«ПОДВОДНЫЕ КАМНИ» ЦИФРОВОЙ ЭКОНОМИКИ

И. Э. Жадан, Л. Н. Мамаева

Саратовский государственный университет, Россия
Саратовский социально-экономический институт (филиал)
РЭУ им. Г. В. Плеханова, Россия
E-mail: inga645@bk.ru, L.Mamaeva2014@yandex.ru

В научной статье предлагаются решения проблем экономической безопасности цифровой экономики. Основные подходы связаны со строительством инфраструктуры борьбы с киберпреступностью на региональном уровне, образованием, технологическим совершенствованием ИТ-программного обеспечения и аппаратного обеспечения, регулированием, использованием финансов и страхования, поддержкой средств массовой информации и созданием кибер- преступления awareculture.

PITFALLS OF THE DIGITAL ECONOMY

I. E. Zhadan, L. N. Mamaeva

The scientific article offers solutions to the problems of economic security of the digital economy. The main approaches are related to the construction of infrastructure to combat cybercrime at the regional level, education, technological improvement of it software and hardware, regulation, use of Finance and insurance, media support and the creation of cyber crime awareness culture. Institutional, systemic, structural-functional and statistical methods were used as the main methods of analysis.

Следует отметить, что развитие современной экономики основанной на использовании новейших цифровых технологий, создании новых материалов, анализе больших массивов данных, разработке новых систем управления приводит к изменению принципов конкурентных отношений. Конкурентная борьба происходит на базе новых цифровых платформ. В таких условиях цифровая экономика изменяет понимание и сущность экономической безопасности государства, бизнеса, домохозяйства, частных лиц порождает новые угрозы и риски для участников экономических процессов и связей [1].

Совершенно очевидно, что расширение цифрового сервиса, индивидуализация многих видов услуг повышает угрозу мошенничества при снижении контроля со стороны пользователей или провайдеров. Риски утечки информации требуют повышения уровня защиты электронных систем. В настоящий момент киберугрозы и ущерб от киберпреступников вышли на второе место в мире после техногенных катастроф.

В 2016 г. произошло более 70 млн. атак на российские объекты экономической инфраструктуры, более 52,5 млн. атак, по данным Совета безопасности РФ, проведены на сайты российских госорганов. Исследования «Allanz Risk Barometer» показали, что ущерб российской экономики в 2016 г. от киберпреступлений составил более 203,3 млрд руб., что соответствует половине годового финансирования здравоохранения или 0,25% ВВП РФ. В последнее время из-

за снижения порога масштаба деятельности организованная киберпреступность направлена на кражи личностных данных через мобильные устройства и финансовые мобильные приложения.

С 1 января 2017 г. в РФ действует новый стандарт Банка России СТО БР ИББС -1.3-2016 «Сбор и анализ технических данных при выявлении и расследовании инцидентов информационной безопасности при осуществлении переводов денежных средств». Этим документом ЦБ РФ устанавливаются требования по информационной безопасности в финансовых организациях и операционных платёжных системах, что должно содействовать сохранению безопасности банковской системы. Развитие и контроль информационной безопасности банковской системы, взаимодействие со службами безопасности коммерческих банков осуществляет центр кибербезопасности Центрального Банка РФ.

Таблица 1

Затраты на ликвидацию последствий кибератак (составлено по оценкам по Group-IB)

Год	Сумма	Риски
2015	79,8 млрд. рублей	риск фишинга – 21 %
2016	159,6 млрд. рублей	риск фишинга – 30%

В последнее время мы можем наблюдать возникновение нового вида преступности – организованной киберпреступности, которое заставляет экономических агентов и государство выделить основные задачи по предотвращению киберугроз в следующих направления:

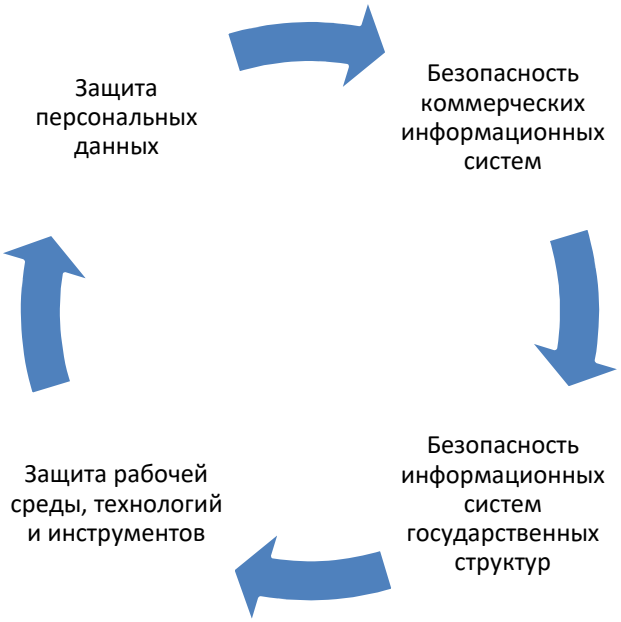
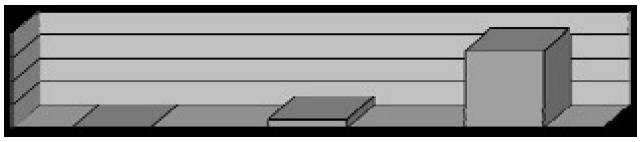


Рис. 1. Направления по предотвращению киберугроз (составлено авторами)

Массированные DDoS-атаки, направленные не только на банки, но и на ICO новых криптовалют и их инфраструктурных объектов, возросли на порядок. Причиной этому является недостаточное количество необходимого защитного оборудования, программного обеспечения и мощностей, отсутствие специальных сервисов, кроме этого многие гибридные решения защиты не решают полностью проблему безопасности и необходим переход к комбинированным,

облачным и операторским технологиям защиты информации. По данным ЦБ РФ за 2017 г. количество кибератак на российские банки увеличилось в 2,3 раза.

Несмотря на то, что информационная безопасность является основой конкурентоспособности современного бизнеса по итогам обследования 248 российских фирм компанией «PwC» в 2017 г. оказалось, что 40% российских компаний не имеет стратегии информационной безопасности, а в 50% компаний отсутствует план реагирования на инциденты информационной безопасности, при этом у 48% компаний нет программ обучения сотрудников направленных на повышение информационной безопасности бизнеса. Такое отношение к кибербезопасности приводит к большому ущербу и потерям экономики. Но, в последнее время ситуация стала меняться, так, на основе рисунка 2 мы можем наблюдать что инвестирование в кибербезопасность предприятиями стала резко возрастать.



0,3% (2015 г.) 12% (2016 г.) 65,79% (2017 г.)

Рис. 2. Объем инвестиций в кибербезопасность

Инновационный, цифровой уклад жизни, внедрение новых информационных программ и технологий, задачи анализа больших данных (БигДата), смена технологической эпохи, появление технологий Блокчейн, Интернета вещей (IoT), заставляет компании по-другому относиться к собственному человеческому ресурсу, знаниям, к знаниевым активам, которые имеют свою специфику, так как пока не оцениваются с позиции редкости и истощаемости.

В нашей стране реализация программы «Цифровая экономика России», утверждённая Правительством РФ 28 июля 2017 г., которая задумана осуществляться по следующим направлениям [3]: нормативное регулирование киберпространства; образование и кадры; формирование исследовательских компетенций и технологических заделов; IT-инфраструктура; кибербезопасность.

Программа должна перевести на новые цифровые, инновационные рельсы экономику, бизнес, социальную сферу, государственное управление и городское хозяйство. Для этого были разработаны подходы и дорожные карты по созданию электронного гражданского оборота и цифровой среды доверия с использованием киберфизических систем, намечены цели по изменению трудового законодательства и устранению законодательных барьеров, препятствующих развитию цифровых технологий. Необходима стандартизация цифровой инфраструктуры, нахождение облачных решений хранения данных, создания цифровых платформ и цифровых кластеров. В настоящее время в данном направлении мы уже можем наблюдать небольшие подвижки.

Россия находится в условиях длительных санкций и сложившейся зако-

номерности захвата технологической основы промышленного и информационного развития американскими, азиатскими и европейскими компаниями, что осложняет переход страны к цифровой экономике во всех направлениях хозяйствования. В связи с этим необходимо выработать новые государственные методы регулирования киберпространства, принципы разумного протекционизма отечественным «интернетным» компаниям и операторам. Вопрос перевода обработки данных с зарубежных на местные сервера, в целях информационной безопасности и защиты данных, становится ещё более актуальным. Необходимо увеличить долю закупок оборудования связи и софта отечественного производителя, использовать сертификацию и лицензирование продукции и интернет-услуг поставляемых из-за рубежа, блокировать работу интернеткомпаниям нарушившим законодательство. Российская Ассоциация компаний интернет-торговли разработала программу защиты интересов граждан Российской Федерации от угроз интернет-услуг и торговли. Программа предусматривает шаги по обеспечению выравнивания конкурентных условий для онлайн-ритейлеров.

Внешние вызовы, глубокая цифровая импортозависимость экономики, диктуют российским компаниям задачу участия в острой международной конкуренции по созданию добавленной стоимости в киберсреде, что требует нахождения путей коммерциализации и защиты интеллектуальной собственности, законодательного решения вопросов оборота цифровых технологий и программного обеспечения, обеспечения информационной безопасности при запуске цифровых платформ и технологий. Для этого необходимо обеспечить безопасность основных инструментов цифровой экономики – защиту электронных подписей и платежей, токенов, симкарт, он-лайн сервисов, защиту информации в электронных облаках, баз данных, развитие криптографии и технологий аутентификации личности, защиту системы электронного документооборота, каналов передачи, защиту серверов, безопасность деятельности коммерческих и государственных электронных торговых площадок, научных лабораторий. Отдельной задачей стоит защита от киберугроз искусственного интеллекта, роботов, беспилотных летательных аппаратов и транспорта, новейших технологий Blockchain, интернета вещей (IoT).

Главные угрозы информационной безопасности цифровой экономики на сегодняшний день составляют вирусы-шифровальщики, например «cryptolocker», проникающие не только в личные компьютеры, но и в сети стратегических объектов и могут вызвать техногенные катастрофы. Потери и ущерб от таких проникновений исчисляется в мире сотнями миллионов долларов. Серьёзную угрозу представляют атаки на публичные размещения акций (ICO) компаний в блокчейн пространстве с целью хищения активов или уничтожения платформ (справочно: объём ICO мессенджера Telegram в 2018 г. составляет более 1,2 млрд. долларов), атаки на криптовалютную инфраструктуру и сервисы, кражи электронных кошельков, паролей, атаки на банки и т.д. По данным Group-IB за последние три года количество киберинцидентов в России увеличилось на 72%, а ущерб от них на 200 % с прогнозом увеличения в три раза [2].

Государству для перевода экономики в киберпространство нужен новый

уровень знаний населения и социальные сети становятся не развлечением, а рабочим инструментом обучения граждан необходимым навыкам и умениям, возможным мостиком общения с госорганами [4]. Лицензионные платежи иностранным компаниям составляют существенную долю в себестоимости отечественных цифровых товаров и услуг.

В эпоху быстрого развития цифровых технологий основные направления поддержания экономической безопасности страны и пути решения по предотвращению угроз и рисков киберпреступлений состоят в следующем:

1. Постоянный обмен информацией об информационных инцидентах и технологиях защиты между компаниями и общественными организациями на международном уровне. Внедрение на объектах центров круглосуточного реагирования на киберинциденты для выявления, анализа и предотвращения киберугроз.

2. Повышение компетенций в информационной безопасности IT-специалистов, всех служб компаний и госструктур, организация взаимодействия бизнес-подразделений, «айтишников» и отделов экономической безопасности.

3. Дальнейшая работа центра кибербезопасности Центрального Банка Российской Федерации по повышению безопасности банковской системы и платёжных систем.

4. Постоянное освещение в средствах массовой информации результатов борьбы с киберпреступностью.

5. Распространение цифровой «гигиены» со школьной скамьи, организация школьных программ, уроков киберграмотности.

6. Повышение технического обеспечения информационной безопасности систем, защита автоматизированных систем управления технологическими процессами от вредоносного программного обеспечения.

7. Законодательное регулирование киберпространства, использования криптовалют и блокчейнтехнологий.

8. Финансирование программ кибербразведки по поиску киберпреступников и уничтожению преступного бизнеса.

9. Скорейшая доработка и реализация программы «Цифровая экономика России».

10. Запуск новых продуктов и программ страхования от киберугроз.

11. Инициирование Российской Федерацией действий по принятию Организацией Объединённых Наций моратория на использование кибероружия.

СПИСОК ЛИТЕРАТУРЫ

1. *Жадан И. Э.* Инофрмация и знания – основные категории экономики XX1 века // Международная научная практическая конференция 31 мая 2017 г. «Проблемы и перспективы развития гуманитарных и социальных наук»: сборник научных трудов / Под отв. ред. Ж. А. Шиповал - г. Белград. Изд.: ООО Агенство периодичных научных исследований АПНИ. Ч. 4. 2017. 138с.

2.*Мамаева Л. Н.* Характерные проблемы информационной безопасности в современной экономике. // Информационная безопасность регионов. 2016. № 1 (22).

3. Программа «Цифровая экономика Российской Федерации» 28.07.2017. [Электронный ресурс]. URL: http://government.ru/rugovclassifier/614/events/ (дата обращения: 29.07.2018).

4.*Удалов Д. В., Мамаева Л. Н., Манахова И. В*. и др. Государственная политика в сфере обеспечения национальной безопасности: экономико-правовой аспект. Саратов. 2016.

ПОДХОД К МОДЕЛИРОВАНИЮ ДЕМОГРАФИЧЕСКИХ ПРОЦЕССОВ ПРИ ПЛАНИРОВАНИИ РАЗВИТИЯ ПЕНСИОННОЙ СИСТЕМЫ В РФ

М. Г. Жиц

Саратовский государственный университет, Россия
E-mail: zhits.maria@gmail.com

Статья посвящена актуальному вопросу реформирования пенсионной системы РФ. В статье рассматриваются факторы, влияющие на демографические процессы, которые необходимо учитывать при планировании развития пенсионной системы. Отмечены некоторые особенности, требующие дифференцированного подхода при составлении прогнозов, как по каждому региону, так и по государству в целом. Предлагается подход, основанный на моделировании отдельных процессов, а не всей системы, для более гибкого учета конкретных явлений.

APPROACH TO DEMOGRAPHIC PROCESSES MODELING IN THE PLANNING OF THE PENSION SYSTEM DEVELOPMENT IN RUSSIAN FEDERATION

M. G. Zhits

The article is concerned with the issue of the Russian Federation pension system reforming. The article examines the factors influencing the demographic processes, which have to be taken into account in planning of the pension system development. Some features requiring a differentiated approach in making forecasts, both for each region and for the state as a whole, are noted. The approach based on the individual processes modeling instead of the entire system one, is proposed for more flexible registration of specific phenomena.

Пенсионная система, как правило, является крупнейшим блоком страхования в любом государстве, поддерживающем пенсионное обеспечение своих граждан по завершении последними своей трудовой деятельности. Российская Федерация в настоящее время осуществляет масштабную реформу системы пенсионного обеспечения, потребность в которой вызвали сложные демографические условия, сложившиеся в результате взаимодействия целого ряда факторов. Все это ставит задачу усовершенствования используемых методов демографического планирования, чтобы своевременно замечать и учитывать различные социально-экономические явления, влияющие на стабильность пенсионной системы в РФ.

С нашей точки зрения, демографическая модель должна учитывать целый