ПРОБЛЕМЫ СОЦИАЛЬНО-ЭКОНОМИЧЕСКОГО РАЗВИТИЯ

Асаул В.В., Михайлова А.О.

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ФОРМИРОВАНИЯ ЦИФРОВОЙ ЭКОНОМИКИ

Аннотация. *Обеспечение информационной безопасности в современных условиях становления цифровой экономики является одной из приоритетных задач, как на государственном уровне, так и на уровне отдельных организаций. В статье проанализированы основные мировые тенденции в области обеспечения информационной безопасности, рассмотрены способы решения проблем сохранности цифровых данных, а также предложены механизмы обеспечения информационной безопасности как уровне государства, так и с точки зрения отдельных экономических субъектов.*

Ключевые слова. *Цифровые технологии, цифровая экономика, информационная безопасность, цифровая трансформация, конкурентоспособность, государственное регулирование.*

Asaul V.V., Mikhailova A.O.

INFORMATION SECURITY UNDER THE CONDITIONS OF FORMATION OF THE DIGITAL ECONOMY

Abstract. *Information security in modern conditions of the digital economy is one of the priorities at the state level and at the level of organizations. The article analyzes the main global trends in the field of information security, discusses ways to solve the problems of digital data security, and suggests mechanisms for ensuring information security both at the state level and in terms of individual economic actors.*

Keywords. *Digital technologies, digital economy, information security, digital transformation, competitiveness, government regulation.*

В настоящее время происходит формирование цифровой экономики, основанной на разработке и внедрении современных цифровых технологий в деятельность населения и организаций [1]. Совершенствование анализа больших данных, широкое использование мобильных устройств, развитие Интернета, появление Интернета вещей, безусловно являются инновационными элементами, призванными решать социально-экономические проблемы, как на уровне отдельных регионов и стран, так и на мировом уровне. Ускорение и усложнение процессов, происходящих в современных условиях развития цифровых технологий, заставляет субъектов экономической деятельности

Статья подготовлена в рамках гранта Президента Российской Федерации НШ-4028.2018.6.
ГРНТИ 06.54.31

Вероника Викторовна Асаул – доктор экономических наук, профессор, заведующий кафедрой экономики строительства и ЖКХ Санкт-Петербургского государственного архитектурно-строительного университета.
Анна Олеговна Михайлова – кандидат экономических наук, доцент кафедры экономики строительства и ЖКХ Санкт-Петербургского государственного архитектурно-строительного университета.
Контактные данные для связи с авторами (Асаул В.В.): 190005, Санкт-Петербург, 2-я Красноармейская ул., д. 4 (Russia, St. Petersburg, 2nd Krasnoarmeyskaya str., 4). E-mail: asaul@inbox.ru.
Статья поступила в редакцию 11.11.2018.

задумываться об информационной безопасности. Кража персональных данных граждан и организаций ведет не только к материальному ущербу, но и выражается в нанесении вреда репутации.

Потеря доверия со стороны контрагентов является крайне нежелательным результатом деятельности, поэтому вопросы обеспечения информационной безопасности требуют решения, как на государственном уровне, так и на уровне отдельных организаций. Информационные атаки могут иметь мировой масштаб: в мае 2017 г. компьютеры в более чем 150 странах были заражены вирусной программой WannaCry, что нарушило деятельность Национальной службы здравоохранения Великобритании (NHS), испанской телекоммуникационной компании Telefónica, американской логистической компании FedEx, крупнейшего железнодорожного оператора Германии Deutsche Bahn и многих других организаций по всему миру [8]; автомобильные концерны Nissan Motor и Renault временно приостановили производство на нескольких производственных площадках [9].

В условиях высокой цифровой взаимозависимости между различными субъектами экономики создание безопасной информационной среды становится неотъемлемым элементом формирования устойчивой цифровой экономики [7]. С точки зрения обеспечения информационной безопасности, наименее контролируемыми направлениями среди множества цифровых технологий являются большие данные, Интернет вещей и технологии искусственного интеллекта. Уже сейчас такие компании как Amazon, Apple и Google сформировали цифровые платформы с использованием искусственного интеллекта, а социальная сеть Facebook запустила технологию DeepTex, с помощью которой появилась возможность по сообщениям распознавать тенденции поведения пользователей [4]. Потенциальные преимущества данных цифровых технологий, безусловно, значительны, однако их внедрение создает угрозы безопасности личной информации населения, и малейшая утечка данных подрывает доверие к инновациям и экономике в целом.

Обеспокоенность последствиями потери личной информации связана с наличием случаев кражи данных, прямо или косвенно связанных с цифровыми технологиями. Значительная часть инцидентов связана с нарушением политики конфиденциальности, целостности и доступности информации, лежащей в основе социально-экономической деятельности в условиях цифровой среды. Данные нарушения со временем становятся всё более масштабными, частыми и сложными с точки зрения устранения их последствий. Нарушение информационной безопасности также происходит из-за мошеннических действий организаций, которым пользователи предоставили личную информацию. Так, в Канаде за 2017 г. жалоб подобного характера зарегистрировано на 49% больше, чем было двумя годами ранее [4]. Утечка информации в данном случае происходит из-за введения пользователей в заблуждение о предлагаемых продуктах, услугах и условиях их приобретения, а также из-за низкого уровня защиты информации на тех или иных онлайн-платформах.

Рост количества нарушений информационной безопасности в условиях цифровизации экономики связан с постоянным усложнением и ростом масштабов применения цифровых технологий. В последние годы как крупные, так и малые организации столкнулись с более частыми и более серьезными информационными атаками на бизнес [6]. Цифровые технологии, применяемые в организации, постепенно становятся главной ценностью компании, поэтому случаи промышленного шпионажа в политических или экономических целях не редки. Так, известен случай кражи информации у Sony Pictures Entertainment в 2014 г., когда ещё не вышедшие в прокат фильмы, данные отделов маркетинга и продаж, электронные письма сотрудников и другая конфиденциальная информация были выложены в открытый доступ [10].

Исследование, проведенное в Великобритании [5], выявило, что чем крупнее организация, тем чаще она сталкивается с нарушениями информационной безопасности: 84% информационных атак приходится на средние и крупные предприятия. Более того, интересен тот факт, что 16% организаций не уверены в том, имели ли место случаи утечки информации, то есть существует доля неопределенности, на которую следует обратить пристальное внимание [там же].

Оценка экономических последствий информационных атак весьма затруднена, некоторые организации стараются не сообщать о нарушениях информационной безопасности, если она не связана с юридическими последствиями кражи коммерческой тайны. Можно сказать, что потеря данных ведет ко многим отрицательным результатам: подрыв деловой репутации, снижение конкурентоспособности, финансовые потери в случае мошенничества, срыв производственных планов, поставок, а также рост затрат из-за необходимости восстановить утерянную информацию.

В современных условиях цифровой экономики каждая организация должна регулярно оценивать уровень своей информационной безопасности, отвечая на следующие вопросы [11]:

1. Насколько рационально распределены финансовые ресурсы между кадровым обеспечением организации и цифровыми технологиями, направленными на защиту данных? Важно учесть, что наем нового персонала без повышения осведомленности существующего о цифровых технологиях является малоэффективным способом повышения информационной безопасности организации. Также цифровые технологии постоянно совершенствуются и для поддержания конкурентоспособности на рынке важно использовать все доступные возможности, предоставляемые современными средствами защиты данных.

2. Правильно ли оценивается важность тех или иных мероприятий по обеспечению информационной безопасности? Определение уровней информационной защиты данных поможет оптимально оценить вклад различных средств обеспечения информационной безопасности.

3. Созданы ли в организации условия для внедрения современных цифровых технологий по защите информации? Использованию новой технологии должно предшествовать планирование и создание условий её эффективного применения, что позволит снизить количество сбоев и ошибок, а, значит, сократить затраты по налаживанию процесса функционирования технологии.

4. Насколько рационально обеспечивается информационная безопасность на всей цепочке оказания услуг или выполнения работ? Организация взаимодействует с множеством контрагентов, с которыми она обменивается данными, поэтому важно проанализировать безопасность передачи информации другим экономическим субъектам.

5. Эффективно ли менеджмент организации справляется с задачами по обеспечению информационной безопасности? Управление организацией является важнейшим элементом формирования информационной защиты, так как от слаженности действий сотрудников в значительной степени зависит успешность реализации мероприятий.

Повышение информационной безопасности организаций может быть обеспечено через проведение многоступенчатого анализа возникающих угроз (рис. 1).

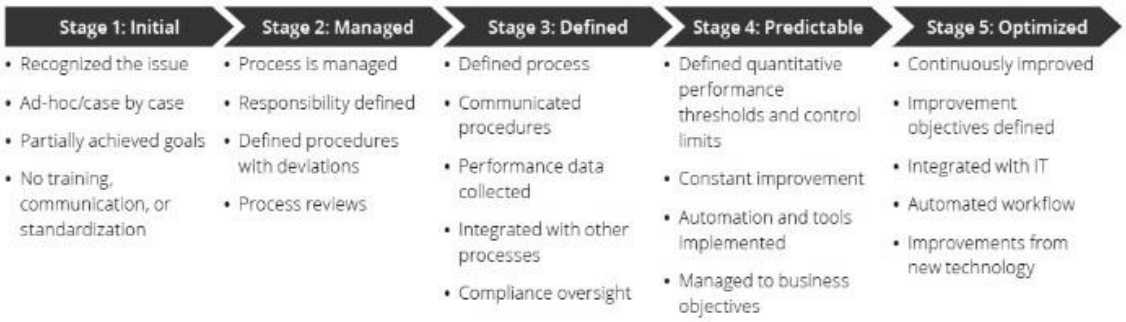

Рис. 1. Этапы анализа информационной безопасности организации [2]

Этап 1: инициация анализа. На данном этапе на основе анализа возникающих информационных угроз определяется потребность в пересмотре принятых в организации способов обеспечения сохранности данных. Как правило, обнаруживается частичное выполнение существующих мероприятий по защите информации, а также требуется разработка внутренних стандартов организации по оптимальной защите данных.

Этап 2: управление процессами. Обеспечение информационной безопасности разделяется на отдельные процессы, распределяется ответственность за каждый из них.

Этап 3: реализация и контроль. Процесс обеспечения информационной безопасности интегрируется в бизнес-модель, согласуется со стратегией развития организации, проводится контроль за выполнением принятых мероприятий, оценивается результативность нововведений.

Этап 4: прогнозирование. Определение потребности в корректировке принятых мер по обеспечению информационной безопасности, дальнейшее внедрение цифровых технологий с целью более полного охвата возможных угроз.

Этап 5: оптимизация. Проводится непрерывное совершенствование системы обеспечения информационной безопасности; защита данных становится полностью автоматизированным процессом, интегрированным во все направления деятельности организации.

В условиях формирования цифровой экономики вопросы защиты информации должны рассматриваться не только на уровне отдельных организаций, но и на государственном уровне. С точки зрения государственного регулирования, предлагаются шаги по обеспечению информационной безопасности, приведенные на рис. 2.

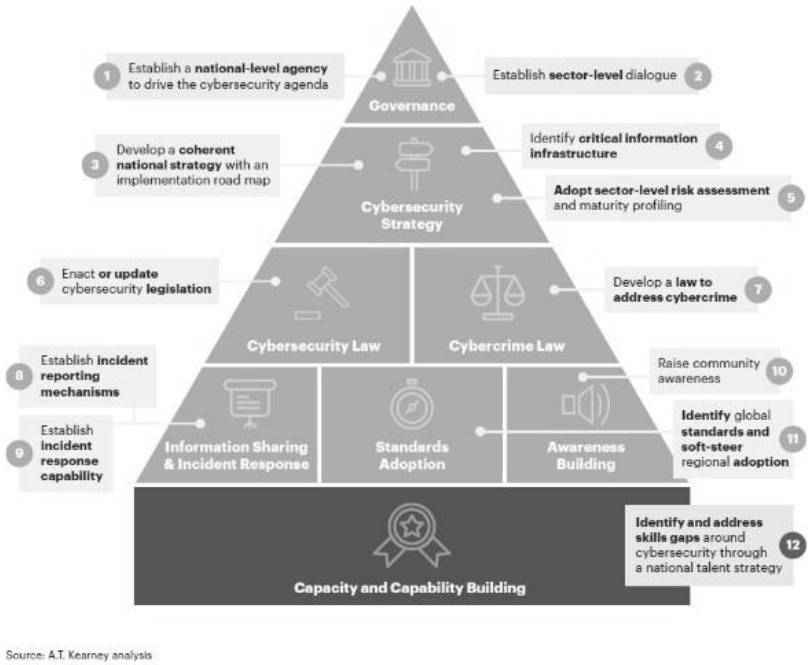

Рис. 2. Структура обеспечения информационной безопасности на государственном уровне [3]

Изначально необходимо на государственном уровне сформировать группу экспертов, которые через межотраслевое сотрудничество будут разрабатывать политику информационной безопасности. Итогом работы должна стать стратегия информационной безопасности с ясными целями, задачами и планом мероприятий в целях её эффективного внедрения; разработанная стратегия должна учитывать различные специфичные аспекты отраслей экономики. Государственная стратегия также должна включать в себя положения об оценке рисков в сфере информационной безопасности в целях оптимального реагирования на их возникновение в различных сферах. Более того, отдельным элементом стратегии должна стать критически важная информационная инфраструктура, от которой зависит национальная безопасность государства.

На следующем этапе необходимо усовершенствовать нормативно-правовое обеспечение информационной безопасности, а также разработать новые правовые нормы для определенных случаев мошенничества, не охваченных существующими законами. Данный этап обеспечения информационной безопасности должен стать непрерывным процессом обновления нормативной базы, так как с каждым днем появляются угрозы сохранности данных, с которыми ранее общество не сталкивалось, либо они не проявлялись столь масштабно.

Далее на основании принятой стратегии и обновленной нормативно-правовой базы в области информационной безопасности необходимо разработать и утвердить отраслевые стандарты обеспечения информационной безопасности. Также важно наладить достоверный сбор данных о случаях нарушения сохранности данных: в настоящее время население и организации не всегда могут с уверенностью утверждать, что они столкнулись с утечкой информации, поэтому необходимо сформировать условия для эффективного сотрудничества государства и других субъектов экономики. Более того, с обеспечением информационной безопасности связана и политика в области образования: в современных условиях развития цифровых технологий постоянно увеличивается количество собираемой и анализируемой информации, что создает новые угрозы, для борьбы с кото-

рыми требуются специальные профессиональные навыки. Следовательно, развитие кадрового потенциала страны является важным элементом поддержания информационной безопасности на всех уровнях экономики.

Таким образом, цифровая трансформация, проводимая во многих отраслях экономики, привела к тому, что изменился масштаб деятельности экономических субъектов и появились новые риски и угрозы, с которым раньше мир не сталкивался. Становление цифровой экономики во многом зависит от обеспечения информационной безопасности: возникновение угроз сохранности цифровых данных становится одним из основных направлений обеспечения безопасности, как на государственном уровне, так и на уровне отдельных организаций и граждан. В настоящее время атаки на системы хранения данных становятся всё более сложным и частым явлением, поэтому вопросы обеспечения информационной безопасности должны выступать приоритетной задачей поддержания устойчивости экономики.

ЛИТЕРАТУРА

1. *Ablyazov T., Asaul V.* On competitive potential of organization under conditions of new industrial base formation // SHS Web of Conferences. 2018. Vol. 44. 00003.
2. Cybersecurity and the role of internal audit, an urgent call to action. Deloitte. 2017.
3. Cybersecurity in ASEAN: an urgent call to action. A.T.Kearney. 2018.
4. Digital Economy Outlook. OECD. 2017.
5. *Klahr R., Amili S., Shah J.N., Button M., Wang V*. Cyber Security Breaches Survey. 2016.
6. Managing digital security and privacy risk // OECD Digital Economy Papers. 2016. № 254.
7. *Mayer R.C., Davis J.H., Schoorman F.D.* An integrative model of organizational trust // The Academy of Management Review. 1995. Vol. 20. № 3. P. 709-734.
8. NHS cyber-attack: GPs and hospitals hit by ransomware. [Электронный ресурс]. Режим доступа: www.bbc.com/news/health-39899646 (дата обращения 05.11.2018).
9. *Sharman J.* Cyber-attack that crippled NHS systems hits Nissan car factory in Sunderland and Renault in France. [Электронный ресурс]. Режим доступа: https://www.independent.co.uk/news/uk/home-news/nissan-sunderland-cyber-attack-ransomware-nhs-malware-wannacry-car-factory-a7733936.html (дата обращения 05.11.2018).
10. Sony Pictures computer system hacked in online attack. [Электронный ресурс]. Режим доступа: www.bbc.com/news/technology-30189029 (дата обращения 05.11.2018).
11. The State of Cybersecurity and Digital Trust. [Электронный ресурс]. Режим доступа: https://www.accenture.com/es-es/_acnmedia/PDF-23/Accenture-State-Cybersecurity-and-Digital-Trust-2016-Report-June.pdf (дата обращения 05.11.2018).