МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ / METHODS AND SYSTEMS OF INFORMATION PROTECTION, INFORMATION SECURITY

DOI: https://doi.org/10.18454/itech.2024.1.1

ЭКОНОМИКА КИБЕРБЕЗОПАСНОСТИ В МИРЕ

Научная статья

Васильев А.[1, *]
[1] ORCID : 0009-0008-9909-2385;
[1] ScienceSoft, Минск, Беларусь

* Корреспондирующий автор (alexey_vasilyev96[at]mail.ru)

Аннотация

Киберпреступность сегодня представляет собой серьезную угрозу, с которой необходимо бороться. Компании по всему миру постепенно осознают этот факт и принимают различные меры безопасности, чтобы избежать и защититься от киберугроз. Целью данной работы является изучение показателей мировых потерь от кибератак и расходов на кибербезопасность, а также исследование экономических вопросов, связанных с кибербезопасностью в общемировом масштабе. В работе рассмотрены наиболее важные статистические данные, касающиеся расходов на кибербезопасность во всем мире. Приведены статистические данные за 2020-2023 год, а также прогнозные показатели по результатам мировых и российских исследований и отчетов по кибербезопасности. На основе анализа зарубежных и российских статистических отчетов были сделаны прогнозы расходов на кибербезопасность. Также в статье были обозначены базовые понятия об оценке рисков, кратко описаны стратегии кибербезопасности для различных государств, понятия киберпространства и кибербезопасности.

Ключевые слова: кибербезопасность, расходы, прогноз, услуги, бюджет, киберугрозы.

THE ECONOMICS OF CYBERSECURITY IN THE WORLD

Research article

Vasilyev A.[1, *]
[1] ORCID : 0009-0008-9909-2385;
[1] ScienceSoft, Minsk, Belarus

* Corresponding author (alexey_vasilyev96[at]mail.ru)

Abstract

Cybercrime today is a serious threat that must be tackled. Companies around the world are gradually realizing this fact and are adopting various security measures to avoid and protect themselves from cyber threats. The aim of this work is to study the indicators of global losses from cyberattacks and cybersecurity expenditures, as well as to examine the economic issues related to cybersecurity on a global scale. The article reviews the most important statistics related to cybersecurity spending worldwide. Statistical data for 2020-2023 are presented, as well as forecast figures based on the results of global and Russian studies and reports on cybersecurity. Based on the analysis of foreign and Russian statistical reports, forecasts of cybersecurity expenditures were made. The paper also outlined basic concepts of risk evaluation, briefly described cybersecurity strategies for various states, and the concepts of cyberspace and cybersecurity.

Keywords: cybersecurity, spendings, forecast, services, budget, cyber threats.

Введение

Проблема киберпреступности становится крайне серьезной, в результате чего предприятия и частные лица терпят огромные убытки. Учитывая быстро развивающуюся цифровую экономику и огромное разнообразие киберугроз, понимание ключевых аспектов кибербезопасности имеет решающее значение не только для ИТ-специалистов и экспертов по безопасности, но также и для владельцев бизнеса, руководителей и всех тех, кто заботится о защите своей конфиденциальной информации. Количество глобальных кибератак увеличилось на 125% в 2021 году и, как ожидается, к 2025 году ущерб от них может составить более 10,5 триллионов долларов США при сохранении нынешних темпов роста. Данный показатель будет на 300% больше, чем в 2015 году.

Кибербезопасность, киберпространство, киберпреступность и оценка рисков

Прежде чем перейти к изложению показателей по экономике кибербезопасности в мире, обозначим базовые понятия в этой области на основе международных стандартов: ГОСТ Р ИСО/МЭК 15408-1-2012, более известного под названием «Общие критерии» часть 1 и ISO/IEC 27032-2012 [1], [2].

Кибербезопасность (или безопасность киберпространства) определяется как сохранение конфиденциальности, целостности и доступности информации в киберпространстве.

Киберпространство (англ. – cyberspace) определяется как комплексная виртуальная среда (не имеющая физического воплощения), сформированная в результате действий людей, программ и сервисов в сети Интернет или других коммуникационных структур посредством информационно-коммуникативной системы (ИКТ) [3].

Киберпреступность – это преступная деятельность, в рамках которой используются либо атакуются компьютер, компьютерная сеть или сетевое устройство [4].

В стратегическом смысле (согласно «Общим критериям») безопасность связана с защитой активов. В качестве активов может рассматриваться чувствительная информация на серверах компании, базы данных, голоса, собранные на выборах и т.д. Среда функционирования – это та среда, куда помещены активы. К примеру, корпоративная сеть предприятия, помещение в банке и т.д. Для взаимосвязи различных понятий безопасности ниже приведен рис. 1 [2].

Рисунок 1 - Понятия безопасности и их взаимосвязь
DOI: https://doi.org/10.18454/itech.2024.1.1.1

Примечание: источник [2]

Необходимо отметить, что построение любой информационно-коммуникативной системы (ИКТ) следует начинать с оценки рисков. Вообще, в основу экономики кибербезопасности положена именно оценка рисков. Риск определяется вероятностью причинения ущерба и величиной ущерба, наносимого ресурсам ИКТ, в случае осуществления угрозы безопасности. В ходе анализа рисков аналитик должен выявить все возможные риски и оценить потенциальный ущерб от них. Общий алгоритм в оценке рисков следующий:

- выявление ключевых активов и ресурсов системы ИКТ;
- определение важности этих ресурсов и активов;
- оценка угроз безопасности и уязвимостей;
- вычисление рисков (количественный метод) или оценка их (качественный метод).

Ресурсы и активы ИКТ бывают трех видов:

1) информационные (базы данных (БД), чувствительная информация, учетные данные и т.д.);

2) программные (программное обеспечение (ПО), операционные системы (ОС), системы управления базами данных (СУБД) и т.д.);

3) технические средства (сервера, рабочие станции, сетевое оборудование и т.д.).

Далее необходимо оценить важность ресурсов или активов, при этом стоит подсчитать ущерб, который будет нанесен злоумышленниками в случае нарушения конфиденциальности, целостности или доступности этого ресурса. Например, данные повреждены или скачены из БД злоумышленником, нарушена целостность веб-приложения, поврежден сервер и т.д.

На следующем этапе составляется модель угроз безопасности. В «Модель угроз» могут быть включены: хакерские атаки, физическое повреждение оборудования, стихийные бедствия, ошибки персонала и т.д. Далее необходимо оценить уязвимости и сделать их классификацию, также стоит оценить угрозы по степени вероятности их осуществления.

В конце данной аналитической работы исследователь производит вычисление рисков. Уровень риска вычисляется на базе стоимости ресурса, уровня угрозы и величины уязвимости. Ниже приводятся формулы для вычисления риска:

$$\text{Риск} = \text{P}(\text{реализации}) * \text{Ущерб} \quad (1)$$

где *P(реализации)* – это вероятность реализации риска, которая вычисляется по формуле:

$$\text{P}(\text{реализации}) = \text{P}(\text{угрозы}) * \text{P}(\text{уязвимости}) \quad (2)$$

где *P(угрозы)* – это вероятность угрозы, *P(уязвимости)* – вероятность уязвимости.

При вычислении рисков для каждого актива исследователь определяет набор мер по обеспечению его информационной безопасности (ИБ) (от 1 до 7), где 1 – это минимальный необходимый набор мер по обеспечению ИБ, а 7 – максимальный [5], [6].

После проведенной аналитической работы необходимо разработать контрмеры по противодействию рискам, а именно:

- снизить вероятность осуществления угроз безопасности;
- устранить уязвимости или уменьшить их величину;
- снизить размер возможного ущерба;
- выявить атаки или другие инциденты ИБ;
- начать восстановление активов или ресурсов ИКТ, которым был нанесен ущерб.

Этот комплекс мероприятий, как правило, прописывается в «Политике безопасности организации». Далее будет показана статистика киберпреступлений, ущерба от утечек и затраченных средств из бюджета на противодействие угрозам для США и некоторых других стран.

Данные по киберпреступлениям, оценке рисков и противодействию киберугрозам в США, России и других странах

По состоянию на 2020 год США занимают первое место в Глобальном индексе кибербезопасности (GCI).

США, набравшие 100 баллов, являются страной, наиболее приверженной идеям и практикам кибербезопасности. Среди стран, обращающих наибольшее внимание на кибербезопасность, Великобритания и Саудовская Аравия делят второе место с 99,54 баллами GCI каждая [7].

В 2022 году в США было зарегистрировано наибольшее количество жертв от киберпреступлений – 479 181 пострадавших.

IC3 определил топ-5 государств, пострадавших от киберпреступлений в 2022 году [1]:

- США – 479 181 пострадавших;
- Великобритания – 284 291 пострадавших;
- Канада – 5517 пострадавших;
- Индия – 2550 пострадавших;
- Австралия – 2489 пострадавших.

В США зафиксирован самый высокий средний размер ущерба от утечки данных – 9,44 миллиона долларов по сравнению с 9,05 миллиона долларов в 2021 году.

В первую пятерку стран или регионов с самым высоким средним размером ущерба от утечки данных вошли [7]:

- США – 9,44 миллиона долларов;
- Ближний Восток – 7,46 миллиона долларов;
- Канада – 5,64 миллиона долларов;
- Великобритания – 5,05 миллиона долларов;
- Германия – 4,85 миллиона долларов.

Согласно «Руководству по расходам на мировую безопасность», составленному Международной корпорацией данных, глобальные расходы на решения и услуги в области кибербезопасности, как ожидается, в 2023 году достигнут около 219 миллиардов долларов [8].

Данный показатель говорит нам о том, что в 2023 году темпы увеличения расходов на кибербезопасность увеличатся на 12,1% по сравнению с 2022 годом.

В отчете показано, что инвестиции в программное обеспечение, оборудование и услуги кибербезопасности также увеличатся и достигнут 300 миллиардов долларов к 2026 году [8].

Как и все прежние годы, Соединенные Штаты в настоящее время являются крупнейшим географическим регионом по расходам на кибербезопасность.

За Соединенными Штатами с достаточно серьезным отставанием идет Западная Европа, которая в настоящее время является вторым по величине регионом по расходам на кибербезопасность [9].

Подобные статистические данные показывают, что как частные лица, так и предприятия принимают активные меры предосторожности для решения проблем связанных с кибербезопасностью.

Что же касается темпов увеличения расходов на кибербезопасность, то Китай здесь занимает первое место. С 2021 по 2023 год совокупный годовой темп прироста (CAGR) в Китае составил около 18,8% [8]. Данный факт демонстрирует приверженность Китая к укреплению мер кибербезопасности и защите своей инфраструктуры от кибератак.

Общие расходы на кибербезопасность в Европе будут продолжать расти устойчивыми темпами на 10% с 2021 по 2026 год [10].

Более того, именно сектор услуг, а не продажа продуктов остается главным компонентом этих расходов. Возможно, это связано с тем, что организации больше заинтересованы в разработке собственных решений, а не в приобретении готового продукта.

По состоянию на 2022 год предприятия во всем мире направили 9,9% своих ИТ-бюджетов на кибербезопасность.

Также было установлено, что такие сектора как здравоохранение, высокие технологии и администрирование (включая страхование) являются ведущими с точки зрения расходов на кибербезопасность.

Что же касается розничной торговли, образования и производственного сектора, то они по-прежнему выделяют относительно меньшую часть своего бюджета на кибербезопасность.

Эти статистические данные подчеркивают разницу в приоритетах для разных секторов экономики, особенно когда дело доходит до защиты их цифровой инфраструктуры [11].

В третьем квартале 2021 года цены на страхование от рисков, связанных с кибербезопасностью в США, выросли на 96%, что является самым значительным ростом с 2015 года.

Отчет Всемирного экономического форума подтвердил эту статистику расходов на кибербезопасность. Кроме того, рост цен на киберстрахование в мире увеличился на 204% по сравнению с прошлым годом.

Более того, недавнее исследование статистики расходов на кибербезопасность показывает, что половина предприятий с более чем 10 000 сотрудников ежегодно инвестируют минимум 1 миллион долларов в развитие своей корпоративной системы кибербезопасности [10].

Значительная часть организаций по всему миру (73%, если быть точным) планируют увеличить свои расходы на кибербезопасность в 2023 году [9].

Как правило, организации выделяют 3-6% от своего общего ИТ-бюджета на меры безопасности. Более того, если компания использует или хранит крайне чувствительную информацию о продуктах, пользователях и т.д., то ей следует выделять более 10% от своего ИТ-бюджета на кибербезопасность. Кроме того, следует добавить еще от 2% до 4% на расходы, связанные с непрерывностью бизнеса [11].

В результате бизнесу следует выделять 10-14% своего общего ИТ-бюджета на расходы, связанные с безопасностью.

Таким образом, организация сможет распознавать киберугрозы и обеспечивать защиту своих ценных активов и данных.

По состоянию на 2022 год глобальный рынок кибербезопасности оценивался от 1,5 до 2,0 триллиона долларов, что в 10 раз превышает размер ежегодного дохода от продажи товаров и услуг на этом рынке [12].

Объем продаж на рынке кибербезопасности составляет около 150 миллиардов долларов. Это открывает огромные возможности для поставщиков технологий и услуг в сфере кибербезопасности. По мнению McKinsey, рост рынка обусловлен, прежде всего, быстро развивающейся цифровой экономикой.

По данным Всемирного экономического форума (ВЭФ), более 39% руководителей организаций во всем мире согласны с тем, что кибербезопасность является ключевым фактором успеха в бизнесе.

Данные, собранные ВЭФ, еще раз подтверждают, что все большее число компаний и их владельцев осознают важность развития данного направления.

К 2028 году выручка компаний, задействованных в сфере кибербезопасности достигнет $256,50 млрд. [15].

Ожидается, что в 2023 году глобальные расходы на решения в области кибербезопасности увеличатся на 12,1% [11].

По данным International Data Corporation, в 2023 мировые расходы на решения в области кибербезопасности, составят 219 миллиардов долларов [16].

Согласно этому же исследованию компании с полностью развернутым искусственным интеллектом и автоматизацией процессов безопасности, в среднем, смогли выявить и сдержать утечку данных на 74 дня быстрее, чем компании, у которых не были задействованы решения с ИИ и автоматизацией. Внедрение систем искусственного интеллекта и автоматизации в сфере безопасности выросло почти на 20% – с 59% в 2020 году до более чем 70% в 2022 году [16].

Стоит обратить внимание и на средний размер экономии бюджета компаний, в которых существует команда реагирования на инциденты (IRTeam). Данные за 2022 год таже свидетельствуют, что в среднем наличие такой команды на крупном предприятии позволяет экономить до 2,66 миллиона долларов ежегодно.

Наличие команды IR и регулярно тестируемого плана IR привело к значительной экономии затрат примерно на 58% среди крупных корпораций.

Интересны исследования, собранные российской компанией INFOWATCH в Аналитическом отчете «Оценка ущерба вследствие утечек информации». Для отчета были проведены опросы на предприятиях различной формы собственности. Почти у 50% компаний отсутствует методика по оценке ущерба от утечки информации. Наиболее часто подвергались утечкам персональные данные, а размер сумм ущерба от их потери превышал 1 млн. рублей. Внутренние нарушители (инсайдеры) очень часто становились виновниками утечек и инцидентов информационной безопасности (ИБ). В 70% случаев утечка данных – результат умышленного действия. Проблематика обостряется еще и тем обстоятельством, что на российском рынке кибербезопасности отсутствуют хорошо проверенные и четкие методики оценки ущерба от инцидентов ИБ. На зарубежном рынке кибербезопасности исследованиями ущерба от утечек занимается Ponemon Institute, который готовит ежегодный отчет «Cost of a Data Breach Report».

Согласно исследованиям аналитиков компании INFOWATCH, проведенном на российских предприятиях как коммерческой, так и государственной форм собственности:

- в 37% случаев причина утечки – умышленные действия сотрудника организации;
- 16% – результат ошибки сотрудников компании;
- 14% случаев – это результат совместной работы внешних и внутренних нарушителей;
- 14% случаев – это последствия компьютерных атак.

Ниже на рис. 2 [17] приведена классификация причин утечек данных на предприятиях РФ по видам причин.

Рисунок 2 - Классификация причин утечек данных на предприятиях РФ
DOI: https://doi.org/10.18454/itech.2024.1.1.2

Примечание: источник [17]

Также интересны данные, собранные аналитиками Лаборатории Касперского (Россия), по ландшафту угроз для объектов промышленной автоматизации. В этом отчете [18] приводятся данные по РФ в сравнении с другими странами.

- В первом полугодии 2023 процент компьютеров автоматизированных систем управления (АСУ), на которых были заблокированы вредоносные объекты (все угрозы), составил 34%;
- Во втором квартале 2023 года в мире процент достиг максимального с 2022 года значения за квартал – 26,8%;
- В регионах показатель за полугодие варьируется от 40,3% в Африке до 14,7% в Северной Европе;
- В странах – от 53,3% в Эфиопии до 7,4% в Люксембурге.

Ниже приведем более подробную статистику по России. В первом полугодии 2023 года в России вредоносные объекты были заблокированы на 31,9% компьютеров АСУ. Это на 2,1% меньше, чем в среднем по миру. В предыдущем полугодии, в основном, в результате массового заражения сайтов (в том числе промышленных организаций), использующих устаревшую версию одной из популярных российских CMS, процент атакованных компьютеров АСУ в России вырос на 9% В первом полугодии 2023 года – уменьшился на 8,3%.

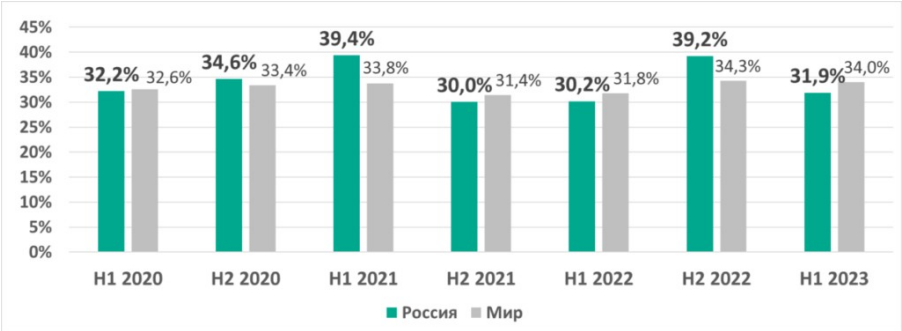

Рисунок 3 - Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты
DOI: https://doi.org/10.18454/itech.2024.1.1.3

В первом полугодии 2023 года в России уменьшился процент атакованных компьютеров для большинства категорий угроз. Выросли только проценты компьютеров, на которых были заблокированы вредоносные документы (на 0,32%) и веб-майнеры (на 0,13%).

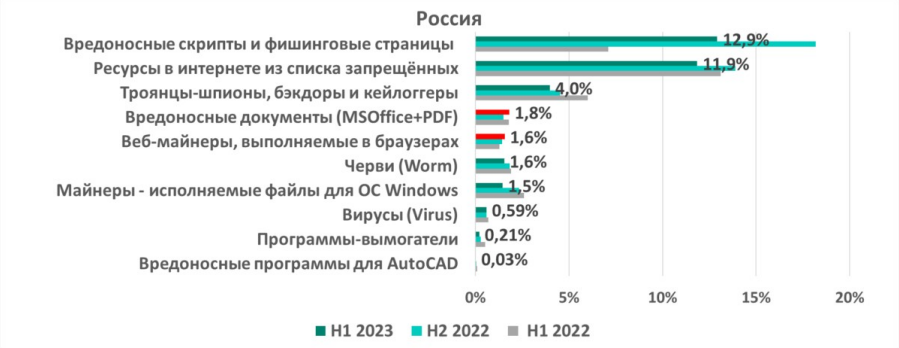

Рисунок 4 - Россия. Процент компьютеров АСУ, на которых были заблокированы вредоносные объекты различных категорий

DOI: https://doi.org/10.18454/itech.2024.1.1.4

Рассмотрим сравнительную статистику по регионам и странам за первое полугодие 2023 года. Как мы видим, в благополучных регионах (Западная Европа, США и Канада, Австралия и Новая Зеландия) в первом полугодии 2023 года процент атакованных компьютеров АСУ вырос на максимальные величины (процентные пункты). В России же (см. диаграмму ниже) ситуация более благополучная [18].

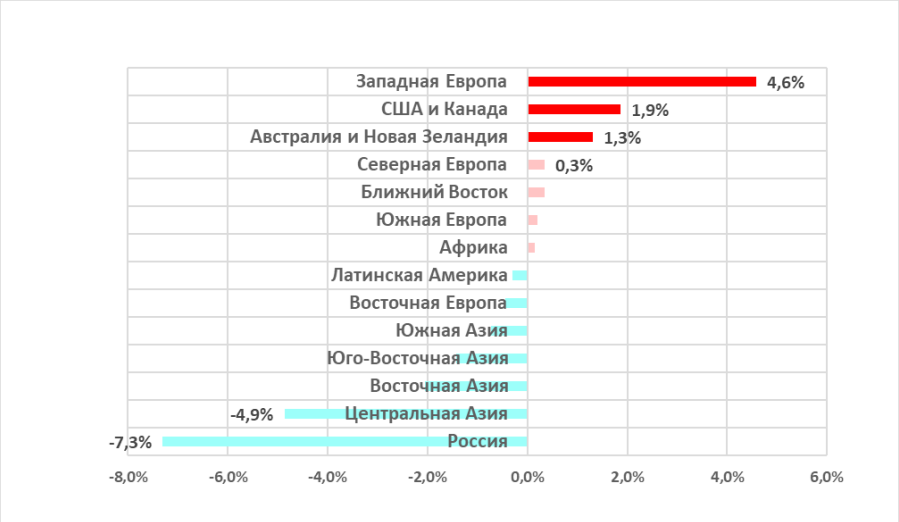

Рисунок 5 - Изменение в регионах процента компьютеров АСУ, на которых были заблокированы вредоносные объекты, за первое полугодие 2023 года

DOI: https://doi.org/10.18454/itech.2024.1.1.5

Примечание: источник [18]

Отдельно приведем данные по утечкам в финансовой сфере, причем сравним ситуацию в мире в целом и в России в частности. В финансовой сфере всего мира за 2022 год зарегистрировано 503 утечки данных, в том числе в российской – 48 утечек.

- Количество утечек из организаций финансовой сферы за 2022 год в мире выросло в 3,7 раза, в России – в 1,7 раза;
- В мире из финансовых организаций утекло более 627 млн записей персональных данных (ПДн) и платежных данных, в России – более 44 млн;
- В мире на банки пришлась примерно каждая третья утечка из организаций финансовой сферы, в России – каждая вторая;
- Более 80% произошедших утечек из финансовых организаций включают персональные данные клиентов и (или) сотрудников;
- Выросла доля утечек коммерческой тайны;
- На фоне роста латентности внутренних нарушений доля умышленных утечек по вине персонала финансовых организаций в России и мире составила около 70%.

Ниже представлена диаграмма, на которой показаны данные по утечкам как в мировой финансовой сфере, так и в российской (за 2021 и 2022 годы) [19].

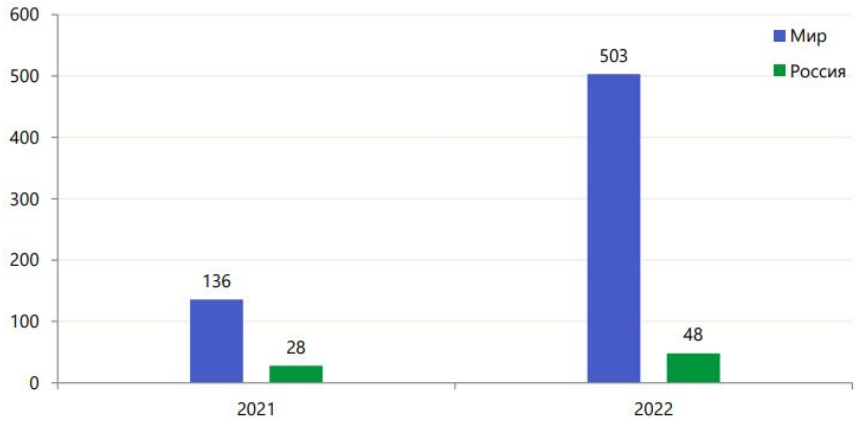

Рисунок 6 - Количество утечек данных в финансовом секторе: Мир и Россия, 2021-2022 гг.
DOI: https://doi.org/10.18454/itech.2024.1.1.6

Примечание: источник [19]

Как видно из данных диаграммы, в Российской Федерации ситуация с информационной безопасностью в финансовой сфере даже лучше, чем во всем остальном мире. Такому улучшению способствует взвешенная политика в сфере ИБ, которую проводит Центробанк России. В последнее время со стороны регулятора были введены меры по противодействию утечкам и угрозам ИБ в организациях финансовой сферы. Для банков стал обязателен аудит веб- и мобильных приложений для дистанционного банковского обслуживания (ДБО) согласно оценочным уровням доверия (ОУД-4), написание профилей защиты и заданий по безопасности, других нормативных документов, а также тестирование на проникновение веб- и мобильных приложений (пентест). Уровень доверия ОУД-4, определенный ГОСТ Р ИСО/МЭК 15408-3-2013 подразумевает достижение максимального доверия к прикладному программному обеспечению путем надлежащего проектирования его безопасности с последующей проверкой полученных результатов.

Какие же можно сделать выводы из собранных данных по США, России, странам ЕС и т.д.? В связи с глобальными изменениями в геополитической ситуации в мире, которые происходят начиная с 2020 года (пандемия коронавируса, СВО, локальные кризисы во многих странах) увеличилось количество различных кибероперация, которые можно смело отнести к кибервойнам. За ними часто стоят хакерские группировки, спонсируемые спецслужбами различных стран. Действия таких группировок стали инструментами политического давления, особенно страдает финансовая система государств. Однако, российская сфера информационной безопасности вполне достойно умеет противостоять угрозам и атакам на современном этапе.

Стратегии кибербезопасности государств, создание кибервойск и экономика кибербезопасности

Как видно из предыдущих разделов статьи, киберпреступления стали столь масштабными, а проблема утечек столь глобальной, что проблема выходит на государственный уровень и требует решений на уровне правительств как отдельных стран, так и на уровне руководства различных политических блоков и организаций. Поэтому при оценке развития экономики кибербезопасности в различных странах необходимо изучить стратегии кибербезопасности этих стран.

Стратегия кибербезопасности – это базовый документ, в котором изложена государственная политика, направленная на обеспечение безопасности государства в киберпространстве.

Существуют следующие уровни стратегий кибербезопасности:

1. Стратегии альянсов государств. К примеру, для ЕС и НАТО такой стратегией является «Таллинское руководство по международному праву, применимому к кибервойне»;
2. Государственные (национальные) стратегии;
3. Отраслевые стратегии (как для мирных отраслей, так и для оборонных);
4. Стратегии для конкретных мероприятий (например, перед проведением Олимпийских игр).

В целях оценки экономики кибербезопасности различных государств при выборе группы государств для анализа необходимо руководствоваться уровнем представленности стран в киберпространстве. Как правило, это страны, у которых есть «кибероружие», есть целая индустрия кибербезопасности и есть «кибервойска».

В данной статье уже приведены определения кибербезопасности и киберпространства. Однако, необходимо отметить, что различные международные документы, а также документы различных государств трактуют эти понятия по-разному. Также на уровне военных ведомств и правительств существует своя трактовка данных понятий. Это «стратегический подход», который непосредственно связывает понятие «кибербезопасность» с понятием «кибервойна» [20].

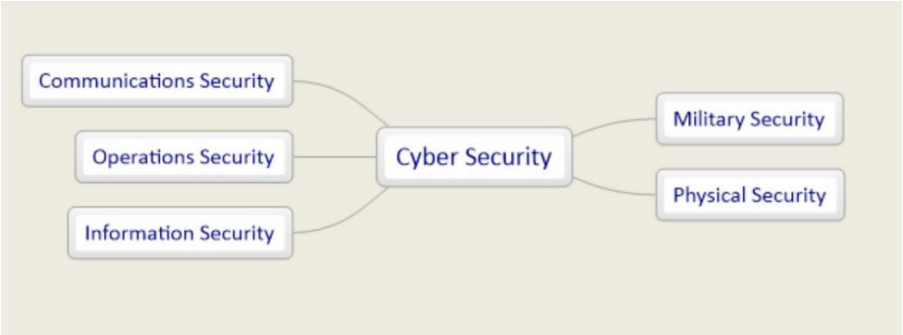

Рисунок 7 - Области понятия «кибербезопасность»
DOI: https://doi.org/10.18454/itech.2024.1.1.7

Примечание: источник [20]

Существуют также понятия «кибервойна» и «информационная война». По мнению автора книги «Кибервойна» Ричарда Кларка:

«действия одного национального государства с проникновением в компьютеры или сети другого национального государства для достижения целей нанесения ущерба или разрушения можно определить как кибервойну».

Информационная война направлена на манипулирование информацией и, как следствие, общественным сознанием.

В Российской Федерации концепция кибербезопасности на уровне государства отсутствует, но в 2010 году был разработан проект такой концепции, который принят не был. В качестве аналогов стратегии кибербезопасности в Российской Федерации возможно рассматривать:

1. «Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации», утверждены Президентом Российской Федерации Д. Медведевым 3 февраля 2012 г., № 8036;
2. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 N 187-ФЗ;
3. Стратегию национальной безопасности;
4. Доктрину информационной безопасности.

В последней редакции Стратегии национальной безопасности Российской Федерации появился новый пункт – «Информационная безопасность». В этом документе также написано, что силовое противоборство стран переходит в новые среды, в том числе – киберпространство стало новым полем для военных действий.

«В случае совершения иностранными государствами недружественных действий, представляющих угрозу суверенитету и территориальной целостности Российской Федерации, в том числе связанных с применением ограничительных мер (санкций) политического или экономического характера либо использованием современных информационно-коммуникационных технологий, Российская Федерация считает правомерным принять симметричные и асимметричные меры, необходимые для пресечения таких недружественных действий, а также для предотвращения их повторения в будущем».

В Доктрине информационной безопасности Российской Федерации от 05.12.2016 г. есть все необходимые положения для формирования государственной политики в этой сфере:

«б) угроза информационной безопасности Российской Федерации (далее – информационная угроза) – совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам в информационной сфере;

в) информационная безопасность Российской Федерации (далее – информационная безопасность) – состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства;

г) обеспечение информационной безопасности – осуществление взаимоувязанных правовых, организационных, оперативно-разыскных, разведывательных, контрразведывательных, научно-технических, информационно-аналитических, кадровых, экономических и иных мер по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления;

д) силы обеспечения информационной безопасности – государственные органы, а также подразделения и должностные лица государственных органов, органов местного самоуправления и организаций, уполномоченные на решение в соответствии с законодательством Российской Федерации задач по обеспечению информационной безопасности» [20].

В США разработана «Национальная киберстратегия» США, которая опубликована в сентябре 2018 года и подписана Д. Трампом. В стратегии США чаще вместо употребления слова «киберпространство» в основном, делают акцент на сети Интернет.

В Великобритании существует Национальная стратегия кибербезопасности (2022). Основной смысл Стратегии кибербезопасности – к 2025 году увеличить устойчивость главных функций правительства Соединенного Королевства к кибератакам, при этом все организации в государственном секторе должны быть устойчивы к известным уязвимостям и методам атак не позднее 2030 года.

Австралийская стратегия кибербезопасности (2020) предполагает инвестиции в размере 1,67 миллиарда долларов в течение 10 лет в кибербезопасность.

Национальная стратегия безопасности киберпространства (2016) Китая описывает базовые позиции и предложения Китая в отношении кибербезопасности. Стратегия направлена на то, чтобы превратить Китай в кибердержаву.

Также необходимо отметить, что в таких странах, как США, России, Великобритании, КНР, Иране, КНДР, Израиле, Южной Корее и некоторых других создаются специальные кибервойска.

Вообще, такой базовый документ, как стратегия кибербезопасности существует у более чем 100 государств [20]. Естественно, для стран, которые развивают цифровую экономику и прошли постиндустриальный переход, киберстратегия и создание собственных кибервойск – это еще один важный шаг в развитии кибербезопасности. К примеру, в 2017 году министр обороны РФ Сергей Шойгу заявил о создании в составе Вооруженных сил Российской Федерации войск информационных операций. Основные цели и задачи этого подразделения – это защита военных компьютерных сетей, защита российских военных систем управления и связи от кибератак [20].

И с макроэкономической точки зрения, расходы на кибербезопасность – это важная позиция в бюджете многих государств.

Заключение

В настоящее время компании и организации по всему миру осознают важность соблюдения строгих мер безопасности. Факт того, что все чаще принимаются решения в пользу увеличения расходов на кибербезопасность, указывает нам на то, что риски от киберугроз становятся все более существенными и необходимо как можно активнее повышать уровень кибербезопасности и вкладывать больше средств в защиту своих цифровых данных от потенциальных атак. Более того, инвестиции в кибербезопасность увеличат степень защиты интеллектуальной собственности, конфиденциальных данных и общей цифровой инфраструктуры.

Также необходимо отметить, что у ведущих государств в области цифровой экономики (США, Великобритания, Россия, Австралия, КНР и т.д.) существуют собственные стратегии кибербезопасности, которые предполагают большие расходы из бюджета на данную отрасль.

В Российской Федерации необходимо развивать работу в следующих направлениях кибербезопасности:

1. Безопасность финансовых организаций (банков, платежных систем и т.д.). Здесь необходимо неукоснительное выполнение требований регулятора (Центробанка РФ) в части следования международным стандартам (например, ОУД-4) по безопасности веб- и мобильных приложений для обслуживания клиентов. Также необходимо регулярно проводить аудиты ИТ-инфраструктуры банков силами специализированных организаций;

2. Безопасность критической информационной инфраструктуры (КИИ). Для предприятий и государственных организаций необходимо следовать требованиям к объектам КИИ, указанным в ФЗ-187 «О безопасности критической информационной инфраструктуры Российской Федерации»;

3. Безопасность персональных данных пользователей. Грандиозные утечки ПДн, которые произошли в последние годы, заставили специалистов по ИБ серьезно взяться за данную проблему, причем не только по противодействию внешним угрозам, но и заняться предотвращением внутренних угроз (борьба с инсайдерами внутри компаний). В защите персональных данных компаниям необходимо руководствоваться положениями Федерального закона «О персональных данных» N 152-ФЗ;

4. Развитие импортозамещения продуктов и систем ИБ. Например, определенные успехи есть уже по производству отечественных межсетевых экранов (МЭ), таких как Diamond, DIONIS DPS, «Континент», «Рубикон», UserGate, Ideco и т.д. Однако, разработчики ставят задачи полностью заместить импортную продукцию и сделать ее конкурентноспособной на международных рынках;

5. Внедрение методик оценки рисков и других методологий из международных стандартов в бизнес-процессы компаний и организаций. Формирование оптимальных бюджетов на кибербезопасность.

Научная новизна данной работы заключается в исследовании структуры экономики кибербезопасности в различных странах мира как на макроэкономическом уровне (государства, бюджет, киберстратегии, кибервойска), так и на уровне микроэкономики (ущерб от утечек в компаниях, расходы на системы и продукты кибербезопасности и т.д.). В статье описаны базовые теоретические концепции (кибербезопасность, киберпространство, киберстратегии, оценка рисков) и показана их связь с чисто практическими понятиями (риски, ущерб, затраты на продукты и услуги по кибербезопасности). Даны направления кибербезопасности, которые необходимо развивать в Российской Федерации.

Конфликт интересов

Не указан.

Рецензия

Все статьи проходят рецензирование. Но рецензент или автор статьи предпочли не публиковать рецензию к этой статье в открытом доступе. Рецензия может быть предоставлена компетентным органам по запросу.

Conflict of Interest

None declared.

Review

All articles are peer-reviewed. But the reviewer or the author of the article chose not to publish a review of this article in the public domain. The review can be provided to the competent authorities upon request.

Список литературы / References

1. ISO/IEC 27032:2012. Information technology. Security techniques. Guidelines for cybersecurity. — Introduced: 2012-07 // International Organization for Standardization. — URL: https://www.iso.org/standard/44375.html (accessed: 29.09.2023).

2. ГОСТ Р ИСО/МЭК 15408-1-2012. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. — Введ. 2013-12-01 // Электронный фонд правовых и нормативно-технических документов. — URL: https://docs.cntd.ru/document/1200101777 (дата обращения: 29.09.2023).

3. Cybersecurity // Gartner Glossary. — URL: https://www.gartner.com/en/information-technology/glossary/cybersecurity (accessed: 29.09.2023).

4. Что такое киберпреступность? Защита от киберпреступности // Лаборатория Касперского. — URL: https://www.kaspersky.ru/resource-center/threats/what-is-cybercrime (дата обращения: 29.09.2023).

5. Коротнев К. Методики управления рисками информационной безопасности и их оценки (часть 1) / К. Коротнев // Безопасность пользователей в сети Интернет. — 2018. — URL: https://safe-surf.ru/specialists/article/5193/587932/ (дата обращения: 14.10.2023).

6. Легчекова Е.В. Метод расчета риска информационной безопасности / Е.В. Легчекова, О.В. Титов // Сборник научных статей международной научно-практической конференции «Проблемы и перспективы электронного бизнеса». — Гомель: Белорусский торгово-экономический университет потребительской кооперации, 2017. — С. 87-89. — URL: https://core.ac.uk/download/pdf/145189961.pdf (дата обращения: 14.10.2023).

7. Dean E. 100+ Cybersecurity Statistics You Need to Know – Where, Who & What is Targeted / E. Dean // Business2Community. — 2023. — URL: https://www.business2community.com/statistics/cybersecurity-statistics (accessed: 04.09.2023).

8. Parvez H. Cybersecurity Spending Statistics 2023: A Closer Look / H. Parvez // Increditools. — 2023. — URL: https://increditools.com/cybersecurity-spending-statistics/ (accessed: 04.09.2023).

9. Gartner forecasts worldwide information security spending to exceed 124 billion in 2012 // Gartner. — URL: https://www.gartner.com/en/newsroom/press-releases/2022-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2012 (accessed: 04.09.2023).

10. Worldwide Security Spending Guide // IDC. — URL: https://www.idc.com/getdoc.jsp?containerId=IDC_P33461 (accessed: 04.09.2023).

11. Worldwide Security // Cisco. — URL: https://newsroom.cisco.com/c/r/newsroom/en/us/index.html (accessed: 04.09.2023).

12. 239 Cybersecurity Statistics (2023) // PacketLabs. — 2023. — URL: https://www.packetlabs.net/posts/239-cybersecurity-statistics-2023/ (accessed: 04.09.2023).

13. How Much do SMBs Really Spend on Cybersecurity? // Pennyrile Technologies. — URL: https://pennyriletechnologies.com/how-much-do-smbs-spend-cybersecurity/ (accessed: 05.09.2023).

14. Benchmarking your cybersecurity budget in 2023 // VentureBeat. — 2023. — URL: https://venturebeat.com/security/benchmarking-your-cybersecurity-budget-in-2023/ (accessed: 05.09.2023).

15. Cyber Security Salary in 2023: Check Jobs and Payscale // KnowledgeHut. — 2023. — URL: https://www.knowledgehut.com/blog/security/cyber-security-salary (accessed: 05.09.2023).

16. Gadient A. The hidden costs of cybersecurity / A. Gadient // Forbes. — 2023. — URL: https://www.forbes.com/sites/forbestechcouncil/2023/05/08/the-hidden-costs-of-cybersecurity/?sh=1cac32eb23e3 (accessed: 05.09.2023).

17. Оценка ущерба вследствие утечек информации // INFOWATCH. — 2023. — URL: https://www.infowatch.ru/analytics/analitika/otsenka-uscherba-vsledstvie-utechek-informatsii (дата обращения: 29.09.2023).

18. Ландшафт угроз для систем промышленной автоматизации. Первое полугодие 2023 // Kaspersky ICS CERT. — 2023. — URL: https://ics-cert.kaspersky.ru/publications/reports/2023/09/13/threat-landscape-for-industrial-automation-systems-statistics-for-h1-2023/ (дата обращения: 14.10.2023).

19. Финансовая сфера: утечки информации за 2022 год // INFOWATCH. — 2023. — URL: https://www.infowatch.ru/analytics/analitika/finansovaya-sfera-utechki-informatsii-za-2022-god (дата обращения: 14.10.2023).

20. Аналитический отчет. Стратегии кибербезопасности // Экспертно-Аналитический центр InfoWatch. — 2022. — URL: https://www.infowatch.ru/sites/default/files/analytics/files/strategii-kiberbezopasnosti-1.pdf (дата обращения: 29.09.2023).

21. Definition of Cybersecurity — Gaps and overlaps in standardisation // European Union Agency for Cybersecurity. — 2016. — URL: https://www.enisa.europa.eu/publications/definition-of-cybersecurity (accessed: 29.09.2023).

Список литературы на английском языке / References in English

1. ISO/IEC 27032:2012. Information technology. Security techniques. Guidelines for cybersecurity. — Introduced: 2012-07 // International Organization for Standardization. — URL: https://www.iso.org/standard/44375.html (accessed: 29.09.2023).

2. GOST R ISO/MEK 15408-1-2012. Informacionnaja tehnologija. Metody i sredstva obespechenija bezopasnosti. Kriterii ocenki bezopasnosti informacionnyh tehnologij [Information technology. Methods and means of ensuring security. Criteria for assessing the security of information technologies]. — Introduced 2013-12-01 // Electronic fund of legal and regulatory documents. — URL: https://docs.cntd.ru/document/1200101777 (accessed: 29.09.2023). [in Russian]

3. Cybersecurity // Gartner Glossary. — URL: https://www.gartner.com/en/information-technology/glossary/cybersecurity (accessed: 29.09.2023).

4. Chto takoe kiberprestupnost'? Zashchita ot kiberprestupnosti [What is cybercrime? Defence against cybercrime] // Kaspersky.ru. — URL: https://www.kaspersky.ru/resource-center/threats/what-is-cybercrime (accessed: 29.09.2023). [in Russian]

5. Korotnev K. Metodiki upravleniya riskami informacionnoj bezopasnosti i ih ocenki (chast' 1) [Methods of Information Security Risk Management and Assessment (Part 1)] / K. Korotnev // Safe-Surf.ru. — 2018. — URL: https://safe-surf.ru/specialists/article/5193/587932/ (accessed: 14.10.2023). [in Russian]

6. Legchekova E.V. Metod rascheta riska informacionnoj bezopasnosti [Method for Calculating Information Security Risk] / E.V. Legchekova, O.V. Titov // Sbornik nauchnyh statej mezhdunarodnoj nauchno-prakticheskoj konferencii «Problemy i perspektivy jelektronnogo biznesa» [Collection of scientific articles of the international scientific and practical conference “Problems and prospects of electronic business”]. — Gomel: Belarusian Trade and Economic University of Consumer Cooperation, 2017. — P. 87-89. — URL: https://core.ac.uk/download/pdf/145189961.pdf (accessed: 14.10.2023). [in Russian]

7. Dean E. 100+ Cybersecurity Statistics You Need to Know – Where, Who & What is Targeted / E. Dean // Business2Community. — 2023. — URL: https://www.business2community.com/statistics/cybersecurity-statistics (accessed: 04.09.2023).

8. Parvez H. Cybersecurity Spending Statistics 2023: A Closer Look / H. Parvez // Increditools. — 2023. — URL: https://increditools.com/cybersecurity-spending-statistics/ (accessed: 04.09.2023).

9. Gartner forecasts worldwide information security spending to exceed 124 billion in 2012 // Gartner. — URL: https://www.gartner.com/en/newsroom/press-releases/2022-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2012 (accessed: 04.09.2023).

10. Worldwide Security Spending Guide // IDC. — URL: https://www.idc.com/getdoc.jsp?containerId=IDC_P33461 (accessed: 04.09.2023).

11. Worldwide Security // Cisco. — URL: https://newsroom.cisco.com/c/r/newsroom/en/us/index.html (accessed: 04.09.2023).

12. 239 Cybersecurity Statistics (2023) // PacketLabs. — 2023. — URL: https://www.packetlabs.net/posts/239-cybersecurity-statistics-2023/ (accessed: 04.09.2023).

13. How Much do SMBs Really Spend on Cybersecurity? // Pennyrile Technologies. — URL: https://pennyriletechnologies.com/how-much-do-smbs-spend-cybersecurity/ (accessed: 05.09.2023).

14. Benchmarking your cybersecurity budget in 2023 // VentureBeat. — 2023. — URL: https://venturebeat.com/security/benchmarking-your-cybersecurity-budget-in-2023/ (accessed: 05.09.2023).

15. Cyber Security Salary in 2023: Check Jobs and Payscale // KnowledgeHut. — 2023. — URL: https://www.knowledgehut.com/blog/security/cyber-security-salary (accessed: 05.09.2023).

16. Gadient A. The hidden costs of cybersecurity / A. Gadient // Forbes. — 2023. — URL: https://www.forbes.com/sites/forbestechcouncil/2023/05/08/the-hidden-costs-of-cybersecurity/?sh=1cac32eb23e3 (accessed: 05.09.2023).

17. Ocenka ushherba vsledstvie utechek informacii [Assessment of Damage Due to Information Leaks] // INFOWATCH. — 2023. — URL: https://www.infowatch.ru/analytics/analitika/otsenka-uscherba-vsledstvie-utechek-informatsii (accessed: 29.09.2023). [in Russian]

18. Landshaft ugroz dlja sistem promyshlennoj avtomatizacii. Pervoe polugodie 2023 [Threat Landscape for Industrial Automation Systems. First half of 2023] // Kaspersky ICS CERT. — 2023. — URL: https://ics-cert.kaspersky.ru/publications/reports/2023/09/13/threat-landscape-for-industrial-automation-systems-statistics-for-h1-2023/ (accessed: 14.10.2023). [in Russian]

19. Finansovaja sfera: utechki informacii za 2022 god [Financial sector: information leaks for 2022] // INFOWATCH. — 2023. — URL: https://www.infowatch.ru/analytics/analitika/finansovaya-sfera-utechki-informatsii-za-2022-god (accessed: 14.10.2023). [in Russian]

20. Analiticheskij otchet. Strategii kiberbezopasnosti [Analytical report. Cybersecurity Strategies] // Expert Analytical Center InfoWatch. — 2022. — URL: https://www.infowatch.ru/sites/default/files/analytics/files/strategii-kiberbezopasnosti-1.pdf (accessed: 29.09.2023). [in Russian]

21. Definition of Cybersecurity — Gaps and overlaps in standardisation // European Union Agency for Cybersecurity. — 2016. — URL: https://www.enisa.europa.eu/publications/definition-of-cybersecurity (accessed: 29.09.2023).