УДК 338.2

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КАК СОСТАВЛЯЮЩАЯ ЦИФРОВОЙ ЭКОНОМИКИ

И.М. ГЛОТИНА, кандидат экономических наук, доцент,
доцент кафедры информационных систем и телекоммуникаций,
Пермский государственный аграрно-технологический университет
e-mail: glotina-i@yandex.ru

Аннотация

Настоящая статья посвящена вопросам информационной безопасности в условиях цифровой экономики. На уровне российского законодательства показана конвергенция проблем информационной и экономической безопасностей. Выделены основные тренды на российском рынке информационной безопасности, формирующиеся под воздействием российского законодательства и изменения спектра внутренних и внешних угроз.

Ключевые слова: *цифровая экономика, стратегия, информационное общество, экономическая безопасность, информационная безопасность, тренды.*

В XXI в. наиболее ярко выраженной тенденцией мировой экономики является опережающее развитие информационных и телекоммуникационных технологий. Для граждан это означает новые формы коммуникации и доступа к информационным ресурсам, начиная с чтения новостей, приобретения товаров в интернет-магазинах, заканчивая онлайн-доступом к сервисам электронного правительства, дистанционным образовательным услугам. Распространение ИКТ для хозяйствующих субъектов связано с изменением принципов взаимодействия с потребителями, переходом к новым формам организации и ведения бизнеса, появлением новых видов экономической деятельности. Информационные и коммуникационные технологии формируют сегодня новый вектор социального и экономического развития страны.

По данным исследований, проведенных Росстатом и Институтом статистических исследований и экономики знаний НИУ ВШЭ, сектор информационно-коммуникационных технологий (ИКТ) в России насчитывал на конец 2016 г. более 166 тыс. организаций, валовая добавленная стоимость которых составляла 3,0 % от ВВП. Генерируемая интернет-экономикой добавленная стоимость сопоставима с результатами деятельности в сельском хозяйстве (4,5% ВВП), финансовом секторе (4,5%), строительстве (6,2%). На рис. 1 показана динамика валовой добавленной стоимости организаций сектора ИКТ за период с 2005 по 2016 г. в сравнении с аналогичными показателями по экономике в целом.

В мае 2017 г. Указом Президента была утверждена «Стратегия развития информационного общества в Российской Федерации на 2017–2020 годы». В этом документе появилось первое официальное определение цифровой экономики: «Цифровая экономика – хозяйственная деятельность, в которой ключевым фактором производства являются данные в цифровом виде, обработка больших объемов и использование результатов анализа которых по сравнению с традиционными формами хозяйствования позволяют существенно повысить эффективность различных видов производства, технологий, оборудования, хранения, продажи, доставки товаров и услуг» [9].

Вслед за указанным документом была утверждена «Стратегия экономической безопасности Российской Федерации на период до 2030 года» [10]. Анализ содержания двух документов приводит к следующим выводам: во-первых, обе стратегии направлены на решение проблем информационной безопасности цифровой экономики; во-вторых, оба документа свидетельствуют о наличии процессов конвергенции информационной и экономической безопасностей.

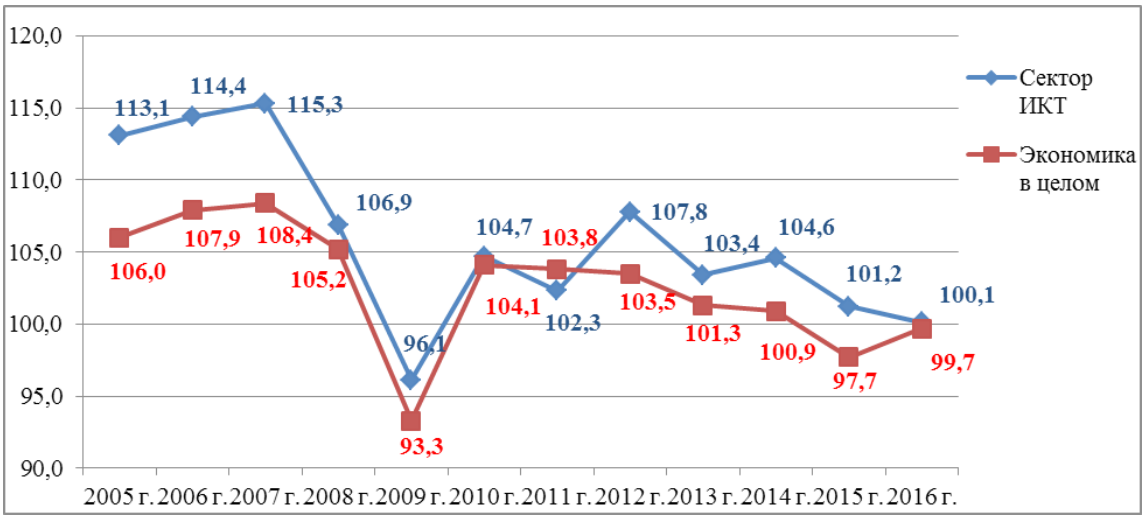

Рис. 1. Динамика валовой добавленной стоимости организаций сектора ИКТ (в % к предыдущему году; в постоянных ценах) (составлен автором на основании данных Росстата и НИУ ВШЭ [1])

В том же году была утверждена Программа «Цифровая экономика Российской Федерации», в рамках которой информационная безопасность стала одним из пяти ключевых направлений [7]. Разработка и реализация мероприятий Программы основаны на следующих принципах информационной безопасности:

– доступность, целостность и конфиденциальность информации и процессов ее обработки должны обеспечиваться за счет использования российских технологий;

– преимущественное использование отечественного программного обеспечения и оборудования;

– использование российских стандартов для криптографической защиты информации.

Все это свидетельствует об особой важности решения проблем информационной безопасности в цифровой экономике.

Под воздействием российского законодательства и изменения спектра внутренних и внешних угроз формируются основные тренды на российском рынке информационной безопасности. Так, анализ данных мониторинга, опубликованных компанией Информзащита, позволил выявить устойчивую положительную динамику роста рынка информационной безопасности за период с 2013 г. по 2017 г. (рис. 2). Стимулом роста послужила реализация требований ФСТЭК России федеральными и региональными органами исполнительной власти в отношении государственных информационных систем [6].

Традиционная модель информационной безопасности, которая долгое время базировалась на конфиденциальности, целостности и доступности, постепенно трансформируется в модель, ориентированную на доступность и киберустойчивость. На первый план выходит способность компаний противостоять информационным угрозам и оперативно восстанавливаться в случае их реализации. Происходит смещение акцентов в сторону рискориентированной безопасности и защиты от разнообразных угроз.

По данным специалистов компании McAfee, мировой ущерб от киберпреступлений только за 2017 г. оценивается примерно в 600 млрд дол., что составляет 0,8% от мирового ВВП. По сравнению с показателями 2014 г. размер ущерба увеличился примерно на 35%. Основными факторами, способствующими росту, явились хакерские атаки, расширение рынка киберкриминальных услуг и распространение криптовалют. Так, в 2017 г. хакеры похитили 172 млрд дол. у 978 млн потребителей в 20 странах мира, на практике доказав, что онлайн-пользователи излишне самоуверены в вопросах кибербезопасности [2].

Целями большинства атак являются компании финансового сектора. По оценкам специалистов Сбербанка РФ, глобальный ущерб от кибератак в 2018 г. составил 1 трлн дол. и в

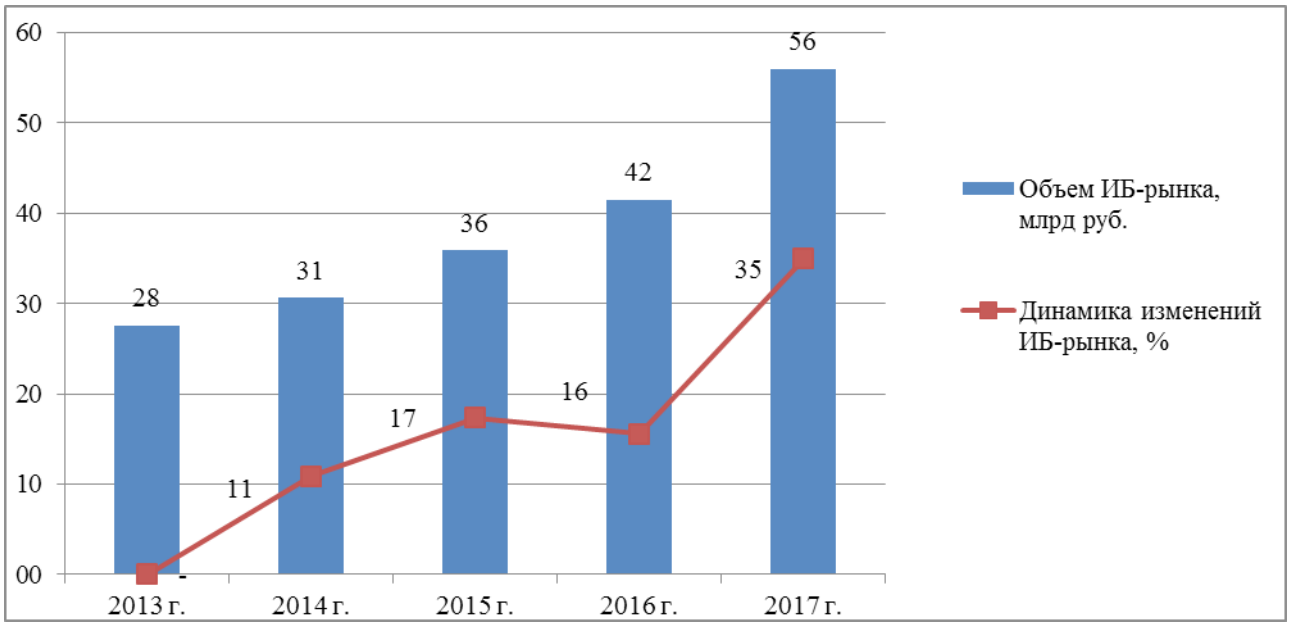

Рис. 2. Годовые объемы рынка информационной безопасности (составлен автором по [6])

2022 г. прогнозируется рост этой суммы до 8 трлн дол. [5]. При этом более 80% хакерских атак основано на методах социальной инженерии. Однако общественности становится известно лишь о 20% инцидентов, поскольку компании стараются не раскрывать эту информацию. Из всех наиболее известных в мире киберугроз можно назвать вирусы-шифровальщики типа WannaCry [5].

В случае возникновения инцидента информационной безопасности размер ущерба во многом зависит от готовности компании своевременно и адекватно реагировать на него и корректности действий сотрудников. Однако исследование, проведенное сотрудниками компании Positive Technologies, показало, что на практике компании редко используют специализированные инструменты обеспечения безопасности. Например, межсетевые экраны уровня приложений (WAF) применяют лишь 23% всех опрошенных промышленных компаний, лишь 17% используют SIEM-системы и только 13% промышленных компаний регулярно проводят тесты на проникновение. В 33% компаний никогда не проводились инвентаризация и контроль за появлением небезопасных ресурсов в пределах периметра сети предприятия. В 40% компаний никогда не проводился анализ защищенности корпоративных беспроводных сетей; 23% обследованных компаний не контролируют установку обновлений программного обеспечения, а регулярное обучение сотрудников основам информационной безопасности проводят только 23% компаний [2].

Осознание компаниями опасности киберугроз способствует более эффективному планированию стратегии обеспечения безопасности. Поэтому на уровне компаний в настоящее время происходит переосмысление роли информационной безопасности как части общей корпоративной бизнес-стратегии и увеличение расходов на защиту информационных ресурсов. Как следствие, в 2017 г. объем заключенных ИБ-контрактов составил 56 млрд р. (рис. 3).

Еще один тренд, который прослеживается на рынке информационной безопасности, – вовлечение высшего руководства предприятий в вопросы информационной безопасности. Это вызвано законом «О безопасности критической информационной инфраструктуры Российской Федерации», который ввел уголовную ответственность за несоблюдение требований информационной безопасности, если это повлекло тяжкие последствия [11].

Высокие темпы роста отрасли информационной безопасности в России сопровождаются ростом кадрового дефицита. Потребность в ИТ-специалистах в 2018 г. составляет 350 тыс. сотрудников, поэтому подготовка кадров входит в число основных приоритетов

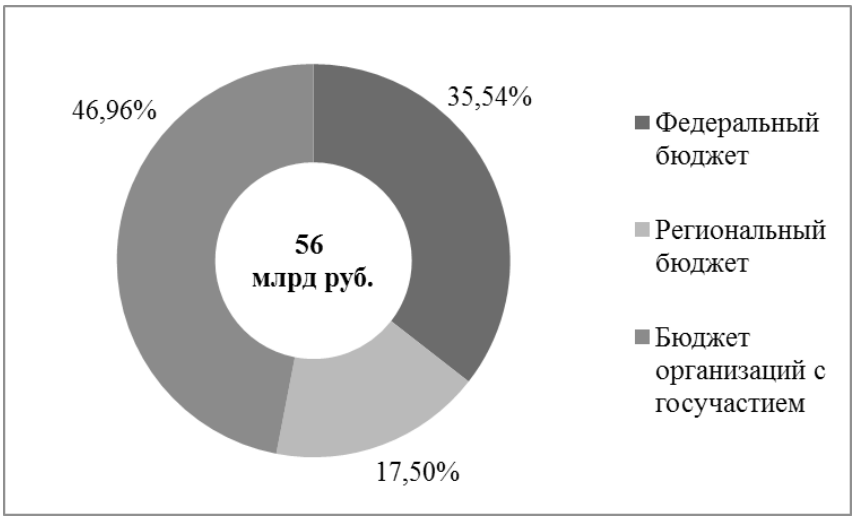

Рис. 3. Объем и составляющие ИБ-рынка в 2017 г. (составлен автором по [6])

Стратегии развития отрасли информационных технологий в РФ на 2014–2020 гг. и на перспективу до 2025 г., утвержденной в октябре 2013 г. [8].

Самый большой спрос на ИТ-специалистов наблюдается в области разработки мобильных приложений и информационной безопасности — на сегодняшний день в этих сферах открыто почти по 3 тыс. вакансий (см. таблицу).

Потребности ИТ-сферы в специалистах (по материалам [3])

Сфера	Количество вакансий
Мобильные приложения	2981
Информационная безопасность	2862
Frontend	2007
Backend	1703

Каналов, по которым передается корпоративная информация, становится больше, а контролировать их все сложнее. Однако самым непредсказуемым источником угроз информационной безопасности остается человек. Поэтому именно на человека смещается фокус интереса разработчиков. В результате на рынке информационной безопасности наблюдается тренд на создание технологий, предупреждающих инциденты за счет анализа поведения пользователя, выявления аномалий в его действиях. Подобные технологии уже используются Сбербанком РФ.

Главным источником угроз информационной безопасности является индустрия вредоносных сервисов, которая постоянно наращивает обороты и приобретает все больше черт развитого рынка с проработанными бизнес-моделями. Поэтому государство и ряд отраслей реагируют на угрозы созданием координационных органов, которые задают стандарты обеспечения ИБ и служат площадками обмена опытом. Примерами таких структур являются Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере FinCERT Банка России и Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА).

На сегодняшний день создать превентивную систему, которая была бы в состоянии обеспечить абсолютную защиту, практически невозможно. Поэтому на передний план выходит задача обнаружения и грамотного реагирования на угрозы. В связи с этим на рынке активно развиваются инициативы SOC (Security Operation Center). Они включают три составляющих:

– технологии защиты;

– сотрудники, ответственные за информационную безопасность;

– регламенты и правила, позволяющие выстроить четкие процессы по предотвращению атак, а также реагированию на инциденты информационной безопасности в случае их возникновения.

Таким образом, развитие цифровой экономики России сопровождается усилением роли информационных технологий и увеличением доли ИТ-отрасли в ВВП страны. Одновременно с этим происходит рост потребностей 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 роли информационной безопасности в условиях цифровой экономики.

Библиографический список

1. Индикаторы цифровой экономики: 2017: статистический сборник / Г.И. Абдрахманова [и др.]. М., 2017.

2. Киберпреступность и киберконфликты: Россия. URL: http:www.tadviser.ru/index.php

3. Обзор рынка труда в сфере ИТ. URL: https://www.crn.ru/news/detail.php?ID=124951

4. Оценка российского ИБ-рынка в 2017 г. URL: https://infosec.ru

5. Потери банков от киберпреступности. URL: http://www.tadviser.ru/index.php

6. Приказ ФСТЭК России от 11.02.2013 № 17 (ред. от 15.02.2017) «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах». URL: http://consultant.ru

7. Программа «Цифровая экономика Российской Федерации». Утв. Распоряжением Правительства Российской Федерации от 28.07.2017 № 1632-р // Собрание законодательства Российской Федерации. М., 2017. 7 августа. № 32. Ст. 5138.

8. Распоряжение Правительства РФ от 01.11.2013 № 2036-р «Об утверждении Стратегии развития отрасли информационных технологий в Российской Федерации на 2014–2020 годы и на перспективу до 2025 года». URL: http://www.consultant.ru/

9. Указ Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2020 годы». URL: http://consultant.ru

10. Указ Президента РФ от 13.05.2017 № 208 «О Стратегии экономической безопасности Российской Федерации на период до 2030 года» . URL: http://consultant.ru

11. Федеральный закон от 26.07.2017 №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». URL: http://www.consultant.ru/