ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

УДК 004.056
DOI: 10.21822/2073-6185-2024-51-4-40-49 Оригинальная статья /Original article

Об оценивании устойчивости функционирования объектов микропараметрического страхования киберрисков

В.А. Воеводин
Национальный исследовательский университет
«Московский институт электронной техники»,
124498, г. Москва, г. Зеленоград, пл. Шокина, 1, Россия

Резюме. Цель. Статья посвящена проблеме оценивания устойчивости функционирования объектов критической информационной инфраструктуры в интересах микропараметрического страхования киберрисков. Обосновывается целесообразность внедрения параметрического страхования как экономического способа обеспечения защиты информации в условиях воздействия угроз и существование проблемы оценивания устойчивости. **Метод.** Применение методов теории надежности в сочетании с методами теории случайных функций позволило учесть динамику устойчивости функционирования объекта защиты на периоде воздействия угроз. **Результат.** В результате представилось возможным получить оценку минимального значения показателя устойчивости функционирования объекта оценивания и соответствующего момента времени наступления этого события, что в совокупности позволило оценить риск, связанный с этим событием. Новизна предлагаемого подхода заключается в том, что для оценивания киберрисков использовалась функция устойчивости объекта оценивания, которая формировалась на основе функций устойчивости отдельных элементов, входящих в состав объекта оценивания с учетом его структуры и имеющегося в распоряжении, для поддержания функциональности, ресурса. Приводится постановка задачи оценивания рисков информационной безопасности (ИБ) для различных структур и описание методов решения задачи параметрического микрострахования, которые сосредоточены на оценивании важности каждого из элементов, входящих в состав объекта страхования. **Вывод.** Материалы статьи могут быть использованы при постановке задачи по разработке методов, моделей и средств обеспечения страхования рисков ИБ, а также при поддержке решений по обеспечению устойчивости.

Ключевые слова: риск, функция устойчивости, устойчивость функционирования, параметрическое страхование, микропараметрическое страхование

Для цитирования:В.А. Воеводин. Об оценивании устойчивости функционирования объектов микропараметрического страхования киберрисков. Вестник Дагестанского государственного технического университета. Технические науки. 2024; 51(4):40-49. DOI:10.21822/2073-6185-2024-51-4-40-49

On assessing the sustainability of functioning of microparametric cyber risk insurance facilities

V.A. Voevodin
National Research University of Electronic Technology,
1 Shokina Square, Moscow, Zelenograd 124498, Russia

Abstract. Objective. The article is devoted to the problem of assessing the durability of critical information infrastructure objects in favor of microparametric risk insurance. The feasibility of introducing parametric insurance as a cost-effective way to protect information against threats and the existence of sustainability problems is being supported. **Method.** The application of reliability theory methods in combination with random function theory allowed to consider the

dynamics of stability of operation of the protection object during the period of the action of threats. **Result.** It was possible to estimate the minimum value of the rating object's performance and the relevant time of occurrence, which in combination allowed for an assessment of the risk associated with the event. The novelty of the proposed approach is that for cyber risk assessment, a function of the object of assessment was performed, which was formed on the basis of the functions of individual elements of the evaluation object, taking into account its structure and available resources for maintaining functionality. The information security (IS) assessment task for different structures and the Parametric Micro-Insurance Solution Methodologies are described, which focus on the importance of each of their elements as part of the insurance object. **Conclusion.**he article's content can be used to set the task of developing methods, models and means for providing IS risk insurance as well as supporting solutions for ensuring sustainability.

Keywords: risk, resilience function, performance resilience, parametric insurance, microparametric insurance.

For citation: V.A. Voevodin. On assessing the sustainability of functioning of microparametric cyber risk insurance facilities. Herald of Daghestan State Technical University. Technical Sciences. 2024; 51(4):40-49. DOI:10.21822/2073-6185-2024-51-4-40-49

Введение. Анализ публикаций по прогнозированию развития и моделированию мировой динамики [1] и долгосрочному технико-экономическому планированию [2, 3] позволяют утверждать, что развитие производства в рамках современного технологического уклада привело к интеграции физических (продуктовых), финансовых (денежных) потоков и информационных процессов. При этом современный технологический уклад все больше ориентируется на управление экономикой через управление рисками [4]. Интеграция продуктовых и информационных потоков и рискориентированный подход к управлению экономикой открыли возможности по интенсификации производства посредством внедрения информационных технологий (ИТ). Однако, экономическая деятельность таких хозяйствующих субъектов (организаций) становится все более уязвимой для угроз информационной безопасности (ИБ) [5-11].

С ростом внедрения информационных технологий и цифровых экосистем создаются нематериальные активы, при этом нематериальные активы современных компаний растут опережающими темпами [1-4]. В такой обстановке страхование призвано снижать рисковую нагрузку хозяйствующих субъектов, в том числе и в условиях воздействия угроз ИБ. В этих условиях привлекательным направлением развития страхового рынка становится страховое обеспечение управления рисками ИБ [12, 13]. В значительной степени это связано с потребностью хозяйствующих субъектов управлять рисками ИБ.

В предыдущей доктрине ИБ страхование рисков ИБ позиционировалось как экономический метод обеспечения информационной безопасности РФ, для внедрения которого предполагалось создание системы страхования информационных рисков физических и юридических лиц, в действующей доктрине ИБ [14] этом метод исключен.

Постановка задачи. Сегодня обеспечение ИБ имеет в своем фундаменте директивные (императивные) начала [15], которые предполагают государственное регулирование отношений в сфере защиты информации посредством установления требований к защите информации и ответственности за их нарушение. При таком подходе решение об обеспечении ИБ принимает регулятор, а не сам хозяйствующий субъект, что порождает парадоксальную, ситуацию при которой угроза исходит от регулятора, но об рискориентированном подходе к обеспечению ИБ речи вообще ни идет. Для внедрения страховой поддержки хозяйствующих субъектов в области обеспечения ИБ требуется совершенствование правового поля, регулирующего отношения при управлении рисками ИБ.

Убытки от компьютерных атак являются существенными, быстро растущими и должны компенсироваться развивающимся рынком страхования рисков ИБ. Однако сложный процесс количественного оценивания ущерба, требующий существенных

временных затрат, не позволяет своевременно получить страховую выплату, что не обеспечивает оперативное реагирование на инцидент ИБ, а также отрицательно отражается на востребованности страхования, как экономического инструмента обеспечения ИБ. На практике очень часто ИБ рассматривают как центр затрат, в то время как ее следует рассматривать как средство для развития бизнеса и его финансовой защиты.

Привлекательным направлением в развитии страхования рисков ИБ является параметрическое страхование, или страхования с фиксированным возмещением, заключается в возможности повысить доверие. Доверие обеспечивается балансом между наступлением события и страховой выплатой, причем выплатой в реальном времени и без учета ущерба. Для этого требуется триггер, с помощью которого фиксируется страховое событие.

Параметрическое страхование направлено на обеспечение определенности покрытия путем минимизации базового риска традиционной политики возмещения, т. е. риска несоответствия между ожиданиями страхователя в отношении покрытия и фактической выплатой возмещения, произведенной в соответствии с договором. При параметрическом страховании не требуется предоставлять подробную информацию о потерях, такую как сумма понесенных убытков. Например, в случае прерывания бизнеса, в полисе может быть предусмотрено, что страховщик будет выплачивать X% от лимита за каждый день простоя, за прерванную услугу, вызванную одним из партнеров. Для определения страховой премии требуется оценка устойчивости функционирования информационной инфраструктуры (ИИ) страхуемого объекта информатизации, особенно для условий воздействия угроз ИБ [16-18]. Для чего необходимы исходные данные, содержащие оценки устойчивости функционирования отдельных элементов в условиях угроз ИБ, которые входят в состав ИИ соответствующего субъекта. Если для штатных условий применения объекта информатизации имеется потенциальная возможность добыть репрезентативную статистику частных показателей устойчивости, то это позволяет использовать ее для оценки количественные методы теории надежности. Зная оценки устойчивости отдельных элементов в штатных условиях применения, представляется возможным оценить, для этих же условий, устойчивость функционирования ИТКС в целом.

Совсем другие условия для нештатного применения. Репрезентативная статистика отсутствует в принципе, что порождает ряд особенностей при оценке устойчивости функционирования ИТКС. Такая ситуация связана, прежде всего, с тем, что сами нештатные условия порождены воздействием угроз ИБ, связанных с поведением лиц, принимающих решения по ее обеспечению, в том числе и источника угроз.

Воздействия угроз, в этом случае, можно позиционировать как редкие явления, их длительность непредсказуема, сама обстановка при нештатных условиях весьма нестабильна. В этих условиях процессы исследуемых событий нельзя принять ни стационарными, ни эргодическими, ни стохастическими. Названные особенности не позволяют в полной мере применить классические методы математической статистики и теории вероятностей. Для решения задачи требуется разработка специальных методов оценки функциональной устойчивости с учетом вышеназванных особенностей [19-22]. Такая неопределенность позиционируется как эпистатическая, и зависит от уровня знаний об исследуемом объекте. Именно разделение риска ИБ со страховщиком является привлекательным в условиях воздействия угроз ИБ. Однако адекватных инструментов оценки рисков ИБ для таких условий нет.

Методы исследования. На текущий момент существует некое стартовое семейство методических инструментов, способствующих внедрению страхования рисков ИБ. Так, Приказом Федерального агентства по техническому регулированию и метрологии от 20 мая 2021 г. № 420-ст утвержден национальный стандарт ГОСТ Р 59516 «Информационные технологии [12]. Принятый стандарт содержит рекомендации: по совершению покупки услуг страхования рисков ИБ как способа распределения риска ИБ со страховщиком; управлению последствиями инцидентов с помощью средств страхового покрытия;

организации коммуникации между страхователем и страховщиком с целью поддержания андеррайтинга, мониторинга и претензионной работы. Основные сведения о математическом обеспечении оценивания рисков информационной безопасности применительно к условиям воздействия угроз ИБ опубликованы [16, 19-22]. Зарегистрирована программа для ЭВМ [23], позволяющая автоматизировать процедуру оценивания рисков ИБ и получать количественные оценки уровня защищенности ИТКС, функционирующих в условиях воздействия угроз.

Следующая идея, которая может положительно повлиять на развитие рынка страхования рисков ИБ и стать признаком страховой компании 2030 – это внедрение «микрострахования», предоставляемого с помощью инновационного, параметрического страхования. Внедрение микростархования позволит расширить выбор страхового продукта тем самым не страховать информационную систему в целом, а страховать лишь самые уязвимые элементы. Для того чтобы реализовать предлагаемый алгоритм, требуется инструмент, который бы позволял по заданным исходным данным, характеризующим защищенность того или иного элемента от воздействия угроз, его восстанавливаемость в случае поражения. и его место в составе информационной инфраструктуры в целом, оценивать его важность (критичность). Имея такой инструмент, возможно было бы страховать не всю информационную систему, а отдельные ее элементы, повышая тем самым привлекательность соответствующих страховых продуктов и эффект от страхования рисков ИБ.

Задачу оценивания устойчивости функционирования объекта критической информационной инфраструктуры (КИИ) в условиях воздействия угроз ИБ целесообразно формулировать отдельно для каждой из возможных структур ИТКС – (1-1), (1-*N*), (*N*-*N*)-полюсные структуры. При постановке задачи принимается ограничение, суть которого заключается в том, что органы управления субъекта КИИ способны принимать управленческие решения и им требуется обмен сообщениями между элементами системы управления (связность) с требуемым качеством, который обеспечивается с помощью информационно-телекоммуникационной сети (ИТКС) [20]. В этом случае показатель связности ИТКС может служить информативной характеристикой устойчивости ее функционирования. Для (1-1)-полюсной структуры задача оценивания устойчивости ИТКС может быть решена посредством разработки методов, моделей и средств оценивания связности между парой абонентов *A* и *B* (рис. 1).

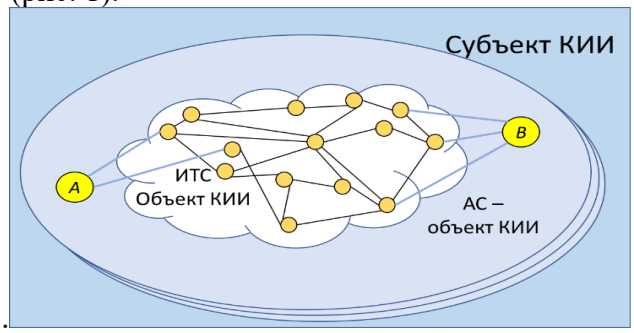

Рис. 1. Вариант (1-1)-полюсной структуры информационно-телекоммуникационной сети
Fig. 1. Option (1-1)-pole information and telecommunications network structure

Для оценивания устойчивости двухполюсной структуры в качестве показателя была выбрана вероятность связности между абонентами *A* и *B*. При этом учитывается допущение, что возможность повреждения самих взаимодействующих абонентов при оценивании устойчивости ИТКС не учитывается, поэтому вероятность их поражения принимается равной нулю. Подобные задачи характерны для систем взаимодействия. В качестве показателя связности используется значение бинарной переменной ***e***, принимающая одно из двух альтернативных значений ***e***=1, когда между абонентами существует хотя бы один путь для обмена сообщениями, ***e***=0 – в противном случаеОбмен сообщениями между абонентами обеспечивается с помощью ИТКС, имеющей (1-1)-полюсную структуру.

При этом принимается допущение, что возможность повреждения самих взаимодействующих абонентов при оценивании устойчивости ИТКС не учитывается.

Для (1-*N*)-полюсной структуры задача заключается в разработке методов и моделей для оценивания связности между центральным абонентом (управляющим) и *N* подчиненными (управляемыми) абонентами (рис. 2).

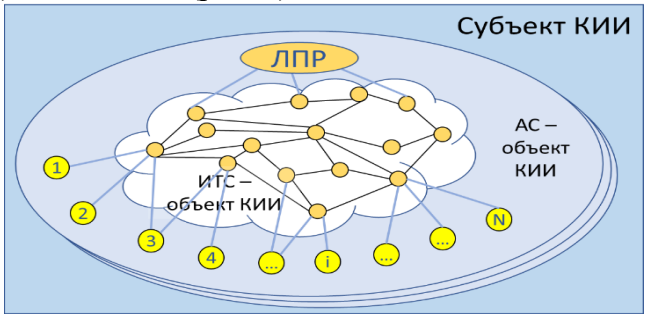

Рис. 2. Вариант (1-*N*)-полюсной структуры информационно-телекоммуникационной сети
Fig. 2. Option (1-*N*)-pole structure of information and telecommunication network

Подобные задачи характерны для систем централизованного управления. Центральному полюсу сопоставляется высшее звено системы управления объекта КИИ, осуществляющее формирование и передачу управляющих приказов (сигналов) централизованного управления, а также, примем, обработку донесений об исполнении команд от управляемых объектов. Конечным полюсам сопоставляются управляемые элементы (объекты управления), которые в ответ на управляющие команды, поступающие от ЛПР, обеспечивают их исполнение, формируют и передают соответствующие донесения.

Таким образом реализуются информационные технологии для поддержки процессов централизованного управления. Связность каждого периферийного элемента с центральным обеспечивается фрагментом ИТКС, имеющим двухполюсную структуру, которая может быть обозначена совокупностью (1,*i*)-двухполюсных структур, *i*=1, 2, …*N*, где *N* – число управляемых объектов или число двухполюсных структур. Объект управления считается управляемым если он находится в состоянии «функционален» и имеет возможность двухстороннего обмена сообщениями с ЛПР.

Постановка задачи оценивания устойчивости ИТКС на вербальном уровне может быть сформулирована следующим образом: пусть имеется центральный элемент оцениваемой системы управления, который позиционируется как ЛПР, и *N* периферийных элементов обеспечивающих исполнение управляющих команд и формирующих соответствующее донесение об их исполнении, требуется разработать методы, модели и средства для оценивания устойчивости функционирования ИТКС.

Для (*N*-*N*) структуры (рис. 3) задача оценивания устойчивости ИТКС может быть сформулирована следующим образом: пусть имеется *K* пар абонентов, между которым требуется обеспечить обмен сообщениями в условиях воздействия угроз безопасности информации.

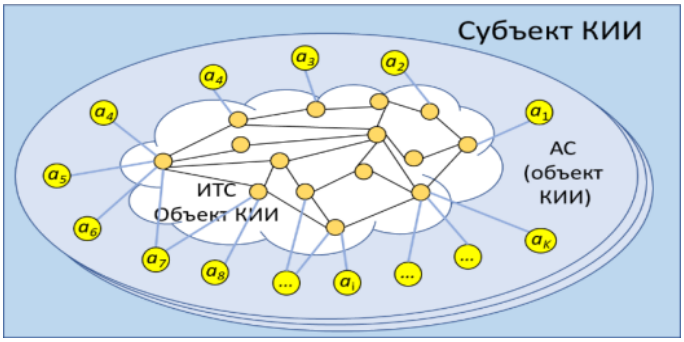

Рис. 3. Вариант (*N*-*N*)-полюсной структуры информационно-телекоммуникационной сети
Fig. 3. Variant (*N*-*N*)-pole structure of information and telecommunication network

Таким образом реализуется технологический процесс взаимодействия между объектами КИИ. Связность между абонентами обеспечивается совокупностью (1,*i*)-двухполюсных структур, *i*=1, 2, …*K*, где *K* – число возможных взаимодействующих пар. При этом принимается условие, что возможность поражения самих взаимодействующих элементов не учитывается.

Обсуждение результатов. Постановка частных задач оценивания важности элементов, входящих в состав объекта информатизации. Для заданных исходных данных, характеризующих:

а) сценарий воздействия угроз $Z=\{\eta_k, n\}$, η_k – ожидаемый момент времени воздействия *k*-й угрозы, *n* – ожидаемое число воздействий угроз в течение периода $(0, T]$, *T* – ожидаемый момент времени окончания массированного воздействия угроз. Характеристики сценария воздействия угроз определяются экспертными методами, в ходе учений или путем регистрации соответствующих событий, если таковые имели место;

б) структуру ИТКС $S=\{A, L\}$, где $A=\{a_i\}$ – множество элементов, входящих в состав структуры оцениваемого объекта, $i=1, 2, \ldots, N$, N – мощность множества A, $L=\{l_{ij}\}$ – множество связей между элементами, l_{ij} – идентификатор *ij*-й связи, если связи между *i*-м и *j*-м элементами предусмотрена проектной документацией то $l_{ij}=1$, $l_{ij}=0$ – в противном случае. $l_{ij}=-1$, если связь была предусмотрена проектной документацией, но была нарушена в результате воздействия угрозы. Определяется на основании технической документации на объект;

в) защищенность от воздействия угроз отдельных элементов $P(u)=\{p_i(u)\}$, где $p_i(u)$ – вероятность поражения *i*-го элемента при воздействии *u*-й угрозы ИБ, $u \in U_i$, где U_i – множество актуальных угроз для *i*-го элемента. Определяется экспертными методами, в ходе учений;

г) $V(u)=\{v_i(u)\}$ восстанавливаемость функциональности объекта информатизации после воздействия *u*-й угрозы, где v_i – показатель, характеризующий восстанавливаемость *i*-го элемента, $v_i(u)=\{\tau_{i\text{н}}(u), \tau_{i\text{в}}(u)\}$, где $\tau_{i\text{н}}(u)$ – нижняя оценка времени восстановления функциональности *i*-го элемента при воздействии *u*-й угрозы, $\tau_{i\text{в}}$ – верхняя оценка времени восстановления функциональности *i*-го элемента при воздействии *u*-й угрозы. Определяются с помощью моделирования процесса восстановления функциональности либо с помощью экспертных методов, либо в результате учений;

д) Π_0 – показатель, характеризующий требуемые производственные возможности подсистемы восстановления функционала: $\Pi_0=\{\boldsymbol{R}_0, \boldsymbol{D}_0\}$, где $\boldsymbol{R}_0=\{r_{0i}\}$ – совокупность типов расходуемого ресурса, имеющегося в составе системы восстановления функциональности для восстановления элемента, $i=1, 2, \ldots, m$; m – число типов невозобновляемого ресурса (пример невозобновляемого ресурса – запасные части, расходный материал и т. п.); $\boldsymbol{D}_0=\{d_{0i}\}$ – совокупность типов возобновляемого ресурса, имеющегося в составе системы восстановления функционала, $i=1, 2, \ldots, k$, k – число типов возобновляемого ресурса (пример возобновляемого ресурса – люди, измерительные приборы и т. п., которые могут использоваться многократно);

е) показатель, характеризующий требуемые производственные возможности расчета восстановления: $\Pi^{\text{Тр}}=\left\{\boldsymbol{R}^{\text{Тр}}, \boldsymbol{D}^{\text{Тр}}\right\}$ – показатель, характеризующий требуемые производственные возможности расчета восстановления, где $\boldsymbol{R}^{\text{Тр}}=\left\{r_i^{\text{Тр}}\right\}$ – совокупность соответствующих единиц невозобновляемого ресурса каждого типа, требуемых для восстановления функционала элемента после успешного воздействия угрозы безопасности информации по *i*-му элементу, $i=1, 2, \ldots, m$, m – число требуемых типов расходуемого ресурса для восстановления функциональности *i*-го элемента; $\boldsymbol{D}^{\text{Тр}}=\left\{d_i^{\text{Тр}}\right\}$ – совокупность типов возобновляемого ресурса, требуемого для восстановления функциональности *i*-го элемента, $i=1, 2, \ldots, k$, k – число требуемых типов возобновляемого ресурса. Требуется разработать методы, модели и средства для оценивания «веса», «значимости» и «вклада»

элементов, входящих в состав объекта страхования. Поставленная задача решается в следующем порядке:

а) разрабатываются методы и модели в соответствии с [19, 21] для расчета функций живучести $\varphi_i(t)$ отдельных элементов, входящих в состав оцениваемого объекта (ИТКС);

б) с помощь методов и моделей, приведенных в [20, 23], рассчитывается функция живучести $\Phi(t)=\{\varphi_i(t)\}$ объекта оценивания и осуществлялся поиск ее минимального значения $\Phi_m = \min\limits_{t\in(0,T]}\left(Z, S, P(u), V(u), \Pi_0, t\right)$. Функция живучести оцениваемого объекта характеризует вероятность того, что он будет находиться в состоянии «функционален» в момент времени t, $t \in (0, T]$.

в) с помощью методов, моделей и средства, приведенных в [24], осуществляется оценивание «веса», «значимости» и вклада отдельных элементов в обеспечение устойчивости функционирования объекта ИТКС.

Понижение минимального значения Φ_m функции живучести $\Phi(t)$ ниже некоторого, наперед заданного порогового значения $\Phi_{Тр}$, предлагается использовать в качестве триггера, обозначающего наступление страхового события.

Для методической поддержки параметрического микрострахования потребуются модели и методы, позволяющие оценить важность каждого из элементов и, на основании этой оценки, задать соответствующий триггер. Но при этом предлагается использовать функции живучести отдельных элементов $\varphi_i(t)$ и показатели, характеризующие важность $w_i = \{\text{вес}_i, \text{значимость}_i, \text{вклад}_i\}$ каждого из элементов в обеспечении устойчивости функционирования объекта оценивания в целом.

Вес [24]**.** Это показатель важности элемента, который может использоваться при отсутствии информации об устойчивости его функционирования. Вес элемента характеризует относительное число таких *критических* состояний объекта, в которых потеря функциональности данного элемента приводит к потере функциональности всего объекта (и, наоборот, восстановление его функциональности приводит к восстановлению функциональности всего объекта), среди всех возможных состояний оцениваемого объекта. Вес элемента характеризует только местоположение его в структуре объекта.

Значимость [24]**.** Это показатель важности элемента, который характеризует изменение вероятности сохранения функциональности объекта оценивания при условии, что оцениваемый элемент «функционален» и «не функционален». Другими словами, этот показатель отражает как реагирует показатель устойчивости функционирования объекта в целом на исключение оцениваемого элемента из структуры. Вес элемента есть частный случай его значимости при одинаковой функциональности всех элементов и вероятности сохранения функциональности равной 0,5. Показатель значимости характеризует не только местоположение оцениваемого элемента, но и зависимость от вероятности сохранения функциональности всех других элементов, кроме самого оцениваемого элемента.

Вклад [24]**.** Это показатель важности элемента, который характеризует местоположение оцениваемого элемента в структуре объекта, условия ее функционирования и связь с вероятностью безотказной работы всех элементов, включая и оцениваемый элемент.

Таким образом, приведенные частные показатели важности элементов имеют различную информационную сущность и позволяют реализовать параметрическое микрострахование рисков ИБ.

Для оценивания названных характеристик требуется формализованное (аналитическое) описание условий функциональности объекта оценивания. Недостатком существующих методов оценивания, ссылки на которые приведены выше, является именно невысокая степень формализации процедуры оценивания для условий воздействия угроз. Основной целью, связанной с оцениванием устойчивости функционирования того или иного объекта, является стремление очистить объект от всего вторичного, рассмотреть лишь его наиболее характерные признаки. Таким образом, в качестве модели информаци-

онной системы предлагается выбирать ее структурную схему, отображающую некоторую совокупность отношений.

Знание структурной схемы объекта оценивания дает возможность определять «слабые места», сосредотачивать страховые усилия на наиболее важных, с точки обеспечения функциональности объекта, элементах. При этом методы исследования структуры позволяют не только количественно оценивать устойчивость функционирования, но и оценивать роль отдельных элементов (и их различных комбинаций) в обеспечении устойчивости функционирования всего объекта оценивания. С этой целью предлагается использовать показатель важности того или иного элемента, который может отражать «вес», «значимость», «вклад» элемента в процессе обеспечения устойчивости функционирования всего объекта в целом.

Вывод. Таким образом, зная оценку важности того или иного элемента, можно обосновать решение о необходимости страхования рисков, связанных с нарушением его функционала. При этом возможно мотивированно отказаться от страхования риска потери функциональности всего объекта и сосредоточится на самых уязвимых элементах. Предлагаемый подход позволяет управлять страховой премией, страховым покрытием, а также страховать наиболее важные элементы и воздерживаться от страхования менее значимых, принимая риск на себя. Внедрение параметрического и микропараметрического страхования позволит обеспечить гибкость управления рисками ИБ. Перспективным направлением исследования является разработка методов и моделей построения функций «веса», «значимости», «вклада» на рассматриваемом интервале времени воздействия угроз, что позволит учитывать их динамику при принятии решения.

Благодарности. Статья подготовлена при поддержке Фонда Потанина.

Acknowledgments. The article was prepared with the support of the Potanin Foundation.

Библиографический список:

1. Садовничий В.А., Акаев А.А., Коротаев А.В., Малков С.Ю. Моделирование и прогнозирование мировой динамики / Научный совет по Программе фунд. исслед. Президиума Российской академии наук «Экономика и социология знания». – М.: ИСПИ РАН (Экономика и социология знания), 2012. – 359 с.
2. Глазьев С.Ю. Экономика и общество / С.Ю. Глазьев, А.В. Щипков. – Москва : Общество с ограниченной ответственностью "Проспект", 2022. – 192 с.
3. Глазьев С.Ю. Стратегия опережающего развития России в условиях глобального кризиса / С.Ю. Глазьев. – Москва : Экономика, 2010. – 287 с.
4. Энциклопедия финансового риск-менеджмента[В.Е. Барбаумов и др.] ; под ред. А.А. Лобанова и А.В. Чугунова. – 4-е изд. – Москва : Альпина Бизнес Букс, 2009. – 931 с.
5. R. Sobers, “98 must-know data breach statistics for 2021” Varonis, May 2021.
6. F. Perumannil, Sabir & Haneef, “Latest trends in cybersecurity after solarwind hacking attack,” Journal of Cyber Security and Mobility, vol. 1, Jan. 2021.
7. O. Analytica, “Critical infrastructure sees rising cybersecurity risk” Emerald Expert Briefings, 2021.
8. F. Curti et al., “Cyber risk definition and classification for financial risk management” Federal Reserve Bank of Richmond, 2019.
9. Gartner, Inc., “Reviews for security threat intelligence products and services reviews and ratings” Worldwide In: Gartner peer insights. https://www.gartner.com/reviews/market/security-threat-intelligence-services, 2019.
10. Coulson, T., Mason, M., & Nestler, V. (2018). Cyber capability planning and the need for an expanded cybersecurity workforce. Communications of the IIMA: Vol. 16: Iss. 2, Article 2 DOI: https://doi.org/10.58729/1941-6687.1401. Retrieved March 6, 2023, from https://scholarworks.lib.csusb.edu/ciima/vol16/iss2/2/BitSight, “Global financial firm reduces risk of third-party breach with bitsight security ratings,” BitSight Website: https://info.bitsight.com/bitsightcase-study-global-financial-firm, 2019.
11. Hoffmann, R., Napiórkowski, J., Protasowicki, T., & Stanik, J. Risk based approach in scope of cybersecurity threats and requirements. Procedia Manufacturing, 2020;44:655-662 https://doi.org/10.1016/j.promfg.2020.02.243.
12. ГОСТ Р 59516–2021. Информационные технологии. Менеджмент информационной безопасности. Правила страхования рисков информационной безопасности. Утвержден и введен в действие

Приказом Федерального агентства по техническому регулированию и метрологии от 20 мая 2021 г. N 420-ст. М.: Стандартинформ. 2021. – 20 с.
13. Косарев А.В. Страхование информационных рисков : автореферат дис. ... кандидата экономических наук : 08.00.10 / Финансовая акад. при Правительстве РФ. - Москва, 2004. - 23 с.
14. Доктрина информационной безопасности Российской Федерации, утверждена Указом Президента Российской Федерации от 05.12.2016 г. № 646 // Консультант Плюс: справ.-правовая система.
15. Федеральный закон "Об информации, информационных технологиях и защите информации" от 27.07.2006 N 149-ФЗ // СПС Консультант Плюс: справ.-правовая система.
16. Воеводин В.А. Генезис понятия структурной устойчивости информационной инфраструктуры автоматизированной системы управления производственными процессами к воздействию целенаправленных угроз информационной безопасности // Вестник Воронежского института ФСИН России. 2023. № 2. С. 30–41.
17. Методика оценки угроз безопасности информации. Методический документ ФСТЭК России от 5 февраля 2021г. Официальный сайт ФСТЭК России [Электронный ресурс]. – URL: https://fstec.ru/component/attachments/download/2919 (дата обращения 08.04.2021).
18. Васильев В.И., Вульфин А.М., Кириллова А.Д., Кучкарова Н.В. Методика оценки актуальных угроз и уязвимостей на основе технологий когнитивного моделирования и Text Mining // Системы управления, связи и безопасности. 2021. № 3. С. 110–134. DOI: 10.24412/2410-9916-2021-3-110-134.
19. Воеводин В.А. Математическая модель оценивания устойчивости функционирования элемента информационной инфраструктуры автоматизированной системы управления, подверженной воздействию угроз информационной безопасности. "Информационные технологии», №1. Том 30. 2024. DOI: 10.17587/it.30.23-31. С. 23–31.
20. Воеводин В.А., Крахотин Н.А. Методы оценивания связности неориентированного двухполюсного помеченного графа с учетом деструктивного воздействия внешних угроз на его вершины . Вестник Дагестанского государственного технического университета. Технические науки. 2024; 51(1):46-60. DOI:10.21822/2073-6185-2024-51-1-46-6046
21. Воеводин В.А. Модель оценки функциональной устойчивости элементов информационной инфраструктуры для условий воздействия множества компьютерных атак. Информатика и автоматизация. 2023. Том 22 № 3. – С. 691–715. https://DOI 10.15622/ia.22.3.8.
22. Воеводин В.А., Виноградов И.В., Волков Д.И. Об оценке устойчивости функционирования объекта информатизации в условиях компьютерных атак при экспоненциальном законе распределения времени до воздействия противника и восстановления работоспособности. Вестник Дагестанского государственного технического университета. Технические науки. 2022; 49(3): 39-51. DOI:10.21822/2073-6185-2022-49-3-39-51.
23. Свидетельство о государственной регистрации программы для ЭВМ № 2023683185 РФ. Программа расчета функции живучести графа двухполюсной структуры, подверженной угрозам информационной безопасности. Свидетельство о государственной регистрации базы данных № 2024614666 от. 28.02.2024. (RU). Бюл. № 3 28.02.2024. Воеводин В.А., Крахотин Н.А.
24. Хохлачев Е. Н. Организация и технологии выработки решений при управлении системой и войсками связи. Часть 2. Выработка решений при восстановлении сетей связи. – М.: ВА РВСН, 2009. 241 с.

References:

1. Sadovnichy V.A., Akaev A.A., Korotaev A.V., Malkov S.Yu. Modeling and forecasting of world dynamics. Scientific Council for the Fundamental Program. research Presidium of the Russian Academy of Sciences "Economics and Sociology of Knowledge". M.: ISPI RAS (Economics and Sociology of Knowledge), 2012;359. (In Russ)
2. Glazyev S.Yu. Economy and society/ S.Yu. Glazyev, A.V. Shchipkov. Moscow: Limited Liability Company “Prospekt”, 2022; 192. (In Russ)
3. Glazyev, S.Yu. Strategy for advanced development of Russia in the context of the global crisis / S.Yu. Glazyev. Moscow: Economics, 2010; 287. (In Russ)
4. Encyclopedia of financial risk management [V.E. Barbaumov et al.]; edited by A.A. Lobanov and A.V. Chugunov. 4th ed. Moscow: Alpina Business Books, 2009; 931. (In Russ)
5. R. Sobers, “98 must-know data breach statistics for 2021” Varonis, May 2021.
6. F. Perumannil, Sabir & Haneef, “Latest trends in cybersecurity after solarwind hacking attack,” Journal of Cyber Security and Mobility, 2021, 1, Jan.
7. O. Analytica, “Critical infrastructure sees rising cybersecurity risk” Emerald Expert Briefings, 2021.
8. F. Curti et al., “Cyber risk definition and classification for financial risk management” Federal Reserve Bank of Richmond, 2019.
9. Gartner, Inc., “Reviews for security threat intelligence products and services reviews and ratings” World-wide. In: Gartner peer insights. https://www.gartner.com/reviews/market/security-threat-intelligence-services, 2019.

10. Coulson, T., Mason, M., & Nestler, V. Cyber capability planning and the need for an expanded cybersecurity workforce. Communications of the IIMA: 2018; 16(2), Article 2 DOI: https://doi.org/10.58729/1941-6687.1401. Retrieved March 6, 2023, from https://scholarworks.lib.csusb.edu/ciima/vol16/iss2/2/BitSight, "Global financial firm reduces the risk of third-party breach with bitsight security ratings," BitSight Website: https http://info.bitsight.com/bitsightcase-study-global-financial-firm, 2019.
11. Hoffmann, R., Napiórkowski, J., Protasowicki, T., & Stanik, J. Risk based approach in scope of cybersecurity threats and requirements. Procedia Manufacturing. 2020;44:655-662 https://doi.org/10.1016/j.promfg.2020.02.243.
12. GOST R 59516–2021. Information technology. Information security management. Information security risk insurance rules. Approved and introduced put into effect by Order of the Federal Agency for Technical Regulation and Metrology dated May 20, 2021 N 420-st. M .: Standartinform. 2021; 20. (In Russ)
13. Kosarev A.V. Insurance of information risks: abstract of diss. .. . candidate of economic sciences: 08.00.10 Financial Academy under the Government of the Russian Federation. Moscow, 2004; 23. (In Russ)
14. The Doctrine of Information Security of the Russian Federation, approved by the Decree of the President of the Russian Federation dated 05.12.2016; 646 // Consultant Plus: reference and legal system. (In Russ)
15. Federal Law "On Information, Information Technologies and Information Protection" dated 27.07.2006 N 149-FZ // SPS Consultant Plus: reference and legal system. (In Russ)
16. Voevodin V.A. Genesis of the concept of structural stability of the information infrastructure of an automated production process control system to the impact of targeted threats to information security. *Bulletin of the Voronezh Institute of the Federal Penitentiary Service Rossii.* 2023; 2:30–41. (In Russ)
17. Methodology for assessing information security threats. Methodological document of the FSTEC of Russia dated February 5, 2021 // Official website of the FSTEC of Russia [Electronic resource]. – URL: https://fstec.ru/component/attachments/download/2919 (date of access 08.04.2021). (In Russ)
18. Vasiliev V.I., Vulfin A.M., Kirillova A.D., Kuchkarova N.V. . Methodology for assessing current threats and vulnerabilities based on cognitive modeling and Text Mining technologies. *Control, Communications and Security Systems*. 202;3:110–134. DOI: 10.24412/2410-9916-2021-3-110 -134. (In Russ)
19. Voevodin V.A. Mathematical model for assessing the stability of functioning of an element of the information infrastructure of an automated control system exposed to information security threats. "*Information Technologies*", 2024; 30(1): 23–31. DOI: 10.17587/it.30.23-31.
20. Voevodin V.A., Krakhotin N.A. Methods for Estimating the Connectivity of an Undirected Bipolar Labeled Graph with taking into account the destructive impact of external threats on its peaks. *Herald of the Dagestan State Technical University. Technical Sciences*. 2024; 51(1):46-60. DOI:10.21822/2073-6185-2024-51-1-46-6046 (In Russ)
21. Voevodin V .A. Model for assessing the functional stability of information infrastructure elements under conditions of exposure to multiple computer attacks. *Computer Science and Automation*. 2023; 22(3):. 691–715. https://DOI 10.15622/ia.22.3.8. (In Russ)
22. Voevodin V.A., Vinogradov I.V., Volkov D.I. On the assessment of the stability of the functioning of an informatization object under computer attacks with an exponential law of distribution of time before the enemy's impact and restoration of operability. *Herald of the Dagestan State Technical University. Technical sciences*. 2022; 49(3): 39-51. DOI:10.21822/2073-6185-2022-49-3-39-51. (In Russ)
23. Certificate of state registration of the computer program No. 2023683185 of the Russian Federation. Program for calculating the survivability function of a graph of a two-pole structure exposed to information security threats. Certificate of state registration of the database No. 2024614666 dated. 02/28/2024. (RU). *Bulletin № 3 02/28/2024*. Voevodin V.A., Krakhotin N.A. (In Russ)
24. Khokhlachev E.N. Organization and technologies of decision-making in managing the communications system and troops. Part 2. Decision-making in restoring communications networks. M.: VA RVSN, 2009; 241. (In Russ)

Сведения об авторе:

Воеводин Владислав Александрович, кандидат технических наук, доцент кафедры информационной безопасности; vva541@mail.ru

Information about author:

Vladislav A. Voevodin, Cand. Sci. (Eng.), Assoc. Prof., Department of Information Security; va541@mail.ru

Конфликт интересов/Conflict of interest.

Автор заявляет об отсутствии конфликта интересов/The author declare no conflict of interest.

Поступила в редакцию/ Received 13.05.2024.

Одобрена после рецензирования / Reviced 10.06.2024.

Принята в печать /Accepted for publication 10.06.2024.