DOI 10.31483/r-108348

Минаков Андрей Владимирович

СОВРЕМЕННОЕ ЗНАЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЗАЩИТЫ ИНФОРМАЦИИ В СИСТЕМЕ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ СТРАНЫ

***Аннотация**: информационная безопасность является важной частью экономической безопасности страны. В настоящее время экономики многих стран испытывают рост влияния на них киберпреступности, поскольку имеют место разного рода преступления, связанные с кражей данных, мошенничеством, взломом счетов, кибератаками с стороны преступников, действующих в информационной сфере как ради финансовой выгоды, так и ради террористических целей, негативно влияя на безопасность финансовой системы и стабильность экономики стран, включая и России. Поэтому, по мнению автора главы, правительство, бизнес и все общество должны предпринимать различные шаги для борьбы с угрозами в сфере информационных технологий.*

***Ключевые слова**: информационная безопасность, защита информации, экономическая безопасность, киберугрозы, конфиденциальность данных, защита данных.*

***Abstract**: information security is an important part of the country's economic security. At present, the economies of many countries are experiencing an increase in the influence of cybercrime on them, since there are various crimes related to data theft, fraud, account hacking, cyber-attacks by criminals operating in the information field both for financial gain and for terrorist purposes, negatively affecting the security of the financial system and the stability of the economies of countries, including Russia. Therefore, the government, business and the whole society must take various steps to combat threats in the field of information technology.*

***Keywords**: information security, information protection, economic security, cyber threats, data privacy, data protection.*

Поскольку информационная безопасность является одним из ключевых аспектов экономической безопасность, сначала необходимо привести определение самой экономической безопасности как многоаспектного явления. А.И. Есир с соавторами под экономической безопасностью страны понимает «комплекс действий, по сдерживанию влияния негативных факторов на экономическую сферу страны и по обеспечению развития общества» [6, с. 49]. По мнению А.Ш. Гулиевой с соавторами, в систему экономической безопасности входят «финансовая, интеллектуальная, кадровая, технико-технологическая, информационная, правовая, экологическая, силовая безопасности» [4, с. 2901]. Информационная безопасность, тем самым – лишь один, но важный аспект обеспечения экономической безопасности.

При этом, информационная безопасность подразумевает набор инструментов и методов, разработанных и реализованных для защиты печатной, электронной или любой другой формы конфиденциальной информации от несанкционированного доступа, неправомерного использования, раскрытия, уничтожения, изменения [4, с. 2901]. Также по мнению В.А. Суслова, информационная безопасность – это «защищенность информации от незаконного использования» [12, с. 38]. А инструменты информационной безопасности используются для защиты информации, как в цифровой, так и в физической форме от повреждения, компрометации или потери [12, с. 38].

Информацией, требующей защиты и конфиденциальности может быть: личные данные, профиль в социальных сетях, данные на мобильном телефоне, биометрические данные, данные коммерческой организации, банка, органа государственной власти и т. д. Конфиденциальность предполагает невозможность несанкционированного попадания данных другим лицам, для кого эти данные не предназначены [12, с. 38].

Информационная безопасность охватывает множество областей исследований, таких как программирование, криптография, мобильные вычисления, киберкриминалистика, анализ социальных сетей в Интернете и т. д. В настоя-

щее время важность защиты информации возрастает, поскольку объем создаваемых и хранимых данных растет высокими темпами. Защита информации важна в государственной сфере, в бизнесе, в финансовой сфере, так как это позволяет предотвратить финансовые потери, утечки данных, ущерб репутации, угрозы в системе национальной безопасности и т. д.

Используя различные стратеги для обеспечения конфиденциальности, доступности и целостности, достигаются цели по снижению информационных рисков. Эффективная информационная безопасность требует комплексного и междисциплинарного подхода с участием людей, процессов и технологий [5, с. 225].

Для обеспечения информационной безопасности применяются следующие виды мер: меры по защите от несанкционированного доступа, по поддержанию точности и согласованности данных, по обеспечению авторизованным пользователям доступа к необходимой информации, по выявлению и смягчению потенциальных угроз безопасности, по аварийному восстановлению, по аутентификации, по шифрованию, по обеспечению безопасности физических объектов, на которых размещены системы безопасности.

Классификация угроз информационной безопасности представим на рисунке 1.

Рис. 1. Угрозы информационной безопасности

Источник: составлено автором на основе [5, с. 225].

Принципы обеспечения информационной безопасности представлены на рисунке 2.

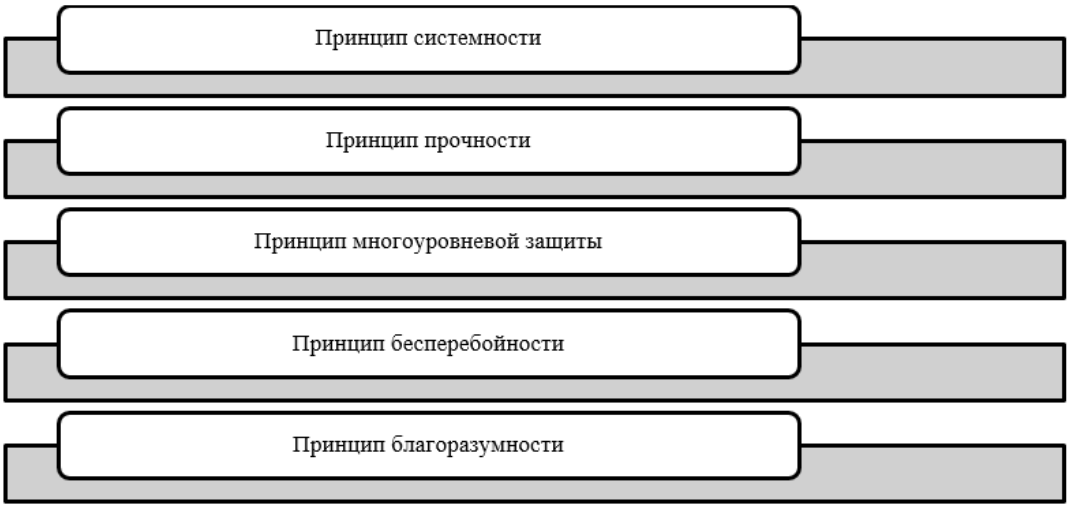

Рис. 2. Принципы обеспечения информационной безопасности

Источник: составлено автором на основе [14, с. 478].

По мнению Т.Д. Агамировой, для защиты информации применяются следующие меры: технические (шифрование и т. д.), организационные (создание службы безопасности), человеческие (обучение), физические (контроль доступа) [1, с. 119].

Инцидент безопасности – это событие, которое приводит к раскрытию конфиденциальных данных неавторизованным лицом.

Причинами инцидентов информационной безопасности могут быть: кибератака (вредоносное ПО, фишинг и т. д.), человеческая ошибка (потеря мобильного устройства, переход по вредоносным ссылкам, слабый пароль), внутренние угрозы (сотрудники, намеренно или непреднамеренно причиняющие вред), устаревшие уязвимые информационные системы, интеграция со сторонними системами и т. д.

Согласно отчету Positive Technologies об общемировых угрозах информационной безопасности по итогам II кв. 2023 года, к основным негативным последствиям кибератак относятся утечка конфиденциальной информации, нарушение основной деятельности, финансовые потери (рис. 3).

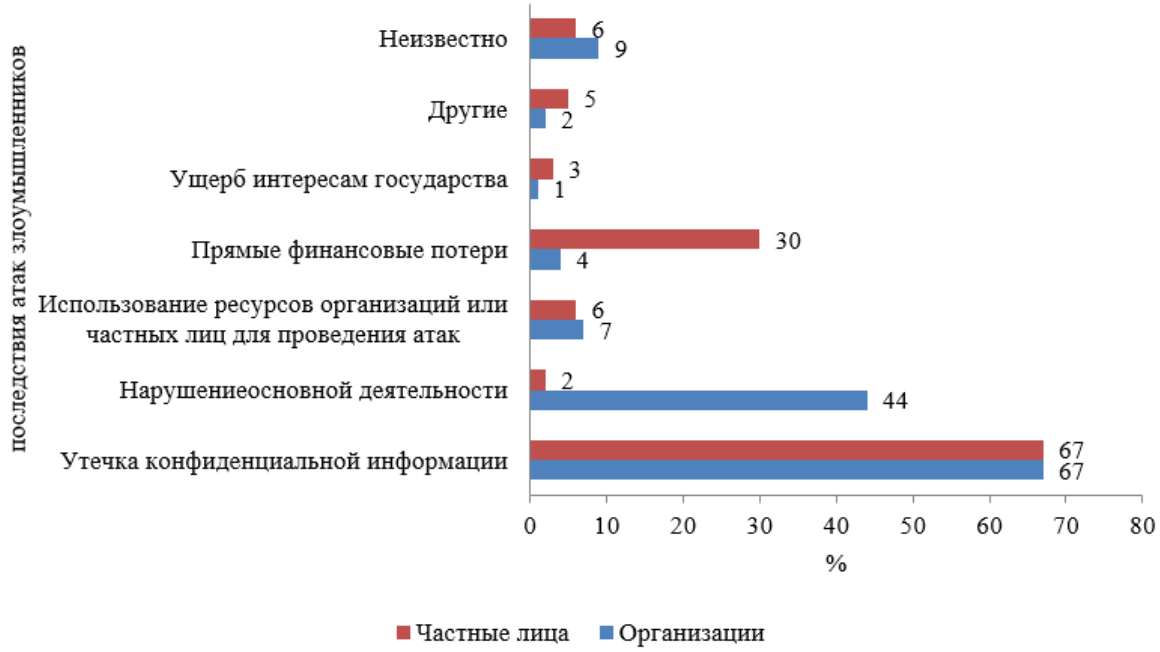

Рис. 3. Последствия атак злоумышленников в информационной сфере, %

Источник: составлено автором на основе [2].

Проведем анализ преступлений в информационной сфере в РФ за последние годы (рис. 4–7).

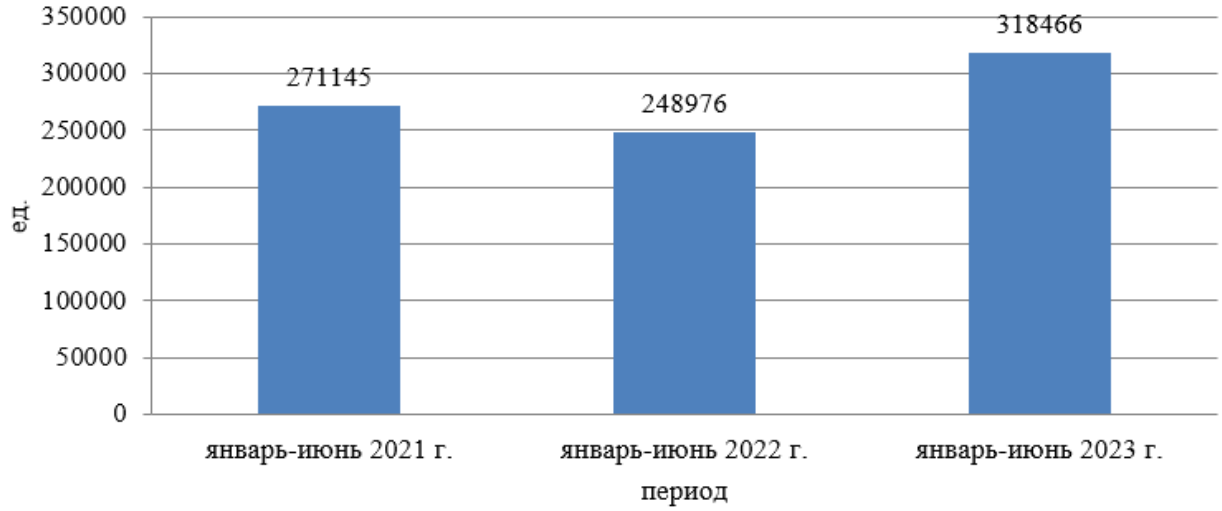

Рис. 4. Динамика количества зарегистрированных преступлений в информационной сфере в РФ, ед.

Источник: составлено автором на основе [7].

В январе–июне 2023 г. в сфере информационных технологий было зарегистрировано более 300 тыс. преступлений, причем это значение превысило показатели за предыдущие 2 года.

Согласно данным статистики, раскрывается только третья часть преступлений в информационной сфере. Уровень раскрываемости в январе-июне 2021 г. составлял 27,9%, в 2022 г. он вырос на 3 п.п., а в 2023 г. еще на 1,6 п.п. (рис. 5).

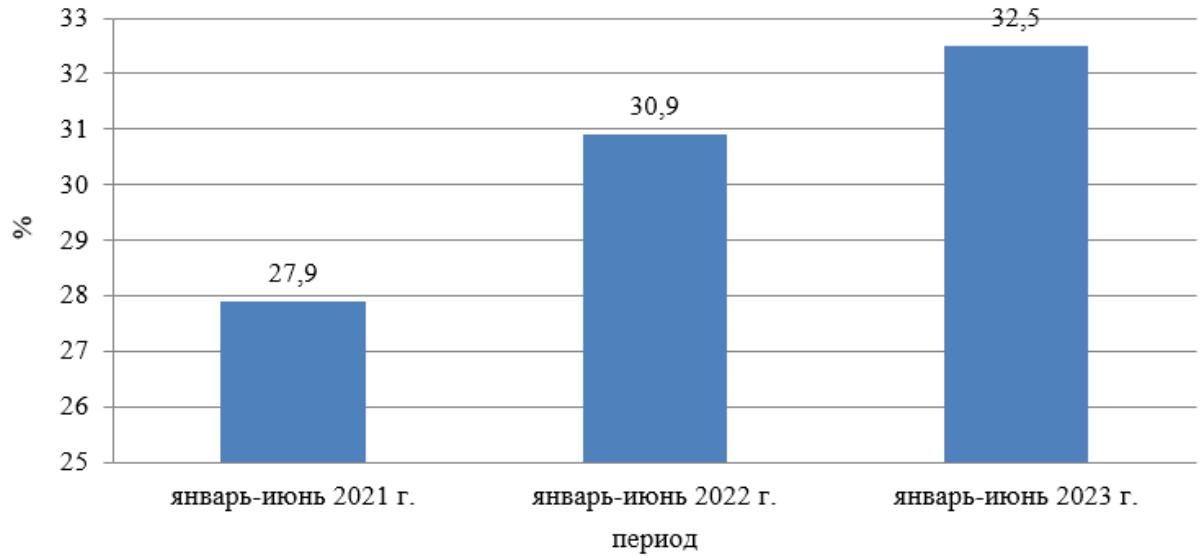

Рис. 5. Изменение уровня раскрываемости преступлений в информационной сфере в РФ, %

Источник: составлено автором на основе [7].

Ежегодно растет число лиц, совершивших преступления в информационной сфере (рис. 6).

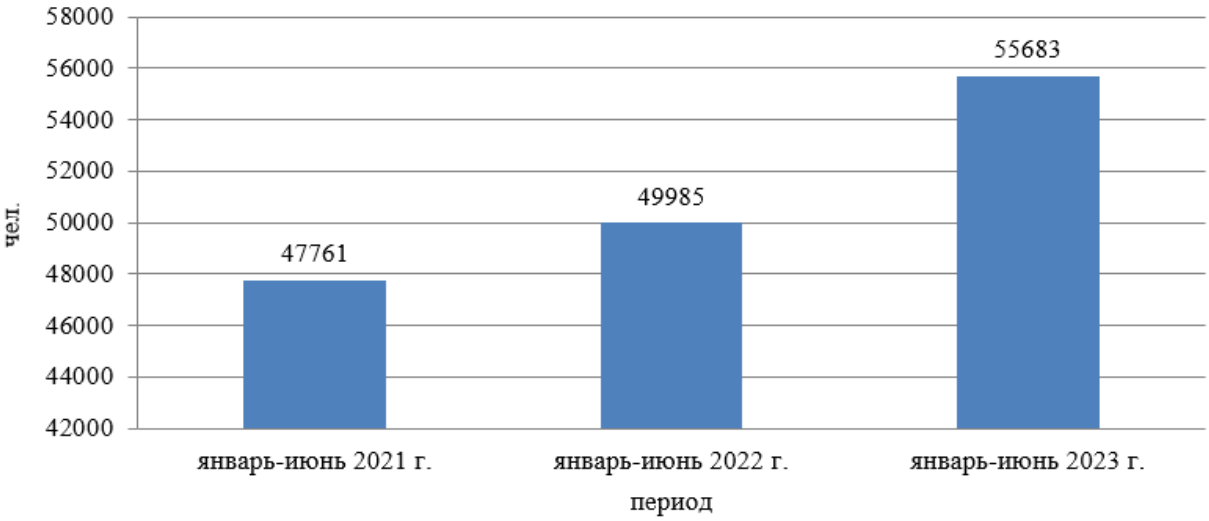

Рис. 6. Динамика числа лиц, совершивших преступления в информационной сфере в РФ, чел.

Источник: составлено автором на основе [7].

Большая часть преступлений в информационной сфере была совершена с помощью Интернета и средств мобильной связи. За последние 2 года выросло количество этих преступлений, а также количество преступлений, совершенных с помощью фиктивных электронных платежей (рис. 7).

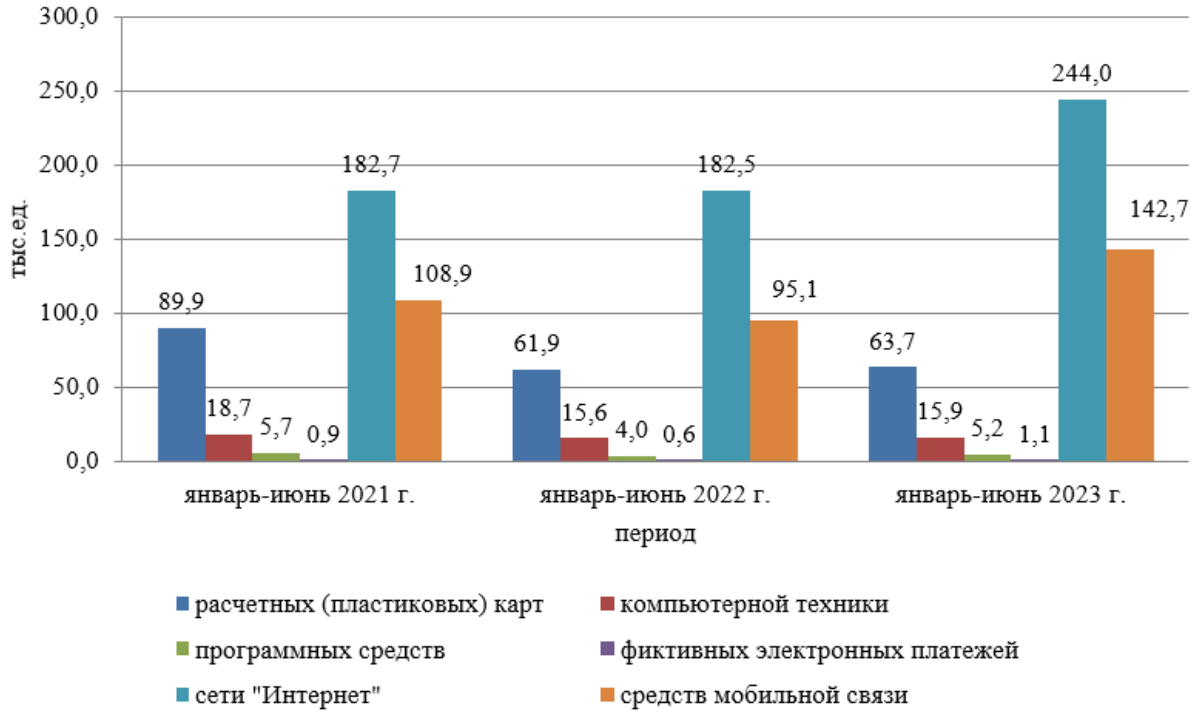

Рис. 7. Динамика применения основных способов совершения преступлений в информационной сфере в РФ, тыс. ед.

Источник: составлено автором на основе [7].

Во 2 кв. 2023 г. Россия стала лидером в мире по количеству заблокированных IP адресов – 8,2 млн (44,2%). В пятерку стран по источникам DDoS-атак также вошли США, Китай, Франция и Индия (рис. 8).

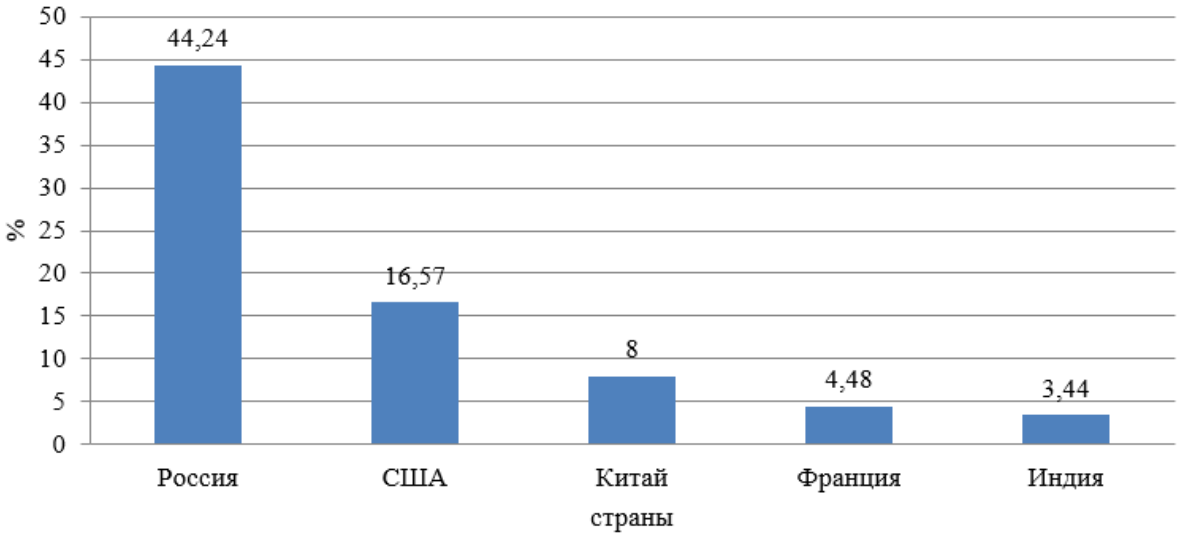

Рис. 8. Географическое распределение источников DDoS-атак в мире, %

Источник: составлено автором на основе [8].

Количество утечек данных в мире в 1 полугодии 2023 г. относительно 1 полугодия 2022 г. выросло в 2,4 раза, в России количество утечек сократилось на 17%, однако объем утекших данных вырос на 72% (до 705 млн записей), количество утечек баз данных, которые оставляют третью часть всех утечек информации, выросло на 28% (рис. 9).

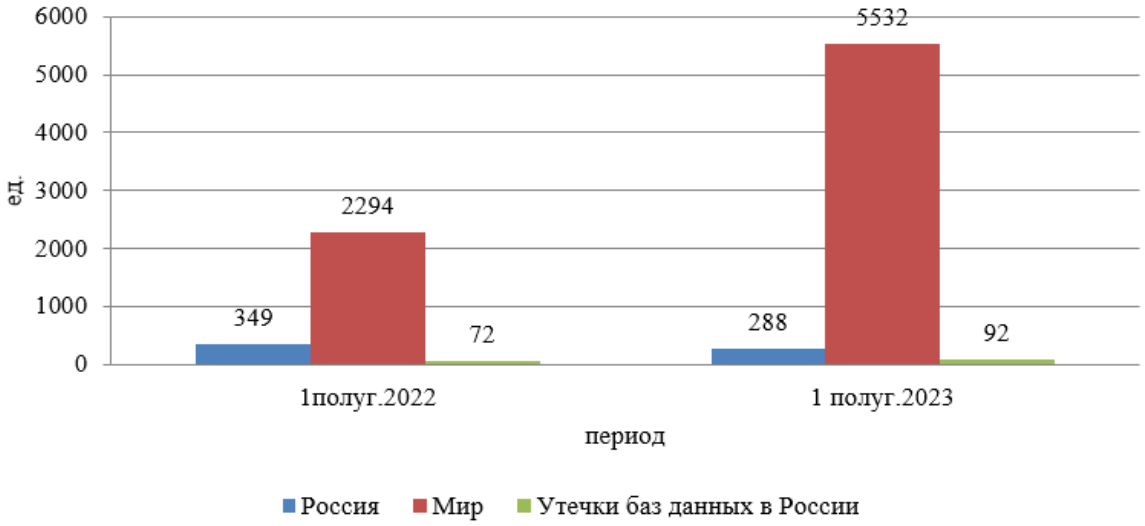

Рис. 9. Динамика количества утечек данных в мире, %

Источник: составлено автором на основе [13].

Киберпреступность представляет наибольшую угрозу для каждой компании, поскольку из-за нее они могут потерять огромные суммы денег. Согласно

опросу, проведенному среди крупных частных или государственных предприятий, в основном из промышленного сектора в России в июле 2023 г. компанией InfoWatch, наибольшую долю в структуре информации, утечка которой привела к ущербу более 1 млн руб., занимали сведения, составляющие коммерческую тайну (30%) (рис. 10).

Рис. 10. Структура информации, утечка которой привела к ущербу более 1 млн руб., %

Источник: составлено автором на основе [9].

В настоящее время в РФ органы власти и бизнес стали уделять повышенное внимание защите информации. За 2020–2022 гг. рынок информационной безопасности (затраты на информационную безопасность) вырос на 35,6% (рис. 11).

Рис. 11. Развитие объема рынка средств информационной безопасности в РФ в 2020–2022 гг., млрд руб.

Источник: составлено автором на основе [3; 10; 11].

Большая часть затрат на информационную безопасность идет на приобретение средств защиты информации: в 2021 г. – 73%, в 2022 г. – 74% (рис. 12).

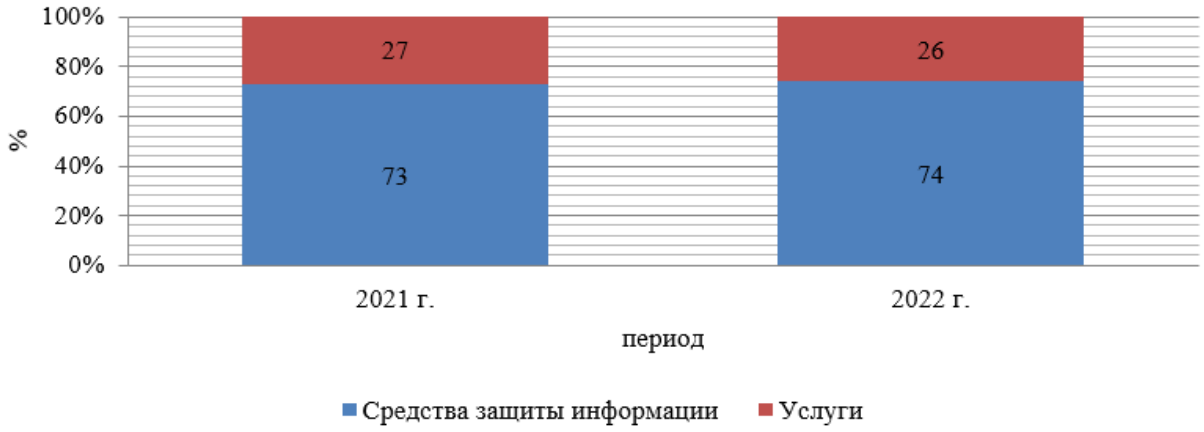

Рис. 12. Структура рынка информационной безопасности в РФ в 2020–2022 гг., %

Источник: составлено автором на основе [11].

Лидерами рынка кибербезопасности России являются Лаборатория Касперского, Positive Technologies, BI.ZONE. За 2022 г. на российском рынке информационной безопасности доля российских вендоров выросла до 70% (из-за санкций). В дальнейшем ожидается еще большее снижение доли иностранных вендоров на российском рынке (рис. 13).

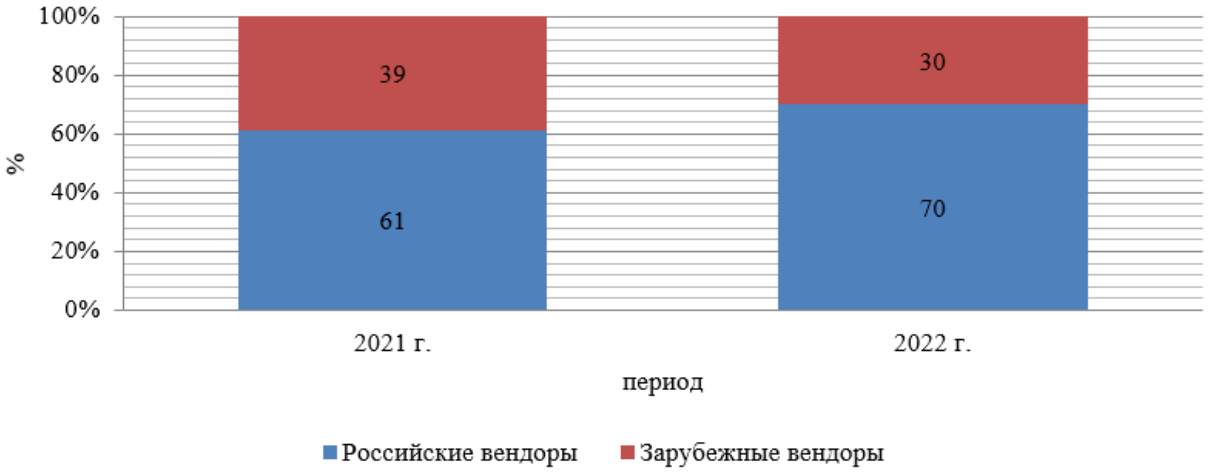

Рис. 13. Доля российских и иностранных вендоров на российском рынке информационной безопасности в 2021–2022 гг., %

Источник: составлено автором на основе [11].

Из-за ухода с рынка информационной безопасности иностранных компаний в настоящее время усиливается конкуренция между отечественными компаниями по занятию освободившихся ниш, что в дальнейшем позитивно скажется на развитии данного сектора в стране. На фоне этого возрастает потребность в специалистах по информационной безопасности, а также в услугах по аутсорсингу информационной безопасности.

Таким образом, важность обеспечения информационной безопасности, как части экономической безопасности растет с каждым годом. Анализ преступлений в информационной сфере в РФ за последние годы выявил их ежегодный рост, а также рост числа лиц, совершивших данные преступления. В России в 1 полугодии 2023 г. относительно 1 полугодия 2022 г. вырос также объем утекших данных на 72% и количество утечек баз данных на 28%. Защита информации важна в государственной сфере, в бизнесе, в финансовой сфере, так как позволяет предотвратить финансовые потери, утечки данных, ущерб репутации, угрозы в системе национальной безопасности и т. д. За 2020–2022 гг. затраты на информационную безопасность в России выросли на 35,6%. На российском рынке продуктов для информационной безопасности преобладают отечественные решения.

В ближайшие годы ожидается дальнейший рост числа хакерских атак как на государственные и промышленные организации, облачную инфраструктуру, программное обеспечение с открытым кодом. В связи с этим для развития системы информационной безопасности в стране необходимо со стороны государства содействие развитию технологий защиты информации, органам власти и бизнесу следить за актуальными технологиями по защите данных, своевременно обновлять защитные веб-технологии, оперативно устранять недостатки в системе безопасности, иметь в каждой государственной и частной организации группу по управлению киберрисками, использовать современные подходы к обучению специалистов в данной сфере, повышать осведомленность общества об информационной безопасности.

Список литературы

1. Агамирова Т.Д. Методы обеспечения информационной безопасности / Т.Д. Агамирова // Матрица научного познания. – 2021. – №12. – С. 119–123.

2. Актуальные киберугрозы: II квартал 2023 года // ICT.Moscow. – 2023 [Электронный ресурс]. – Режим доступа: https://ict.moscow/research/aktualnye-kiberugrozy-ii-kvartal-2023-goda/

3. Анализ российского рынка информационной безопасности [Электронный ресурс]. – Режим доступа: https://www.anti-malware.ru/analytics/Market_Analysis/Russian-InfoSec-Market

4. Гулиева А.Ш. Понятие и сущность национальной экономической безопасности в законе / А.Ш. Гулиева, Н.В. Минаева, И.С. Моховиков // Столыпинский вестник. – 2022. – №4. – С. 2901–2909. EDN PWOHAC

5. Ершова Е.Е. Информационная безопасность как элемент экономической безопасности / Е.Е. Ершова // Управление образованием: теория и практика. – 2022. – №6. – С. 225–230. DOI 10.25726/v8343-7232-2832-p. EDN PTTSSD

6. Есир А.И. Исследование теоретических аспектов понятия «Экономическая безопасность» / А.И. Есир, О.А. Кискул, И.В. Толмачева // Теория и практика общественного развития. – 2022. – №8. – С.49–54. DOI 10.24158/tipor.2022.8.6. EDN EXMTLO

7. Краткая характеристика состояния преступности в Российской Федерации [Электронный ресурс]. – Режим доступа: https://мвд.рф/reports/item/40116049/

8. Обзор DDoS-атак во втором квартале 2023 года // Qrator. – 2023 [Электронный ресурс]. – Режим доступа: https://qrator.net/ru/obzor-ddos-atak-vo-vtorom-kvartale-2023-goda_178/

9. Оценка ущерба вследствие утечек информации // ICT.Moscow. – 2023 [Электронный ресурс]. – Режим доступа: https://ict.moscow/research/otsenka-ushcherba-vsledstvie-utechek-informatsii/

10. Прогноз развития рынка кибербезопасности в Российской Федерации на 2022–2026 годы // Фонд «Центр стратегических разработок». – 2022 [Электронный ресурс]. – Режим доступа: https://www.csr.ru/upload/iblock/13f/ufleu9rg5zc3ldu66srqt3a89j0mrve5.pdf

11. Прогноз развития рынка кибербезопасности в Российской Федерации на 2023–2027 годы // Фонд «Центр стратегических разработок». – 2023 [Электронный ресурс]. – Режим доступа: https://www.csr.ru/upload/iblock/0da/cl25xkzy12if5l4xs425yi25ezp1a11z.pdf

12. Суслов В.А. Информационная безопасность как форма экономической безопасности / В.А. Суслов // Наука через призму времени. – 2023. – №4. – С. 38–40. EDN XJPHXK

13. Утечки информации ограниченного доступа в мире и в России. I полугодие 2023 года // ICT.Moscow. – 2023 [Электронный ресурс]. – Режим доступа: https://ict.moscow/research/utechki-informatsii-ogranichennogo-dostupa-v-mire-i-rossii-v-i-polugodii-2023-goda/

14. Чесноков А.Д. Информационная безопасность / А.Д. Чесноков // StudNet. – 2022. – №5. – С. 478–489. EDN IIPKSO

Минаков Андрей Владимирович – д-р экон. наук, профессор кафедры экономики и бухгалтерского учета ФГКОУ ВО «Московский университет МВД России имени В.Я. Кикотя», Россия, Москва.