КОНЦЕПТУАЛЬНАЯ МОДЕЛЬ АНАЛИЗА РИСКА БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

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

Аннотация. *Целью исследования является обобщение и структуризация процессов, определяющих уровень риска информационной безопасности субъекта социально-экономической деятельности.*

Концептуальная модель разработана на основе:

- *анализа процесса деятельности субъекта и декомпозиции ее на отдельные состояния в пространстве эффектов деятельности;*
- *анализа информационного процесса, обеспечивающего управление деятельностью субъекта, и декомпозиции его в виде множества элементарных информационных операций;*
- *анализа жизненного цикла системы информационных технологий как среды протекания информационного процесса, уязвимости которой обусловливают возможность реализации угроз информационной безопасности.*

Модель представляет собой обобщенное формализованное описание информационных процессов и технологий, а также процессов экономической деятельности субъекта, образующих «каналы влияния» источников угроз безопасности информации на эффекты (результаты) социально-экономической деятельности.

Модель является инструментом предварительного (качественного) анализа риска информационной безопасности, применяемым в интересах выявления ключевых факторов, подлежащих детальному (количественному) анализу при оценке уровня риска.

Ключевые слова: *анализ риска, угроза информационной безопасности, способ реализации угрозы, автоматизированная система в защищенном исполнении, информационный процесс, жизненный цикл автоматизированной системы, информационная инфраструктура, процесс деятельности, эффект деятельности, последствие реализации угрозы.*

DOI: 10.21681/2311-3456-2020-2-02-10

Введение

Понятие риска является ключевым понятием в области безопасности вообще [1, 2] и информационной безопасности в частности [3-7]. Риск информационной безопасности, с одной стороны, интегрирует в себе спектр вопросов, связанных с угрозами безопасности информации, включая выявление источников угроз и уязвимостей защищаемых информационных технологий, определение способов, вероятности и возможных последствий реализации угроз. С другой стороны, риск интегрируется в процессы технико-экономического анализа и принятия решений, связанных с обеспечением информационной безопасности, созданием средств и организацией системы защиты информационных технологий, определением ее состава, архитектуры и конфигурации.

К характерным особенностям оценки риска информационной безопасности относятся:

- высокая размерность и связанная с этим трудоемкость процесса оценки, обусловленная большим количеством потенциальных угроз безопасности и уязвимостей защищаемых информационных технологий;
- необходимость оценивать риск на всех стадиях жизненного цикла информационной технологии, начиная от формирования требований к продукту до его применения по назначению и вывода из эксплуатации;
- необходимость оценивать риск на различных уровнях деятельности по управлению информационной безопасностью, включая управление рисками и аудит информационной безопасности.

Процесс «развертывания» риска, структура которого показана на рисунке 1, может быть представлен как последовательное воздействие угроз безопасности:

- на протекающие в информационной системе процессы;
- на процессы управления деятельностью субъекта (обладателя информации);
- на результаты деятельности на уровне отдельных

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, заместитель начальника 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

субъектов и, в целом, на уровне сферы деятельности.

На каждой из этих стадий «развертывания» риска для его анализа применяются соответствующие показатели, например:

- вероятность возникновения инцидента, показатели безопасности информации: конфиденциальность, целостность, доступность;
- качество функционирования информационной системы, возможность выполнения информационной системой возложенных на нее задач;
- возможный ущерб субъекта от нарушения процесса управления его деятельностью, вероятность возникновения ущерба.

Рисунок 1. Структура процесса анализа риска

Высокая размерность и многоуровневость задачи анализа риска обусловливает широкое использование на практике качественных (эвристических) методов ее решения. Однако качественные методы анализа не в полной мере соответствуют современной ситуации в информационной сфере, характеризующейся высокой значимостью информационной инфраструктуры, интенсивностью информационного противоборства и высокими рисками информационной безопасности. Важным направлением повышения эффективности анализа риска является применение формальных (количественных) методов анализа, базирующихся, в частности, на результатах формализации разного рода процессов, связанных с обеспечением информационной безопасности [2]. Классическим представителем таких методов является формальная модель управления доступом, позволяющая строго описать информационные потоки в системе [3, 8]. Диаграммы потоков данных DFD, диаграммы операций языка моделирования UML, формализм деревьев применяются, в частности, для моделирования угроз при проектировании защищенных приложений [9].

В работе [10] формализм деревьев и графов использован для построения модели угроз. В работе [11] разработана модель управляемого процесса реализации угроз, включающего этапы изучения системы защиты, изучения средств защиты на выбранной траектории атаки и реализации деструктивного воздействия. Динамика реализации угроз безопасности информации может моделироваться с использованием аппарата сетей Петри-Маркова [12], позволяющего учитывать параллелизм и логическую взаимосвязь процессов реализации угроз. Марковские модели применяются также для исследования угроз и выбора оптимального набора средств защиты информации [13, 14].

Формализм отдельных процессов, сопутствующих обеспечению информационной безопасности, и отдельных этапов анализа риска является базой для системных исследований. Так, в работе [15] представлена методика оценки рисков нарушения безопасности критически важных объектов, заключающаяся в декомпозиции объекта на множество компонентов, определении множества связанных с ними угроз, вычислении рискообразующих потенциалов объекта с учетом рископонижающих потенциалов мер защиты. В работе [16] представлена структурированная процедура анализа риска с использованием экспертных оценок и статистических данных об инцидентах информационной безопасности. В работе [17] для оценки риска применен метод анализа иерархий, обеспечивающий широкие возможности по анализу вложенных многоуровневых структур. В работах [18, 19] рассмотрены вопросы применения аппарата нечеткой логики для оценки величины ущерба, возникающего при реализации угроз безопасности информации. В работе [20] при построении интеллектуальной (экспертной) автоматизированной системы анализа угроз и оценки риска использован математический аппарат байесовых сетей. В работе [21] для снижения рисков предложено использовать аппарат иммунных сетей и когнитивные вычисления.

Основная часть

Особенностью настоящей работы является процессный подход [1, 3] к анализу риска информационной безопасности, основанный на декомпозиции следующих процессов:

- процесса деятельности субъекта в определенной сфере (отрасли);
- информационного процесса в системах, обеспечивающих управление деятельностью субъекта;
- процесса жизненного цикла информационных технологий и технологий защиты.

Процессы деятельности субъекта рассматриваются в контексте структуры, приведенной в таблице 1.

DOI: 10.21681/2311-3456-2020-2-02-10

Таблица 1

Обобщенная характеристика структуры практической деятельности

Название уровня	Содержание уровня	Типовые характеристики
Процессы деятельности субъекта	Технологические операции	Функциональные, технические характеристики выполняемых операций
	Производственные процессы	Показатели жизненного цикла продукции, ресурсоемкости, производительности, качества, эффективности, надежности, безопасности
	Организационно-экономические процессы	Финансовые, кадровые, маркетинговые показатели процессов
Субъекты деятельности	Организации, предприятия, учреждения	Финансовые, кадровые, маркетинговые показатели субъектов
	Интегрированные структуры	Показатели деятельности в соответствии с целевыми программами, проектами и планами
Сферы (отрасли) деятельности	Здравоохранение, наука, транспорт, связь, энергетика, банковская сфера, топливно-энергетический комплекс, атомная энергетика, оборонная, ракетно-космическая, горнодобывающая, металлургическая, химическая промышленность	Социальная, политическая, экономическая, экологическая значимость, значимость для обеспечения обороны страны, безопасности государства и правопорядка

Деятельность рассматривается как множество $\boldsymbol{P}$ элементарных процессов. Каждый *i*-й элементарный процесс характеризуется множеством положительных эффектов $\boldsymbol{S}_i^+$, выражающих степень реализации функционального назначения процесса, и множеством отрицательных эффектов $\boldsymbol{S}_i^-$, выражающих ресурсоемкость процесса и побочные (не имеющие отношения к функциональному назначению) последствия, связанные с его реализацией.

Каждый уровень деятельности представляет собой систему последовательно-параллельных элементарных процессов (операций), формализуемую методами теории графов. Ребро графа соответствует элементарному процессу P_i, а соседние вершины – множеству входных $\boldsymbol{S}_{i\triangleleft}$ и множеству выходных $\boldsymbol{S}_{i\triangleright}$ эффектов этого процесса:

$$\boldsymbol{S}_{i\triangleleft} = \{\boldsymbol{S}_{j\triangleright}^+, \boldsymbol{S}_{k\triangleright}^+, \dots, \boldsymbol{S}_{l\triangleright}^-, \boldsymbol{S}_{m\triangleright}^-, \dots\},$$

где индексы $j, k, \dots, l, m \dots \in \mathbb{N}$,

$j, k, \dots, l, m \dots < i$ являются индексами тех процессов P_j, P_k,…, P_l, P_m,…, от выходных эффектов которых зависит выходной эффект i-го процесса;

$\boldsymbol{S}_{i\triangleright} = \{\boldsymbol{S}_i^+, \boldsymbol{S}_i^-\} = f_s(\boldsymbol{S}_{i\triangleleft}, \boldsymbol{U}_i, \boldsymbol{E}_i)$, где $\boldsymbol{U}_i$ – множество параметров управления *i*-м процессом, $\boldsymbol{E}_i$ – множество параметров внешней среды, влияющих на *i*-й процесс, $f_s(*)$ – операция отображения множества $\{\boldsymbol{S}_{i\triangleleft}, \boldsymbol{U}_i, \boldsymbol{E}_i\}$ в множество $\boldsymbol{S}_{i\triangleright}$.

Принцип декомпозиции процесса деятельности на элементарные процессы заключается в определении узловых точек деятельности (моментов времени или событий технологического цикла), в которых могут быть однозначно определены возникающие эффекты, удовлетворяющие хотя бы одному из следующих условий:

- эффекты являются существенными для дальнейшей деятельности в соответствии с ее технологией (в том числе для формирования управляющих воздействий);
- эффекты являются существенными с точки зрения соответствия деятельности нормативным требованиям.

В основе принятого подхода к представлению практической деятельности в виде системы элементарных процессов лежат следующие допущения:

1) на уровне технологических операций (таблица 1) каждый *i*-й элементарный процесс считается неделимой сущностью;

2) течение и результат *i*-го элементарного процесса зависят только от множества входных эффектов и множества параметров управления;

3) на других уровнях деятельности, начиная с уровня производственных процессов, в качестве элементарного процесса рассматривается некоторая совокупность процессов предшествующего уровня, для которой имеют место допущения 1) и 2).

Представление практической деятельности в виде графа иллюстрируется на рисунке 2.

Таким образом, деятельность формализуется последовательностью состояний системы элементарных процессов в пространстве эффектов $\{\boldsymbol{S}^+, \boldsymbol{S}^-\}$. Вложение состояний одного уровня деятельности в состояния другого может осуществляться путем скаляризации эффектов предшествующего уровня либо оперирования состоянием-вектором (без преобразования вектора эффектов предыдущего уровня в скалярный эффект следующего уровня). В результате обеспечивается возможность последовательного обобщения эффектов отдельных технологических операций вплоть до эффектов деятельности субъекта и отрасли в целом. В множестве эф-

фектов деятельности субъекта (отрасли) выделяется подмножество интегральных эффектов $S_\Sigma \subset \{S^+, S^-\}$, по величине которых оценивается степень соответствия деятельности определенным целям и установленным требованиям.

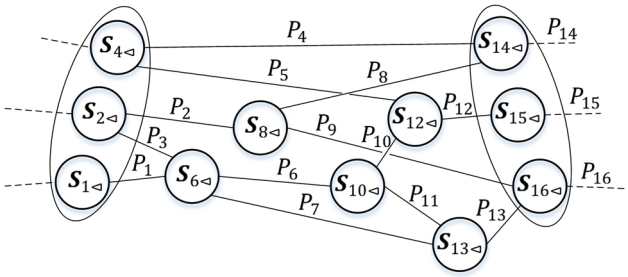

Рисунок 2. Иллюстрация представления практической деятельности системой элементарных процессов и эффектов: $S_{2\triangleleft} = S_{3\triangleleft}$, $S_{4\triangleleft} = S_{5\triangleleft}$, $S_{6\triangleleft} = S_{7\triangleleft}$,

$$S_{6\triangleleft} = \{S_{1\triangleright}, S_{3\triangleright}\},\ S_{8\triangleleft} = S_{9\triangleleft},\ S_{10\triangleleft} = S_{11\triangleleft},$$
$$S_{12\triangleleft} = \{S_{5\triangleright}, S_{10\triangleright}\},\ S_{13\triangleleft} = \{S_{7\triangleright}, S_{11\triangleright}\},$$
$$S_{14\triangleleft} = \{S_{4\triangleright}, S_{8\triangleright}\},\ S_{16\triangleleft} = \{S_{9\triangleright}, S_{13\triangleright}\}$$

(эллипсами обозначен пример выделения соседних состояний процесса следующего уровня деятельности)

Информационные процессы, лежащие в основе управления процессами практической деятельности, протекают в контексте информационных систем и, шире, в контексте информационной инфраструктуры (таблица 2).

Методическим аналогом технологической операции процессов практической деятельности в информационных процессах являются информационные операции, которые реализуются вычислительными и коммуникационными информационными системами в соответствии с заданными алгоритмами и протоколами и направлены на решение следующих задач (рисунок 3):

- реализация абстрактной модели практической деятельности в пространстве состояний S;
- формирование управляющих параметров U, обеспечивающих целевую траекторию процесса практической деятельности в пространстве состояний S с учетом условий внешней среды.

Значения параметров управления $U = f_u(O^+, Q^{o+}, O^-, Q^{o-}, C, T^o)$ определяются такими характеристиками информационного процесса, как:

- множество информационных операций O^+, предусмотренных алгоритмами (протоколами) информационного процесса;
- вероятность того, что *i*-я предусмотренная операция будет выполнена, $Q_i^{o+} \in Q^{o+}$;

Таблица 2

Обобщенная характеристика информационной инфраструктуры

Название уровня	Содержание уровня	Типовые характеристики
Информационные процессы	Организационно-экономическая, производственная, технологическая информация	Параметры управления процессами практической деятельности
	Общедоступная информация, коммерческая тайна, персональные данные, служебная информация ограниченного распространения	Свойства информации (конфиденциальность, целостность, доступность, подлинность и т.п.)
Жизненный цикл информации	Создание, обработка (преобразование), передача, хранение, уничтожение (удаление)	Показатели соответствующих информационных операций
Информационная инфраструктура	Государственные информационные системы, объекты критической информационной инфраструктуры, автоматизированные системы управления, информационные системы персональных данных, информационные системы общего пользования, информационно-телекоммуникационные сети	Показатели защищенности от несанкционированного доступа, уязвимости информационных систем, средств и технологий (уязвимости программного обеспечения, сетевых протоколов, наличие технических каналов утечки, организационные недостатки и т.п.)
	Системы защиты информации, системы обеспечения безопасности	Организационные меры защиты, программные и технические средства защиты информации, функции безопасности средств защиты, показатели устойчивости к атакам
Жизненный цикл объектов информационной инфраструктуры	Разработка концепции, эскизно-техническое проектирование, разработка рабочей документации, ввод в действие, эксплуатация, модернизация, вывод из эксплуатации	Показатели ресурсоемкости, показатели доверия (в том числе уровни контроля отсутствия уязвимостей и недекларированных возможностей)
Угрозы безопасности информации	Антропогенные, техногенные, природные угрозы (преднамеренные и непреднамеренные действия человека, снижение надежности технических систем, метеорологические явления и т.п.)	Характеристики угроз безопасности информации, компетенция, мотивация, ресурсы (потенциал) нарушителей безопасности информации

- множество непредусмотренных (нештатных) операций $\boldsymbol{O^-}$, реализация которых возможна в информационной системе под влиянием внутренних факторов или внешней среды;
- вероятность того, что будет реализована *i*-я непредусмотренная операция, $Q_i^{o-} \in \boldsymbol{Q^{o-}}$;
- показатель качества (степени выполнения) i-й операции $C_i \in \boldsymbol{C}$;
- продолжительность выполнения *i*-й операции $T_i^o \in \boldsymbol{T^o} = \{\boldsymbol{T^{o+}}, \boldsymbol{T^{o-}}\}$.

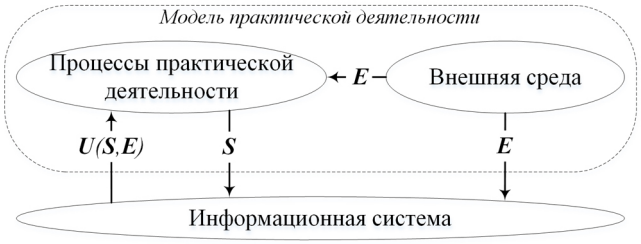

Рисунок 3. Иллюстрация принципа управления практической деятельностью ($\boldsymbol{S}$ – состояние процессов практической деятельности, $\boldsymbol{E}$ – параметры внешней среды, $\boldsymbol{U}$ – параметры управления)

Множеству значений характеристик информационных процессов $\boldsymbol{H} = \{\boldsymbol{Q^{o+}}, \boldsymbol{O^-}, \boldsymbol{Q^{o-}}, \boldsymbol{C}, \boldsymbol{T^o}\}$ может быть поставлено в соответствие множество значений характеристик (свойств) подвергаемой обработке информации, классическими среди которых являются конфиденциальность, целостность, доступность.

Типовым методическим подходом к анализу информационных процессов является их представление на нескольких уровнях. Так, в вычислительных информационных системах рассматриваются следующие уровни: прикладной язык программирования; операционная система; архитектура набора команд; микроархитектура; цифровой логический уровень. В коммуникационных информационных системах к таким уровням относятся: прикладной уровень; уровень представления; сеансовый уровень; транспортный уровень; сетевой уровень; канальный уровень; физический уровень. В базах данных выделяются концептуальный, логический и физический уровни представления, а на каждом из них используются определенные модели представления данных.

Элементарная информационная операция O информационного процесса рассматривается в настоящей модели как множество, включающее входную информацию V, инструкцию I, в соответствии с которой осуществляется обработка входной информации, и результат выполнения операции W: $O = \{V, I, W\}$ (рисунок 4).

Структурно информационный процесс определяется отношением предшествования (либо отношением следования) Ξ, заданным на множестве информационных операций $\boldsymbol{O}$: *i*-я операция O_i предшествует *j*-й операции O_j, $O_i \Xi O_j$, если результат выполнения *i*-й операции является входной информацией для j-й операции. В общем случае инструкция I операции может зависеть от результатов выполнения одной или нескольких предшествующих операций, что формально задается отношением влияния ϕ на множестве $\boldsymbol{O}$: *i*-я операции O_i влияет на *j*-ю операции O_j, $O_i \phi O_j$, если от результата выполнения *i*-й операции зависит инструкция *j*-й операции.

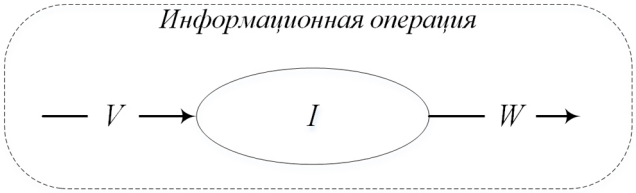

Рисунок 4. Модель информационной операции

Информационные процессы реализуется с применением системы информационных технологий, приведенных в таблице 3.

Приведенная система информационных технологий является средством воздействия субъектов $\boldsymbol{A}$, определяющих ее содержание, на значения характеристик $\boldsymbol{H}$ реализуемых информационных процессов. Субъект *A* рассматривается в качестве источника угрозы, если его действия способны привести к инциденту информационной безопасности – к выполнению одной или нескольких непредусмотренных информационных операций из множества $\boldsymbol{O^-}$ – либо снизить эффективность выполнения предусмотренных операций, оцениваемую в соответствии с показателями из множества $\{\boldsymbol{C}, \boldsymbol{T^{o+}}\}$. Соответствие между угрозами и информационными технологиями, посредством которых возможна их реализация (таблица 4), удобно задать бинарной матрицей: $(m_{i,j})$: $m_{i,j} = 1$, если *j*-я информационная технология может быть использована для реализации *i*-ой угрозы; $m_{i,j} = 0$, если *j*-я информационная технология не может быть средством реализации *i*-ой угрозы.

Вероятностный характер возникновения и реализации угроз безопасности информации, а также противодействие угрозам с применением системы защитных технологий (таблица 5), влечет вероятностный характер показателей информационных процессов $\boldsymbol{H}$ и, как следствие, параметров управления $\boldsymbol{U}$ и эффектов практической деятельности $\boldsymbol{S}$. Целью применения защитных технологий является предотвращение выхода средних значений интегральных эффектов $\overline{\boldsymbol{S}}_{\boldsymbol{\Sigma}}$ за пределы допустимой области $\overline{\boldsymbol{S}}^*_{\boldsymbol{\Sigma}}$ в условиях наличия угроз безопасности информации.

Заключение

Предлагаемая модель в тезисной форме намечает этапы «развертывания» риска информационной безопасности. В качестве показателя, характеризующего уровень риска, принято множество средних значений интегральных эффектов деятельности субъекта $\boldsymbol{S}_{\boldsymbol{\Sigma}}$,

Таблица 3

Типовая система информационных технологий

Стадия жизненного цикла	Содержание информационной технологии	Субъекты, определяющие содержание информационной технологии
Концептуальное проектирование	Определение цели, задач и функций информационной системы	Заказчик
Эскизно-техническое проектирование	Реализация структуры: состав, архитектура (топология), конфигурация программных и аппаратных средств	Разработчик, регулятор
	Реализация функционирования: алгоритмы, протоколы, операции	
Внедрение	Разработка эксплуатационной и организационно-распорядительной документации	Разработчик
	Интеграция программных и аппаратных средств	Интегратор
	Реализация организационной структуры	Заказчик, разработчик, регулятор
	Подготовка персонала	Заказчик, оператор
Эксплуатация	Сопровождение	Разработчик
	Реализация эксплуатационных характеристик	Оператор, техногенные и природные факторы
	Реализация информационных процессов	Персонал, пользователи

Таблица 4

Способы реализации угроз

Объекты доступа	Виды воздействий	Уязвимости
Физический доступ		
Контролируемая зона	Проникновение	Организационные недостатки
Персонал	Социальная инженерия	
Аппаратные и технические средства	Специальные воздействия	Ограниченная устойчивость к воздействию физических полей
	Природные воздействия	Ограниченная устойчивость к воздействию природных факторов
	Техногенные воздействия	Ограниченная надежность
	Механические воздействия	Ограниченная прочность
Среда функционирования аппаратных и технических средств	Перехват физических полей (сигналов)	Технические каналы утечки
Логический доступ		
Сетевая среда	Вторжение (компьютерная атака)	Уязвимости сетевых протоколов и каналов передачи данных
Операционная среда	Программно-математические воздействия	Уязвимости программно-алгоритмического и программно-аппаратного обеспечения
Данные	Чтение, модификация, запись, удаление	Неполнота и/или некорректность разграничения доступа

Таблица 5

Система типовых защитных технологий

Задачи	Защитные технологии	Методы решения задач
Разработка системы защиты	Средства защиты от несанкционированного доступа; средства антивирусной защиты; средства криптографической защиты; средства обеспечения доступности информации	Формальные модели управления доступом; формальные модели целостности и доступности; методы дискретного программирования
Организация функционирования системы защиты	Идентификация и аутентификация; управление доступом; антивирусная защита; обеспечение целостности обеспечение доступности; защита технических средств; подготовка персонала	Методы исследования операций

DOI: 10.21681/2311-3456-2020-2-02-10

Задачи	Защитные технологии	Методы решения задач
Управление конфигурацией системы защиты	Средства контроля (анализа) защищенности; средства управления событиями информационной безопасности; системы обнаружения вторжений; средства защиты от утечек информации	Методы оптимизации; методы теории игр
Управление информационной безопасностью	Аудит безопасности; управление инцидентами; управление активами; управление рисками	Методы системного анализа

определяющих степень соответствия деятельности ее целям и нормативным требованиям в условиях наличия угроз безопасности информации. Использование $\overline{S}_{\Sigma}$ в качестве показателя уровня риска позволяет учесть как масштаб возможных последствий реализации угроз информационной безопасности, так и вероятность возникновения таких последствий. Анализ риска в соответствии с предлагаемой моделью осуществляется последовательным решением следующих задач.

1) Анализ угроз безопасности информации и разработка модели угроз. В ходе решения этой задачи исследуются источники угроз, причины и вероятность их возникновения, возможность и способы реализации угроз с учетом применяемых информационных технологий.

2) Анализ последствий реализации угроз по информационным показателям. При решении этой задачи исследуется влияние инцидентов информационной безопасности на эффективность процессов, реализуемых информационными технологиями, а также на качество функционирования информационной системы в целом.

3) Анализ последствий реализации угроз по организационно-техническим показателям. При решении этой задачи исследуется влияние качества функционирования информационной системы на управление автоматизируемыми процессами производственной и организационной деятельности.

4) Анализ последствий реализации угроз по социально-экономическим показателям. При решении этой задачи исследуется влияние эффективности производственной и организационной деятельности на интегральные показатели $\overline{S}_{\Sigma}$, характеризующие степень соответствия деятельности ее целям и нормативным требованиям.

5) Разработка системы защиты информации. При решении этой задачи исследуется возможность, способы и средства достижения допустимых значений показателей $\overline{S}^{*}_{\Sigma}$ за счет противодействия угрозам безопасности информации. Сравнительная оценка вариантов построения системы защиты информации осуществляется по комплексному показателю $\{\overline{S}^{*}_{\Sigma}, F\}$, включающему стоимость жизненного цикла F системы защиты информации.

Системообразующим элементом процесса анализа риска информационной безопасности является комплекс информационных, технических, организационных и социально-экономических показателей, обеспечивающих оценку риска на отдельных этапах анализа. Подобная особенность задачи анализа риска информационной безопасности позволяет говорить о ней как о типичной задаче системного анализа, а также провести параллель с аналогичными по структуре и сложности задачами из смежной области радиоэлектронной борьбы: задачей анализа риска формирования научно-технического и технологического задела для создания систем радиоэлектронной борьбы [22] и задачей развития таких систем [23].

Рецензент: *Язов Юрий Константинович, доктор технических наук, профессор, главный научный сотрудник управления ФАУ «ГНИИИ ПТЗИ ФСТЭК России», г. Воронеж, Россия. E-mail: Yazoff_1946@mail.ru.*

Литература

1. Петренко С. А., Симонов С. В. Управление информационными рисками. Экономически оправданная безопасность. М.: ДМК Пресс, 2004. 400 с.
2. Probabilistic Modeling in System Engineering/By ed. A. Kostogryzov. -London: IntechOpen, 2018. 278 p. DOI: 10.5772/intechopen.71396
3. Барабанов А.В., Дорофеев А.В., Марков А.С., Цирлов В.Л. Семь безопасных информационных технологий. М.: ДМК Пресс, 2017. 224 с.
4. Булдакова Т.И., Миков Д.А. Реализация методики оценки рисков информационной безопасности в среде MATLAB, Вопросы кибербезопасности. 2015, №4 (12). С. 53-61. DOI: 10.21681/2311-3456-2015-4-53-61
5. Марков А.С., Цирлов В.Л. Управление рисками - нормативный вакуум информационной безопасности, Открытые системы. СУБД. 2007, №8. С. 63-67.
6. Райкова Н.О., Шахалов И.Ю. Сравнение ISO/IEC 27001:2005 и ISO/IEC 27001:2013, ИТ-Стандарт. 2015, № 1 (2). С. 45-48.
7. Ревенков П.В., Крупенко Д.С. Оценка рисков информационной безопасности в условиях применения систем мобильного банкинга, Вопросы кибербезопасности. 2019, № 2 (30). С. 21-28. DOI: 10.21681/2311-3456-2019-2-21-28
8. Грушо А.А., Применко Э.А., Тимонина Е.Е. Теоретические основы компьютерной безопасности. – М.: Academia, 2009. 272 с.
9. Ховард М., Лебланк Д. Защищенный код. 2-е изд. М.: Русская редакция, 2004. 704 с.

10. Баранкова И.И., Михайлова У.В., Афанасьева М.В. Минимизация рисков информационной безопасности на основе моделирования угроз безопасности, Динамика систем, механизмов и машин. 2019. Том 7, № 4. С 60-66. DOI: 10.25206/2310-9793-7-4-60-66
11. Горохов Д.Е. Априорная оценка величины риска информационной безопасности на основе моделирования процесса реализации информационных угроз, Информационная безопасность. 2009, №4. С. 593-598.
12. Текунов В.В., Язов Ю.К. Моделирование динамики реализации угроз безопасности информации с использованием аппарата сетей Петри-Маркова, Информация и безопасность. 2018. Т. 21, № 1. С. 38-47.
13. Касенов А.А., Магазев А.А., Цырульник В.Ф. Марковская модель совместных киберугроз и ее применение для выбора оптимального набора средств защиты информации, Моделирование и анализ информационных систем. 2020. Т. 27, № 1. С. 108-123. DOI: 10.18255/1818-1015-2020-1-108-123
14. Чобанян В.А., Шахалов И.Ю. Анализ и синтез требований к системам безопасности объектов критической информационной инфраструктуры, Вопросы кибербезопасности. 2013, № 1 (1). С. 17-27.
15. Кононов А.А., Котельников А.П., Черныш К.В. Оценка защищенности критически важных объектов на основе построения моделей событий рисков, Управление рисками и безопасностью. Труды ИСА РАН. 2012. Том 62, № 4. С. 69-75.
16. Васильева Т.Н., Львова А.В. Применение оценок рисков в управлении информационной безопасностью, Прикладная информатика. 2009, № 5 (23).
17. Аникин И.В. Метод анализа иерархий в задачах оценки и анализа рисков информационной безопасности, Информатика и управление. Вестник КГТУ им. А.Н. Туполева. 2006, № 3. С. 11-18.
18. Аникин И.В. Нечеткая оценка факторов риска информационной безопасности, Безопасность информационных технологий. 2016. Т. 23, № 1. С. 78-87.
19. Казаров Е.Г., Рудаков А.М., Митюшов Д.Г. Использование теории нечетких множеств при моделировании угроз безопасности информации, Вестник Ярославского высшего военного училища противовоздушной обороны. 2019, No 2 (5). С. 192-200.
20. Гаськова Д.А., Массель А.Г. Технология анализа киберугроз и оценка рисков нарушения кибербезопасности критической инфраструктуры, Вопросы кибербезопасности. 2019, № 2 (30). С. 42-49. DOI: 10.21681/2311-3456-2019-2-42-49
21. Петренко С.А. Обзор методов иммунной защиты индустрии 4.0, Защита информации. Инсайд. 2019, № 5 (89). С. 36-48.
22. Боев А.С., Бывших Д.М., Коробейников А.С., Строкова Т.М. Анализ рисков при подготовке научно-технического и технологического задела инноваций, РИСК: Ресурсы. Информация. Снабжение. Конкуренция. 2013, №3. С.214-221.
23. Ласточкин Ю.И., Ярыгин Ю.Н., Бывших Д.М. Система показателей для комплексного анализа состояния и перспектив развития сил и средств войск радиоэлектронной борьбы ВС РФ, Вооружение и экономика. 2017, № 4 (41). С. 21-31.

CONCEPTUAL MODEL OF INFORMATION TECHNOLOGY SECURITY RISK ANALYSIS

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

Abstract. *The aim of the study is to generalize and structure processes that determine the level of information security risk of a subject of socio-economic activity.*

The conceptual model is developed on the basis of:

- *analysis of the subject's activity process and its decomposition into separate states in the space of activity effects;*
- *analysis of the information process that ensures the management of the subject, and its decomposition in the form of a set of elementary information operations;*
- *analysis of the life cycle of an information technology system as an environment for the flow of an information process, vulner*abilities of which determine the possibility of realizing threats to information security.

The model is a generalized formalized description of information processes and technologies, as well as the processes of the economic activity of the subject, forming the «channels of influence» of sources of threats to information security on the effects (results) of socio-economic activity.

The model is a tool for preliminary (qualitative) analysis of information security risk, used to identify key factors that are subject to detailed (quantitative) analysis in assessing the level of risk.

4 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

5 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

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

Keywords: *risk analysis, information security threat, threat implementation method, automated system in secure execution, information process, life cycle of an automated system, information infrastructure, activity process, activity effect, consequence of threat realization*

References

1. Petrenko S. A., Simonov S. V. Upravlenie informacionnymi riskami. Ekonomicheski opravdannaya bezopasnost'. M.: DMK Press, 2004. 400 s.
2. Probabilistic Modeling in System Engineering/By ed. A. Kostogryzov. -London: IntechOpen, 2018. 278 p., DOI: 10.5772/intechopen.71396.
3. Barabanov A.V., Dorofeev A.V., Markov A.S., Cirlov V.L. Sem' bezopasnyh informacionnyh tekhnologij. M.: DMK Press, 2017. 224 p.
4. Buldakova T.I., Mikov D.A. Realizaciya metodiki ocenki riskov informacionnoj bezopasnosti v srede MATLAB, Voprosy kiberbezopasnosti [Cybersecurity issues], 2015, No4 (12). S. 53-61.
5. Markov A.S., Cirlov V.L. Upravlenie riskami - normativnyj vakuum informacionnoj bezopasnosti, Otkrytye sistemy. SUBD. 2007, No8. S. 63-67.
6. Rajkova N.O., SHahalov I.YU. Sravnenie ISO/IEC 27001:2005 i ISO/IEC 27001:2013, IT-Standart. 2015, No 1 (2). S. 45-48.
7. Revenkov P.V., Krupenko D.S. Ocenka riskov informacionnoj bezopasnosti v usloviyah primeneniya sistem mobil'nogo bankinga, Voprosy kiberbezopasnosti [Cybersecurity issues], 2019, No 2 (30). S. 21-28.
8. Grusho A.A., Primenko E.A., Timonina E.E. Teoreticheskie osnovy komp'yuternoj bezopasnosti. – M.: Academia, 2009. 272 c.
9. Hovard M., Leblank D. Zashchishchennyj kod. 2-e izd. M.: Russkaya redakciya, 2004. 704 s.
10. Barankova I.I., Mihajlova U.V., Afanas'eva M.V. Minimizaciya riskov informacionnoj bezopasnosti na osnove modelirovaniya ugroz bezopasnosti, Dinamika sistem, mekhanizmov i mashin. 2019. Tom 7, No 4. S 60-66. DOI: 10.25206/2310-9793-7-4-60-66.
11. Gorohov D.E. Apriornaya ocenka velichiny riska informacionnoj bezopasnosti na osnove modelirovaniya processa realizacii informacionnyh ugroz, Informacionnaya bezopasnost'. 2009, No4. S. 593-598.
12. Tekunov V.V., YAzov YU.K. Modelirovanie dinamiki realizacii ugroz bezopasnosti informacii s ispol'zovaniem apparata setej Petri-Markova, Informaciya i bezopasnost'. 2018. T. 21, No 1. S. 38-47.
13. Kasenov A.A., Magazev A.A., Cyrul'nik V.F. Markovskaya model' sovmestnyh kiberugroz i ee primenenie dlya vybora optimal'nogo nabora sredstv zashchity informacii, Modelirovanie i analiz informacionnyh sistem. 2020. T. 27, No 1. S. 108-123. DOI: 10.18255/1818-1015-2020-1-108-123.
14. CHobanyan V.A., SHahalov I.YU. Analiz i sintez trebovanij k sistemam bezopasnosti ob"ektov kriticheskoj informacionnoj infrastruktury, Voprosy kiberbezopasnosti [Cybersecurity issues], 2013, No 1 (1). S. 17-27.
15. Kononov A.A., Kotel'nikov A.P., CHernysh K.V. Ocenka zashchishchennosti kriticheski vazhnyh ob"ektov na osnove postroeniya modelej sobytij riskov, Upravlenie riskami i bezopasnost'yu. Trudy ISA RAN. 2012. Tom 62, No 4. S. 69-75.
16. Vasil'eva T.N., L'vova A.V. Primenenie ocenok riskov v upravlenii informacionnoj bezopasnost'yu, Prikladnaya informatika. 2009, No 5 (23).
17. Anikin I.V. Metod analiza ierarhij v zadachah ocenki i analiza riskov informacionnoj bezopasnosti, Informatika i upravlenie. Vestnik KGTU im. A.N. Tupoleva. 2006, No 3. S. 11-18.
18. Anikin I.V. Nechetkaya ocenka faktorov riska informacionnoj bezopasnosti, Bezopasnost' informacionnyh tekhnologij. 2016. T. 23, No 1. S. 78-87.
19. Kazarov E.G., Rudakov A.M., Mityushov D.G. Ispol'zovanie teorii nechetkih mnozhestv pri modelirovanii ugroz bezopasnosti informacii, Vestnik YAroslavskogo vysshego voennogo uchilishcha protivovozdushnoj oborony. 2019, No 2 (5). S. 192-200.
20. Gas'kova D.A., Massel' A.G. Tekhnologiya analiza kiberugroz i ocenka riskov narusheniya kiberbezopasnosti kriticheskoj infrastruktury, Voprosy kiberbezopasnosti [Cybersecurity issues], 2019, No 2 (30). S. 42-49. DOI: 10.21681/2311-3456-2019-2-42-49.
21. Petrenko S.A. Obzor metodov immunnoj zashchity industrii 4.0, Zashchita informacii. Inzajd. 2019, No 5 (89). S. 36-48.
22. Boev A.S., Byvshih D.M., Korobejnikov A.S., Strokova T.M. Analiz riskov pri podgotovke nauchno-tekhnicheskogo i tekhnologicheskogo zadela innovacij, RISK: Resursy. Informaciya. Snabzhenie. Konkurenciya. 2013, No3. S.214-221.
23. Lastochkin YU.I., YArygin YU.N., Byvshih D.M. Sistema pokazatelej dlya kompleksnogo analiza sostoyaniya i perspektiv razvitiya sil i sredstv vojsk radioelektronnoj bor'by VS RF, Vooruzhenie i ekonomika. 2017, No 4 (41). S. 21-31.