляет собой формальную модель угроз и характеризуется высокой размерностью (большим числом степеней свободы). На практике комбинации факторов риска из подмножества Σ_R, существенные с точки зрения потенциального ущерба декларированному назначению технологий $\boldsymbol{T_A}$, систематизируются в форме банков данных угроз и уязвимостей. При этом система информационных технологий $\boldsymbol{T_A}$ может считаться защищенной, если при ее создании приняты во внимание все факторы риска из подмножества Σ_R, имеющие соответствие в банке данных.

Заключение

В процессе декомпозиции системы информационных технологий сформировано множество ее параметров $\Sigma = \{\Sigma_U, \Sigma_R\}$, позволяющее записать в эквивалентной форме отображение множества применяемых сторонами A и B информационных технологий в множество состояний системы практической деятельности $\{\boldsymbol{T_A}, \boldsymbol{T_B}\} \to (\boldsymbol{S}, \boldsymbol{P})$: $\{\Sigma_U, \Sigma_R\} \to (\boldsymbol{S}, \boldsymbol{P})$, где $\boldsymbol{P}$ – вероятностная мера на множестве состояний $\boldsymbol{S}$. Эквивалентная запись оптимальной стратегии стороны A, предполагающей реализацию множества технологий $\boldsymbol{T_A^*}$ с параметрами Σ_U^* при заданном множестве факторов риска Σ_R, будет иметь вид:

$$\Sigma_U^* = arg\left(\max_{\Sigma_U} \boldsymbol{S}_A^+(\Sigma_U, \Sigma_R) \,\&\, \left(\boldsymbol{S}_A^-(\Sigma_U, \Sigma_R) \subseteq \boldsymbol{S}_{\text{доп}}^-\right)\right)$$

Параметрическое представление системы информационных технологий в виде множества Σ позволяет решать задачу поиска параметров Σ_U^*, обеспечивающих нейтрализацию недопустимых информационных рисков практической деятельности, с применением эвристических методов дискретной оптимизации [17]. В ходе решения этой задачи реализуются стандартные этапы оценки рисков (таблица 2 [18,19]):

- идентификация рисков с целью содержательного наполнения абстрактных параметров, образующих множество Σ;
- анализ рисков (задача $\{\Sigma_U, \Sigma_R\} \to (\boldsymbol{S}, \boldsymbol{P})$) с применением качественных методов (анализ на высоком уровне обобщения) или количественных методов (детальный анализ);
- оценка значимости рисков с применением критериев оценивания (задача $(\boldsymbol{S}, \boldsymbol{P}) \to R$).

Таблица 2

Этапы оценки (моделирования) риска (risk assessment)

Наименование этапа	Наименование мероприятий
Идентификация риска (risk identification)	Идентификация активов (identification of assets)
	Идентификация угроз (identification of threats)
	Идентификация мер защиты информации (средств управления рисками) (identification of existing controls)
	Идентификация уязвимостей (identification of vulnerabilities)
	Идентификация последствий (identification of consequences)

Наименование этапа	Наименование мероприятий
Анализ риска (risk analysis)	Оценка последствий инцидентов (assessment of consequences)
	Оценка вероятности инцидентов (assessment of incident likelihood)
	Установление значения (величины) риска (risk estimation), оценка (определение) уровня риска (level of risk determination), количественная оценка рисков
Оценка (определение) значимости (оценивание) риска (risk evaluation)	Применение критериев оценивания рисков (risk evaluation criteria)

При оценке рисков на основе множества параметров системы информационных технологий $\{\Sigma_U, \Sigma_R\}$ определяются оба основных фактора риска: величина потенциального ущерба (ресурсоемкости) $\boldsymbol{S}_A^-$ и вероятностная мера его возникновения $\boldsymbol{P}_A^-$. Количественное значение ущерба может быть определено либо непосредственно на основе вложения модели системы информационных технологий в модель практической деятельности (отображение $\{\Sigma_U, \Sigma_R\} \to (\boldsymbol{S}_A^-, \boldsymbol{P}_A^-)$), либо опосредованно на основе введения промежуточного множества Ψ^* показателей, характеризующих эффективность системы информационных технологий (композиция отображений $\{\Sigma_U, \Sigma_R\} \to \Psi^* \to (\boldsymbol{S}_A^-, \boldsymbol{P}_A^-)$). Вероятностный характер потенциального ущерба обусловлен вероятностным характером факторов риска Σ_R и влиянием случайных природных и техногенных факторов.

Литература

1. Бусленко Н.П., Калашников В.В., Коваленко И.Н. Лекции по теории сложных систем. М.: Советское радио, 1973. 440 с.
2. Месарович М., Такахара Я. Общая теория систем: математические основы. М.: Мир, 1978. 312 с.
3. Цветков В.Я. Основы теории сложных систем. СПб.: Лань, 2019. 152 с.
4. Аникин И.В., Емалетдинова Л.Ю., Кирпичников А.П. Методы оценки и управления рисками информационной безопасности в корпоративных информационных сетях // Вестник технологического университета. 2015. Т. 18. № 6. С. 195-197.
5. Миков Д.А. Анализ методов и средств, используемых на различных этапах оценки рисков информационной безопасности // Вопросы кибербезопасности. 2014. № 4(7). С. 49-54.
6. Glushenko S.A. An adaptive neuro-fuzzy inference system for assessment of risks to an organization's information security. Business Informatics, 2017, no. 1(39), pp. 68-77. DOI: 10.17323/1998-0663.2017.1.68.77.
7. Минаев В.А., Сычев М.П., Вайц Е.В., Грачева Ю.В. Риск-ориентированный подход к моделированию процесса противодействия угрозам информационной безопасности // Вопросы радиоэлектроники. 2017. № 6. С. 83-92.
8. Радько М.Н., Скобелев И.О. Риск-модели информационно-телекоммуникационных систем при реализации угроз удаленного и непосредственного доступа. М.: РадиоСофт, 2010. 232 с.
9. Емельянов А.А. Имитационное моделирование в управлении рисками. СПб.: Инжэкон, 2000. 375 с.
10. Костогрызов А.И., Зубарев И.В. Моделирование процессов для эффективного управления рисками в обеспечение качества и безопасности функционирования современных и перспективных систем реального времени // Радиопромышленность. 2017. № 2. С. 91-100. DOI: 10.21778/2413-9599-2017-2-91-100.
11. Костогрызов А.И., Лазарев В.М., Любимов А.Е. Прогнозирование рисков для обеспечения эффективности систем информационной безопасности в их жизненном цикле // Правовая информатика. 2013. № 4. С. 4-16.
12. Юрьев В.Н. Игровой подход к оценке риска и формированию бюджета информационной безопасности предприятия // Прикладная информатика. 2015. Том. 10. № 2(56). С. 121-126.
13. Курило А.П., Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. Основы управления информационной безопасностью. М.: Горячая линия-Телеком, 2019. 244 с.
14. Петросян Л.А., Зенкевич Н.А., Шевкопляс Е.В. Теория игр. СПб.: БХВ-Петербург, 2012. 432 с.
15. Челноков А.Ю. Теория игр. М.: Юрайт, 2018. 223 с.
16. Белоусов А.И., Ткачев С.Б. Дискретная математика. М.: Изд-во МГТУ им. Н.Э. Баумана, 2004. 744 с.
17. Зуев Ю.А. Современная дискретная математика: от перечислительной комбинаторики до криптографии XXI века. М.: Ленанд, 2019. 720 с.
18. Петренко С.А., Симонов С.В. Управление информационными рисками. Экономически оправданная безопасность. М.: ДМК Пресс, 2004. 400 с.
19. Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. Управление рисками информационной безопасности. М.: Горячая линия-Телеком, 2019. 130 с.

FORMALIZED RISK-ORIENTED MODEL OF THE INFORMATION TECHNOLOGY SYSTEM

Anosov R.S.[4], Anosov S.S.[5], Shakhalov I.Yu.[6]

Abstract. *The aim of the study is to systematize the principles of building information technologies that are essential from the point of view of information risk assessment, and to form, on this basis, a model that provides the ability to analyze risk factors when building secure information systems.*

Methods: *when developing the model, the methods of game theory and set theory were used.*

The result: *the model is focused on taking into account the conflicting nature of interaction between information technologies and sources of threats to information security*

The information technology system is considered as an interconnected set of technologies of the warring parties, providing the processes of practical activity of one of them, which allows, on a unified methodological basis, to analyze the vulnerabilities of information technologies, scenarios for the implementation of threats, as well as to optimize technological solutions for information protection.

The model is characterized by a high degree of generalization, since its main elements are abstract entities: a set of information technologies used by the parties; sets of information operations, implemented by technologies; information and control relationships on sets of technologies and operations. To use the model requires a preliminary development of the list and characteristics of these sets and relations in relation to specific information technologies.

Keywords: *information conflict, information operations, information risk, computer architecture, network architecture, risk factors.*

References

1. Buslenko N.P., Kalashnikov V.V., Kovalenko I.N. Lekcii po teorii slozhnyh sistem. M.: Sovetskoe radio, 1973. 440 s.
2. Mesarovich M., Takahara YA. Obshchaya teoriya sistem: matematicheskie osnovy. M.: Mir, 1978. 312 s.
3. Cvetkov V.YA. Osnovy teorii slozhnyh sistem. SPb.: Lan', 2019. 152 s.
4. Anikin I.V., Emaletdinova L.YU., Kirpichnikov A.P. Metody ocenki i upravleniya riskami informacionnoj bezopasnosti v korporativnyh informacionnyh setyah // Vestnik tekhnologicheskogo universiteta. 2015. T. 18. № 6. S. 195-197.
5. Mikov D.A. Analiz metodov i sredstv, ispol'zuemyh na razlichnyh etapah ocenki riskov informacionnoj bezopasnosti // Voprosy kiberbezopasnosti. 2014. № 4(7). S. 49-54.
6. Glushenko S.A. An adaptive neuro-fuzzy inference system for assessment of risks to an organization's information security. Business Informatics, 2017, no. 1(39), pp. 68-77. DOI: 10.17323/1998-0663.2017.1.68.77.
7. Minaev V.A., Sychev M.P., Vajc E.V., Gracheva YU.V. Risk-orientirovannyj podhod k modelirovaniyu processa protivodejstviya ugrozam informacionnoj bezopasnosti // Voprosy radioelektroniki. 2017. № 6. S. 83-92.
8. Rad'ko M.N., Skobelev I.O. Risk-modeli informacionno-telekommunikacionnyh sistem pri realizacii ugroz udalennogo i neposredstvennogo dostupa. M.: RadioSoft, 2010. 232 s.
9. Emel'yanov A.A. Imitacionnoe modelirovanie v upravlenii riskami. SPb.: Inzhekon, 2000. 375 s.
10. Kostogryzov A.I., Zubarev I.V. Modelirovanie processov dlya effektivnogo upravleniya riskami v obespechenie kachestva i bezopasnosti funkcionirovaniya sovremennyh i perspektivnyh sistem real'nogo vremeni // Radiopromyshlennost'. 2017. № 2. S. 91-100. DOI: 10.21778/2413-9599-2017-2-91-100.
11. Kostogryzov A.I., Lazarev V.M., Lyubimov A.E. Prognozirovanie riskov dlya obespecheniya effektivnosti sistem informacionnoj bezopasnosti v ih zhiznennom cikle // Pravovaya informatika. 2013. № 4. S. 4-16.
12. YUr'ev V.N. Igrovoj podhod k ocenke riska i formirovaniyu byudzheta informacionnoj bezopasnosti predpriyatiya // Prikladnaya informatika. 2015. Tom. 10. № 2(56). S. 121-126.
13. Kurilo A.P., Miloslavskaya N.G., Senatorov M.YU., Tolstoj A.I. Osnovy upravleniya informacionnoj bezopasnost'yu. M.: Goryachaya liniya-Telekom, 2019. 244 s.
14. Petrosyan L.A., Zenkevich N.A., SHevkoplyas E.V. Teoriya igr. SPb.: BHV-Peterburg, 2012. 432 s.
15. CHelnokov A.YU. Teoriya igr. M.: YUrajt, 2018. 223 s.
16. Belousov A.I., Tkachev S.B. Diskretnaya matematika. M.: Izd-vo MGTU im. N.E.Baumana, 2004. 744 s.
17. Zuev YU.A. Sovremennaya diskretnaya matematika: Ot perechislitel'noj kombinatoriki do kriptografii XXI veka. M.: Lenand, 2019. 720 s.
18. Petrenko S.A., Simonov S.V. Upravlenie informacionnymi riskami. Ekonomicheski opravdannaya bezopasnost'. M.: DMK Press, 2004. 400 s.
19. Miloslavskaya N.G., Senatorov M.YU., Tolstoj A.I. Upravlenie riskami informacionnoj bezopasnosti. M.: Goryachaya liniya-Telekom, 2019. 130 s.

4 Roman Anosov, Ph.D., Associate Professor, Military Training and Scientific Center of the Air Force «Air Force Academy named after Professor N.E. Zhukovsky and Yu.A. Gagarin», Voronezh, Russia. E-mail: an_rs@list.ru

5 Sergey Anosov, Head of department of Federal State Unitary Enterprise «Scientific and Technical Center «Zarya», Moscow, Russia. E-mail: serg-anosov@mail.ru

6 Igor Shakhalov, Associate Professor of Bauman Moscow State Technical University, Scientific-Production Association Echelon Joint-Stock Company, Moscow, Russia. E-mail: i-shahalov@npo-echelon.ru