УДК 330.47

ИНСТРУМЕНТЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЭКОНОМИКЕ РОССИИ

М.Е. ЛИСТОПАД, доктор экономических наук, доцент, профессор кафедры мировой экономики и менеджмента, Кубанский государственный университет
e-mail: mlistopad@inbox.ru

А.З. НАГУМАНОВ, магистрант программы «Экономическая безопасность и устойчивость», Кубанский государственный университет
e-mail: arthur.nagumanov@yandex.ru

Аннотация

В статье рассматривается вопрос оценки эффективности системы безопасности с точки зрения системы обеспечения информационной безопасности (информационные ресурсы информационной системы в организации). Уровень безопасности информационной системы в организации определяется инструментами эффективности системы безопасности. Эффективность системы информационной безопасности в основном зависит от функциональных свойств ее компонентов и других факторов, возникающих в ее среде.

Ключевые слова: *инструменты, механизмы, информационная безопасность, анализ, цифровая среда.*

Тенденции современного мира сформировали новые критерии конкурентных преимуществ государств для обеспечения информационной безопасности. В роли локомотивов на сегодня выступает цифровая экономика, развитие инфраструктурного блока, компьютеризация процессов управления и производства и интеллектуальная собственность в ИКТ.

Инструменты обеспечения информационной безопасности – это совокупность корпоративных правил, стандартов работы и процедур защиты безопасности данных, сформированных на основе аудита информационной системы компании, а также анализа существующих рисков безопасности в соответствии с требованиями нормативных документов Российской Федерации и положениями стандартов в области информационной безопасности. Это особенно важно для российских компаний, активно взаимодействующих с зарубежными партнерами. Решая проблему информационной безопасности, разработка единой политики информационной безопасности компании занимает ведущее место; поэтому данная статья будет посвящена рассмотрению этих вопросов. Авторы настоящего исследования исходят из объективно-субъективной предопределенности любых явлений и процессов внешнего мира. В этом формате исследование опирается на общенаучные методы в виде системного анализа, а также группировки эмпирических данных и нормативных требований; диалектического (формального) мышления, такого как синтез (анализ), либо индукция (дедукция), либо гипотеза (аналогия); плюс специализированные подходы нормативного изучения в виде правовой справки исторического (сравнительного) характера с интерпретацией нормативных требований. В результате проведенной оценки можно сделать вывод, что на сегодня ключевым индикатором в развитии цифрового государства выступает обеспечение целостности жизненных и социальных интересов граждан, которые напрямую зависят от обеспечения информационной безопасности.

Это исследование представляет собой научный обзор современных способов обеспечения информационной безопасности как в

прикладном, так и в юридическом контекстах [1].

Уже 20 лет существует неотъемлемая тенденция в прогрессивном росте цифровой экономики по всему миру. С геометрической прогрессией развивается весь ИКТ-комплекс, полностью поглощая зоны управления и промышленности. Для обычного человека это в первую очередь новый опыт в части коммуникативных процессов либо получения доступа к справочно-информационным данным, а также ежедневное чтение информационных сводок либо покупка необходимых продуктов на интернет-площадках с возможностью в любой момент времени воспользоваться личным кабинетом на портале государственных услуг для получения справки или иной информации в электронном виде от представителей власти, заканчивая дистанционным обучением. Внедрение в повседневную жизнь информационно-технологического комплекса с различными типами коммуникативной связи позволило объектам бизнеса по-новому взаимодействовать с клиентами, а также побудило к созданию новых видов компаний и предпринимательской деятельности с последующим становлением различных форм деятельности в рыночной экономике. Сегодня ИКТ создает новую веху экономического (социального) развития государства. Институт статистических исследований и экономики знаний НИУ ВШЭ совместно с Росстатом в конце 2016 г. провел оценку сферы ИКТ в РФ и установил около 170 тыс. компаний. Их общая величина капитализации составила 3,2% от ВВП страны.

Сегодня, переходя в цифровую среду, капитализация организаций приближается к таким областям, как строительство (6,4 % от ВВП), сельскохозяйственный кластер (4,7 %), финансовая зона (4,8 %). На диаграмме (рис. 1) можно увидеть вариативную тенденцию затрат организаций на развитие в области ИКТ за 1,5 десятилетия в сопоставлении с общими издержками в экономике [7].

На протяжении нескольких лет Правительство разрабатывало федеральные программы по развитию государства в области цифровой экономики. Основными документами стали Доктрина по информационной безопасности (ИБ) и стратегия экономической безопасности (ЭБ). Оба документы составлены с прогнозом до 2030 г. Детальную оценку содержащихся там нормативов и предписаний можно свести к двум трактовкам. Первая характеризуется тем, что экономическая и информационная безопасность взаимозависимы и неотъемлемы друг от друга. Вторая обусловлена тем, что вектор программ нацелен на поиски решений значимых проблем в области обеспечения информационной безопасности в рамках становления цифровой экономики.

Наряду с выполнением поставленных задач из перечисленных выше программ была утверждена новая Федеральная программа «Цифровая экономика РФ». Ключевое место в этом документе занимает обеспечение информационной безопасности частного и бизнес-сектора экономики [2].

Все утвержденные и действующие программы построены на единых критериях ИБ:

– применение отечественных нормативов (требований) для обеспечения криптографической безопасности данных;

– российское ИКТ оборудование и ПО имеет приоритет над зарубежными аналогами;

– все составляющие надежности и сохранности данных (конфиденциальность, целостность, доступность) необходимо обеспечить преимущественно посредством отечественного оборудования.

Перечисленные критерии указывают на особую степень контроля при решении проблем в области обеспечения ИБ в условиях цифровизации рыночной экономики.

В результате осуществляемых правительственными органами мер с принятием новых постановлений и нормативных актов, а также при постоянно меняющейся внешней политике на отечественном рынке появляются новые тренды в сфере ИБ. Одна из причин – внутренние и внешние угрозы со стороны правительств, компаний либо частных групп.

За последние 7 лет можно наблюдать увеличение динамики затрат и всего рынка в области ИБ. К такому выводу пришла компания «Информзащита» на основании многолетней

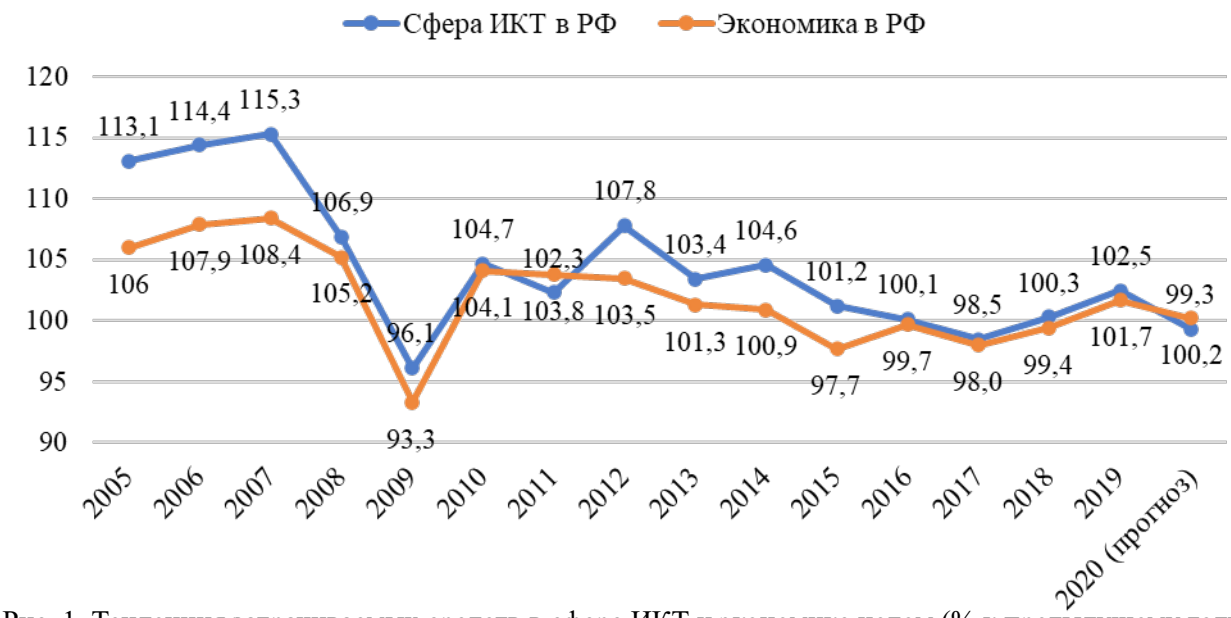

Рис. 1. Тенденция затрачиваемых средств в сфере ИКТ и экономике целом (% к предыдущему году). Составлен автором по [8]

оценки и сбора данных (рис. 2). Одним из критериев роста затрат и темпов внедрения ИКТ стали новые условия ФСТЭК России для государственных (региональных) органов в части использования правительственных систем информационного назначения.

Стандартная концепция ИБ, предусматривавшая целостность, доступность и конфиденциальность, поэтапно превращается в структуру, опирающуюся на принципы киберустойчивости и доступности данных. В этом случае основной акцент в организации должен ставиться на умение противодействовать внешним (внутренним) цифровым угрозам, а также в максимально короткие сроки возобновлять работу всех ИКТ-систем при отключении, взломе или выходе из строя. Можно наблюдать смещение значимых критериев в части рисков, связанных с ИБ, защитой данных от всевозможных взломов, проникновений либо угроз.

За последние 2 года по сведениям отчетов аналитической компании McAfee ущерб, нанесенный киберпреступниками, оценен в 1,5 млрд дол., что составляет примерно 2 % от ВВП всех стран. Если брать динамику за 5 лет, то размер ущерба увеличился на 40 % в 2019 г. по сравнению с 2014 г. Ключевыми индикаторами роста числа киберпреступлений стали: распространение электронной денежной валюты – криптовалюты; атаки хакерских группировок; увеличение рынка криминальных услуг в сфере ИБ. К примеру, с 2017 по 2019 г. хакерам удалось украсть около 350 млрд дол. у почти 2 млн граждан в нескольких десятках стран. Это в очередной раз доказало, насколько низкий уровень знаний об ИБ рядового пользователя в части принятия онлайн-решений [3].

Подаувляющее большинство кибервзломов нацелены на финансовые организации. Из аналитических сводок ПАО «Сбербанк» следует, что годовой ущерб от всех киберугроз составляет 1 трлн дол., а уже через пару лет он вырастет в 10 раз и составит около 10 трлн. дол. В качестве основного механизма для взлома злоумышленники используют социальную инженерию. На её долю приходится около 82 % преступлений. Из всех совершенных краж и утерь данных только 23 % попадает в аналитические отчеты и сводки, так как большинство компаний и физических лиц стараются скрыть информацию про утечки информации. Наиболее популярным во всех странах признан вирус-шифровальщик вида WannaCry. После установки такого ПО блокируются все окна и невозможно работать в системе. Единственное окно – с требовани-

ем о переводе фиксированной суммы денег на электронный кошелек после чего блокировка будет снята.

В большинстве случаев величина нанесенного вреда при случившемся взломе обусловлена своевременной готовностью организации принять удар, реально дать оценку возникшей ситуации, а также от компетентных, правильных (отлаженных) действий ответственных сотрудников. Тем не менее анализ, который был сделан работниками Positive Technologies, дал понять, что в большинстве случаев организации редко применяют специальное ИКТ-оборудование либо ПО для обеспечения ИБ. В результате получается, что только 14 % промышленных предприятий на постоянной основе используют тесты систем ИКТ на фактор взлома. SIEM-системы применяют 18 % опрошенных компаний, а межсетевые экраны типа WAF используют только 23 %. В одной трети всех предприятий не используется система инвентаризации либо различные инструменты контроля за выявлением потенциальных угроз со стороны ПО либо ИКТ-системы. Всего лишь четверть компаний проводит постоянное обучение сотрудников в части ИБ. Более половины организаций не выявляют степень защищенности корпоративной сети. Каждая пятая компания не обеспечивает контроль над установкой и обновлением ПО.

По данным исследования, проведенного компанией «СерчИнформ» в мае 2020 г., выяснилось, что меньше половины всех компаний, которые используют дистанционный способ работы сотрудников, обеспечены средствами контроля за счет специализированного ПО. В 70 % организаций, работающих по такому принципу, не сформировалась объективное представление о потенциально возможных внутренних угрозах в ИБ. В итоге более 30 % компаний не в состоянии оценить, как изменяется количество угроз ИБ в связи с экстренным переводом сотрудников на удаленную работу [6].

Если организация правильно оценивает степень своей компетенции в сфере ИБ и понимает уровень рисков и угроз со стороны киберпреступников, это благоприятно сказывается на результативной стратегии по организации системы ИБ, что побуждает заново переоценивать не только степень финансирования кластера ИБ, но и всю структуру организации. За счет этого в последние годы выросло количество сделок, совершенных в рамках обеспечения ИБ, их сумма составила более 60 млрд р.

Одним из ключевых инструментов в рамках обеспечения ИБ в последние годы является

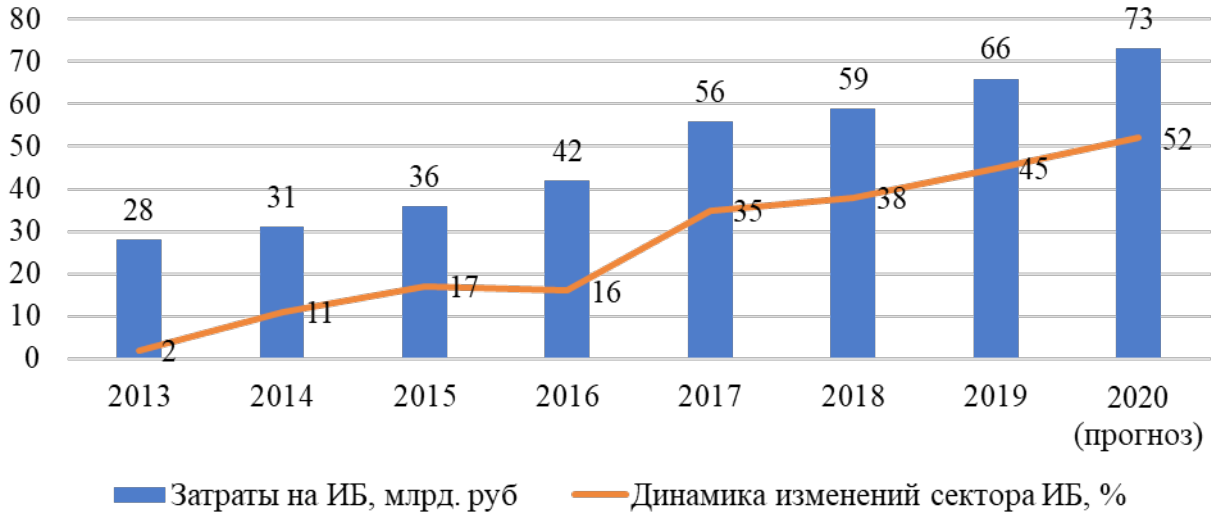

Рис. 2. Затраты в сектор ИКТ (составлен автором по [4])

вовлеченность высших звеньев руководства компаний. Такие меры были вызваны утверждением нового закона «О безопасности критической информационной инфраструктуры Российской Федерации». И есть примечание о том, что, если не будут выполняться утвержденные нормы в обеспечении ИБ, то будет применена уголовная ответственность [9].

Эффективность системы безопасности зависит от следующих факторов:

– количество охраняемых информационных ресурсов информационной системы;

– число рисков и уязвимостей, характерных для информационных ресурсов;

– количественный и качественный выбор технических и/или организационных конфигураций;

– эффективность отдельных конфигураций безопасности;

– метод управления различными конфигурациями механизмов безопасности;

– подход к оценке эффективности (прикладной метод оценки эффективности).

Информационная безопасность очень важна, поэтому для ее обеспечения необходимо внедрить эффективную систему управления информационной безопасностью, «движимую» надежной системой безопасности. Информационная безопасность может быть гарантирована путем внедрения соответствующих конфигураций безопасности, определенных на этапе проектирования системы безопасности и тестирования на этапе эксплуатации трассы или внутреннего аудита. В целом надлежащим образом построенные и реализованные технические и организационные конфигурации безопасности должны: уменьшить потенциальные потери и уменьшить уязвимость ресурсов, повысить устойчивость к атакам (превентивные меры), поскольку они останавливают выбросы негативных последствий и могут способствовать выявлению рисков (меры по выявлению рисков). Эффективная система безопасности может не только предотвратить риск, но и снизить его эффективность и вероятность возникновения.

Уровень безопасности информационных ресурсов информационной системы в организации является результатом правильно выбранных конфигураций безопасности в отношении набора защищенных информационных ресурсов и определенных видов рисков и уязвимости.

Наборы рисков и уязвимости меняются со временем. Это ведет к изменениям в наборе активных мер безопасности. Обновленный набор мер безопасности требует перенастройки (отображения) набора используемых в настоящее время конфигураций безопасности в набор вновь созданных конфигураций безопасности.

Анализ рисков и управление информационной безопасностью должны быть неотъемлемой частью процесса принятия решений, который способствует сознательному и правильному выбору, установлению приоритетов деятельности и признанию альтернативных направлений действий в случае существующих угроз, событий и критической ситуации. Правильный анализ рисков основан на передовой практике и доступных источниках информации, таких как исторические данные, опыт, информация об обратной связи от всех заинтересованных сторон, замечания, прогнозы и мнения экспертов, включая их разнообразие и ограничения, следовательно, он в то же время способствует сбору данных из многих источников, включая и уровень их неопределенности (см. таблицу).

Таким образом, инструменты обеспечения ИБ в России предполагают усиление роли информационных технологий и увеличение доли ИТ-отрасли в ВВП страны. Одновременно с этим происходит рост потребности в защите информационных ресурсов и критически важной информационной инфраструктуры. За последние годы в Российской Федерации сделано много для развития отечественного рынка информационной безопасности, ведущими потребителями услуг которого являются организации, обрабатывающие большие объемы персональных данных и финансовой информации. Тренды на рынке информационной безопасности, сформировавшиеся в последние годы под воздействием российского законодательства и разнообразия информационных угроз, свидетельствуют о повышении

Механизм управления информационными рисками в цифровой экономике (составлена автором по [5])

Форма управления	Контрольные действия		
	Существенный аспект	Фактор времени	Полученный фактор
Гибкие	Адаптация решений по управлению информационными рисками в текущей ситуации	Осуществляется во время проведения информационного риска	Профилактика некоторых побочных эффектов
Традиционные	Максимальное снижение негативного воздействия риска на другие события на момент его осуществления и в будущем	Осуществляется с момента возникновения информационного риска	Нераспространение ущерба во времени и пространстве
Инициатива (инновационная)	Применение всех средств воздействия и использование всех источников информации	Осуществляется до возникновения информационного риска	Доведение информационных рисков до листа минимальной возможности их проявления

роли информационной безопасности в условиях цифровой экономики.

Библиографический список

1. *Булатенко М.А., Тарасова Н.В.* Повышение эффективности управления инновационными рисками организаций – как основа обеспечения экономической безопасности государства // Russian Journal of Management. 2019. Т. 7, № 3. С. 46–50.

2. *Северин В.А.* Концептуальные аспекты безопасности информации при производстве и реализации товаров // Безопасность бизнеса. 2017. № 1. С. 30–35.

3. *Итальянцева В.С., Колмацуй А.И.* Информационная безопасность как инструмент обеспечения экономической безопасности предприятия // Актуальные вопросы права, экономики и управления: сб. ст. XII Междунар. науч.-практ. конф. в 2 ч. М., 2018.

4. *Калашников А.О.* Анализ систем классификации защищенности автоматизированных и информационных систем значимых объектов критической информационной инфраструктуры Российской Федерации // Информация и безопасность. 2018. № 1 (4). С. 28–37.

5. *Петров Ю.И.* Обеспечение безопасности информации в облаке федерального органа управления // Информация и безопасность. 2018. № 2 (4). С. 211–220.

6. *Фокина Е.А.* Оценка уровня развития информационно-телекоммуникационного сектора экономики России // Вопросы региональной экономики. 2018. № 1 (34). С. 129–136.

7. Российский интернет-портал и аналитическое агентство TAdviser. 2020 г. URL: http:// www.tadviser.ru

8. Официальный сайт Федеральной службы государственной статистики, 2020 г. URL: http://www.gks.ru/folder/10705

9. Официальный сайт Национального исследовательского университета «Высшая школа экономики» // Статистические сборники ВШЭ, 2020 г. URL: http:// www.hse.ru/ primarydata/