МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ / METHODS AND SYSTEMS OF INFORMATION PROTECTION, INFORMATION SECURITY

DOI: https://doi.org/10.60797/IRJ.2024.146.38

ЭКОНОМИКА КИБЕРБЕЗОПАСНОСТИ: АНАЛИТИЧЕСКИЕ МОДЕЛИ

Научная статья

Милаков А.С.[1, *]
[1] ORCID : 0009-0007-9029-7993;
[1] Студия MissoffDesign, Санкт-Петербург, Российская Федерация

* Корреспондирующий автор (as[at]infsecacademy.com)

Аннотация

В статье рассматриваются актуальные вопросы кибербезопасности в условиях расширяющего ландшафта угроз, привнесённых цифровой трансформацией. Рассмотрены вопросы экономики кибербезопасности на основе оценки рисков. Рассмотрена и решена задача оптимального вложения инвестиций в средства обеспечения информационной безопасности (ИБ) с учётом допустимого ущерба в активы систем информационно-коммуникационных технологий (ИКТ), что является одной из актуальных задач экономики кибербезопасности.

В настоящей работе деятельность по минимизации рисков ИБ рассмотрена как решение экстремальной задачи, и предложен метод ее формализации на основе математического аппарата для этого класса задач – линейного программирования (ЛП). На основе решения задач ЛП, а также сложившихся «лучших практик», приведены базовые уравнения аналитических моделей расчёта рисков нарушения ИБ продуктов и систем информационных технологий.

Ключевые слова: экономика, кибербезопасность, информационная безопасность, риски, угрозы, ущерб, активы, линейное программирование, уравнения, аналитическая модель.

ECONOMICS OF CYBERSECURITY: ANALYTICAL MODELS

Research article

Milakov A.S.[1, *]
[1] ORCID : 0009-0007-9029-7993;
[1] Studio MissoffDesign, Saint-Petersburg, Russian Federation

* Corresponding author (as[at]infsecacademy.com)

Abstract

The article examines current issues of cybersecurity in the context of the expanding threat landscape brought by digital transformation. Issues of the economics of cybersecurity based on risk assessment are considered. The problem of optimal investment in information security (IS) means, taking into account acceptable damage to the assets of information and communication technology (ICT) systems, is considered and solved, which is one of the urgent tasks of the economics of cybersecurity.

In this paper, activities to minimize information security risks are considered as a solution to an extremal problem, and a method of its formalization is proposed based on the mathematical apparatus for this class of problems – linear programming (LP). Based on the solution of LP problems, as well as established “best practices”, the basic equations of analytical models for calculating the risks of violation of information security of products and information technology systems are given.

Keywords: economics, cybersecurity, information security, risks, threats, damage, assets, linear programming, equations, analytical model.

Введение

Четвёртая промышленная революция (Индустрия 4.0.) и порождённая ею цифровая трансформация (ЦТ) общественных и производственных отношений вызвали бурное развитие информационно-коммуникационных технологий (ИКТ), что, в свою очередь, расширило ландшафт возможных угроз и уязвимостей на поле цифрового социума. Эти факторы приводят к тому, что предъявляются повышенные требования к средствам и механизмам защиты и распознаванию уязвимостей продуктов и систем ИКТ. Таким образом, пресловутое состязание «снаряда и брони» продолжается уже на новом качественном уровне. И в этом состязании по мере всё возрастающего потенциала нарушителя должна совершенствоваться и система защиты от киберугроз конкретных систем ИКТ. Защита информации (ЗИ) продуктов и систем ИКТ требует соответственных инвестиций в средства обеспечения ИБ контента и самой системы от последствий реализации кибератак. Среди практикующих специалистов по ИБ сложилась практическая оценка инвестиций в безопасность систем ИКТ в размере до 30% от стоимости системы. Такая опосредованная оценка является аналогией «средней температуре тела по больнице» и не учитывает многих особенностей информационных систем и важности обрабатываемых или хранимых в них данных, таких как системы критической информационной инфраструктуры (КИИ) или системы, оперирующие с государственными секретами.

Таким образом, задача нахождения оптимального вложения инвестиций в средства обеспечения ИБ, с учётом допустимого ущерба в активы систем ИКТ, является одной из актуальных задач экономики кибербезопасности.

Далее, исходя из вышеизложенных принципов, перейдём к конкретной реализации наших исследований.

Методика научных исследований

В исследовании применены методы математического программирования (симплекс-метод), экспертной оценки, анализа оптимальных инвестиций в ИБ, группировки и сравнения.

Цель работы:

1) обобщить литературные источники по экономическим проблемам информационной безопасности;

2) рассмотреть проблему минимизации рисков ИБ как решение экстремальной задачи;

3) предложить решение экстремальной задачи методом ее формализации на основе линейного программирования.

Основной целью работы является разработка методики, с помощью которой организация может определить, сколько рекомендуется инвестировать в защиту цифрового информационного актива.

Для достижения этой цели в данной работе будут рассмотрены следующие три исследовательских вопроса:

1. Как можно определить расходы на оборону и рассчитать потери?

2. Как можно измерить эффективность контроля безопасности с точки зрения снижения вероятности будущих потерь?

3. Как можно оптимизировать инвестиции в кибербезопасность, направленные на защиту актива?

Аналитические модели экономики кибербезопасности

Рассмотрим основные понятия и определения кибербезопасности, столь тонкой и специфичной именной сущности информационного мироздания, с учётом новых видов противоборства в киберпространстве [1].

В связи с глобальными изменениями в геополитической ситуации в мире, которые происходят начиная с 2020 года (пандемия коронавируса, СВО, локальные кризисы во многих странах) увеличилось количество различных кибероперациий, которые можно смело отнести к кибервойнам. За ними часто стоят хакерские группировки, спонсируемые спецслужбами различных стран. Действия таких группировок стали инструментами политического давления, в результате которого особенно страдает финансовая система.

Кибербезопасность – представляет собой совокупность средств, стратегий, принципов обеспечения безопасности, гарантий безопасности, подходов к управлению рисками, действий, профессиональной подготовки, страхования и технологий, которые применяются для защиты киберпространства, ресурсов организаций и пользователей.

Киберпространство – это совокупность информационных систем (в том числе банков и баз данных, телекоммуникационных систем), технологий их сопровождения и использования.

Существует и другое понятие киберпространства.

Киберпространство — это среда информационных технологий, которая включает в себя связанные между собой сети и ИТ-инфраструктуры, в которых сотрудники пересылают друг другу данные и постоянно работают. Также в этой среде киберпреступники осуществляют вредоносную деятельность с целью получения финансовой выгоды, по политическим мотивам и др. причинам, используя разные виды атак, которые совершенствуются с течением времени.

Риск – это вероятность реализации угрозы информационной безопасности. Оценка рисков заключается в моделировании картины наступления неблагоприятных условий в виде учета возможных факторов, определяющих риск. Данные понятия будут определены нами как основа риск-ориентированного подхода в оценке экономики кибербезопасности.

Согласно исследованию [10], экономика кибербезопасности – это область знаний, связанная с проблемой, достаточно ли организация тратит на защиту своих активов и тратится ли бюджет на безопасность на правильные средства защиты. Расходы на оборону – это то, что организация решила инвестировать для защиты своих активов. Несмотря на растущее количество исследований в области экономики кибербезопасности, вопрос для специалистов по кибербезопасности о том, сколько инвестировать в защиту информационных активов организации, остается открытым.

Экономика кибербезопасности применяет экономические принципы к анализу проблем кибербезопасности. По мнению авторов исследования [11], проблематика экономики кибербезопасности посвящена компромиссам между затратами и выгодами, с которыми сталкиваются рациональные участники рынка, их стратегическому поведению и рыночным результатам с точки зрения благосостояния участников. В экономике кибербезопасности участвуют не только компании и потребители, но и государственные и сторонние игроки, в том числе противники (хакеры и т. д.). Кроме того, эта область охватывает анализ рыночных механизмов и кризисов рынка, а также экономическое влияние регулирования на кибербезопасность. В основе экономики кибербезопасности лежат риски безопасности. Также важна финансовая выгода как мотивация для киберпреступности. Большая часть литературы в этой области посвящена моделированию решений об инвестициях в киберпреступность и кибербезопасность, измерению затрат на киберпреступность, моделированию страхования от киберпреступлений или влиянию обмена информацией между компаниями.

Исследователи в своем труде [11] отмечают такую специфическую область, как *экономика неприкосновенности частной жизни*, которая фокусируется на стимулах и действиях фирм и потребителей в отношении персональных данных пользователей. В основе анализа научной публикации [11] лежат риски (или неопределенность) для неприкосновенности частной жизни и амбивалентные последствия для благосостояния, возникающие в результате раскрытия персональных данных. Экономика конфиденциальности фокусируется на компромиссах между затратами и выгодами участников, их стратегических действиях, рыночных результатах и падениях рынка, подобно экономике кибербезопасности. Кроме того, эта область включает в себя изменение конкуренции между фирмами, которые персонализируют продукты или услуги и/или цены, сталкиваясь при этом с потребителями, которые неоднородны в предпочтениях в отношении конфиденциальности. В этой сфере большое значение имеет экономический эффект государственного регулирования.

Как правило, инвестиции в расходы на оборону и контроль безопасности направлены на защиту активов организации; когда это не удается, возникают расходы, связанные с ущербом и убытками. Эти два потока затрат исследуются авторами научного труда [10] для того, чтобы лучше понять, как классифицировать и количественно

оценивать такие затраты. В работе [10] авторы создали модель для количественной оценки затрат на кибербезопасность для повышения точности, объективности и сопоставимости. Критерий авторов этой модели для расчета затрат и выгод следующий:

а) затраты на управление информационной безопасностью (в данном исследовании называются затратами на оборону);

б) затраты, связанные с мерами информационной безопасности (в данном исследовании называются затратами на оборону);

в) затраты, связанные с инцидентами информационной безопасности (в данном исследовании называются потерями);

г) стоимость капитала, вызванная рисками информационной безопасности (рассматривается вне рамок данного исследования).

Далее авторы в работе [10] описывают аналитическую модель экономики кибербезопасности, основанную на оценке рисков. Это подход ISMS-Layers к количественной оценке затрат на информационную безопасность, который рассматривает перспективу управления информационной безопасностью. Согласно ISMS (Information Security Management System) – это процесс управления рисками, в котором участвуют люди, процессы и технологии для защиты активов организаций. Далее авторы работы [10] обсуждают измерение, определяемость (сложность атрибуции безопасности) и коэффициент затрат на информационную безопасность (процент, относимый к безопасности).

Подход ISMS-Layers представляется адекватным для определения затрат на информационную безопасность. Коэффициент затрат на безопасность, каким бы привлекательным он ни был, менее полезен, поскольку следует ожидать существенных различий между организациями. Предполагается, что операционные показатели являются прямыми затратами, а другие уровни – косвенными. Таким образом, для оценки затрат и выгод от защиты актива необходимо дальнейшее изучение того, как могут быть определены затраты на оборону и рассчитаны убытки. Далее необходимо задать следующий вопрос для правильного построения модели экономики кибербезопасности: как определить расходы на оборону и рассчитать потери?

Данный исследовательский вопрос будет проверяться с помощью следующих утверждений:

Предложение А: Прямые расходы на оборону могут быть определены как любые расходы на безопасность, которые направлены исключительно на защиту одного или нескольких, но не всех активов.

Предложение Б: Косвенные расходы на оборону можно определить как любые затраты на безопасность, которые направлены на защиту всех активов.

Предложение В: Расходы на оборону могут быть разделены между некоторыми или всеми активами, а также между бюджетами, связанными с безопасностью, и бюджетами, не связанными с безопасностью.

Предложение Г: Стоимость ущерба и убытков, вызванных киберинцидентом, может быть разделена на краткосрочные и долгосрочные потери.

В следующем разделе перейдем непосредственно к построению математической модели, основанной на анализе рисков.

3.1. Методы оценки рисков

В настоящей работе проблема по нахождению минимума рисков ИБ предложена как решение экстремальной задачи, и найдена методика ее формализации на основе математического аппарата для этого класса задач – линейного программирования (ЛП). Как известно, задача ЛП представляет собой набор переменных $\mathbf{x} = (x_1, x_2, \dots x_n)$ и функции этих переменных $\mathbf{f(x)} = f(x_1, x_2, \dots x_n)$, т.е. целевую функцию.

Далее решается проблема нахождения экстремума целевой функции f(x), при условии, что переменные **x** принадлежат некоторой области G.

Такая задача является транспортной задачей ЛП, она служит объединением многих задач в единую математическую модель. Необходимо отметить, что задачи такого класса обладают большим количеством переменных, а это значит, что решить их простыми методами очень трудно.

Если рассмотреть детально данную задачу, то к ней прилагаются большие системные ограничения, что требует достаточно специфических методов решения.

Эти методы заключаются в нахождении начального решения, а затем в постепенном улучшении его. Таким образом, мы приходим к последовательности эталонных решений, итогом которых становится оптимальное решение.

Исходя из подобных предпосылок, рассмотрим существующие методы и лучшие практики экономической оценки минимизации рисков систем и продуктов ИТ.

Существующие международные стандарты в области менеджмента риска ИБ допускают использование как количественных, так и качественных методов оценки рисков. В предыдущем разделе был упомянут метод ISMS-Layers, который базируется на международных стандартах по ИБ.

Хорошо описанный в научной литературе вариант решения этой задачи, согласуемый с международными стандартами, заключается в перемножении вероятности реализации угрозы на значение величины ущерба. Далее идет сопоставление результата с заданной шкалой результатов. Таким образом, проблема уменьшения риска обобщенно описывается как усилия, предпринятые для снижения вероятности, негативных последствий или того и другого вместе, связанных с риском.

Согласно ISO/IEC 27001 «Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования» [2], выбранная модель должна давать гарантию, что оценки риска показывают сравнимые и воспроизводимые результаты. В самом же стандарте не показываются формулы расчета.

Национальный институт стандартов США (NISA) в своём руководстве NIST 800-30 «Risk management guide for information technology systems» дает классическую формулу расчета риска [3]:

$$R = P(t) \cdot S \quad (1)$$

где R – значение риска;

P(t) – вероятность реализации угрозы информационной безопасности (применяется смесь качественной и количественной шкалы);

S – степень влияния угрозы на актив (цена актива в качественной и количественной шкале).

По вышеприведенной формуле можно определить значение риска в относительных единицах. А далее это значение можно ранжировать по уровню значимости для процесса управления рисками информационной безопасности.

По ГОСТ Р ИСО/МЭК ТО 13335-3-2007 «Информационные технологии. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий» [4], вычисление величины риска, в отличие от стандарта NIST 800-30 «Risk management guide for information technology systems. Recommendations of the National Institute of Standards and Technology», производится по следующей формуле:

$$R = P(t) \cdot P(v) \cdot S \quad (2)$$

где P(t) – вероятность реализации угрозы информационной безопасности;

P(v) – вероятность наличия уязвимости;

S – ценность актива.

Значения вероятностей P(t) и P(v) могут быть в виде трех показателей (низким, средним и высоким). S представлено в интервале от 0 до 4. Конкретно сопоставить S необходимому значению предстоит специалисту по ИБ в конкретной организации.

Согласно BS ISO/IEC 27001: 2005 (7799-2:2005). «Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования» [5], уровень риска вычисляется с учетом следующих показателей: ценности ресурса, уровня угрозы и степени уязвимости. При возрастании этих значений риск возрастает. Таким образом, формулу можно представить данным образом:

$$R = S \cdot L(t) \cdot L(v) \quad (3)$$

где S – ценность актива (ресурса);

L(t) – уровень угрозы;

L(v) – уровень (степень уязвимости).

В реальных условиях определение рисков ИБ проводится по специальным таблицам, в которых уже приведены значения уровня угроз, степени вероятности использования уязвимости и стоимости актива. Таким образом, величина риска может быть в диапазоне от 0 до 8. Исходя из этих данных, по каждому активу выдается список угроз с разными величинами риска. Согласно международному стандарту, шкала ранжирования рисков:

1) низкий (0–2);

2) средний (3–5);

3) высокий (6–8).

Применяя данную шкалу, можно выявить наиболее критичные риски.

Согласно РС БР ИББС-2.2-200 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения информационной безопасности» [6], оценка степени возможности реализации угрозы информационной безопасности вычисляется по следующей качественно-количественной шкале: нереализуемая угроза – 0%, средняя – от 21% до 50% и т. д.

В данном стандарте оперируют значениями капитала банка, выраженными в процентах. Таким образом, вычисление степени тяжести последствий для разных типов информационных активов проводится по качественно-количественной шкале: минимальное значение – 0,5% от величины капитала банка и высокое – от 1,5% до 3% от величины капитала банка.

Чтобы провести качественную оценку рисков информационной безопасности необходимо ориентироваться на таблицу соответствия степени тяжести последствий и вероятности реализации угрозы.

В случае вычисления количественной оценки применяется формула:

$$R = P(v) \cdot S \quad (4)$$

где S – ценность актива (степень тяжести последствий).

В итоге, отметим, что вычисление величины риска проводится исходя из значений угроз и ценности активов (размер ущерба). Результат получается в виде условных значений. Условные значения не имеют единиц измерения, применимых в практике, т.е., не являются денежным эквивалентом. Это означает, что полученные результаты не дают специалистам ИБ наглядного представления уровня риска, который можно перенести на реальные активы объекта защиты. Чтобы усовершенствовать формулы расчета рисков, было предложено разделить процедуру расчета риска на следующие этапы:

1) вычисление значения технического риска;

2) вычисление потенциального ущерба.

Технический риск – это риск информационной безопасности, состоящий из вероятностей реализации угроз и использования уязвимостей каждого компонента информационной инфраструктуры с учетом уровня их конфиденциальности, целостности и доступности.

Первый этап вычисляется с помощью следующих формул:

$$R_c = K_c \cdot P(T) \cdot P(V) \quad (8)$$

$$R_i = K_i \cdot P(T) \cdot P(V) \quad (9)$$

$$R_a = K_a \cdot P(T) \cdot P(V) \quad (10)$$

где R_c – значение риска конфиденциальности;
K_c – коэффициент конфиденциальности информационного актива;
P(T) – вероятность реализации угрозы;
P(V) – вероятность использования уязвимости;
R_i – значение риска целостности;
K_i – коэффициент целостности информационного актива;
R_a – значение риска доступности;
K_a – коэффициент доступности информационного актива.

Этот алгоритм дает возможность произвести более точную оценку риска и получить в результате безразмерное значение вероятности возникновения риска компрометации каждого информационного актива в отдельности. Далее можно вычислить значения ущерба. Чтобы выполнить данное действие, необходимо взять усредненное значение риска каждого информационного актива и размер потенциальных потерь. Значение ущерба (L) вычисляется по формуле:

$$L = R_{ср} \cdot S \quad (11)$$

где $R_{ср}$ – среднее значение риска;
S – потери, усл. ед.

Далее приводятся практические формулы для вычисления риска [7], [8]:

$$\text{Риск} = P\ (\text{реализации}) \cdot \text{Ущерб} \quad (12)$$

где P (реализации) – это вероятность реализации риска, которая определяется по формуле:

$$P(\text{реализации}) = P(\text{угрозы}) \cdot P\ (\text{уязвимости}) \quad (13)$$

где P (угрозы) – это вероятность угрозы, P (уязвимости) – вероятность уязвимости.

В процессе вычисления рисков для каждого актива выдается набор мер по обеспечению его информационной безопасности (ИБ) (от 1 до 7), где 1 – это минимальный необходимый набор мер по обеспечению ИБ, а 7 – максимальный [7], [8].

При оценке затрат на ИБ, как правило затрагиваются показатели отдачи от инвестиций, рассмотрим ниже, как их вычислять в ИБ.

Рассмотрим два основных показателя: ROI (Return on Investment – отдача от инвестиций) и ROSI – отдача инвестиций в ИБ.

Ниже приведем известную формулу для расчёта ROI:

$$ROI = (\text{Доходы} - \text{Расходы}) \ / \ \text{Инвестиции} \quad (14)$$

В экономике показатель ROI является основным критерием, который показывает, как эффективно дают отдачу инвестиции, вложенные в бизнес.

В сфере информационной безопасности существует свой специфичный индекс ROSI:

$$ROSI = (\Delta\ \text{Доходы} - \Delta\ \text{Расходы}\ ) / \Delta\ \text{Инвестиции} \quad (15)$$

где ROSI – указывает на изменения индекса ROI по причине инвестиций в ИБ;
Δ Доходы – показывает изменения в доходах, которые произошли из-за инвестиций в ИБ;
Δ Расходы – показывает изменения в расходах, которые произошли из-за инвестиций в ИБ;
ΔИнвестиции – инвестиции, сделанные в ИБ.

После того, как был вычислен ROSI, специалисты ИБ проводят его оценку, с помощью специальной таблицы. Таким образом оценивается эффективность внедрённого проекта в сфере информационной безопасности. Ниже приведем параметры, исходя из которых, необходимо производить такую оценку.

1. Если ROSI < 0, это означает, что в результате внедрения проектных решений произошел убыток и эффективность проекта отрицательная. Далее следует перейти к страхованию рисков ИБ.

2. Если ROI > ROSI > 0, более сложный случай. В целом, проект по ИБ не убыточен, но его внедрение в организации снижает общий ROI.

3. Если ROSI > ROI > 0 – данный вариант является позитивным результатом. В целом, внедрение проекта по ИБ приведёт к возрастанию общего ROI в организации.

Следует отметить, что внедрение средств и решений в области информационной безопасности на дает увеличение объема продаж и не влияет напрямую на прибыль компании. Индекс ROSI оказывает косвенное влияние на основной бизнес компании.

Заключение

Предложенная методика позволяет корректно оценить значение риска информационной безопасности и заранее просчитать денежные потери в случае возникновения инцидентов безопасности.

Научная новизна данной работы заключается в исследовании структуры экономики кибербезопасности как методами ЛП (симплекс-метод), так и на уровне микроэкономики с использованием риск-ориентированного подхода).

По сравнению с другими подобными работами [7], [8], [10], [11] автор применяет комплексный подход к решению проблемы экономики кибербезопасности. К примеру, авторы работы [7] используют только методы оценки рисков, а в

работе [8] дают только один метод расчета, основанный на риск-ориентированном подходе. В некоторых исследованных автором работах описывается решение экстремальной задачи линейного программирования, но не используется методика расчета рисков. Не во всех источниках авторы используют нормативную документацию (международную и национальную) в качестве основы для экономических расчетов в области кибербезопасности. В этой статье наиболее глубоко проанализирована нормативная база экономики кибербезопасности, причем как для обычного бизнеса, так и для финансового сектора (банки и т.д.), который регулируется намного серьезнее. Также автор грамотно вписал и метод вычисления показателей отдачи от инвестиций (ROI и ROSI) для сферы информационной безопасности, что важно для бизнеса. В результате подобного подхода:

а) затраты на ИБ были разделены на прямые и косвенные;

б) стоимость ущерба и убытков была классифицирована как краткосрочная и долгосрочная;

в) был дан ответ на ключевой вопрос экономики ИБ: как определить расходы на оборону и рассчитать потери;

г) определена структура векторов риска.

В аналогичных работах по экономике ИБ не всегда приводится связь экономических понятий с теоретическими концепциями, принятыми в ИБ, поэтому бывает непонятно, как именно можно связать определения, принятые в кибербезопасности, с основными экономическими концепциями и методами линейного программирования.

В данной статье описаны базовые теоретические концепции (кибербезопасность, киберпространство, киберстратегии, оценка рисков) и показана их связь с чисто практическими понятиями (риски, ущерб, затраты на продукты и услуги по кибербезопасности, эффективность инвестиций в ИБ).

Определенной новизной этой работы является также заключение, что научный подход к экономике кибербезопасности работает намного лучше, чем специфический маркетинг в сфере ИБ, основанный на страхе и запугивании бизнеса. Математические модели позволяют грамотно оценить затраты на информационную безопасность. Таким образом, данное исследование показало, как можно классифицировать стоимость ущерба и убытков, и, зная как стоимость защиты, так и связанные с ней убытки, определяется стоимость риска актива. В этой статье дается ответ на ключевой вопрос экономики ИБ: как определить расходы на оборону и рассчитать потери.

Исследование показало, как вероятность потери актива может быть измерена по характеристикам средств безопасности, защищающих его. Выводы и логические рассуждения связывают существующие знания из разных областей науки, создавая синтез, который расширяет знания, полученные из обзора литературы. Это отвечает на исследовательский вопрос: как можно измерить эффективность контроля безопасности с точки зрения снижения вероятности будущих потерь.

Представленная математическая модель, использующая методы линейного программирования, показала ответ на вопрос: как инвестиции в кибербезопасность могут быть направлены на оптимизацию защиты актива.

Исследование проверило и продемонстрировало, как организации могут определить оптимальный уровень инвестиций в защиту активов, и это тематическое исследование было использовано в качестве проверки сформулированных теорий. С помощью междисциплинарного научного подхода в документе содержатся рекомендации для ведущих бизнес-практиков, чтобы помочь им в принятии решений по кибербезопасности. Этот подход может быть интегрирован с существующими практиками управления рисками и усилить обсуждение бизнес-кейсов и коммуникацию по вопросам кибербезопасности с руководством компаний. Применяя этот подход, организация может сбалансировать свои операционные расходы на безопасность.

Конфликт интересов

Не указан.

Рецензия

Сообщество рецензентов Международного научно-исследовательского журнала
DOI: https://doi.org/10.60797/IRJ.2024.146.38.1

Conflict of Interest

None declared.

Review

International Research Journal Reviewers Community
DOI: https://doi.org/10.60797/IRJ.2024.146.38.1

Список литературы / References

1. Артамонов В. А. Кибернетические и информационные войны: основные вызовы и игроки : информационное пособие / В. А. Артамонов, Е. В. Артамонова, А. Е. Сафонов. — Санкт Петербург : Афина, 2022. — 120 с.

2. ГОСТ Р ИСО/МЭК 27001-2021 «Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования». — Введ. 2022–01–01.

3. NIST 800-30 "Risk management guide for information technology systems". Recommendations of the National Institute of Standards and Technology. — 2002.

4. ГОСТ Р ИСО/МЭК ТО 13335-3-2007 «Информационные технологии. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий». — 2007. — 49 с.

5. BS ISO/IEC 27001 (7799-2:2005) "Information technology. Security methods. Information security management systems. Requirements". — 2005.

6. РС БР ИББС-2.2-200 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения информационной безопасности». — Введ. 2010–01–01.

7. Коротнев К. Методики управления рисками информационной безопасности и их оценки (часть 1) / К. Коротнев. — 2018. — URL: https://safe-surf.ru/specialists/article/5193/587932/ (дата обращения: 14.04.2024).

8. Легчекова Е. В. Метод расчета риска информационной безопасности / Е. В. Легчекова, О. В. Титов. — С. 87–89. — URL: https://core.ac.uk/download/pdf/145189961.pdf (дата обращения: 14.04.2024).

9. Петренко С. А. Оценка затрат на кибербезопасность / С. А. Петренко // Труды ИСА РАН. — М., 2006. — Т. 27. — С. 234–265.

10. Ekelund S. Cybersecurity Economics – Balancing Operational Security Spending / S. Ekelund, Z. Iskoujina // Information Technology & People. — 2019. — Vol. 32. — № 5. — P. 1318–1342. — DOI: 10.1108/ITP-05-2018-0252

11. Jentzsch N. State-of-the-Art of the Economics of CyberSecurity and Privacy, IPACSO – Innovation Framework for ICT Security Deliverable / N. Jentzsch. — Waterford Institute of Technology (WIT), 2016. — URL: http://ipacso.eu/downloads/category/9-ipacso-project-public-deliverables.html? download=27:ipacso-state-of-the-art-economics-of-cyber-security-and-privacy-4-1 (accessed: 14.04.2024).

Список литературы на английском языке / References in English

1. Artamonov V. A. Kiberneticheskie i informacionnye vojny: osnovnye vyzovy i igroki [Cybernetic and information wars: the main challenges and players] : an information guide / V. A. Artamonov, E. V. Artamonova, A. E. Safonov. — St. Petersburg : Athena, 2022. — 120 p. [in Russian]

2. GOST R ISO/MJeK 27001-2021 «Informacionnye tehnologii. Metody obespechenija bezopasnosti. Sistemy upravlenija informacionnoj bezopasnost'ju. Trebovanija» [GOST R ISO/IEC 27001-2021 "Information technology. Security methods. Information security management systems. Requirements"]. — Introd. 2022–01–01. [in Russian]

3. NIST 800-30 "Risk management guide for information technology systems". Recommendations of the National Institute of Standards and Technology. — 2002.

4. GOST R ISO/MJeK TO 13335-3-2007 «Informacionnye tehnologii. Metody i sredstva obespechenija bezopasnosti. Chast' 3. Metody menedzhmenta bezopasnosti informacionnyh tehnologij» [GOST R ISO/IEC TO 13335-3-2007 "Information technologies. Methods and means of ensuring security. Part 3. Methods of information technology security management"]. — 2007. — 49 p. [in Russian]

5. BS ISO/IEC 27001 (7799-2:2005) "Information technology. Security methods. Information security management systems. Requirements". — 2005.

6. RS BR IBBS-2.2-200 «Obespechenie informacionnoj bezopasnosti organizacij bankovskoj sistemy Rossijskoj Federacii. Metodika ocenki riskov narushenija informacionnoj bezopasnosti» [RS BR IBBS-2.2-200 "Ensuring information security of organizations of the banking system of the Russian Federation. Methodology for assessing the risks of information security violations"]. — Introd. 2010–01–01. [in Russian]

7. Korotnev K. Metodiki upravlenija riskami informacionnoj bezopasnosti i ih ocenki (chast' 1) [Methods of information security risk management and their assessment (part 1)] / K. Korotnev. — 2018. — URL: https://safe-surf.ru/specialists/article/5193/587932/ (accessed: 14.04.2024). [in Russian]

8. Legchekova E. V. Metod rascheta riska informacionnoj bezopasnosti [Method of calculating information security risk] / E. V. Legchekova, O. V. Titov. — P. 87–89. — URL: https://core.ac.uk/download/pdf/145189961.pdf (accessed: 14.04.2024). [in Russian]

9. Petrenko S. A. Ocenka zatrat na kiberbezopasnost' [Assessment of costs for cybersecurity] / S. A. Petrenko // Trudy ISA RAN [Proceedings of the ISA RAS]. — M., 2006. — Vol. 27. — P. 234–265. [in Russian]

10. Ekelund S. Cybersecurity Economics – Balancing Operational Security Spending / S. Ekelund, Z. Iskoujina // Information Technology & People. — 2019. — Vol. 32. — № 5. — P. 1318–1342. — DOI: 10.1108/ITP-05-2018-0252

11. Jentzsch N. State-of-the-Art of the Economics of CyberSecurity and Privacy, IPACSO – Innovation Framework for ICT Security Deliverable / N. Jentzsch. — Waterford Institute of Technology (WIT), 2016. — URL: http://ipacso.eu/downloads/category/9-ipacso-project-public-deliverables.html? download=27:ipacso-state-of-the-art-economics-of-cyber-security-and-privacy-4-1 (accessed: 14.04.2024).