УДК 338.14

ЗАЩИТА КОММЕРЧЕСКОЙ ИНФОРМАЦИИ В ЦИФРОВОМ ПРОСТРАНСТВЕ И МЕТОДЫ ПРЕДОТВРАЩЕНИЯ УТЕЧЕК

Д. Г. Плотников

студент экономического факультета, Пермский государственный национальный исследовательский университет, г. Пермь, Россия, e-mail: plotnikov59rus@gmail.com

Научный руководитель: **А. В. Бобков**

кандидат экономических наук, доцент, доцент кафедры предпринимательства и экономической безопасности, Пермский государственный национальный исследовательский университет, г. Пермь, Россия, e-mail: bobkovav@yandex.ru

Одним из результатов цифровизации является увеличение ущерба от утечек. Проанализированы причины и статистические характеристики данного явления. Рассмотрены технические и правовые методы противодействия утечкам информации. Дана оценка государственной политике в сфере защиты персональных данных, а также авторские рекомендации по использованию принципа ограничения доступа сотрудников к массивам информации.

Ключевые слова: утечка информации; персональные данные; информационная безопасность; мониторинг; коммерческая тайна.

PROTECTION OF COMMERCIAL INFORMATION IN THE DIGITAL SPACE AND LEAK PREVENTION METHODS

D. G. Plotnikov

Student of the Faculty of Economics, Perm State University, Perm, Russia, e-mail: plotnikov59rus@gmail.com

Supervisor: **A. V. Bobkov**

PhD in Economics, Associate Professor, Associate Professor of the Department of Entrepreneurship and Economic Security, Perm State University, Perm, Russia, e-mail: bobkovav@yandex.ru

One of the results of digitalization is an increase in damage from leaks. The causes and statistical characteristics of this phenomenon are analyzed. Technical and legal methods of combating information leaks are considered. An assessment of the state policy

in the field of personal data protection is given, as well as the author's recommendations on the use of the principle of limiting employee access to arrays of information.

Keywords: information leakage; personal data; commercial information; information security; prevention of information leaks.

Развитие информационно-телекоммуникационных технологий, и как следствие цифровизация современной экономики, характеризуется заменой традиционных физических носителей информации на облачные системы хранения данных. Вместе с тем, экспоненциальный рост демонстрирует и само количество данных, так объем генерируемых за год данных к 2025 году составит 175 зеттабайт (рис. 1).

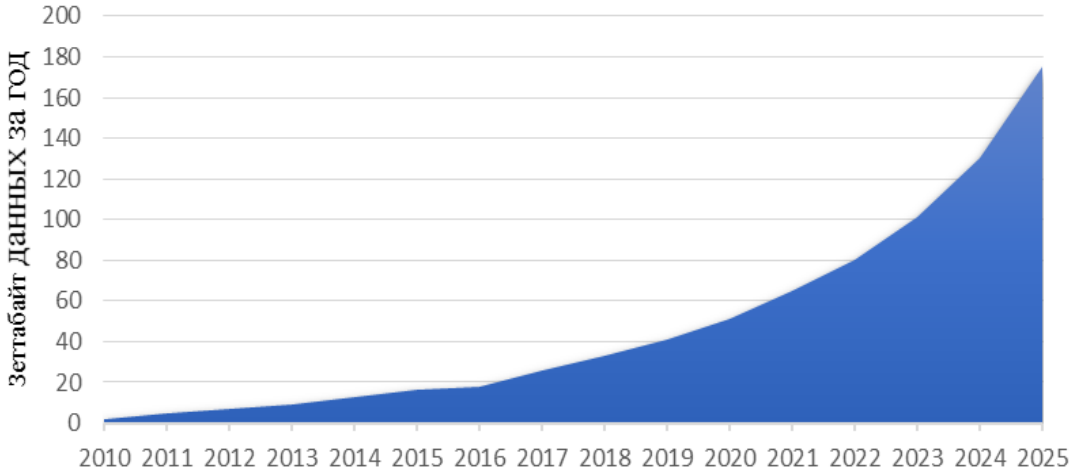

Рис. 1. Годовой объем генерируемых глобальных цифровых данных (ЗБ)

Составлено по: [5].

Закономерным результатом такого тренда является проблема утечки информации, особенно остро ограниченного доступа, ответственность за хранение которой несут коммерческие организации. Согласно данным ежегодного отчета «Cost of a Data Breach Report 2023», формируемого Ponemon Institute при поддержке компании IBM, средний ущерб после утечки информации составляет $4,5 млн, что на 15 % больше, чем три года назад [2]. Помимо прямого денежного ущерба, организация сталкивается с такими рисками как: неспособность компании исполнять собственные финансовые обязательства (Liquidity risk), например, возникает ввиду необходимости компенсации морального вреда, причиненного субъектам персональных данных; рыночный, влекущий снижение стоимости активов (Market risk), чаще всего возникает в результате инцидентов, сопряженных с инсайдерской торговлей и последующей потерей стоимости акций на определенный

срок; операционный (Operation risk), характерен для ситуаций, вследствие которых разглашение конфиденциальной информации влечет снижение эффективности бизнес-процессов.

Наиболее часто компрометации подвергаются персональные данные (39 %), за ними следуют сведения, составляющие коммерческую тайну (24 %), составляющие служебную тайну (18 %), ноу-хау или секреты производства (8 %), банковскую тайну (5 %) (рис. 2).

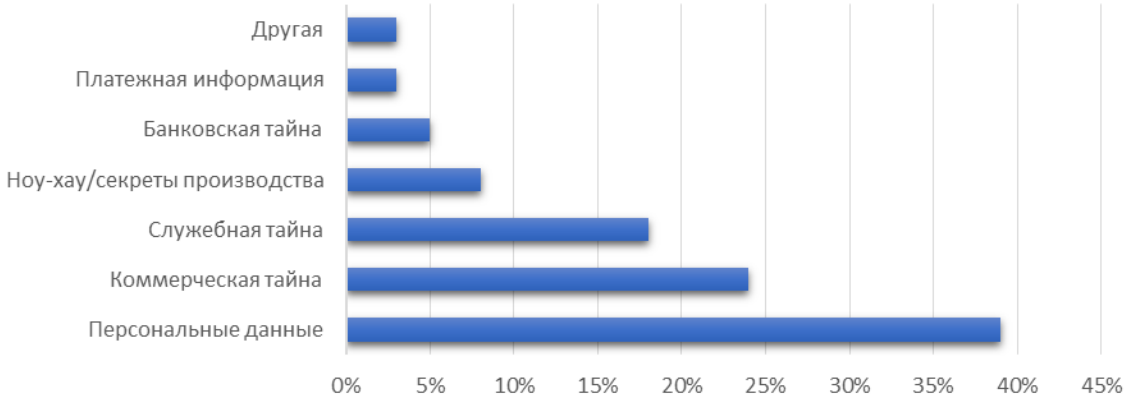

Рис. 2. Распределение видов скомпрометированной информации (% от общего объема)

Составлено по: [3].

Исключительно эффективной мерой противодействия подобного рода утечкам является внедрение Data Loss Prevention (DLP) систем. Данные системы представляют собой программные продукты, обеспечивающее информационную защиту компании в целом и конфиденциальных сведений в частности путем мониторинга исходящей и входящей информации и своевременной блокировки операций, идентифицированных системой как подозрительные. Системой используются такие технологии, как поведенческий анализ, файловый краулер, контроль идентификаторов, цифровые отпечатки, графические шаблоны. На практике, 75 % организаций в полной мере не удовлетворяют требованиям Федерального закона «О персональных данных» и подвержены риску наложения штрафных санкций [1].

Опциональным методом противодействия является заключение соглашения о неразглашении (Non-disclosure agreement, NDA), при котором объектом неразглашения становятся сведения, составляющие профессиональную тайну, зачастую не попадающие под законодательные определения. Такое соглашение позволяет на двустороннем уровне определить санкции по отношению к нарушителям, на практике, значительно превышающие предусмотренные административные штрафы.

Методом борьбы также является ужесточение ответственности за нарушения законодательства в области защиты персональных данных. В настоящее время ведется законотворческий процесс по внесению в Кодекс Российской Федерации об административных правонарушениях изменений, содержащих прогрессивную систему штрафов для юридических лиц, чем большего количества субъектов коснется утечка – тем больший штраф будет наложен. За повторное же нарушение может быть наложен оборотный штраф на выручку суммой вплоть до 500 млн рублей [4]. Предлагаемый размер штрафов для правонарушителей – юридических лиц, ответственных за утечку персональных данных более 10 тыс. субъектов оценивается как недостаточный и требует значительного увеличения пропорционально объему лиц, чьи права были нарушены в результате утечки. На текущем этапе разработки законопроекта прогрессивная система не способна принуждать компании с массивным объемом клиентов к проявлению ответственности при принятии мер по противодействию утечкам данных, что сказывается на конечной эффективности предлагаемых законодателем изменений.

Только при переработке размеров штрафных санкций в области утечек персональных данных компании будут находиться в условиях, когда внедрение систем предотвращения утечек информации и применение иных современных мер противодействия будет экономически выгоднее уплаты административного штрафа, что ведет к повышению меры их ответственности. Реализация таких изменений в законодательстве не только не потребует увеличения расходов бюджетов бюджетной системы государства, но и способна обеспечить рост поступлений в бюджетную систему.

Помимо подчинения административной политике государства, коммерческим организациям необходимо самостоятельно принимать меры по противодействию утечкам информации, придерживаясь принципа ограничения доступа сотрудников к массивам данных. Так, при работе с клиентской базой, сотрудник в рамках своих профессиональных функций имеет доступ к ограниченному объему информации из общего массива, что минимизирует риск неправомерного использования или распространения. Также необходимо применение мер по обезличиванию персональных данных, что препятствует идентификации личности без дополнительных запросов в корпоративной системе, оставляющих цифровой след, позволяющий беспрепятственно установить личность сотрудника при внутренней проверке специалистом по информационной безопасности.

Применение описанных в работе организационных, правовых, программных и технических мер по защите информации позволяет миними-

зировать риск неправомерного распространения и использования сведений ограниченного доступа, соответственно, значительно снизить величину ущерба от утечек информации.

Библиографические ссылки

1. Inc. Russia – Журнал для предпринимателей [Электронный ресурс]. URL: https://incrussia.ru/news/o-personalnyh-dannyh/ (дата обращения: 04.10.2023).

2. Аналитический отчет «Cost of a Data Breach Report 2023». International Business Machines [Электронный ресурс]. URL: https://www.ibm.com/reports/data-breach– (дата обращения: 28.09.2023).

3. Аналитический отчет «Оценка ущерба вследствие утечек информации». Экспертно-аналитический центр InfoWatch. 2023 г. [Электронный ресурс]. URL: https://www.infowatch.ru/analytics/analitika/otsenka-uscherba-vsledstvie-utechek-informatsii (дата обращения: 01.10.2023).

4. Информационное телеграфное агентство России (ИТАР-ТАСС) [Электронный ресурс]. URL: https://tass.ru/politika/18842775 (дата обращения: 06.10.2023).

5. Исследование Seagate и International Data Corporation «Data Age2025» [Электронный ресурс]. URL: https://www.seagate.com/files/www-content/our-story/trends/files/Seagate-WP-DataAge2025-March-2017.pdf (дата обращения: 26.09.2023).

6. Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 06.02.2023) «О персональных данных» // СПС КонсультантПлюс [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 04.10.2023).