Обеспечение экономической безопасности Российской Федерации в разрезе нормативно-методической адаптации ИТ-инфраструктуры

Гайсина Алина Ринатовна
Студент
Санкт-Петербургский государственный экономический университет, г. Санкт-Петербург, Россия
E-mail: alinagaysina020401@gmail.com

Шехова Наталия Владимировна
доктор экономических наук, профессор
Балтийский государственный технический университет «Военмех» им. Д.Ф.Устинова, г. Санкт-Петербург, Россия
E-mail: nataly65vf@gmail.com

Аннотация. Вопросы о сроках адаптации отрасли информационной безопасности РФ после ухода западных вендоров с отечественного рынка и нестабильного 2022 года, вызвавшего иные структурные изменения в отрасли, остаются открытыми. Суть дискуссии заключается в высокой конкурентоспособности продуктов отечественных производителей, которая на начало 2023 года не способна оказать влияние на повышение качества компонент продуктов информационной безопасности. Авторами были приняты условия, при которых решение задачи создания собственных альтернативных высокоёмких технологических ИТ-компонент при реализации политики импортозамещения является долгосрочным. Проведённая оценка перспектив дальнейшего развития отрасли информационной безопасности РФ требует внедрения комплексного подхода, при котором совершенствование инструментально-технического обеспечения и наполнения элементов безопасности должно поддерживаться качественным нормативно-правовым регулированием. В статье выявлена и обоснована необходимость развития отечественной информационной отрасли в новом векторе: переходе от развивающейся формы информационной безопасности (ИБ) к результативной. В этой связи методическим инструментом исследования явилось изучение перечня актуализированных положений нормативно-правовых актов, регламентирующих меры обеспечения ИБ в современных условиях, и сопоставление действующих норм с условиями развития кибер-отрасли РФ в период 2022–2023 гг. На этой основе представлен перечень ключевых уязвимостей ИТ-инфраструктуры РФ в процессах импортозамещения элементов ИБ. Руководствуясь оценкой достаточности имеющегося технического ИТ-обеспечения и учитывая выявленные несовершенства нормативно-правовых актов, авторы разработали направления реформирования организации ИТ-инфраструктуры и методологии обеспечения ИБ страны на всех уровнях (физические лица, организации, государства)..

Ключевые слова: ИТ-инфраструктура; критическая информационная инфраструктура (КИИ); кибератаки; киберграмотность; мошенничество; информационная безопасность; инцидент; уязвимость; программное обеспечение (ПО); средства защиты информации (СЗИ); Единая платформа верификации телефонных вызовов (ЕПВВ).

JEL codes: F01; O32 ; P11

Для цитирования: Кекелева, А.Р. Обеспечение экономической безопасности Российской Федерации в разрезе нормативно-методической адаптации ИТ-инфраструктуры. /А.В Гайсина, Н.В. Шехова. - Текст : электронный // Теоретическая экономика. - 2023 - №8. - С87-97. - URL: http://www.theoreticaleconomy.ru (Дата публикации: 30.08.2023)

Введение

Политическое противостояние России и ряда зарубежных стран, обострившееся в марте 2022 года, вылилось в санкционное давление, результатом которого стал уход большинства зарубежных компаний из РФ. Несмотря на превентивные и в большей степени успешные меры по формированию достаточного уровня автономности российской ИТ-инфраструктуры, которые были предприняты еще в 2016 году с принятием доктрины информационной безопасности РФ , процессы активного импортозамещения на начало 2023 года выявляли ряд уязвимостей отечественной отрасли ИБ

[1]. Целью данного исследования является выявление уязвимостей нормативно-правового и инструментального обеспечения экономической безопасности ИТ-инфраструктуры РФ.

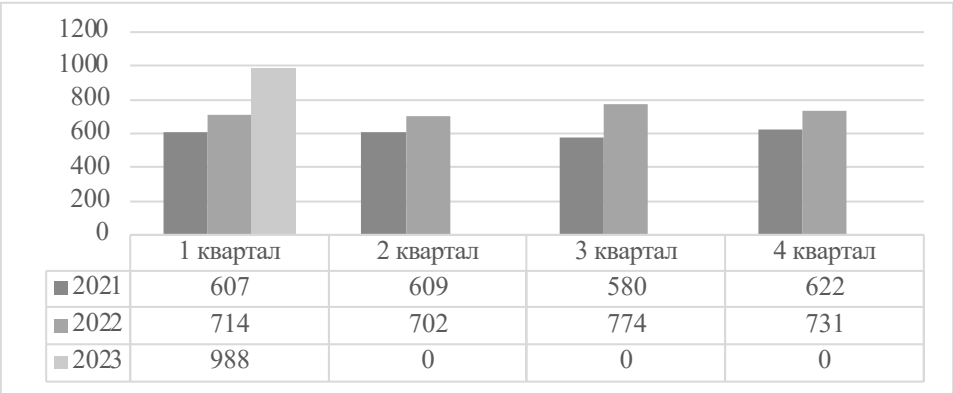
Методы исследования

Информационной основой исследования стали аналитические отчеты информационных вендоров России (в частности, исследования экспертно-аналитического центра InfoWatch, Positive Technologies), заключения специалистов в сфере ИБ о состоянии уровня киберграмотности граждан и нормативно-правовая база регулирования соответствующего вопроса.

В ходе исследования использовались методы анализа, синтеза и обобщения статических данных состояния преступности в сфере информационных технологий для выявления причин образования уязвимостей ИТ-инфраструктуры России. При формировании комплекса направлений совершенствования нормативно-правового регулирования вопросов обеспечения ИБ РФ применялись методы аналогии и абстрагирования.

Обсуждение и результаты исследования

Наличие существенных уязвимостей ИТ-инфраструктуры России ярко отражается в динамике увеличения количества кибератак в отношении физических и юридических лиц в первом квартале 2023 года на 38% по сравнению с аналогичным периодом прошлого года (см. рис.1) [2].



	1 квартал	2 квартал	3 квартал	4 квартал
2021	607	609	580	622
2022	714	702	774	731
2023	988	0	0	0

Рисунок 1 – Количество успешных инцидентов[1] ИТ-инфраструктуры РФ в динамике 2021–2022 гг., усл.ед.

Источник: составлено авторами на основе [3, 4, 14, 15]

Одной из ключевых причин роста количества инцидентов является организация ИТ-инфраструктуры большинства российских компаний на базе западных технологий и методик (среди наиболее востребованных - использование международных сертификационных стандартов безопасности и правил эксплуатации оборудования). Безусловно, успешный переход отечественных организаций на отечественное ПО позволил сократить возможности использования мошенниками каналов уязвимостей при совершении кибератак (см. рис.2). Однако сохраняющиеся превалирующие доли канала заражения ПО, что само по себе является уязвимостью ИТ-отрасли РФ, свидетельствует о том, что борьба с кибермошенничеством и формирование высокого уровня защищенности российской информационной среды должны строиться не просто на замене зарубежного сервисного обслуживания, но и на качественной адаптации внутреннего наполнения данных продуктов под текущие потребности ИТ-инфраструктуры РФ [5].

Исследователи отмечают, что мощный стимул структурным изменениям дала вступившая в силу в 2022 году новая редакция Указа Президента РФ «О дополнительных мерах по обеспечению ИБ РФ» [1, с. 68]. Проведенная актуализация методики оценки угроз безопасности информационной

1 Инциденты, которые привели к негативным последствиям физических лиц и компаний (ущерб)

составляющей субъектов КИИ[2] (в том числе, порядок и алгоритм формирования банка угроз) базируется на трёх ключевых пунктах: создание специализированного подразделения ИБ, закрепление персональной ответственности руководителя подразделения за обеспечение ИБ; запрет на использование сервисных продуктов защиты ИБ недружественных стран (см. рис.3). Главным преимуществом такого подхода к защите информационной среды субъектов КИИ является включение подразделения ИБ в структуру деятельности организации как важнейшего составляющего звена системы [5, с. 560].

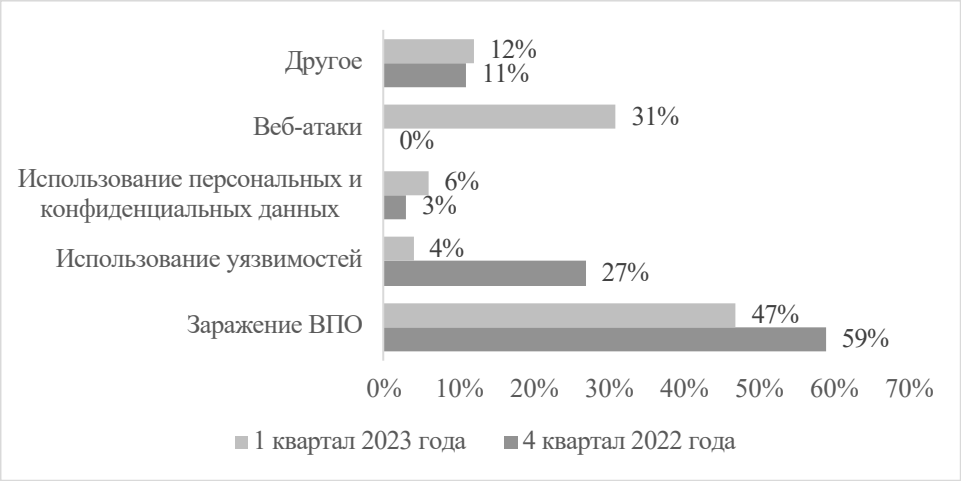


Рисунок 2 –Кибератаки в РФ, %

Источник: составлено авторами на основе [2]

Таким образом, в установленные законом сроки организации «первой волны»[3], должны создать подразделение в соответствии в закрепленными целями и задачами, сформировать и закрепить перечень необходимой организационно-распорядительной документации, регламентирующей его деятельность. Более того, субъекты непрерывного процесса применения дополнительных мер по обеспечению информационной безопасности РФ должны возложить функцию персональной ответственности за инциденты и обеспечение ИБ на конкретное лицо. Поскольку данный шаг поднимает приоритетность функции обеспечения ИБ в общей иерархии функционирования организации, закономерным становится необходимость закрепления возможности и широты полномочий ответственного лица в принятии соответствующих стратегически важных решений (например, в случае необходимости принятия оперативного решения без согласования на уровне руководства) [6].

Ожидаемое развитие в рамках нормативно-правового акта получил и процесс импортозамещения. Введенный запрет на использование зарубежных СЗИ в целом не должен вызвать трудностей у отечественных организаций при замещении ПО. Отечественные разработчики предлагают качественные операционные системы, системы управления базами данных (СУБД) и среды разработки. Согласно заявлениям руководителя аналитического центра компании Zecurion , отрасль кибербезопасности в процессах естественного импортозамещения (начиная с 2016 года) показала свою высокую конкурентоспособность и завоевала доверие потребителей. На данный момент Министерство цифрового развития, связи и массовых коммуникаций РФ (Минцифры России) подтверждает наличие российского ПО в объеме 13224 программных продукта (все классы) от 4195 разработчиков, в евразийском реестре – 61 программа 19 правообладателей [3].

2 Компании, работающие в стратегически важных для государства областях (здравоохранение, наука, транспорт, связь, энергетика, банковская сфера, топливно-энергетический комплекс и иных), а также организации, обеспечивающие взаимодействие систем или сетей критической информационной инфраструктуры.

3 Организации, закрепленные в соответствующем перечне Указом Президента РФ от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности РФ».

Рисунок 3 – Вопросы к решению при редакции Указа Президента РФ от 01.05.2022 №250 «О дополнительных мерах по обеспечению информационной безопасности РФ»

Источник: составлено авторами на основе [7]

Несмотря на достаточную инструментально-техническую оснащенность, на практике фиксируется лишь частичный отказ организаций от зарубежных СЗИ при реформировании собственной ИТ-среды. Учитывая то, что российские операционные системы уже использовались органами власти и госкомпаниями (и большинством других групп организаций, которые входят в перечень субъектов КИИ), возникают споры о необходимости полного перехода на отечественные СЗИ. Причиной этому являются сложности замещения частично привлеченных зарубежных элементов СЗИ с большим количеством исходных кодов (например, ERP и SAP), что грозит потерей данных для организации [7]. Данный фактом и апеллируют руководители организаций, отмечая то, что большая доля используемых СЗИ преимущественно отечественная, поэтому необходимость в полном переходе экономически и стратегически не обоснована.

На деле это формирует уязвимости отечественного ПО, которые уже активно используются мошенниками. Так, решения SAP содержат в себе возможности по удаленному управлению, в том числе по удалению баз данных и механизмы отложенных действий. Решением споров должно стать изменение порядка процесса полного импортозамещения, формирование последовательного плана адаптации ИТ-инфраструктуры организации. Первостепенную реализацию должна получить апробация отечественных операционных систем и автоматизаций бизнес-процессов, а также оценка сопоставимости их функционирования с доступными для российских организаций пакетами СЗИ. Закрепленные на государственном уровне рекомендации позволят значительно сократить временные и операционные издержки организаций и ускорят процессы ликвидации уязвимостей ИТ-инфраструктуры РФ.

Определение запрета на использование иностранных сервисных и методических элементов ИТ-инфраструктуры российскими организациями не содержит ответа на вопрос о судьбе международных сертификатов безопасности специалистов кибербезопасности.

До недавнего времени у отечественного работодателя не было проблем с выявлением необходимого уровня компетенций и отбором квалифицированного персонала на тендерах. Международный сертификат безопасности выполнял роль «красного флажка». На текущий период ситуация изменилась и в перспективе есть риск неполучения российскими специалистами котирующегося на международном уровне сертификата безопасности. Об этом свидетельствуют

ограничения возможности соискателей в сдаче онлайн-экзамена, сложности с его оплатой (появилась необходимость поиска организаций, использующих элементы SWIFT-системы) и иные ограничивающие факторы [7].

В совокупности данные факторы уже отразились на изменении запрашиваемых работодателями компетенций для соискателей профиля «специалиста по кибербезопасности». Так, требование о наличии сертификата встречалось в 10% вакансий в 2020 и 2022 годах и в 11% в 2021 году. Спецификация требований к обязательному наличию CISSP, CISA, CISM за этот период встречалась в 4% вакансий [8].

В действительности в период до 2022 года Минцифры России рассматривало инициативу по созданию российских сертификатов безопасности для подтверждения квалификации специалистов [8]. По заявлениям ведомства, ключевым ограничением являлась низкая практикоориентированность отрасли кибербезопасности РФ. Вместе с тем, на отечественном рынке уже есть примеры организации прототипов таких платформ на коммерческой основе. Так, у Академии информационных систем есть курс повышения квалификации (512 часов), после которого выдается подтверждающий документ о наличии CISSP, CISA, CISM и иных квалификаций [2].

В общем сформировалось два ключевых подхода к разрешению вопроса о целесообразности создания российской системы сертификации. Приверженцы первого подхода объясняют необходимость создания такой системы, исходя из динамики резкого оттока ИТ-специалистов в зарубежные страны. Несмотря на все предпринятые меры поддержки ИТ-сектора (третий пакет мер поддержки ИТ-отрасли[4]), по заявлениям Минцифры России, на конец 2022 года Россию покинули 100 тыс. специалистов, из них лишь 40% продолжают работать на отечественный рынок [9].

Безусловно, на отток кадров оказывает влияние множество факторов (нестабильность курса рубля, «релокация» компаний-партнёров и пр.). Но ещё более вероятным «переезд» специалистов ИБ в другие страны делают программы поддержки «ИТ-умов». Среди наиболее востребованных можно назвать программы Франции (French Tech Visa), Великобритании (Global Talent), Германии (Freiberufler Visa), Венгрии (White Card) [10]. В перспективе с полным ограничением действия международных сертификатов возможен риск утраты кадрового резерва, в связи с чем следует «удерживать» квалифицированных специалистов, обеспечивая необходимую инфраструктуру их профессиональной деятельности.

Бизнес-консультант ИБ Positive Technologies Алексей Лукацкий и Директор по стратегическому развитию бизнеса компании Innostage Андрей Тимошенко, будучи представителями второго подхода, говорят об экономической нецелесообразности создания системы сертификации, которая ставит под сомнение качество и признание российского диплома сертифицированного специалиста-кибербезопасника [2].

Можно считать экономически и стратегически необоснованным создание автономной системы сертификации, которая на неограниченный промежуток времени не сможет отвечать мировым требованиям и признаваться зарубежными сообществами. Ведь с практической точки зрения, для российского работодателя нет необходимости в международном сертификате безопасности, если речь идет о подтверждении квалификации сотрудника (даже несмотря на то, что сертификат является гарантом систематизированности соискателя).

Однако неоспорима значимость реформирования и адаптации системы выдачи диплома сертифицированного сотрудника ИБ под потребности российской системы ИБ. Результативность данной системы будет заключаться в содержательных изменениях: включении в образовательные процессы экзаменов типовых и содержательных элементов, необходимых для сдачи общего экзамена (CISSP, CISA, CISM и иных), организации со стороны государства грамотно выстроенного контроля поддержания компетенций обладателя документа и постоянной актуализации методологической

4 Указ Президента РФ от 02.03.2022 № 83 «О мерах по обеспечению ускоренного развития отрасли информационных технологий в РФ»

базы.

Стратегически важным в процессе реформирования отечественной ИТ-инфраструктуры являлось закрепление Концепции формирования и развития культуры ИБ граждан РФ [1, с. 559]. Это объясняет и статистика нарушений. Так, большинство инцидентов ИБ происходят не по причине нехватки СЗИ и недоработанности методики обеспечения ИБ, а из-за влияния человеческого фактора (см. рис.4).

Таким образом, причиной ошибок персонала и физических лиц при защите информационной среды, согласно систематизации аналитических данных IBM (International Business Machines) Managed Security Services, является не сколько низкая квалификация и недостаточная комплектация СЗИ, сколько низкий уровень грамотности населения в области ИБ [2].

Согласно проведенному Минцифры России совместно с Национальным агентством финансовых исследований (НАФИ) анализу киберграмотности, общий индекс киберграмотности населения составил 48,2 пункта из 100 возможных. В ходе исследования проверялись знания россиян об актуальных киберугрозах и способах защиты от них. Исследование строилось на проверке уровня осведомленности российскими гражданами об актуальных киберугрозах и способах защиты от них. Результаты тестирования говорят о низком уровне киберграмотности граждан относительно текущей повестки активных информационных атак. Так, 41% респондентов не способны указать ни на одну из существующих угроз, лишь 20% из них знают про компьютерные вирусы и заражение ПО, около 19% знакомы со схемами взломов аккаунтов в социальных сетях. Парадоксальным является критически низкий показатель осведомленности граждан о телефонном мошенничестве – всего 16%. И это при том, что, по расчётам Минцифры России, 83% российских граждан в среднем один раз подвергались попытке телефонного мошенничества в 2022 году, а совокупные объёмы денежных потерь за аналогичный период превысили 14,2 млрд рублей (при максимальной единоразовой похищенной сумме в 500 млн рублей) [11].

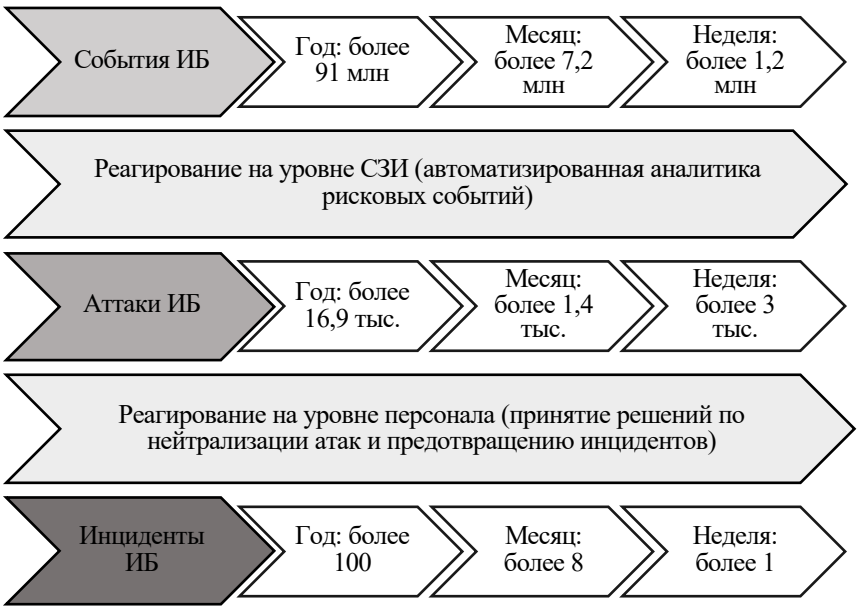


Рисунок 4 – Влияние человеческого фактора при реализации инцидентов ИБ

Источник: составлено авторами на основе [13, 14]

Такая противоречивая статистическая картина на первый взгляд может объясняться большим диапазоном выборки возрастных категорий (от 13 до 65 лет) граждан, принявших участие в эксперименте. Однако стоит признать и тот факт, что в лице российских граждан возможности мошенников в успешности использования методов социальной инженерии (которые, получив несколько положительных ответов от жертв, способны убедить их в переводе денежных средств) сильно недооценены (см. рис.5).

Наиболее высокие значения индекса киберграмотности отличают жителей России в возрасте от 25 до 34 лет, с увеличением возраста значение индекса постепенно снижается. Ключевыми выводами Минцифры России по итогам проведенного исследования стал тезис о наименьшем уровне защищенности россиян в возрасте от 45 до 55 лет (больше всего страдающих от телефонного мошенничества) и необходимостью принятия мер по этому поводу [12].

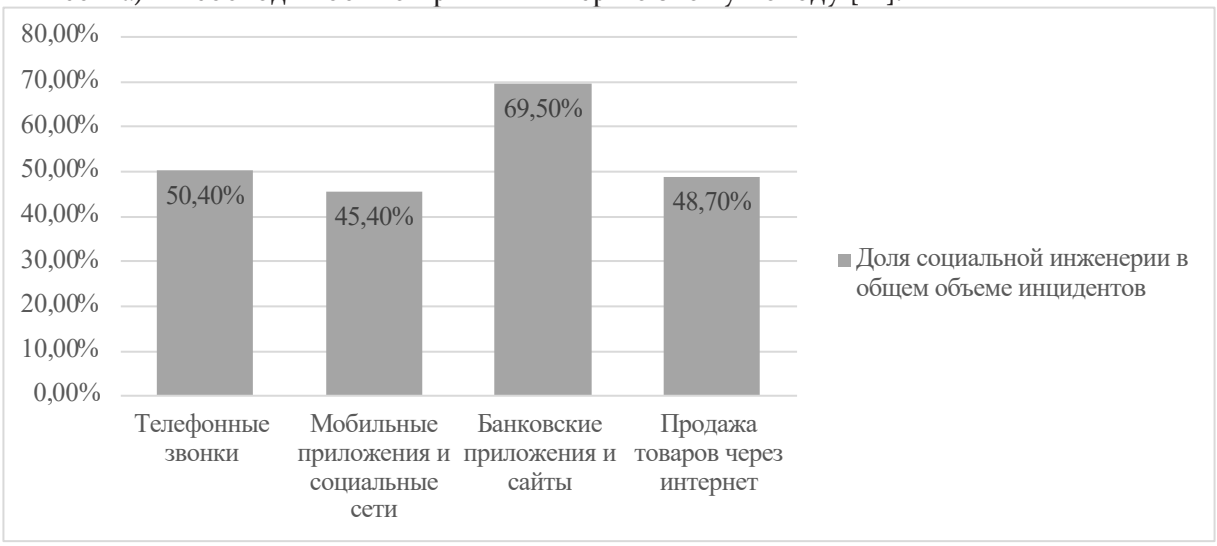


Рисунок 5 – Объемы социальной инженерии в киберпреступлениях, %

Источник: составлено авторами на основе [13, 14]

В этой связи с 1 января 2023 года вступили в силу требования статьи 46.1 Федерального закона от 07.07.2003 №126-ФЗ «О связи», направленные на борьбу с преступниками, использующими подменные номера. При поддержке отечественных операторов связи и Роскомнадзора Минцифры России организовали деятельность ЕПВВ для предупреждения телефонных преступлений [15]. Трехэтапный процесс подключения всех операторов к системе должен закончиться к концу 2025 года, тогда как рост киберпреступности продолжает стремительно расти, а способы свершения преступлений адаптируются под актуальные условия обеспечения ИБ граждан РФ.

Заключение

Подводя итог, следует отметить, что среди главных трендов развития мошенничества в сфере кибербезопасности в 2023 году находится омоложение портрета потенциальной жертвы мошенников. В связи с этим ключевыми уязвимостями ИТ-отрасли при формировании нормативно-правовой и методической основы её развития должны считаться недооценённость методов социальной инженерии при совершении преступлений (избирательность и индивидуальный подход мошенников к потенциальным жертвам), а также низкий уровень киберграмотности граждан РФ.

Главное отличие результативной ИТ-инфраструктуры от развивающейся является единство применения сервисных и методических средств защиты [16].

В условиях политико-экономической нестабильности и постоянной изменчивости достаточности условий обеспечения ИБ для России неоспорима необходимость комплексности принимаемых мер по предупреждению преступлений в сфере ИБ граждан (см. рис.6).

Таким образом, деятельность специалистов по кибербезопасности должна быть подкреплена высоким уровнем осведомленности граждан об имеющихся мошеннических схемах и уязвимостях ИБ в целом. Ограничение действующих нормативно-правовых актов в числе концепций и программ повышения уровня грамотности граждан РФ в кибер-отрасли заключается в ориентации преимущественно на возрастной состав, когда главным преимуществом преступников выступает использование методов социальной инженерии (см. рис.5). Требуется реализация программ на базе государственного обеспечения для всех возрастных групп при имеющемся информационно-

методическом базисе корпоративных организаций при учёте психологического портрета «жертвы», которым пользуются мошенники. Помимо целевого эффекта в повышении уровня киберграмотности граждан, это будет содействовать и реализации услуг, отвечающих требованиям потребителя, что обеспечит процесс качественного и структурного обновления информационно-технической и методологической базы противодействия киберпреступности.

Базовым направлением в успешности применения сервисной защиты является формирование привлекательной инфраструктуры профессиональной реализации кибербезопасников (разрешение вопроса о сертификации, единая сформированная система методических и инструментальных средств, подкрепленная безотказным отечественным ПО и пр.). На текущий период качество российского ПО позволяет создать систему, отвечающую достаточным требованиям, поэтому все входящие изменения законодательства должны касаться разъяснений и адаптации методического комплекса принимаемых мер [17].

В действительности поднятый вопрос требует принятие активных мер со стороны государства. На начало 2023 года в стране зафиксирована острая нехватка ИТ-кадров. По подсчётам Минцифры России, на февраль 2023 года в стране не хватало от 500 тыс. до 1 млн специалистов в различных сферах информационных технологий (из них 65% - в сфере кибербезопасности) [2, 18].

Рисунок 6 – Инструментальная основа перехода ИТ-инфраструктуры РФ от развивающейся к результативной

Источник: составлено авторами на основе [5]

В данных ограничениях на период выравнивания баланса принимаемых мер по предотвращению киберпреступлений организациям и российским вендорам следует обратить внимание на аттестацию объектов информатизации и возможности привлечения ГосСОПКА на уровне подрядчика (по обнаружению и принятию мер реагирования). Для организаций, не входящих в перечень субъектов КИИ, решением станет переход к защите решений в рамках технологии Zero-code (или no-code) по автоматизации разработки без программирования [19].

СПИСОК ЛИТЕРАТУРЫ

1. Карцхия,А.А. Правовые аспекты современной кибербезопасности и противодействия киберпреступности / А.А.Карцхия, Г.И.Макаренко // Вопросы кибербезопасности. - 2023. - №1(53). - С.58-74 // Режим доступа: https://elibrary.ru/item.asp?id=50337103 (дата обращения: 18.05.2023).

2. Positive Technologies: отчет «Кибербезопасность. Тренды 2022-2023 годов» // Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/ogo-kakaya-ib/ (дата обращения: 10.06.2023).

3. Экспертно-аналитический центр InfoWatch: аналитический отчет по статистике киберинцидентов АСУ ТП за 2022 год // Режим доступа: https://www.infowatch.ru/analytics/daydz6esty-i-obzory/statistika-kiberintsidentov-asu-tp-za-proshedshiy-god (дата обращения: 10.06.2023).

4. Экспертно-аналитический центр InfoWatch: отчет об исследовании утечек информации ограниченного доступа в 2021 году // Режим доступа: file:///C:/Users/1/Downloads/utechki-2021-otchyot-InfoWatch%20(1).pdf (дата обращения: 10.06.2023).

5. Беззатеев, С.В. Методика оценки рисков информационных систем на основе анализа поведения пользователей и инцидентов информационной безопасности / С.В.Беззатеев, Т.Н.Елина, В.А. Мыльников, И.И.Лившиц // Научно-технический вестник информационных технологий, механики и оптики. - 2021. - Т. 21. - № 4. - С. 553–561 // Режим доступа: https://elibrary.ru/item.asp?id=46495307 (дата обращения: 05.04.2023).

6. Гайсина,А.Р. Несовершенство судебного урегулирования вопросов обеспечения и предупреждения безопасности критической информационной инфраструктуры РФ / А.Р.Гайсина // Теоретические и прикладные вопросы комплексной безопасности: Мат-лы V Междунар. научно-практ. конф. (г.Санкт-Петербург, 23 марта 2022 года). – СПб.: СПб. ин-т природопользования, промышленной безопасности и охраны окружающей среды, 2022. - С.143-147 // Режим доступа: https://elibrary.ru/item.asp?id=48566891 (дата обращения: 03.04.2023).

7. FBK Cybersecurity: экспертные материалы на тему «Информационная безопасность в России после указа президента №250 от 1 мая 2022 года)» // Режим доступа: https://fbkcs.ru/kommentarii-ekspertov-k-ukazu-prezidenta-250-ot-pervogo-maya?ysclid=lh0jkghg8c864296496 (дата обращения: 10.06.2023).

8. Ростелеком: отчет «Кибератаки на российские компании в 2022 году» // Режим доступа: https://rt-solar.ru/upload/iblock/4a4/ghus61x9rd8cv5vczms5ig1svts4tlep/Otchet-o-kiberatakakh-na-rossiyskie-kompanii-v-2022-godu.pdf?ysclid=lhdk36punc703562989 (дата обращения: 11.06.2023).

9. Соловьев,С.В. Состояние и перспективы развития методического обеспечения технической защиты информации в информационных системах / С.В.Соловьев, М.А.Тарелкин, В.В.Текунов, Ю.К.Язов // Вопросы кибербезопасности. - 2023. - №1(53). - С. 41-57 // Режим доступа: https://elibrary.ru/item.asp?id=50337102 (дата обращения: 06.05.2023).

10. Матвеев,В.В. Обеспечение экономической безопасности при утечке конфиденциальной информации / В.В.Матвеев, А.К.Зайцев, А.Р.Гайсина // Национальная безопасность и стратегическое планирование. - 2022. - №3(39). - С.52-75 // Режим доступа: https://elibrary.ru/item.asp?id=48566891 (дата обращения: 11.04.2023).

11. Коренев,П.В. Актуальность проведения исследований в области создания новых способов поиска уязвимостей с применением отечественных высокотехнологичных вычислительных платформ / П.В.Коренев, В.А.Пиков, А.Г.Вилесов // Вопросы защиты информации. - 2022. - №4(139). - С.37-46 // Режим доступа: https://elibrary.ru/item.asp?id=49891088 (дата обращения: 14.05.2023).

12. Толстой,А.И. Систематика понятий в области информационной безопасности / А.И.Толстой // Безопасность информационных технологий. - 2023. - Т.30. - №1. - С.130-148 // Режим доступа: https://elibrary.ru/item.asp?id=50337119 (дата обращения: 15.06.2023).

13. Экспертно-аналитический центр InfoWatch: отчёт об исследовании утечек информации ограниченного доступа в I половине 2022 года // Режим доступа: https://www.infowatch.ru/sites/default/files/analytics/files/otchyot-ob-utechkakh-dannykh-za-1-polugodie-2022-goda_1.

pdf?ysclid=lfee27gic1326182485 (дата обращения: 14.06.2023).

14. Экспертно-аналитический центр InfoWatch: отчет об исследовании утечек информации ограниченного доступа в 2021 году // Режим доступа: file:///C:/Users/1/Downloads/utechki-2021-otchyot-InfoWatch%20(1).pdf (дата обращения: 10.06.2023).

15. Котенко,И.В. Подсистема предупреждения компьютерных атак на объекты критической информационной инфраструктуры: анализ функционирования и реализации / И.В.Котенко, И.Б.Саенко, Р.И.Захарченко, Д.В.Величко // Вопросы кибербезопасности. - 2023. - №1(53). - С.13-27 // Режим доступа: https://elibrary.ru/item.asp?id=50337100 (дата обращения: 19.04.2023).

16. Королев,В.Н. Обеспечение безопасности субъекта критической информационной инфраструктуры / В. Н. Королев // Молодой ученый. - 2021. - №20 (362). - С.31-33 // Режим доступа: https://moluch.ru/archive/362/80964/ (дата обращения: 02.04.2023).

17. Зайцев,А.К. Экономические преступления с использованием цифровых технологий / А.К.Зайцев, В.В.Матвеев // Национальная безопасность и стратегическое планирование. - 2022. - №1 (37). - С. 63-81 // Режим доступа: https://elibrary.ru/item.asp?id=48486986 (дата обращения: 05.04.2023).

18. Экспертно-аналитический центр InfoWatch: отчет о новых проектах в области биометрических персональных данных // Режим доступа: https://www.infowatch.ru/analytics/daydzhesty-i-obzory/novye-proekty-v-oblasti-biometricheskikh-personalnykh-dannykh (дата обращения: 10.06.2023).

19. Шарамок,А.В. Об особенностях формирования требований безопасности информации для масштабируемой доверенной платформы / А.В.Шарамок, Д.С.Брагин, О.П.Симонова // Вопросы защиты информации. - 2022. - №4(139). - С.13-20 // Режим доступа: https://elibrary.ru/item.asp?id=49891084 (дата обращения: 08.06.2023).

Ensuring the Economic Security of the Russian Federation in the Term of Regulatory and Methodological Adaptation of IT-Infrastructure

Gaysina Alina Rinatovna
student
St. Petersburg State University of Economics,St. Petersburg, Russian Federation
E-mail: alinagaysina020401@gmail.com

Shekhova Natalya Vladimirovna
Doctor of Economics
Baltic State Technical University «Voenmeh» named after D.F.Ustinov, St. Petersburg, Russian Federation
E-mail: nataly65vf@gmail.com

Annotation. The issue of timing of the adaptation of the information security industry of the Russian Federation after the withdrawal of Western vendors from the domestic market and the unstable 2022, which caused other structural changes in the industry, remain open. The issue of the discussion lies in the high competitiveness of products of domestic manufacturers, which at the beginning of 2023 is not capable of influencing the improvement of the quality of information security product components. The authors accepted the conditions under which the solution of the problem of creating their own alternative high-capacity technological IT components in the implementation of the import substitution policy is long-term. The assessment of the prospects for further development of the information security industry of the Russian Federation requires the introduction of an integrated approach: the improvement of instrumental and technical support and the filling of security elements should be supported by high-quality legal regulation. Thus, the article identified and substantiated the need for the development of the domestic information industry in a new vector: the transition from a developing form of information security (IS) to a productive one. In this connection, the methodological tool of the study was to study the list of updated provisions of legal acts regulating measures to ensure information security today, and to compare the current standards with the conditions for the development of the cyber industry of the Russian Federation in the period 2022–2023. On this basis, a list of key vulnerabilities of the IT infrastructure of the Russian Federation in the processes of import substitution of information security elements is presented. Guided by the assessment of the sufficiency of the existing technical IT support and taking into account the identified shortcomings of the regulatory legal acts, directions for reforming the organization of the IT infrastructure and methodology for ensuring the country's information security at all levels (individuals, organizations and the state) were developed.

Keywords: IT infrastructure; CII subjects; cyber attacks; specialist; cyber literacy; fraud; Information Security; incident; vulnerability; software (software); information security tools (ISZ); Unified Phone Call Verification Platform (SVVV)