УДК 004.056.5 DOI: 10.37468/2307-1400-2022-2-98-104

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННОГО СОПРОВОЖДЕНИЯ В СИСТЕМЕ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ

Агаев Руслан Шахинович [1]
Агаев Рафаэль Шахинович [1]
Графов Александр Александрович [1]

[1] Санкт-Петербургский государственный экономический университет, Санкт-Петербург, Россия

АННОТАЦИЯ

Дана краткая характеристика терминов «информационное сопровождение» и «информационная безопасность» субъектов экономической деятельности. Обоснована необходимость обеспечения защиты информационного сопровождения в системе экономической безопасности организаций. Проведена классификация информационных атак и риски их возникновения. Представлена классификация стратегий обеспечения защиты информационной среды субъектов экономической деятельности.

Ключевые слова: информационное сопровождение, информация, информационная безопасность, экономическая безопасность.

SECURITY OF INFORMATION SUPPORT IN THE ECONOMIC SECURITY SYSTEM

Agaev Ruslan Sh. [1]
Agaev Rafael Sh. [1]
Grafov A. A. [1]

[1] St. Petersburg State University of Economics, St. Petersburg, Russia

ABSTRACT

A brief description of the terms “information support” and “information security” of subjects of economic activity is given. The necessity of ensuring the protection of information support in the system of economic security of organizations is substantiated. The classification of information attacks and the risks of their occurrence has been carried out. A classification of strategies for ensuring the protection of the information environment of subjects of economic activity is presented.

Keywords: information support, information, information security, economic security.

Организация деятельности системы экономической безопасности строится на сборе и обработке информации о текущем состоянии субъекте экономической деятельности, его структуре, деятельности, возможностях, технических средствах и других сведениях, которые формируют информационное сопровождение. Информационное сопровождение – обеспечение субъекта экономической деятельности необходимыми сведениями в целях реализации регулирования деятельности, повышения эффективности и управления угрозами.

Сегодня главной проблемой в системе экономической безопасности для информацион-

ного сопровождения является время обработки массивов данных, а для самой информации – это ее безопасность. Общедоступность сведений может негативно отразиться на реализации планов по развитию организаций, обеспечению их экономической безопасности, а также привести к нарушению ряда нормативных правовых актов Российской Федерации, таких как: Федеральный закон от 27.07.2006 №149 «Об информации, информационных технологиях и о защите информации», Федеральный закон «О персональных данных» от 27.07.2006 N 152-ФЗ, Федеральный закон от 29.07.2004 N 98-ФЗ «О коммерческой тайне». Отсюда следует необходимость в управлении информационными рисками, то есть защите информации, находящейся в распоряжении экономического субъекта. Информационная безопасность (ИБ) – процесс обеспечения конфиденциальности, целостности и доступности информации, где:

1. Конфиденциальность информации – ведение контроля (административный, логический, физический), гарантирующего необходимый уровень безопасности данных экономических объектов для предотвращения несанкционированного или нежелательного раскрытия.

2. Целостность – контроль потока информации, его обработка и гарантия предотвращения ее искажения.

3. Доступность – сетевая среда, реализующая надежный и эффективный доступ к информации уполномоченных лиц, когда это необходимо [1].

Для выполнения мер по обеспечению защиты в соответствии с действующим документом ФСТЭК России «Общие требования по обеспечению безопасности информации в ключевых системах информационной структуры» определяется важность информации и устанавливаются следующие требования:

- обеспечение информации в информационной среде;
- планирование обеспечения безопасности информации;
- оценка рисков реализации угроз информационного воздействия;
- защита коммуникаций;
- информирование и обучение персонала по вопросам информационной безопасности;
- реагирование на инциденты (нарушения) ИБ;
- защита носителей информации;
- обеспечение целостности программного обеспечения информационной среды;
- аудит безопасности информации [2, 3].

Реализация необходимых требований по защите информационной среды субъектов экономической деятельности обеспечит минимальный уровень защиты от деструктивных информационных воздействий. В зависимости от содержания предъявляемых требований к безопасности информации происходит предотвращение или минимизация воздействия различного рода информационных атак (табл. 1).

Информационные атаки, представленные

Таблица 1 – Классификация атак, направленных на информационное сопровождение организаций

№	Тип атаки	Риск
1	Сканирование сети	Определение протоколов, активных сетевых сервисов, идентификаторов и паролей пользователей
2	Навязывание ложного маршрута	Несанкционированное изменение маршрутно-адресных данных, навязывание ложных сообщений
3	Внедрение ложного объекта сети	Перехват и просмотр трафика; несанкционированный доступ к сетевым ресурсам, навязывание ложной информации
4	Атака на пароли	Выполнение различных действий, направленных на получение несанкционированного доступа
5	Подмена доверенного объекта сети	Изменение маршрута прохождения данных; несанкционированный доступ к сетевым ресурсам, навязывание ложной информации
6	Отказ в обслуживании	Невозможность передачи данных из-за отсутствия корректных маршрутно-адресных данных
7	Удаленный доступ	Нарушение конфиденциальности, целостности, доступности информации с применением соответствующих незаконных программных средств

в таблице 1, могут быть направлены на разные структурные подразделения организаций (рис. 1), общая цель которых – получение различного рода информации.

Из данных гистограммы, представленной на рис. 1, можно заметить, что главными направлениями атак по получению информации являются отрасли высоких технологий, здравоохранения, госорганов и силовых структур. Но с 2019 года повышение уровня защиты в государственных информационных системах позволило уменьшить процент утечки. Связано это с изменением политики в обеспечении информационной безопасности, а именно с увеличением применения DLP-систем, способных выявить каналы утечки данных для дальнейшей их нейтрализации.

Рассмотрим динамику изменения выявленных утечек информации в сравнении с их общим количеством для оценивания эффективности работы в системе обеспечения защиты информации (рис. 2).

Из рис. 2 видно, что в 2019 году было резкое увеличение общего количества утекших данных, которое связано с началом эпидемиологической ситуации (Covid-19), вынудившей общество перейти на дистанционный формат взаимодействия во многих сферах: учеба, бизнес, покупка товаров и др. Увеличение потребности в дистанционных технологиях привело к резкому увеличению хранимых персональных данных, которые не успевали обрабатывать существующие системы защиты, а неопытность пользователей во многом

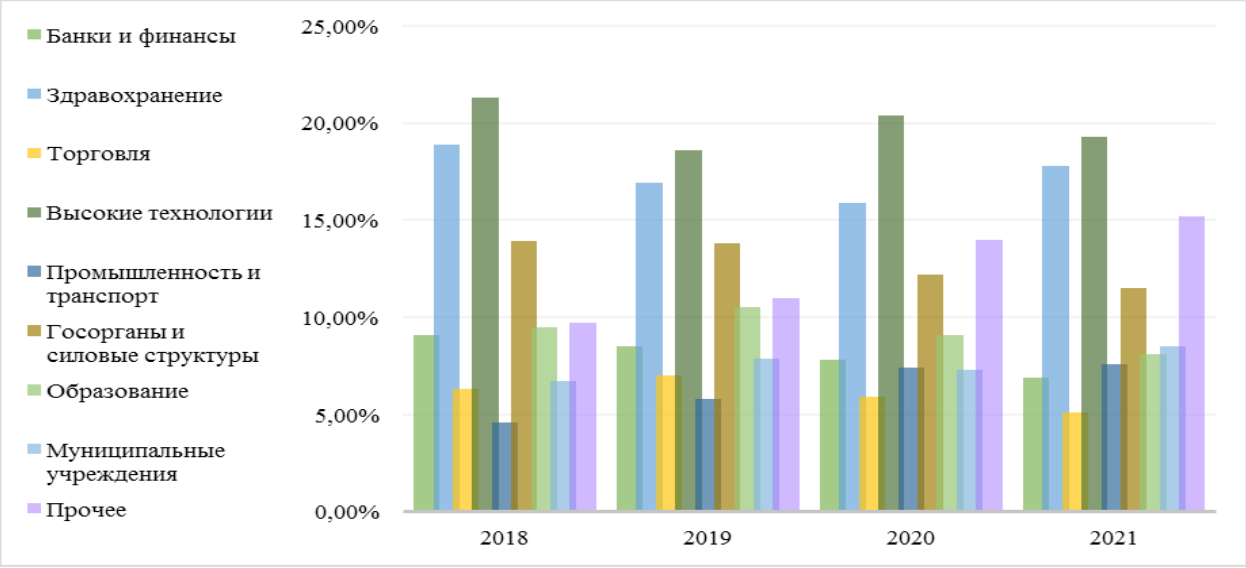


Рисунок 1 – Соотношение утечек информации по отраслям в период 2018–2019 гг. [4]

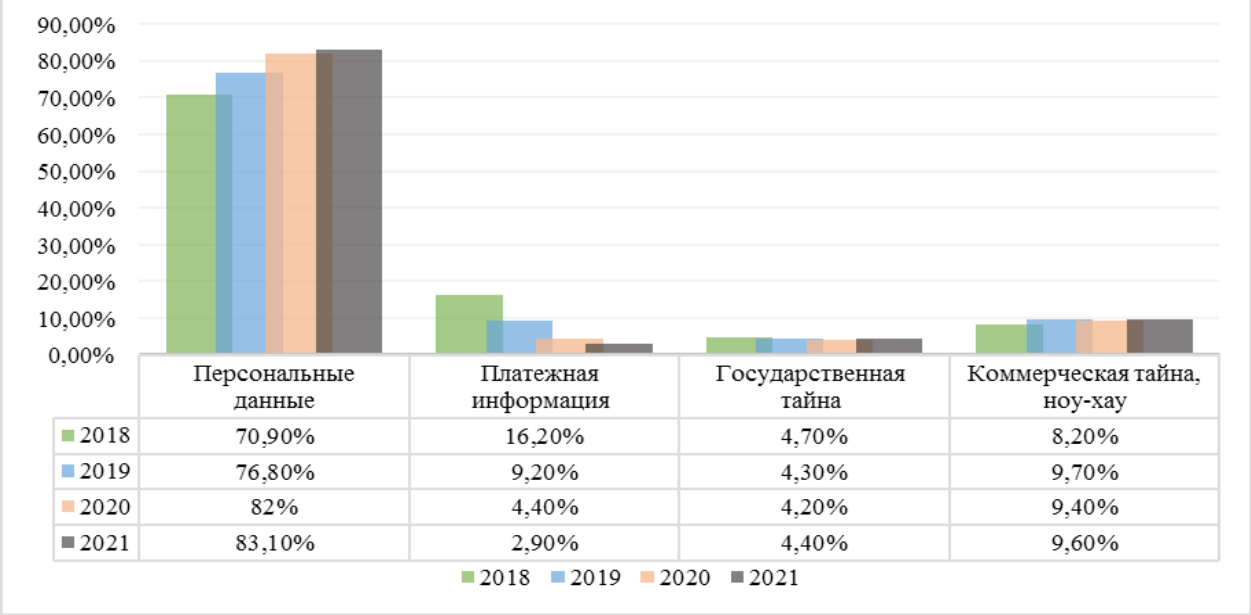
Рисунок 2 – Соотношение выявленных утечек данных к их общему количеству в мире (млн.)

не позволяла применять существующие стратегии безопасности. Но к 2021 году началось активное совершенствование цифровой среды в обществе, обучение персонала в области ИБ, что позволило сократить общее количество утечек на 55,7%. Виды утечек информации могут быть классифицированы по типам данных (рис.3).

В задачи системы информационной безопасности входит: регистрация и учет данных; тестирование и анализ данных; управление доступом данных; мониторинг нарушений безопасности; защита информации от утечки по техническим каналам; обеспечение резервного копирования программных средств и данных, необходимых для обеспечения бесперебойного функционирования информационного сопровождения системы экономической безопасности. Анализ информации и определение требуемого уровня защиты в зависимости от важности информации определяет стратегию ее обеспечения (табл. 2).

Применение стратегий (табл. 2) в целях эффективного обеспечения защиты информационного сопровождения должно характеризоваться:

- надежностью (уровень защиты должен быть соответствующим возможной угрозе и последствиям);
- комплексностью (разработка мер по защите учитывает все возможные риски);
- разумностью (внедрение стратегии обеспечения безопасности информации не должно мешать деятельности компании);
- постоянностью (меры по выполнению стратегии обеспечения защиты информации



	Персональные данные	Платежная информация	Государственная тайна	Коммерческая тайна, ноу-хау
2018	70,90%	16,20%	4,70%	8,20%
2019	76,80%	9,20%	4,30%	9,70%
2020	82%	4,40%	4,20%	9,40%
2021	83,10%	2,90%	4,40%	9,60%

Рисунок 3 – Распределение утечек информации по типу данных в период 2018–2021 гг. [4]

Таблица 2 – Классификация стратегий обеспечения защиты информационной среды

Стратегии обеспечения безопасности информационного сопровождения		
1. Стратегии по организации защиты	**2. Стратегии по направлению действий**	**3. Стратегии по признаку адаптивности**
Эшелонированная защита	Отвлечения (обмана)	Плановой защиты
Тотальный контроль	Пресечения	Адаптивной защиты
Ключевых элементов	Игнорирования последствий и резервирования информации	Смешанная стратегия
Периметровая защита	Смешанная стратегия	
Дифференцированный контроль и реакция		

должны выполняться постоянно независимо от режима работы субъекта);
– разнообразием (обеспечение информационной защиты субъекта реализуется при внедрении различных мер защиты в соответствии с уровнем важности информации).

Развитие информационных технологий приводит к развитию (увеличению) средств по дестабилизации деятельности компаний, краже информации или ее подмене, что подразумевает реализацию экономических угроз. В век цифровых технологий для эффективной защиты информации применяются следующие комплексные решения:

1. SIEM-системы (Security Information and Event Management) – системы сбора и управления информацией о безопасности, а также анализа и корреляции событий [5].

2. DLP-системы (Data Leak Prevention) – специализированное программное обеспечение, предназначенное для защиты от утечек и кражи конфиденциальной корпоративной информации, использующее технологии блокировки передачи информации через разные каналы (например, сервисы мгновенных сообщений, корпоративная почта, принтеры и т.д.), мониторинг поведения сотрудников и других участников локальной сети [6].

3. Корпоративные антивирусные программы – модульное программное обеспечение для защиты информации и оборудования от вредоносного программного обеспечения, кибер-атак и вирусных угроз [7].

Об успешном предотвращении утечек информации сегодня в открытых источниках не всегда можно найти данные, информация о таких происшествиях может вызывать множество угроз, в частности, репутационные. Рассмотрим некоторые наиболее крупные происшествия за последнее время, связанные с утечкой информации компаниями (табл. 3).

Данные из табл. 3 свидетельствуют о том, что применение систем защиты цифровых данных не всегда предотвращает их утечку, а последствия от реализации угроз наносят ущерб в миллионы долларов или увеличение недоверия к компании. Например, на сегодняшний день самой крупной выплатой штрафа за несоблюдение прав пользователей об их конфиденциальности считается выплата Uber в 2016 году в размере $148 млн, а потери от недоверия к компании Nintendo после утечки привели к уменьшению стоимости акций компании на 9%. Потери от различных цифровых атак в общем по годам составили $1,4 млрд в 2017 году, $2,7 мрлрд в 2018 году, $3,5 млрд в 2019 году и $4,2 млрд в 2020 году (рис. 4.).

Увеличение количества кибератак и нанесенного ущерба приводит не только к необходимости расширения применения средств защиты информационных систем и их развития, но и к изменениям в законодательстве [8]. Так, в частности, с 1 января 2020 г. вступил в силу закон о приватности потребителей в США – CCPA (California Consumer Privacy Act), с 25 мая 2018 г. во всех государствах-членах Европейского Союза был введен новый закон о защите персональных

Таблица 3 – Утечка информации и их последствия на примере компаний

Компания	Объем утечки	Последствия
Nintendo (2020 г.)	Данные 300 тыс. пользователей	Уменьшение стоимости акций компании на 9%; возвращение средств пользователей при их похищении
EasyJet (2019 г.)	Данные 9 млн. пользователей	Крупный иск за утечку данных на сумму 18 млрд фунтов стерлингов
Uber (2016 г.)	Данные 57 млн. пользователей	Выплата штрафа в размере $148 млн.
BitHumb (2018 г.)	Данные 30 тыс. пользователей	Похищение более $30 млн

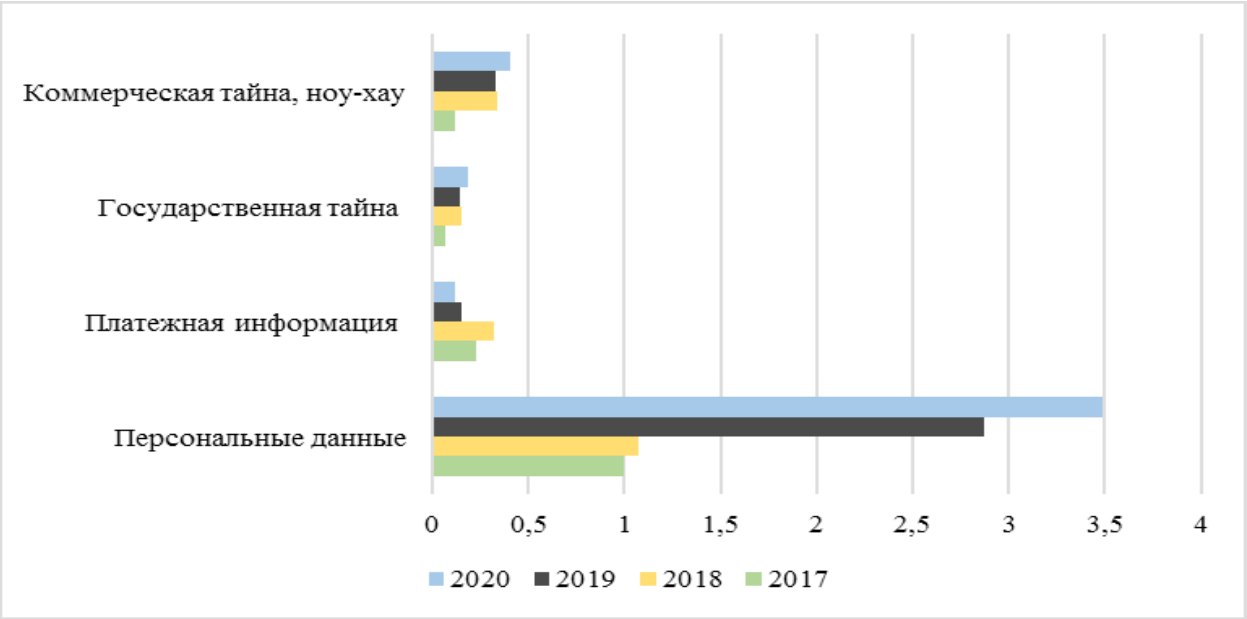


Рисунок 4 – Ущерб от утечки информации по типу данных (млрд. $)

данных – GDPR (General Data Protection Regulation), в Российской Федерации в 2017 г. вступил в силу Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» № 187-ФЗ от 26.07.2017.

Непрерывное развитие информационной среды увеличивает количество находящейся в ней информации и вместе с тем растут угрозы утечки данных. Увеличение угроз сказывается на временных и трудовых затратах, необходимых для их выявления и реализации действий по их нейтрализации, что в свою очередь является необходимым условием для обеспечения устойчивого функционирования субъектов экономической деятельности и обеспечения их экономической безопасности. Именно с учетом увеличения количества угроз и их влияния на экономическую составляющую коммерческих организаций в различных странах мира, формирование системы защиты информационного сопровождения и ее развитие с каждым годом набирает все большую важность в системе экономической безопасности.

Список литературы

1. *Ясенев В.Н., Дорожкин А.В., Сочков А.Л., Ясенев О.В* // Информационная безопасность: учебное пособие / Под общей редакцией проф. Ясенева В.Н. – Нижний Новгород: Нижегородский госуниверситет им. Н.И. Лобачевского, 2017. – 515 с.

2. *Галатенко В.А.* Основы информационной безопасности: учебное пособие. – 3-е изд. – М.: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. – 266 с. – ISBN 978-5-4497-0675-1.

3. *Метельков А.Н.* Киберучения: зарубежный опыт защиты критической инфраструктуры // Правовая информатика. – 2022. – № 1. – С. 51-60. – DOI 10.21681/1994-1404-2022-1-51-60. – EDN NMTEXO.

4. InfoWatch Traffic Monitor. Отчет об исследовании утечек информации ограниченного доступа в 2021 году. [Электронный ресурс]. – Режим доступа: https://www.infowatch.ru/sites/default/files/analytics/files/v-2021-stalo-bolshe-umyshlennykh-utechek.pdf (дата обращения 12.03.2022).

5. *Рыбин И.О., Графов А.А.* Способы обеспечения безопасности и соблюдения конфиденциальности информации в организациях // Национальная безопасность и стратегическое планирование. – 2020. – № 1(29). – С. 71-75. – DOI 10.37468/2307-1400-2020-1-71-75. – EDN RTPDJR.

6. InfoWatch Traffic Monitor – DLP-система, которая предотвращает утечки конфиденциальной

информации на основе полноценного контентного анализа информационных потоков // DLP-система Infowatch Traffic Monitor [Электронный ресурс] – Режим доступа: https://www.infowatch.ru/products/traffic-monitor (дата обращения 12.03.2022).

7. *Грошева Е.К., Невмержицкий П.И.* Информационная безопасность: современные реалии й // Бизнес-образование в экономике знаний. – 2017. – № 3(8). – С. 35-38. – EDN ZNHUHH.

8. *Метельков А.Н.* О проблеме технических мер в системе мер по обеспечению информационной безопасности // Национальная безопасность и стратегическое планирование. – 2020. – № 2(30). – С. 36-42. – DOI 10.37468/2307-1400-2020-2-36-42. – EDN EJCYIS.

Статья поступила в редакцию 18 марта 2022 г.
Принята к публикации 04 июня 2022 г.

Ссылка для цитирования: Агаев Р. Ш., Агаев Р. Ш., Графов А. А. Безопасность информационного сопровождения в системе экономической безопасности // Национальная безопасность и стратегическое планирование. 2022. № 2(38). С. 98-104. DOI: https://doi.org/10.37468/2307-1400-2022-2-98-104

Сведения об авторах:

АГАЕВ РУСЛАН ШАХИНОВИЧ – *студент Санкт-Петербургского государственного экономического университета, г. Санкт-Петербург, Россия*

АГАЕВ РАФАЭЛЬ ШАХИНОВИЧ – *студент Санкт-Петербургского государственного экономического университета, г. Санкт-Петербург, Россия*

ГРАФОВ АЛЕКСАНДР АЛЕКСАНДРОВИЧ *– кандидат экономических наук, доцент, доцент кафедры экономической безопасности Санкт-Петербургского государственного экономического университета, г. Санкт-Петербург, Россия*
e-mail: ershalaim33@mail.ru