УДК 338.24:004.056
DOI 10.33764/2618-981X-2024-6-49-55

И. Н. Гутов[1]*, *А. В. Шабурова*[1]

Анализ методик расчета экономического ущерба от потери или утечки информации

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

Аннотация. Статья посвящена актуальному вопросу, по количественной оценке, экономического ущерба от потери или утечки информации. Учитывая, что в современном мире цифровая информация играет большую роль в хозяйственной деятельности, а защита информации стала важной частью организации работы предприятий, расчет экономических потерь имеет большое значение для принятия управленческих решений в области защиты информации. Результаты таких расчетов помогают бизнесу в понимании важности разработки стратегии защиты информации, выборе соответствующих мер и технологий безопасности. Они помогают руководству оценить потенциальные финансовые потери и принять обоснованные решения о выделении ресурсов на обеспечение информационной безопасности на предприятии. Для понимания тенденций в области утечки информации, в статье приведена статистика утечек данных, как в мире, так и в России, на основании которой обосновывается важность оценки экономического ущерба. В статье приведен результат анализа существующих методик на описание методологии, сферы применения и соответствия современным требованиям. Данный анализ показал, что для расчета экономического ущерба от потери или утечки информации необходимо актуализировать существующие методики и проработать расширенную методику, включающую в себя более широкую сферу применения, а не только оценку ущерба от утечки персональных данных.

Ключевые слова: экономические потери, утечка информации, информационная безопасность, методики расчета

I. N. Gutov[1]*, *A. V. Shaburova*[1]

Analysis of methods for calculating economic damage from loss or leakage of information

[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 quantifying the economic damage caused by loss or leakage of information. Considering that in the modern world digital information plays an important role in economic activity, and information protection has become an important part of the organization of enterprises, the calculation of economic losses is of great importance for making management decisions in the field of information protection. The results of such calculations help businesses understand the importance of developing an information security strategy, choosing appropriate security measures and technologies. They help management assess potential financial losses and make informed decisions about allocating resources to ensure information security at the enterprise. To understand trends in information leakage, the article provides statistics on data leaks, both in the world and in Russia, on the basis of which the importance of assessing economic damage is justified. Further, the article presents the result of an analysis of existing methods for the completeness of the description of the methodology, scope of appli-

cation and compliance with modern requirements. This analysis showed that in order to calculate the economic damage from loss or leakage of information, it is necessary to update existing methods and work out an expanded methodology that includes a wider scope of application, and not only an assessment of damage from leakage of personal data.

Keywords: economic losses, information leak, information security, calculation methods

Введение

С развитием современных средств вычислительной техники и телекоммуникаций цифровая информация стала занимать одну из основных областей деятельности и играть большую роль в жизни населения. Но с широким распространением цифровой информации появились новые угрозы и уязвимости, специфичные для компьютерных систем и сетей, с ними появились и новые формы имущественных и неимущественных преступлений. Это стало возможным из-за того, что большая часть деятельности предприятий (интернет-магазины, банки, документооборот и пр.) перешла в цифровую среду.

В связи переходом деятельности в цифровую среду стала иметь очень большое значение защита цифровой информации от потерь и утечек. Но для обеспечения информационной безопасности для предприятия необходимо иметь понятные методики расчета экономических параметров внедрения стратегий и механизмов защиты информации, оценки экономического ущерба от утечки или потери информации.

Важность оценки экономических рисков от потери или утечки информации для предприятия неоспорима, т.к. она помогает принимать управленческие решения в области защиты информации, что позволит минимизировать риски и обеспечить непрерывность работы предприятия, рассчитывать страховые взносы при страховании предприятия от ущерба при утечке или потери информации. Также наличие количественного расчета может служить для правильной квалификации правонарушения в области цифровой информации и определения вида ответственности, т.к. согласно главе 28 Уголовного Кодекса Российской Федерации (УК РФ) [1], наказание, в зависимости от нанесённого ущерба, может быть от штрафа до ограничения свободы.

Учитывая происходящие глобальные изменения в мире, стремительное изменение и развитие технологий в современном цифровом пространстве, соответствие методик расчета ущерба современным тенденциям имеет очень важное значение.

В данной статье ставится задача проанализировать существующие методики количественной оценки экономического ущерба от утечки информации.

Методы и материалы

Проведем анализ утечек. Для этого воспользуемся данными отчетов экспертно-аналитического центра (ЭАЦ) InfoWatch – компании, которая занимается исследованиями в области информационной безопасности.

На рис. 1 показан график количества утечек за 2022 год и первое полугодие 2023 года [2].

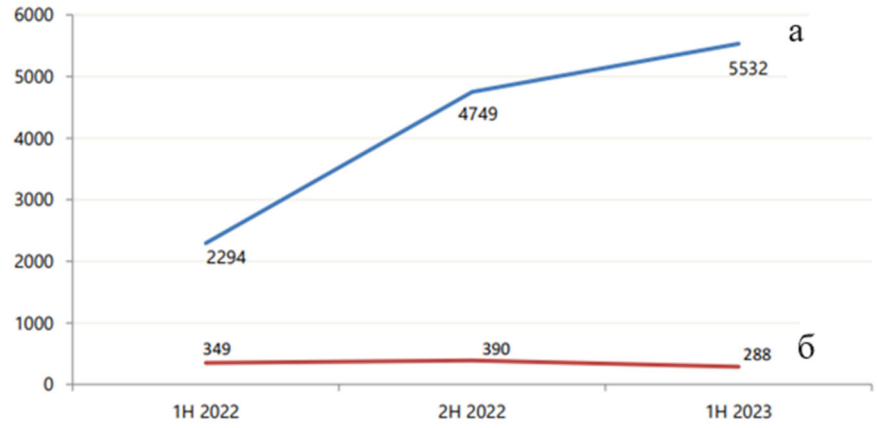

Рис 1. Количество утечек данных: «а» - Мир, «б» - Россия

Как видим, количество утечек увеличивается со временем и тенденции к снижению не предвидится (по данным ЭАЦ InfoWatch в первом полугодии 2018 года было зафиксировано всего 1039 утечек).

В отчете ЭАЦ InfoWatch за первое полугодие 2023 года [2] приведены данные, собранные на основании открытых источников, о распределении утечек по содержанию типов данных за первое полугодие 2022 и первое полугодие 2023 (рис. 2).

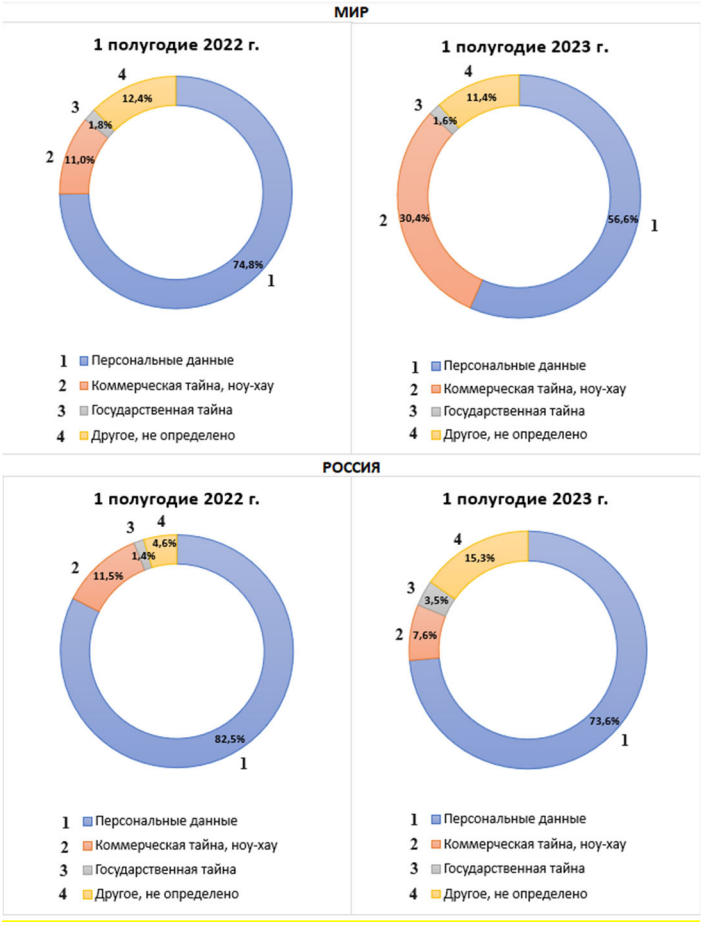

Рис. 2. Распределение утечек информации по типам данных в мире и России

Как следует из рис. 2, основная часть утечек приходится на персональные данные. В тоже время в мире за год возросла доля утечек коммерческой тайны и ноу-хау. А в России за год возросло количество утечек государственной тайны, что, скорее всего связано с политическими изменениями, начавшимися в феврале 2022 года.

По результатам исследования ЭАЦ InfoWatch, проведенного в 2023 году в виде анонимного опроса среди крупных частных и государственных предприятий промышленного сектора, картина распределения скомпрометированной информации по типам данных несколько другая (рис. 3) [3]. В этом исследовании не фигурирует информация, содержащая государственную тайну, т.к. предприятия не раскрывают такие данные, она поступает в основном из открытых источников, но зато существует информация содержащая служебную тайну.

Рис. 3. Распределение утечек информации по типам данных по России

Согласно исследованию, проведенному в 2014 году компанией Zecurion [4], производителя отечественной DLP-системы – в среднем российские компании различных отраслей среднего и крупного бизнеса теряют от каждой утечки информации около 820 тысяч долларов, максимальный ущерб в этом же 2014 году составил 30 млн. долларов. Также эксперты компании подсчитали, что более 90 % российских компаний сталкиваются с крупными утечками информации, которые потенциально могут привести к серьезным финансовым потерям, вплоть до банкротства, при этом в 30 % компаний крупного и среднего бизнеса фиксируют по две попытки в месяц похитить ценную информацию. И только 8 % компаний не страдают от утечек.

Основными статьями ущерба вследствие утечек являются прямые потери, упущенная выгода, а также штрафы со стороны регуляторов. Если говорить о российской практике, то наибольшие потери компаний приходятся на косвенный ущерб вследствие ухудшения клиентской базы (особенно в высококонкурентных отраслях) или из-за получения конкурентами других преимуществ.

По результатам опроса предприятий, проведенного ЭАЦ InfoWatch в 2023 году, у почти половины предприятий (47 %) отсутствует методика по оценке

ущерба от утечки информации. При этом опрос показал, что подавляющее большинство организаций (71 % опрошенных) не застрахованы от ущерба в случае утечки или потери информации.

Таким образом можно выявить список возможных источников ущерба:

- косвенный ущерб, связанный с ухудшением клиентской базы;
- потери, связанные с упущенной выгодой;
- штрафы регуляторов и надзорных органов;
- судебные издержки по искам, в случае утечки конфиденциальных и персональных данных;
- отзыв лицензии и потеря рынка госзаказов, в случае утечки гостайны;
- стоимость восстановления потерянной информации или разработки новых технологических решений.

На основании полученных данных решено провести анализ существующих методик расчета экономического ущерба от утечки персональных данных, коммерческой тайны и гостайны.

Анализ методик

Для понимания проблемы был проведен поиск методик расчета экономического ущерба от утечки или потери информации.

Большинство методик расчета ущерба в информационной сфере основаны на оценке угроз и анализе рисков. Одними из основных документов, регламентирующих данные методики, являются методический документ ФСТЭК [5] и ГОСТ Р ИСО/МЭК 27005-2010 «Менеджмент риска информационной безопасности» [6], в области защиты персональных данных меры защиты описаны в Федеральном законе «О персональных данных» [7].

Так в работе [8] в главе 3 описан алгоритм оценки стоимости информационных ресурсов, критичных к утечке (персональные данные). Этот алгоритм основан на описании в табличном виде списка угроз и связанных с ними статей из Кодекса Российской Федерации об административных нарушениях (КоАП РФ) [9], в которых прописаны штрафы за нарушения. Также в таблицу добавлен столбец по оценке стоимости восстановления утраченной информации, взятой из прайс-листа компании, предоставляющей данную услугу.

Для оценки размера ущерба для предприятия в данном расчете учитывается и размер предприятия по уровню оборота и количеству сотрудников.

На странице 84 данной работы [8] приведен полный алгоритм итогового расчета ущерба от угрозы безопасности информационного ресурса. Данный алгоритм описывает оценку ущерба, связанного с нарушениями безопасности персональных данных и на настоящее время это наиболее полное описание методики расчета такого ущерба.

Проблематика расчета ущерба также была поднята в работах [10] и [11]. Но в них нет количественной оценки ущерба. Только проведен анализ и описано направление.

В следующей работе [12] приведена методика анализа и управления рисками на основе стоимостных оценок. Данная методика наиболее приближена к реальной ситуации и наиболее близка и понятна бизнесу, который оперирует денежными категориями.

В работе [13] приведен сравнительный анализ программных комплексов, использующихся для оценки и анализа рисков. Список программных комплексов разделен по типу используемых методик: качественного анализа, количественной оценки и смешанного типа. Но в этой же статье отмечается, что используемые в настоящее время методики малоэффективны, т.к. у многих предприятий процессы управления рисками проводятся независимо каждым подразделением, соответственно отсутствует централизованный контроль над их действиями, что исключает возможность реализации единого и целостного подхода к управлению рисками во всей организации.

Вывод

Практически в каждой найденной работе, посвященной оценке, анализу и управлению рисками в информационной среде, поднимается вопрос об отсутствии однозначности при расчетах оценки ущерба в информационной среде, а также отсутствии единого подхода. Все это приводит к многовариантности, усложнению, неоднозначности решений в сфере обеспечения информационной безопасности и, как следствие, недооценки бизнесом важности данной сферы деятельности.

Заключение

Целью данный статьи было проведение анализа существующих методик расчета экономического ущерба от утечки или потери информации. В результате анализа пришли к заключению, что нет ясного и понятного механизма создания таких методик. Многие методики приняты на основе зарубежного опыта, который не всегда применим в отечественной сфере. При этом найденные методики расчетов разработаны до 2020 года, а учитывая кардинальные мировые изменения, идущие последние два года, требуется их пересмотр и, при необходимости, актуализация методов на соответствие современным реалиям.

В дальнейшем предполагается на основе существующих методик проработать общий инструмент создания методик расчета и, возможно, на основе этого инструмента разработать программный модуль для автоматизации расчетов.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Российская Федерация. Законы. Уголовный кодекс Российской Федерации на 1 февраля 2023 года. Включая составы преступлений, связанные с мобилизацией : [принят Государственной думой 24 мая 1996 года : одобрен Советом Федерации 5 июня 1996 года]. – Москва : Кладезь, 2023. – 320 с.

2. Утечки информации ограниченного доступа в мире и России, первое полугодие 2023 г. Аналитический отчет. – Экспертно-аналитический центр InfoWatch. 2023. – 17 с.

3. Оценка ущерба вследствие утечек информации. Аналитический отчет. – Экспертно-аналитический центр InfoWatch. 2023. – 26 с.

4. Практические аспекты защиты информации от утечек в России. - Zecurion Analitics., 2015. - 17 стр. - Текст : электронный // URL: https://filearchive.cnews.ru/img/files/2014/10/28/praktika_zashiti_zecurion.pdf (дата обращения: 20.04.2024).

5. 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.

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. Российская Федерация. Законы. Федеральный закон «О персональных данных». Текст с изменениями и дополнениями на 2023 год : Федеральный закон № 152-ФЗ : [принят Государственной думой 8 июля 2006 года : одобрен Советом Федерации 14 июля 2006 года]. – Москва : Эксмо, 2023. – 32 с.

8. Шинаков К. Е. Минимизация рисков нарушения безопасности при построении системы защиты персональных данных. Диссертация на соискание ученой степени кандидата технических наук : 05.13.19 / К. Е. Шинаков – Брянск., 2017.– 256 с.

9. Российская Федерация. Законы. Кодекс Российской Федерации об административных правонарушениях. Текст с изменениями и дополнениями на 01.02.2023 года : Федеральный закон № 195-ФЗ [принят Государственной думой 20 декабря 2001 года : одобрен Советом Федерации 26 декабря 2001 года]. – Москва : Эксмо, 2023. – 704 с.

10. Финансовые риски при утечке информации / А.А. Нечай, Л.С. Минухина, П.Е. Котиков // Наука, образование, общество. – 2014. – № 1 (1). – С. 33-41.

11. Утечка информации как угроза экономической безопасности предприятия / О.Г. Назарова, В.А. Довыденко // Экономика. Социология. Право. – 2020. – № 2 (18). – С.28-34.

12. Применение оценок рисков в управлении информационной безопасностью / Т.Н. Васильева, А.В. Львова // Прикладная информатика. – 2009. – №5 (23). – С. 68-76.

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