Вестник Самарского университета. Экономика и управление. 2024. Т. 15. № 4. С. 9–21
doi: 10.18287/2542-0461-2024-15-4-9-21 ISSN: 2782-3008(online), ISSN 2542-0461(print)

УДК 332.142.6

Моделирование деятельности компании, предоставляющей услуги в области информационной безопасности

А. Р. Богдашкин[1], **Е. П. Ростова**[2]

[1]Поволжский государственный университет сервиса,
Россия, 445017, г. Тольятти, Гагарина, д. 4.
[2]Самарский национальный исследовательский университет имени академика
С. П. Королева, Россия, 443086, Самара, Московское шоссе, 34.

Аннотация

Исследование посвящено описанию актуальных проблем киберугроз для экономических агентов. Разработана модель деятельности компании, предоставляющей услуги по обеспечению информационной безопасности. Изучены различные ситуации, связанные с ликвидацией последствий киберугроз клиентов и позволяющие осуществить планирование деятельности с учетом различных случайных факторов.

Ключевые слова: киберугрозы; информационная безопасность; риски; моделирование; ущербы; случайные величины.

Получение: 19 сентября 2024 г. / Исправление: 19 октября 2024 г. /
Принятие: 18 ноября 2024 г. / Публикация онлайн: 28 января 2025 г.

Региональная и отраслевая экономика (научная статья)

Образец для цитирования:
Богдашкин А. Р., Ростова Е. П. Моделирование деятельности компании, предоставляющей услуги в области информационной безопасности // *Вестник Самарского университета. Экономика и управление*, 2024. Т. 15, № 4. С. 9–21. doi: http://doi.org/10.18287/2542-0461-2024-15-4-9-21.

Сведения об авторах:
Александр Романович Богдашкин http://orcid.org/0009-0000-0748-2426
аспирант высшей школы интеллектуальных систем и кибертехнологий;
e-mail: bogdash999@gmail.com

Елена Павловна Ростова http://orcid.org/0000-0002-6432-6590
доктор экономических наук, доцент; заведующий кафедрой математики и бизнес-информатики;
e-mail: rostova.ep@ssau.ru

Введение

В условиях современного мира, где технологии развиваются с невероятной скоростью, а бизнес-процессы всё больше переходят в цифровую сферу, обеспечение информационной безопасности становится ключевым аспектом, гарантирующим стабильность и надёжность функционирования организаций. В условиях, когда киберугрозы [1], такие как фишинг, DDoS-атаки и вредоносное ПО, представляют серьёзную опасность для конфиденциальности данных, финансовой стабильности и репутации компаний, исследование деятельности компаний, предоставляющих услуги в области информационной безопасности, приобретает особую актуальность.

Рост числа киберинцидентов [2, 3] свидетельствует о том, что информационная инфраструктура многих организаций всё ещё не обладает достаточным уровнем защиты. Убытки от кибератак могут быть весьма значительными, что вынуждает компании уделять повышенное внимание вопросам информационной безопасности и предпринимать эффективные меры для защиты своих данных. По данным аналитического отчета компании «Ростелеком-Солар» [4], в октябре-декабре 2023 года было выявлено 473 тыс. событий информационной безопасности (ИБ) – подозрений на инцидент после обработки первой линией мониторинга и фильтрации ложных срабатываний. Это на 20% больше, чем в предыдущем квартале 2023 года, и на 68% больше показателя IV квартала 2022 года. Рост событий ИБ в разрезе одной компании в IV квартале, по сравнению с III кварталом составляет 18%, а по отношению к аналогичному периоду 2022 года – 55%. Таким образом, исследование деятельности компаний, предоставляющих услуги в области информационной безопасности, имеет практическую значимость и может способствовать повышению уровня защищённости организаций от киберугроз.

Внедрение комплексных решений в сфере информационной безопасности [5] не только минимизирует риски потери данных и финансовых ресурсов, но и способствует укреплению доверия клиентов и партнёров к компании. Эффективная защита информационных активов обеспечивает стабильность бизнеса и снижает вероятность возникновения кризисных ситуаций, связанных с киберугрозами.

Проблема информационной безопасности особенно остро стоит перед компаниями из таких жизненно важных секторов, как финансовый [6, 7], энергетический [8], здравоохранение [9] и транспорт [10]. Для этих организаций защита данных является неотъемлемой частью их развития и стабильности. Современные исследования помогают лучше понять, как меры информационной безопасности могут стать важнейшим элементом их бизнес-модели.

Среди последних публикаций особое внимание уделяется оценке экономической эффективности этих мер. В исследовании Албины Орландо предлагается использовать модель «Кибер-ценность под угрозой (Cy-VaR)» для оценки рисков и планирования инвестиций в информационную безопасность [11]. Данная модель позволяет компаниям количественно оценить потенциальные потери от кибератак и принимать обоснованные решения о ресурсах, необходимых для предотвращения ущерба.

Следует отметить исследование, опубликованное в журнале *MDPI* [12], в котором анализируются стратегии, направленные на укрепление кибербезопасности. В статье рассматриваются ключевые аспекты создания систем управления инцидентами и внедрения автоматизированных решений, которые помогают организациям лучше противостоять киберугрозам. Авторы исследования акцентируют внимание на том, как автоматизация процессов мониторинга и реагирования на инциденты снижает финансовые риски и минимизирует потери от кибератак. Они также подчёркивают необходимость создания эффек-

тивных систем управления рисками, которые обеспечат долгосрочную устойчивость организаций.

В 2024 году IBM и Ponemon Institute опубликовали отчёт [13] о средней стоимости утечек данных. Этот отчёт наглядно показывает, что компании, которые заранее готовятся к возможным инцидентам, могут существенно снизить свои финансовые потери. Также из отчета следует, что в 2024 году средний мировой ущерб от утечки данных превысил 4,88 миллионов долларов, что на 10% выше, чем за аналогичный период 2023 и выше, чем когда-либо в истории. Отчёт акцентирует внимание на важности управления рисками и разработки стратегий по предотвращению утечек данных для устойчивого развития бизнеса и минимизации экономического ущерба.

Исследования в области управления рисками и защиты данных свидетельствуют о необходимости комплексного подхода к обеспечению безопасности в современных организациях [14, 15]. Этот подход должен сочетать в себе экономические модели [16] и технологические решения, позволяющие оперативно выявлять и предотвращать потенциальные угрозы.

Компании, предоставляющие услуги в сфере информационной безопасности (ИБ), играют ключевую роль в защите данных, систем и процессов своих клиентов. В условиях стремительного развития цифровых технологий и увеличения частоты кибератак [1, 2] эти организации разрабатывают комплексные стратегии и внедряют многоуровневые меры безопасности, направленные на снижение рисков.

Управление рисками в сфере информационной безопасности [17] предполагает поиск баланса между затратами на защиту и вероятностью возникновения инцидентов. При оценке рисков учитываются экономические последствия кибератак и рентабельность инвестиций в защитные меры.

Одним из ключевых аспектов деятельности организаций в области информационной безопасности является внедрение и поддержание решений, направленных на защиту от потенциальных угроз, как внешних, так и внутренних. Основные направления угроз представлены на рис. 1.

Внешние угрозы включают в себя попытки несанкционированного доступа, фишинговые атаки и $DDoS$ – атаки, цель которых – нарушить функционирование систем. Внутренние угрозы обычно связаны с утечками данных и непреднамеренными действиями сотрудников, которые могут поставить информацию под угрозу.

С целью защиты от внешних атак организации внедряют и настраивают системы предотвращения вторжений (IPS), межсетевые экраны (фаерволы) и системы обнаружения угроз, такие как решения на основе анализа поведения пользователей (UBA). Эти системы позволяют отслеживать активность в сети, выявлять подозрительные действия и предотвращать инциденты до того, как они приведут к ущербу.

Внутренние угрозы, такие как несанкционированные утечки информации и непреднамеренные ошибки сотрудников, требуют применения особых методов. Одним из таких методов является ограничение доступа к конфиденциальным данным, а также проведение обучающих мероприятий для персонала.

Многие компании, работающие в сфере информационной безопасности, для эффективного противодействия киберугрозам предлагают услуги по мониторингу и оперативному реагированию в режиме реального времени. Этот процесс включает в себя непрерывный анализ сетевой активности с целью выявления аномалий и подозрительных событий.

В случае обнаружения аномалий специалисты оперативно идентифицируют и классифицируют инцидент, оценивают его последствия и разрабатывают меры по нейтрализации

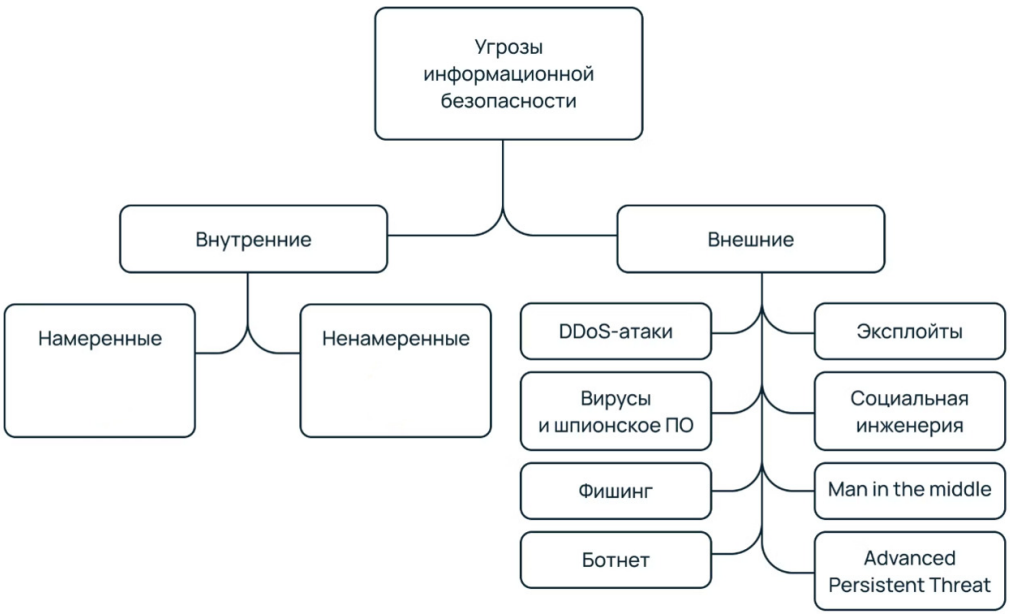

Рис. 1: Угрозы информационной безопасности.
Fig. 1: Threats to information security.

угрозы. В настоящее время всё чаще применяются автоматизированные системы и инструменты на основе машинного обучения, которые не только обнаруживают аномалии, но и способны прогнозировать потенциальные риски, основываясь на анализе больших данных. Это позволяет компаниям существенно сократить время реагирования и повысить свою готовность к оперативному реагированию на кибератаки. После успешного завершения кибератаки или полного устранения инцидента компании, специализирующиеся на информационной безопасности, оказывают своим клиентам всестороннюю поддержку в восстановлении нормальной работы и минимизации последствий произошедшего.

Этот процесс включает в себя комплекс мероприятий, направленных на восстановление утраченных данных, анализ причин инцидента и разработку мер по предотвращению подобных угроз в будущем. Организации также помогают клиентам сформировать план обеспечения непрерывности бизнеса (BCP) и план аварийного восстановления (DRP), что позволяет минимизировать время простоя и потери. Восстановительные меры могут включать в себя установку более строгих систем контроля, обучение персонала и внедрение дополнительных средств защиты, если они не были предусмотрены ранее.

Деятельность компаний в области ИБ охватывает несколько ключевых направлений:

1. Оценка и управление рисками.
2. Защита от внутренних и внешних угроз.
3. Мониторинг и оперативное реагирование на инциденты.
4. Восстановление после атак.

Следует отметить, что работа в сфере информационной безопасности сопряжена с определёнными рисками и непредвиденными расходами. Организации сталкиваются с необходимостью значительных инвестиций в обновление инфраструктуры, обучение персонала и внедрение передовых технологий. Это обусловлено непрерывным развитием методов кибератак, которые становятся всё более изощрёнными и угрожающими. В случае масштабного инцидента могут потребоваться дополнительные ресурсы для оперативного восстановления и привлечения внешних специалистов для устранения последствий. Фи-

нансовые риски включают также затраты на судебные разбирательства в случае нарушения конфиденциальности данных или неисполнения обязательств перед клиентами.

Компании, обеспечивающие информационную безопасность, должны оперативно реагировать на изменения в технологиях и законодательстве. Это требует дополнительных вложений и гибкости, что, в свою очередь, создаёт дополнительные риски. Таким образом, деятельность организаций в области информационной безопасности представляет собой не просто комплекс технических мер по защите данных, но и комплексный подход к управлению рисками и обеспечению безопасности. Такой подход позволяет значительно снизить вероятность возникновения инцидентов и минимизировать последствия возможных кибератак.

Компании, занимающиеся информационной безопасностью, стремятся к установлению долгосрочных отношений с клиентами, что приводит к стабильному доходу и расширению клиентской базы. С точки зрения экономики, установление долгосрочных отношений является выгодным решением, поскольку оно позволяет сократить издержки, связанные с привлечением новых клиентов. Постоянные клиенты, получающие комплексные услуги, с большей вероятностью останутся с компанией на длительный срок. Клиентам предлагают широкий спектр услуг, включая полный комплекс услуг «под ключ», а также возможность выбора отдельных сервисов, таких как регулярные проверки безопасности или обучение сотрудников. Это позволяет компаниям гибко адаптироваться к различным сегментам рынка и удовлетворять потребности своих клиентов.

Экономическая модель компании также включает в себя выбор подходящей бизнес-модели и методов монетизации. Наиболее распространёнными бизнес-моделями являются подписная, проектная и смешанная модели. Характеристики таких моделей представлены в таблице 1.

Таблица 1: Характеристика бизнес-моделей.
Table 1. Characteristics of business models.

Название модели	**Характеристика**
Подписная модель	Обеспечение регулярного потока доходов. Хорошо подходит для услуг мониторинга и реагирования. Позволяет компании строить долгосрочные финансовые стратегии и поддерживать стабильный денежный поток.
Проектная модель	Инструмент, используемый для выполнения разовых задач, таких как аудит или развёртывание инфраструктуры безопасности. Позволяет зафиксировать прибыль от проекта и снизить риски, связанные с долгосрочными обязательствами.
Смешанная модель	Комбинирование фиксированных платежей за основные услуги с возможностью дополнительной оплаты по мере необходимости. Обеспечивает компании гибкость в ценообразовании и позволяет расширять спектр услуг в соответствии с потребностями клиентов.

1. Описание системы и ее моделирование.

Рассмотрим деятельность компании, оказывающей услуги по обеспечению информационной безопасности. Доходы компании R складываются из поступлений в рамках долгосрочных договоров и запланированных проектов RD и разовых договоров, возникающих,

как правило, в случае возникновения непредвиденных ситуаций RS. Расходы компании C состоят из постоянных издержек CF, расходов в рамках запланированных работ по долгосрочным контрактам или проектам CD, а также расходов, возникающих под влиянием внешних факторов – случайных расходов CS. Тогда прибыль компании запишем следующим образом:

$$P = R - C. \tag{1}$$

$$R = RD + RS. \tag{2}$$

$$C = CF + CD + CS. \tag{3}$$

Доходы компании по плановым договорам и проектам RD есть сумма поступлений по каждому договору и проекту

$$RD = \sum RD_i. \tag{4}$$

Случайные поступления от незапланированных договоров обусловлены возникновением у клиента непредвиденной ситуации. Причина подобной непредвиденной ситуации может быть различна: технический сбой без возникающих внешних угроз (внутренний риск) и внешние угрозы (внешний риск).

Выделение двух причин обусловлено их различной природой, вероятностью возникновения и размерами ущербов. Технический сбой, обозначающий реализацию внутреннего риска, возникающего с вероятностью p_j, приносит рассматриваемой компании доход в размере RS_j.

Внешняя угроза информационной безопасности клиента возникает с вероятностью p_l и приносит рассматриваемой компании доход в размере RK_l. Тогда ожидаемый доход от случайных поступлений запишем следующим образом:

$$M[RS] = \sum p_j M[RS_j] + \sum p_l M[RK_l]. \tag{5}$$

Доход RS_j и RK_l будем считать случайными величинами, поскольку они зависят от масштабов угрозы информационной безопасности клиента, от размера бизнеса, а также от ряда факторов.

Таким образом, запишем (2) с учетом (4) и (5)

$$M[R] = \sum RD_i + \sum p_j M[RS_j] + \sum p_l M[RK_l]. \tag{6}$$

Расходы компании по заключенным договорам и планируемым проектам CD складываются из сумм расходов по отдельному договору и проекту

$$D = \sum D_i. \tag{7}$$

Расходы компании CS, обусловленные случайными событиями, возникающими у клиентов с вероятностью p_j, для j-го события составляют CS_j. Данная сумма является случайной величиной, поскольку зависит от ряда факторов, перечисленных при описании случайных доходов RS_j.

Аналогично для внешних угроз, возникающих у клиентов с вероятностью p_l и сопровождающихся для компании расходами CK_l. Помимо указанных расходов CS_j, связанных с потребностями клиентов, компания может иметь случайные расходы, связанные с воз-

никающими внешними угрозами и необходимостью быть готовой обеспечить защиту от данных угроз будущим клиентам.

Компания инвестирует в новые технологии и исследования, отвечая на возникающие киберугрозы. Такие затраты не связаны непосредственно с текущими потребностями клиентов и не приносят моментальной отдачи в виде доходов по заключенным контрактам.

Однако, учесть подобные затраты в структуре расходов компании необходимо. Обозначим описанные затраты на новые технологии CT_k, возникающие с вероятностью p_k, k – тип угрозы.

Тогда ожидаемый размер CS запишем в следующем виде:

$$M[CS] = \sum p_j \, M[CS_j] + \sum p_l \, M[CK_l] + \sum p_k \, M[CT_k]. \tag{8}$$

Запишем случайные расходы (3) с учетом расходов по запланированным работам (7) и случайных затрат (8)

$$M[CS] = \sum D_i + \sum p_j M[CS_j] + \sum p_l M[CK_l] + \sum p_k M[CT_k]. \tag{9}$$

Ожидаемая прибыль рассматриваемой компании (1) запишем как математическое ожидание прибыли

$$M[P] = M[R - C] = M[R] - M[C]. \tag{10}$$

С учетом соотношений (6) и (9) перепишем формулу (10) в следующем виде

$$\begin{gathered} M[P] = \sum RD_i + \sum p_j M[RS_j] + \sum p_l M[RK_l] - \\ - \sum D_i - \sum p_j M[CS_j] - \sum p_l M[CK_l] - \sum p_k M[CT_k]. \end{gathered} \tag{11}$$

Однако, не каждая компания, обеспечивающая информационную безопасность, владеет достаточной статистической информацией о деятельности различных фирм, которые могут стать потенциальными клиентами, что делает невозможным расчет вероятности внутренних и внешних угроз.

Однако, рассматриваемая компания имеет статистическую информацию о своей деятельности – количестве экстренных обращений от незапланированных клиентов, доходах по данным обращениям.

В этой связи следует модифицировать модель (11) и рассматривать ожидаемый доход от незапланированных клиентов в целом для компании, а не по каждому клиенту отдельно.

Аналогично с затратами по подобным экстренным ситуациям – целесообразно рассматривать затраты в целом, а не по каждому случаю отдельно.

$$M[P] = \sum RD_i + M[RS] + M[RK] - \sum D_i - M[CS]^{\smile} M[CK] - \sum p_k M[CT_k]. \tag{12}$$

Произведем моделирование деятельности компании при следующих допущениях:

1. Доход от устранений экстренных реализаций внутреннего риска клиента RS и расходы по проведению данных работ CS распределены по логнормальному закону распределения: $RS \sim \log_N(\mu_{RS}, \sigma_S), S \sim \log_N(\mu_{CS}, \sigma_S), \mu_{CS} < \mu_{RS}$.
2. Доход от устранений экстренных реализаций внешнего риска клиента RK и расходы

по проведению данных работ СК распределены по нормальному закону распределения: $RK \sim N(\mu_{RK}, \sigma_K), CK \sim N(\mu_{CK}, \sigma_K), \mu_{CK} < \mu_{RK}$.

3. Величина возможных расходов компании CTk, на новые технологии и исследования, связанные с возникающими новыми угрозами k-го типа, а также число этих угроз nk распределены по логнормальному закону распределения: $nk \sim \log_N(\mu_k, \sigma_k)$, $CTk \sim \log_N(\mu_{CTk}, \sigma_{Tk})$.

Определим значения слагаемых (12) с учетом введенных допущений:

$$M[RS] = \int_0^{\widehat{RS}} \frac{1}{\sigma_S\sqrt{2\pi}} \cdot e^{-\frac{(\ln x - \mu_{RS})^2}{2\sigma_S^2}} dx, \quad M[CS] = \int_0^{\widehat{CS}} \frac{1}{\sigma_S\sqrt{2\pi}} \cdot e^{-\frac{(\ln x - \mu_{CS})^2}{2\sigma_S^2}} dx,$$

$$M[RK] = \int_0^{\widehat{RK}} \frac{1}{\sigma_K\sqrt{2\pi}} e^{-\frac{(x - \mu_{RK})^2}{2\sigma_S^2}} dx, \quad M[CK] = \int_0^{\widehat{CK}} \frac{1}{\sigma_K\sqrt{2\pi}} e^{-\frac{(x - \mu_{CK})^2}{2\sigma_K^2}} dx,$$

$$p_k = \int_0^{\widehat{n}} \frac{1}{x\sigma_K\sqrt{2\pi}} e^{-\frac{(\ln x - \mu k)^2}{2\sigma_k^2}} dx, \quad M[CTk] = \int_o^{\widehat{CT_k}} \frac{1}{\sigma_{CT_k}\sqrt{2\pi}} \cdot e^{-\frac{(x - \mu_{CT_k})^2}{2\sigma_{CT_k}^2}} dx,$$

где – максимально возможное значение соответствующей переменной.

В таблице 2 представлено моделирование деятельности компании для значений параметров модели. Моделирование осуществлялось относительно значения среднего ущерба от инцидента.

Таблица 2: Рисковое событие и параметры.
Table 1. Risk event and parameters.

Рисковое событие	**Параметр**	**Значение**
Случайный технический сбой	μ_{RS}	m
	μ_{RS}	0,1m
	σ_{RS}	0,5m
Внешняя угроза	μ_{RK}	2m
	μ_{CK}	m
	σ_K	0,6m
Появление новых угроз	μ_{STK}	0,75m
	σ_{STK}	0,3m

Начальные значения и большие значениях среднего ущерба соответствует затратам, превышающим доходы – компания несет убытки. Компания получает прибыль только при значениях среднего ущерба, находящихся в зоне малых значений (Рис.2).

Однако, компания помимо случайных затрат и доходов имеет запланированные денежные потоки, соответствующие подписной бизнес-модели. Произведем моделирование с учетом плановых затрат и поступлений, которые могут составлять определенную долю от среднего ущерба от случайных инцидентов.

Рассмотрим ситуации, представленные на рис. 3, когда плановые доходы превышают расходы в k раз.

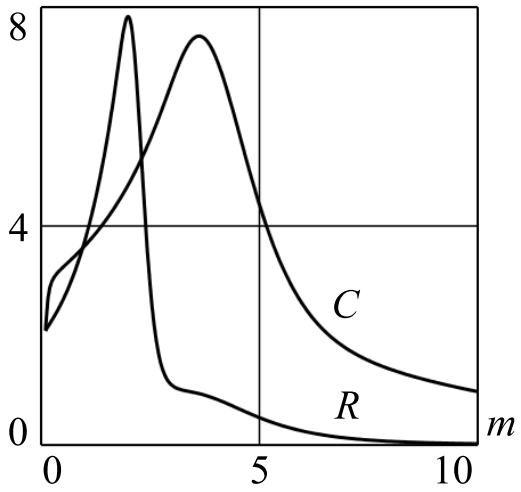

Рис. 2: Моделирование доходов и расходов при параметрах Таблицы 2.
Fig. 2: Modeling income and expenses with the parameters of Table 2.

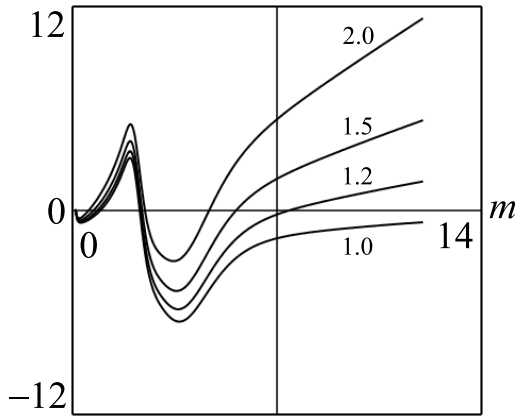

Рис. 3: Моделирование прибыли при различных значениях параметра k.
Fig. 3: Modeling profit for different values of parameter k.

Результат моделирования показал, при каких значения среднего ущерба от инцидента и при каких значениях повышающего коэффициента для планируемых доходов, компания будет иметь убыток или прибыль.

Компании, предоставляющие услуги в сфере информационной безопасности, стремятся разработать комплексные решения для защиты информационных активов своих клиентов. Это позволяет им не только снизить риски, но и обеспечить стабильный доход, а также повысить свою конкурентоспособность на рынке. Экономическая модель таких компаний основана на оптимизации структуры, эффективном распределении ресурсов и построении долгосрочных отношений с клиентами.

Компании, предоставляющие услуги в области информационной безопасности, сталкиваются с рисками и непредвиденными затратами, вызванными необходимостью оперативного реагирования на новые угрозы. Кибератаки, требующие немедленных инвестиций в исследования и обновление технологий, могут существенно увеличить операционные расходы. Однако компании применяют стратегию диверсификации услуг и модернизации процессов реагирования, что позволяет минимизировать негативное влияние инцидентов

на рентабельность.

Заключение

1. В статье были рассмотрены ключевые аспекты деятельности компаний, специализирующихся на информационной безопасности. Проведен анализ их бизнес-моделей. Особое внимание уделяется комбинированию стратегий долгосрочного партнёрства, которое позволяет обеспечить стабильный доход и спрогнозировать издержки фирмы, и стратегий проектной деятельности, возникающей в случае необходимости экстренного реагирования по запросу клиентов.
2. Разработанная экономико-математическая модель компании, функционирующей в области информационной безопасности, базируется на диверсификации источников дохода и стратегическом взаимодействии с клиентами. Эти меры обеспечивают устойчивый рост и конкурентоспособность в условиях возрастающего спроса на защиту данных.
3. Соотношение доходов и расходов от разных бизнес-моделей и их комбинация позволили исследовать изменение доходов, расходов и прибыли при различных входных параметрах. Разработанная модель позволяет осуществлять планирование деятельности компании, предоставляющей услуги по обеспечению информационной безопасности, с учетом различных видов доходов и расходов, обусловленных разными бизнес-моделями.

Конкурирующие интересы: Конкурирующих интересов нет.

Библиографический список

1. Обзор рисков для российских компаний в 2022 году: виды атак и экономические потери // Positive Technologies Security. [Электронный ресурс]. Режим доступа: https://www.ptsecurity.com/ru-ru/analytics/research/attacks-statistics (дата обращения: 08.10.2024).
2. Разведение угроз: с какими кибератаками столкнулись российские компании в 2023 году // Forbes Russia. [Электронный ресурс]. Режим доступа: https://www.forbes.ru/tekhnologii/506712-razvedenie-ugroz-s-kakimi-kiberatakami-stolknulis-rossijskie-kompanii-v-2023-godu (дата обращения: 15.10.2024).
3. Антонян Е.А., Клещина Е.Н. Киберпреступность на современном этапе: тенденции и направления противодействия // Вестник экономической безопасности. – 2022. – № 5. – С. 11–15. EDN: SXPUMZ.
4. Кибератаки на российские компании в 2023 году // RT-Solar. [Электронный ресурс]. Режим доступа: https://rt-solar.ru/analytics/reports/4094/ (дата обращения: 18.10.2024).
5. Нестеровский О.И., Пашковская Е.С., Бутрик Е.Е. Методический подход к организации проведения контроля защищенности информации на объектах критической информационной инфраструктуры // Вестник Воронежского института МВД России. – 2021. – № 2. – С. 126–133. EDN: BLUVGP.
6. Курманова Д.А., Султангареев Д.Р., Хабибуллина Л.Р. Модели управления рисками финансовых технологий // Вестник УГНТУ. Наука, образование, экономика. Серия: Экономика. – 2020. – № 2 (32). – С. 82–91. EDN: ZPVSFW.
7. Миргородская М.Г., Котова И.Б., Аничкина О.А., Целуйко Г.А. Проблемы кибербезопасности в финансовом секторе цифровой экономики // Экономические науки. – 2024. – № 234. – С. 279–285. EDN: ANXKVN.

8. Шестакова А.А., Ефимов Д.Н. Кибербезопасность объектов энергетики и ее индикаторы // В сборнике: Повышение эффективности производства и использования энергии в условиях Сибири. Материалы Всероссийской научно-практической конференции с международным участием. – 2023. – С. 113–117. EDN: BNVUEV.
9. Гаджиев Г.К. Кибербезопасность в области здравоохранения: вызовы и перспективы // Научный Альманах ассоциации France–Kazakhstan. – 2024. – № 3. – С. 164–168. EDN: CRZJSA.
10. Куценко С.М., Губанова А.Д. Обеспечение кибербезопасности в секторе логистики транспортных систем // Экономика и предпринимательство. – 2024. – № 3 (164). – С. 1343–1345. EDN: JRLZMT.
11. Orlando A. Cyber Risk Quantification: Investigating the Role of Cyber Value at Risk // Risks. – 2021. – Vol. 9 (10). – pp. 184. DOI: 10.3390/risks9100184
12. Peter R. J. Trim, Yang-Im Lee. Managing Cybersecurity Threats and Increasing Organizational Resilience// Big Data Cogn. Comput. – 2023. – Vol. 7 (4). – pp. 177. DOI: 10.3390/bdcc7040177.
13. IBM, Ponemon Institute. Отчёт о средней стоимости утечек данных. – 2021. [Электронный ресурс]. Режим доступа: https://www.ibm.com/security/data-breach (дата обращения: 12.10.2024).
14. Леднева О.В., Сидорова О.Е. Анализ информационной безопасности и современные подходы к управлению информационными рисками // В сборнике: Цифровая экономика и информационные технологии. Материалы I Всероссийской научно-практической конференции. Министерство науки и высшего образования Российской Федерации Южно-Уральский государственный университет, кафедра цифровой экономики и информационных технологий. – 2022. – С. 32–37. EDN: ZCUUPF.
15. Эскерханова Л.Т., Натальсон А.В., Маташева Х.П. Экономическая устойчивость в цифровую эпоху: роль информационных технологий // Экономика и управление: проблемы, решения. – 2023. – Т. 4. – № 9 (139). – С. 5–12. EDN: OVUNAH.
16. Сидельников А.П., Калач А.В., Сидельников П.А. Модель оценки уязвимости элементов структуры управления информационными ресурсами технических систем // Технологии техносферной безопасности. – 2023. – № 4 (102). – С. 157–168. EDN: QNENZP.
17. Глущенко И.С., Баранова Е.М., Баранов А.Н., Борзенкова С.Ю. Современные информационные системы анализа и управления рисками в сфере информационной безопасности // Известия Тульского государственного университета. Технические науки. – 2021. – № 2. – С. 311–316. EDN: ATMCEK.

Vestnik of Samara University. Economics and Management. 2024, vol. 15, no. 4, pp. 9–21
doi: 10.18287/2542-0461-2024-15-4-9-21 ISSN: 2782-3008(online), ISSN 2542-0461(print)

Modeling the activities of a company providing information security services

A. R. Bogdashkin[1], **E. P. Rostova**[2]

[1] Volga Region State University of Service, 4, Gagarin st., Tolyatti, Russia.
[2] Samara National Research University, 34, Moskovskoye shosse, Samara, 443086, Russia.

Abstract

The study is devoted to the description of current problems of cyber threats for economic agents. A model of the activity of a company providing information security services has been developed. Various situations related to the elimination of the consequences of cyber threats to clients and allowing for the planning of activities taking into account various random factors have been studied.

Keywords: cyber threats; information security; risks; modeling; damages; random variables.

Received: Thursday 19th September, 2024 / Revised: Saturday 19th October, 2024 / Accepted: Monday 18th November, 2024 / First online: Tuesday 28th January, 2025

Competing interests: No competing interests.

References

1. Risk Review for Russian Companies in 2022: Types of Attacks and Economic Losses // Positive Technologies Security. [Electronic resource]. Access mode: https://www.ptsecurity.com/ru-ru/analytics/research/attacks-statistics (accessed: 08.10.2024) (In Russ.)
2. Breeding threats: what cyberattacks did Russian companies face in 2023 // Forbes Russia. [Electronic resource]. Access mode: https://www.forbes.ru/tekhnologii/506712-razvedenie-ugroz-s-kakimi-kiberatakami-stolknulis-rossijskie-kompanii-v-2023-godu (accessed: 15.10.2024). (In Russ.)

Regional and Sectoral Economics (Research Article)

Please cite this article in press as:
Bogdachkin A. R., Rostova E. P. Modeling the activities of a company providing information security services, *Vestnik Samarskogo Universiteta. Ekonomika i Upravlenie = Vestnik of Samara University. Economics and Management*, 2024, vol. 15, no. 4, pp. 9–21. doi: http://doi.org/10.18287/2542-0461-2024-15-4-9-21 (In Russian).

Authors' Details:
Alexander R. Bogdashkin http://orcid.org/0009-0000-0748-2426
Postgraduate Student of the Higher School of Intelligent Systems and Cybertechnologies;
e-mail: bogdash999@gmail.com

Elena P. Rostova http://orcid.org/0000-0002-6432-6590
Dostor of Economics, associate professor; head the Department of Mathematics and Business Informatics;
e-mail: rostova.ep@ssau.ru

3. Antonyan E.A., Kleshchina E.N. Cybercrime at the present stage: trends and directions of counteraction // Bulletin of Economic Security. – 2022. – No. 5. – pp. 11–15. EDN: SXPUMZ. (In Russ.)
4. Cyberattacks on Russian companies in 2023 // RT-Solar. [Electronic resource]. Access mode: https://rt-solar.ru/analytics/reports/4094/ (accessed: 18.10.2024). (In Russ.).
5. Nesterovsky O.I., Pashkovskaya E.S., Butrik E.E. Methodological approach to organizing the control of information security at critical information infrastructure facilities // Bulletin of the Voronezh Institute of the Ministry of Internal Affairs of Russia. – 2021. – No. 2. – pp. 126–133. EDN: BLUVGP. (In Russ.)
6. Kurmanova D.A., Sultangareev D.R., Khabibullina L.R. Models of financial technology risk management // Bulletin of USPTU. Science, education, economics. Series: Economics. – 2020. – No. 2 (32). – pp. 82–91. EDN: ZPVSFW. (In Russ.)
7. Mirgorodskaya M.G., Kotova I.B., Anichkina O.A., Tseluiko G.A. Cybersecurity issues in the financial sector of the digital economy // Economic sciences. – 2024. – No. 234. – pp. 279–285. EDN: ANXKVN. (In Russ.)
8. Shestakova A.A., Efimov D.N. Cybersecurity of energy facilities and its indicators // In the collection: Improving the efficiency of production and use of energy in Siberia. Proceedings of the All-Russian scientific and practical conference with international participation. – 2023. – pp. 113–117. EDN: BNVUEV. (In Russ.)
9. Gadzhiev G.K. Cybersecurity in the field of healthcare: challenges and prospects // Scientific Almanac of the France–Kazakhstan Association. – 2024. – No. 3. – pp. 164–168. EDN: CRZJSA. (In Russ.)
10. Kutsenko S.M., Gubanova A.D. Ensuring cybersecurity in the logistics sector of transport systems // Economy and entrepreneurship. – 2024. – No. 3 (164). – pp. 1343–1345. EDN: JRLZMT. (In Russ.)
11. Orlando A. Cyber Risk Quantification: Investigating the Role of Cyber Value at Risk // Risks. – 2021. – Vol. 9 (10). – pp. 184. DOI: 10.3390/risks9100184
12. Peter R. J. Trim, Yang-Im Lee. Managing Cybersecurity Threats and Increasing Organizational Resilience// Big Data Cogn. Comput. – 2023. – Vol. 7 (4). – pp. 177. DOI: 10.3390/bdcc7040177.
13. IBM, Ponemon Institute. Average Cost of Data Breach Report. – 2021. [Electronic resource]. Access mode: https://www.ibm.com/security/data-breach (accessed: 12.10.2024). (In Russ.)
14. Ledneva O.V., Sidorova O.E. Analysis of information security and modern approaches to information risk management // In the collection: Digital Economy and Information Technology. Proceedings of the I All-Russian Scientific and Practical Conference. Ministry of Science and Higher Education of the Russian Federation South Ural State University, Department of Digital Economy and Information Technology. – 2022. – pp. 32–37. EDN: ZCUUPF. (In Russ.)
15. Eskerkhanova L.T., Natalson A.V., Matasheva H.P. Economic sustainability in the digital age: the role of information technology // Economy and management: problems, solutions. – 2023. – Vol. 4. – No. 9 (139). – pp. 5–12. EDN: OVUNAH. (In Russ.)
16. Sidelnikov A.P., Kalach A.V., Sidelnikov P.A. Model for assessing the vulnerability of elements of the information resources management structure of technical systems // Technologies of technosphere safety. – 2023. – No. 4 (102). – pp. 157–168. EDN: QNENZP. (In Russ.)
17. Glushchenko I.S., Baranova E.M., Baranov A.N., Borzenkova S.Yu. Modern information systems for risk analysis and management in the field of information security // Bulletin of Tula State University. Technical sciences. – 2021. – No. 2. – pp. 311–316. EDN: ATMCEK. (In Russ.)