УДК 338.24:004.056
DOI 10.33764/2618-981X-2025-6-54-59

И. Н. Гутов[1]✉, *А. В. Шабурова*[1]

Методика создания алгоритма расчета финансовых рисков от потери информации

[1]Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
e-mail: igutov@yandex.ru

Аннотация. Статья посвящена актуальному вопросу расчета финансовых рисков предприятий от потери или утечки информации. Учитывая, что бизнес в современном мире оперирует в основном цифровой информацией, защита информации стала важной частью организации работы предприятий, и расчет финансовых рисков имеет большое значение для принятия управленческих решений в области защиты информации. Результаты расчетов помогают бизнесу в оценке финансовых вложений для разработки стратегии защиты информации, выборе соответствующих мер и технологий безопасности. Они помогают руководству оценить потенциальные финансовые потери и принять обоснованные решения о выделении бюджета на обеспечение информационной безопасности на предприятии.

Ключевые слова: финансовые риски, информационная безопасность, потеря информации, алгоритмы расчета

I. N. Gutov[1]✉, *A. V. Shaburova*[1]

Methodology for creating an algorithm for calculating financial risks from information loss

[1]Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: igutov@yandex.ru

Abstract. The article is devoted to the topical issue of calculating the financial risks of enterprises from loss or leakage of information. Considering that business in the modern world operates mainly with digital information, information protection has become an important part of the organization of enterprises, and the calculation of financial risks is of great importance for making managerial decisions in the field of information protection. The calculation results help businesses evaluate financial investments to develop an information protection strategy and select appropriate security measures and technologies. They help management assess potential financial losses and make informed decisions about allocating a budget to ensure information security at the enterprise.

Keywords: financial risks, information security, information loss, algorithm for calculating

Введение

Со стремительным развитием современных средств вычислительной техники и телекоммуникаций цифровая информация стала играть большую роль в деятельности предприятий. В связи с этим информация стала иметь значимость для предприятий как финансовый и репутационный актив и не только.

Но, в то же время, широкое распространение цифровой информации имеет и свои минусы – как актив цифровая информация стала целью как конкурентов,

так и различных хакерских группировок, имеющих финансовые и политические интересы, что увеличивает риски потери или утечки информации. При этом методы и способы получения несанкционированного доступа к цифровой информации развиваются с каждым днем и поэтому защита информации на предприятиях имеет очень большое значение.

Для обеспечения информационной безопасности на предприятиях необходимо иметь понятные и простые методики расчета финансовых рисков, на основании которых будут приниматься решения о внедрении стратегий и механизмов защиты информации от утечки или потери.

При этом важность оценки финансовых рисков от потери или утечки информации для предприятия неоспорима, так как она помогает принимать управленческие решения в области защиты информации, что позволяет минимизировать риски и обеспечить непрерывность работы предприятия, а также рассчитать страховые взносы при киберстраховании предприятия от ущерба при утечке или потери информации.

На рынке присутствуют продукты для анализа рисков, но ни один из них не отвечает требованиям универсальности, при этом большинство методик основано на зарубежных разработках и в них не учитывается специфика российских предприятий.

В данной статье ставится задача описать методику создания универсального алгоритма расчета финансового риска предприятия от потери информации на основе процессного подхода.

Анализ существующих методик расчета рисков

Самой большой сложностью при принятии мер по обеспечению информационной безопасности являются ограничения бюджета и отсутствие поддержки со стороны руководства, хотя в этой части в последнее время есть положительная тенденция.

Чтобы донести до руководства необходимость выделения бюджета на обеспечение информационной безопасности и нужны расчеты, которые могут показать, сколько денег потеряет предприятие при реализации угроз, какие места наиболее уязвимы и какие меры требуется предпринять, чтобы повысить уровень защищенности инфраструктуры.

Для решения таких задач разработаны методики CRAMM (британской компанией Insight Consulting) и RiskWatch (американской компанией RiskWatch). На основе этих методик соответственно были разработаны программные комплексы анализа и контроля информационных рисков. Но данные методики достаточно трудоемки в реализации и поддержке, при этом в Российской Федерации практически отсутствуют специалисты по этим продуктам, что не позволяет полноценно применять данные методики на практике [1].

Есть отечественная корпоративная система управления информационной безопасностью от компании Digital Security, которая включает в себя систему анализа и управления корпоративными рисками «ГРИФ» и средство для управления политикой информационной безопасностью «Кондор». Данная система

была востребованы в банковской сфере, но последние упоминания производителя о данной системе датированы 2006 годом, а в информационных материалах система упоминалась в 2021 году [2]. Таким образом сложно говорить об актуальности данной системы.

Также имеются разработки по оценке величины ущерба от воздействия на информацию различных угроз на основе математического моделирования. Одна из разработак описана в работе [3]. Но данная методика описывает модель на основе одной информационной системы, а в инфраструктуре современных предприятий таких систем может быть десятки, и тогда моделирование усложняется.

Анализ методик, проведенный в работе [4], показывает проблематику отсутствия единого подхода к расчетам рисков, что приводит к неоднозначности результатов и, как следствие, недооценки бизнесом данной сферы деятельности предприятия. При этом стоит рассматривать риски информационной безопасности как неотъемлемую часть рисков ведения всего бизнеса [5].

Алгоритм расчета рисков

Многие отечественные методики построены с учетом стандарта ГОСТ Р ИСО/МЭК 27005-2010 «Менеджмент риска информационной безопасности» [6] и начинаются с идентификации и описания активов. Далее проводится идентификация угроз, связанных с активами, идентификация существующих контролей, идентификация уязвимостей и последствий.

В данной работе предлагается начинать не с информационных активов, а с описания бизнес-процессов предприятия как актива. Учитывая, что деятельность предприятий неотрывна связана с созданием, обработкой и передачей цифровой информации, можно рассматривать предприятие как некий механизм, перерабатывающий цифровую информацию для получения прибыли (рис. 1).

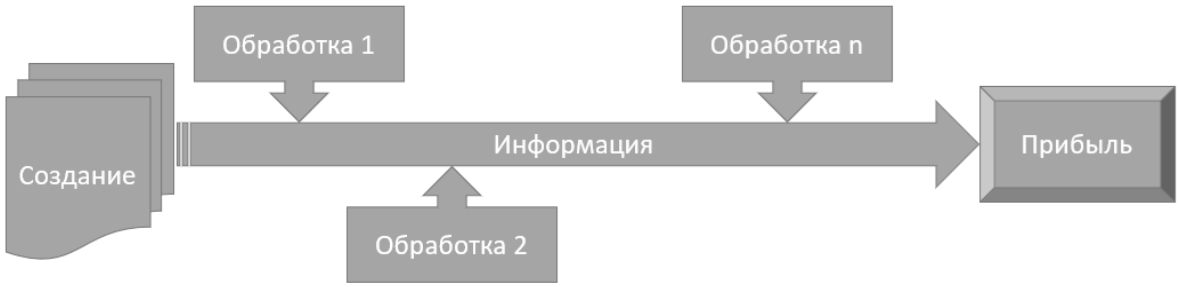

Рис 1. Схема прохождения информации на предприятии

Если принять как основу информационной безопасности три основных принципа: целостность, доступность и конфиденциальность информации, то любое нарушение работы механизма может нарушить любой из этих принципов. Тогда и прохождение, и целостность информации будут нарушены.

Соответственно мы можем рассматривать работу предприятия как механизма с помощью описания бизнес-процессов (БП). Для этого составляем карту бизнес-процессов предприятия (рис.2).

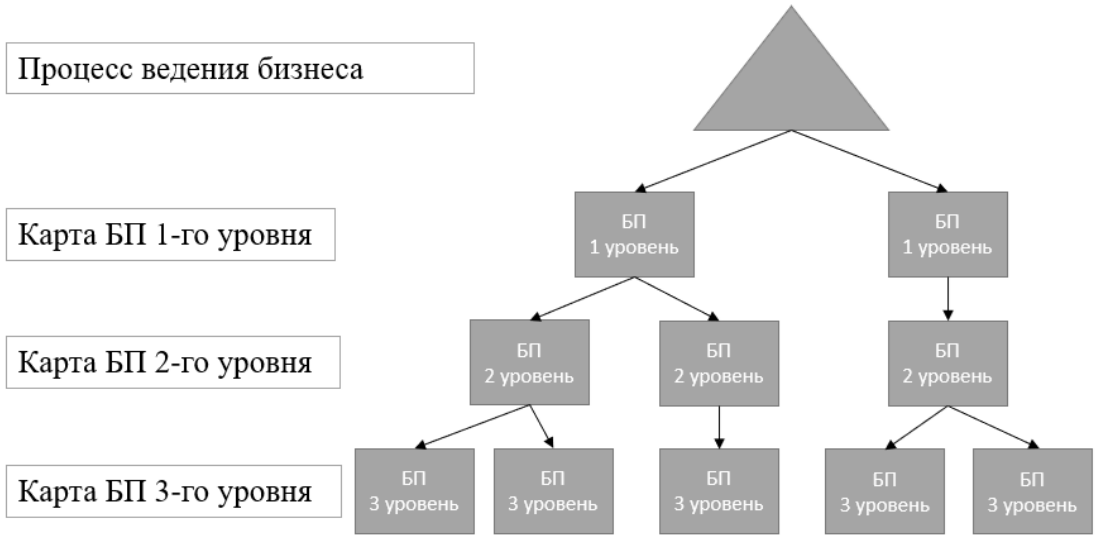

Рис 2. Построение карты бизнес-процессов

Далее ранжируем бизнес-процессы по важности на примере таблицы 1.

Таблица 1 – Значения важности бизнес-процесса

Уровень важности	Описание
Особой важности	Кратковременное прерывание в работе приводит к существенному ущербу для бизнес-процесса
Важный	Остановка в работе приводит к существенному ущербу для бизнес-процесса
Средней важности	Кратковременное прерывание в работе приводит к ограниченным потерям
Маловажный	Остановка в работе приводит к ограниченным потерям
Неважный	Перерыв в работе не вызывает существенных потерь

Следующим шагом необходимо провести анализ связности бизнес-процессов с информационными активами. Если на предприятии ведется документирование инфраструктуры, то в регламентах должно быть описание информационной системы, ее зависимость от системных сервисов и влияние на вышестоящие активы, в том числе бизнес-процессы. На основании этих данных можно сделать описание угроз информационным системам и уязвимости сервисов как это описано в документах [6] и [7].

Далее оцениваем влияние бизнес-процесса на общую деятельность предприятия, например, можно сделать косвенную оценку, насколько уменьшится эффективность работы подразделений, связанных с работой данного бизнес-процесса.

В итоге всех этих шагов мы будем иметь данные о вероятности наступления угрозы информационным активам, связанным с бизнес-процессом, также можем оценить возможные значения ущерба активу при реализации угроз. Необходимо учитывать и ущерб, который понесут еще и связанные активы.

Результат анализа сводим в таблицу 2.

Таблица 2 – Сводная таблица бизнес-процессов

Описание бизнес-процесса	Уровень воздействия на деятельность (в долях от 1)	Вероятность наступления угрозы в течение года	Итоговый коэффициент воздействия
Бизнес-процесс №1	0,35	0,02	0, 007
Бизнес-процесс №2	0,15	0,2	0,03
Бизнес-процесс №3	0,55	0,05	0,0275
Бизнес-процесс №4	0,25	0,1	0,025
ИТОГО			0,0895

Таким образом при нарушении работы одного из бизнес-процессов эффективность работы предприятия упадет от 15 до 55 %. Но с учетом вероятности наступления угрозы, влияющей на бизнес-процесс, итоговый результат будет ниже. На основании этой оценки мы можем рассчитать финансовые потери от нарушения работы того или иного бизнес-процесса.

Для принятия решения необходимо учитывать коэффициент воздействия нарушения работы бизнес-процесса на деятельность предприятия и вероятность реализации угроз системам, связанных с данным бизнес-процессом. Чем выше коэффициент воздействия и вероятность наступления угрозы, тем скорее должны быть приняты меры по обеспечению информационной безопасности.

Выводы и заключение

В этой работе был описан механизм создания методики расчета финансовых рисков предприятия от потери или утечки информации с учетом процессов работы предприятия. Данная методика позволяет сделать наглядным воздействие угроз на работу бизнес-процессов предприятия. Но для полноценной картины на предприятии должно быть полное документирование инфраструктуры с описанием систем, сервисов, их взаимодействие и воздействие на зависимые бизнес-процессы. Так как финансовые показатели работы предприятия напрямую зависят от бизнес-процессов предприятия и на них влияют все риски ведения бизнеса, то введение рисков информационной безопасности в общую картину бизнеса

позволит изменить отношение владельцев бизнеса к информационной безопасности.

Целью данный статьи было описание создания алгоритма расчета финансовых рисков на основе описания бизнес-процессов и их взаимодействия с инфраструктурой предприятия. Но требуется дальнейшая проработка алгоритма, чтобы позволить автоматизировать данный процесс и, возможно, в дальнейшем на его основе разработать программный модуль для встраивания в учетные системы.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Баранова Е.К. Методики анализа и оценки рисков информационной безопасности / Е.К. Баранова // Образовательные ресурсы и технологии. – 2015. – № 1(9). – С.73-79.

2. Глущенко И.С., Баранова Е.М., Баранов А.Н., Борзенкова С.Ю. Современные информационные системы анализа и управления рисками в сфере информационной безопасности / И.С. Глущенко, Е.М. Баранова, А.Н. Баранов, С.Ю. Борзенкова // Известия ТулГУ. Технические науки. – 2021. – Вып.2. – С.311-316.

3. Росенко А.П., Аветисов Р.С. Математическое моделирование вероятного ущерба от утечки конфиденциальной информации в автоматизированной информационной системе / А.П. Росенко, Р.С. Аветисов // Вестник Ставропольского государственного университета. – 2009. - № 63. – С.51-61.

4. Гутов И.Н., Шабурова А.В. Анализ методик расчета экономического ущерба от потери или утечки информации / И.Н. Гутов, А.В. Шабурова // Магистерская научная сессия «Первые шаги в науке». – 2024. – Том 6. – С.49-55.

5. Краснов И.З., Карелин О.И. Методика анализа и оценки рисков организации / И.З. Краснов, О.И. Карелин // Вестник СибГАУ. – 2014. - № 2(54). - С.37-44.

6. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности = Information technology. Security techniques. Information security risk management : национальный стандарт Российской Федерации : издание официальное : утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 30 ноября 2010 г. № 632-ст : введен впервые : дата введения 2011-12-01 – Москва : Стандартинформ, 2011. – 51 с.

7. Федеральная служба по техническому и экспортному контролю. Методический документ. Методика оценки угроз безопасности информации. [Утвержден ФСТЭК России 5 февраля 2021 года]. – Москва, 2021. – 83 с.