УДК 338.12

Булатенко М.А.
ФГБОУ ВО «МИРЭА – Российский технологический университет», Москва,
e-mail: mabulatenko@gmail.com

Горонок Д.Л.
ФГБОУ ВО «МИРЭА – Российский технологический университет», Москва,
e-mail: den-gor@inbox.ru

КЛЮЧЕВЫЕ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ В СОВРЕМЕННЫХ УСЛОВИЯХ

Ключевые слова: экономическая безопасность, информационная безопасность, цифровая экономика.

Вопрос обеспечения достойного уровня экономической безопасности предприятий и формирования на предприятии функционирующей системы выявления, оценки и минимизации экономических рисков с каждым днем набирает все большую актуальность. Одной из особенностей цифровой экономики является смещение акцента с материальных ресурсов на информационные ресурсы (информация, данные, знания). 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. Следствием этого и выступает, что в последние годы крупные и малые организации подвергаются более частым и серьезным угрозам в цифровой среде, что влияет на их экономическую безопасность. С экономической точки зрения подобные угрозы могут влиять на репутацию организаций, финансовую составляющую, нанося ущерб их конкурентоспособности, подрывая их усилия по инновациям и позиции на рынке. В статье поэтапно выделяются и обосновываются ключевые цифровые угрозы экономической безопасности на уровне предприятий в условиях цифровизации экономики, такие как кража корпоративных данных, промышленный шпионаж, хакерские атаки, недостаточная обеспеченность цифровыми технологиями и компетентными кадрами.

Bulatenko M.A.
MIREA – Russian technological university, Moscow, e-mail: mabulatenko@gmail.com

Goronok D.L.
MIREA – Russian technological university, Moscow, e-mail: den-gor@inbox.ru

KEY PROBLEMS OF ENSURING ECONOMIC SECURITY OF THE ENTERPRISE IN MODERN CONDITIONS

Keywords: economic security, information security, digital economy.

The issue of ensuring a decent level of economic security of enterprises and the formation of a functioning system in the enterprise for the identification, assessment and minimization of economic risks is gaining increasing relevance every day. One of the features of the digital economy is the shift of focus from material resources to information resources (information, data, knowledge). Improving the analysis of big data, the widespread use of mobile devices, the development of the Internet, and the emergence of the Internet of Things are certainly innovative elements designed to solve social and economic problems, both at the level of individual regions and countries, and at the global level. The consequence of this is that in recent years, large and small organizations are exposed to more frequent and serious threats in the digital environment, which affects their economic security. From an economic point of view, such threats can affect the reputation of organizations, the financial component, damaging their competitiveness, undermining their innovation efforts and market position. The article gradually identifies and substantiates key digital threats to economic security at the enterprise level in the conditions of digitalization of the economy, such as corporate data theft, industrial espionage, hacker attacks, insufficient provision of digital technologies and competent personnel.

Введение

Вопрос обеспечения достойного уровня экономической безопасности предприятий и формирования на предприятии функционирующей системы выявления, оценки и минимизации экономических рисков с каждым днем набирает все большую актуальность.

Влияние внешних и внутренних факторов ежедневно создает отечественным предприятиям новые риски функционирования, которые вследствие реализации при определенных обстоятельствах, имеют вероятность перерасти в угрозу или опасность и тем самым привести к потерям или, в худшем случае, привести к банкротству [1]. Именно благодаря грамотно построенной и функционирующей системе выявления и оценки есть возможность своевременного выявления, нейтрализации или минимизации рисков и угроз экономической безопасности, влияющих на деятельность предприятия.

Кража персональных данных предприятий безусловно ведет не только к материальному ущербу, но и выражается в нанесении вреда репутации, что не может не сказываться на финансовом благополучии организаций [2].

Постараемся разобраться в том, как кибератаки (кража, изменение, модификация, копирование, распространение информации, хранящейся на цифровых носителях) влияют на предприятия с экономической стороны, и можно ли с уверенностью утверждать, что в современных условиях кибербезопасность является наиболее важной частью экономической безопасности.

Цель исследования: рассмотреть влияние современных условий функционирования предприятий на их систему обеспечения экономической безопасности.

Материал и методы исследования

Данная статья базируется на научных работах российских и зарубежных исследователей проблематики цифровой трансформации предприятий, основными методами исследования выступают анализ, синтез, индукция, дедукция, логические исследования, системный подход.

Результаты исследования и их обсуждение

Вопросам характеристики экономической безопасности предприятий, различных отраслей экономики, посвящено значительное количество научных работ. Однако следует отметить, что среди ученых, занимающихся проблемами экономической безопасности, на сегодняшний день не сформировано единое понятие экономической безопасности предприятия, несмотря на то что авторские определения различных ученых значительно схожи.

Несмотря на большой интерес к проблемам экономической безопасности отечественных и зарубежных ученных и практиков, следует отметить, что существующие разработки в основном посвящены различным аспектам национальной и региональной безопасности, и в значительно меньшей степени – вопросам экономической безопасности предприятий.

Все это не позволило ученым, которые занимаются проблемами экономической безопасности, выработать единый подход к пониманию экономической безопасности предприятия.

Обобщая определения различных авторов, экономическую безопасность можно определить как состояние защищенности его экономического, научно–технического, производственного и кадрового потенциала от прямых или косвенных экономических угроз, связанных с действием неблагоприятных факторов внешней среды, и способность к их воспроизводству [3].

Экономическую безопасность предприятия можно охарактеризовать как такое состояние экономического субъекта, при котором обеспечивается защищенность его интересов от внешних и внутренних экономических угроз, стабильное развитие и эффективная деятельность при максимально оптимальном использовании всех имеющихся и привлеченных ресурсов.

Система обеспечения экономической безопасности предприятия включает в себя следующие функциональные области:

1) финансово-экономическая безопасность предприятия;

2) интеллектуально-кадровая безопасность;

3) технико-технологическая безопасность;

4) политико-правовая безопасность;

5) информационная безопасность;

6) экологическая безопасность;

7) физическая безопасность.

В основе экономической безопасности лежит использование системного

подхода, при котором различные отдельные элементы системы, выполняя различные функции, взаимодействуют между собой определенным образом, слажено и сообща, для достижения единой цели.

На сегодняшний день с активной цифровизацией любых сфер общественной жизни, в том числе и экономической, важнейшим объектом безопасности является информация, сведения, данные, в том числе используемые в цифровой деятельности.

В настоящее время происходит формирование цифровой экономики, основанной на разработке и внедрении современных цифровых технологий в деятельность населения и организаций [4]. 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 задумываться об информационной безопасности.

Одной из особенностей цифровой экономики является смещение акцента с материальных ресурсов на информационные ресурсы (информация, данные, знания), которые, в свою очередь, не исчезают при потреблении, могут быть неоднократно использованы различными субъектами без привязки к месту, времени и субъекту создания (возникновения), что приводит к простоте тиражирования информационных ресурсов.

Следствием этого и выступает, что в последние годы крупные и малые организации подвергаются более частым и серьезным угрозам в цифровой среде, что влияет на их экономическую безопасность. С экономической точки зрения подобные угрозы могут влиять на репутацию организаций, финансовую составляющую, нанося ущерб их конкурентоспособности, подрывая их усилия по инновациям и позиции на рынке. Такие угрозы могут нарушить доступность, целостность или конфиденциальность информационных систем, на которых основывается экономическая деятельность [5].

Одной из важнейших задач системы экономической безопасности является обеспечение защиты конфиденциальных данных какого- либо субъекта хозяйствования. К ним относятся различные ноу- хау, коммерческие тайны, секреты производства и др. В условиях конкуренции даже такие сведения, как данные о клиентах либо о поставщиках и условия их сотрудничества, могут значительно ухудшить финансовое состояние организации. Поэтому в современных реалиях нередки случаи кражи корпоративных данных и промышленный шпионаж.

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, вследствие чего компания понесла существенное снижение прибыли от продаж [6].

Согласно опубликованному заявлению Equifax, с мая по июль 2017 года злоумышленники использовали уязвимость в системе безопасности приложения на веб-сайте компании и получили доступ к номерам социального страхования, датам рождения, адресам и в ряде случаев к номерам водительских удостоверений. Кроме того, преступники получили доступ к данным кредитных карт 209 тысяч человек и к документам с персональными данными еще 182 тысяч человек. Впоследствии, стоимость акций Equifax просела более, чем на 35% [7].

Рост количества нарушений информационной безопасности в условиях цифровизации экономики связан с постоянным усложнением и ростом масштабов применения цифровых технологий. И здесь стоит отметить, что большинство угроз информационной, а впоследствии, и экономической безопасности кроется в самих цифровых технологиях. Уязвимости (так называют угрозы в мире информационной безопасности) есть в веб- и мобильных приложениях, на официальном сайте предприятия, в подключенных коммутаторах и серверах компании и т.д.

Информационные атаки, в первую очередь, направленные на нахождение уязвимостей и получение корпоративной информации, в конечном итоге могут привести к прямым финансовым потерям (кража денежных средств, находящихся на электронном счету, проведение фальшивых транзакций и сделок и т.д.), упущенной выгоде (из-за утечки данных и потери конкурентных преимуществ), а также к снижению деловой репутации и, как следствие, потере капитализации компании.

Таким образом, просматривается прямая зависимость между степенью развития и внедрения цифровой экономики в деятельность предприятий и их экономической безопасностью, в том числе и кибер- безопасностью.

С одной стороны, цифровая трансформация существующих предприятий необходима для повышения конкурентоспособности и капитализации предприятий за счет кардинального повышения производительности, снижения количества вовлечённых сотрудников в цепочку создания ценности и повышения скорости и качества принятия управленческих решений. Это подтверждается текущим Рейтингом 100 самых дорогих глобальных брендов [8]: на основе текущей стоимости бренда и прогнозируемого потенциала роста британские исследовательская и издательская компании (Kantar Millward Brown и The Financial Times соответственно) вывели стоимость бренда компании Google в 302 млрд долларов США, а следующие три места заняли такие передовые высокотехнологичные компании в цифровой сфере, как Apple, Microsoft и Amazon. Исследователи Международного института управленческого развития (International Institute of Management Development, IMD) [9] привели обоснование печальному факту, что через пять лет около 40% текущих компаний, не осознающих необходимость цифровых перемен своего бизнеса, полностью уйдут с рынка.

С другой стороны, цифровые технологии, применяемые в организации, постепенно становятся главной ценностью компании, поэтому случаи промышленного шпионажа и кибер- атак в экономических целях не редки, что безоговорочно указывает на значимость достойного уровня кибербезопасности в обеспечении экономической безопасности предприятия в современных условиях.

Совершенно очевидно, что в «умных» домах и городах будут жить все те же люди, что и сегодня. Несмотря на то, что потенциал искусственного интеллекта еще не до конца оценен, уже сейчас стоит задуматься, что он не может быть лишен уязвимости, и появятся «умные» мошенники и грабители увидят в цифровой экономике широкие возможности цифровых преступлений, фальсификации данных и коррупции. Воровство финансовых средств и интеллектуальной собственности, шантаж, вымогательство, взлом информационных хранилищ, получение несанкционированного доступа к чужим персональным данным для нарушений закона – далеко не полный перечень известных преступлений из мира цифровой экономики.

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. Но с уверенностью 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 [2].

Оценивая все издержки в комплексе (сумму выкупа в случае использования шифратора при атаке, расходы от снижения производительности, последующее усиление мер безопасности, имиджевый ущерб и т.д.) индустрия киберпреступности обошлась миру в три триллиона долларов в 2015 году и, по прогнозам, к 2021 году сумма вырастет до шести триллионов [10].

И если действия киберпреступников – это основные внешние угрозы экономической безопасности предприятия, то ключевыми внутренними угрозами являются непосредственно сотрудники предприятия. Еще большую проблему обеспечения экономической безопасности предприятия в современных усло-

виях создают компетенции сотрудников службы экономической безопасности на предприятии. Связано это, в первую очередь, с тем, что ключевым требованием рекрутеров [11] при приеме на должности начальника и заместителя начальника службы экономической безопасности предприятия является опыт работы в правоохранительных органах, либо в органах внутренних дел. К сожалению, данный опыт работы не сможет помочь предприятиям в полноценной борьбе с теми вызовами и угрозами, которые несет с собой уже начавшаяся цифровая трансформация экономики.

Выводы или заключение

Таким образом, в результате проведенного исследования систематизированы проблемы экономической безопасности предприятия на современном этапе, кибербезопасность выделена как один из главных элементов обеспечения экономической безопасности в условиях цифровой экономики (в современных условиях).

К основным проблемам экономической безопасности отнесены проблемы защиты данных предприятия от кибер атак, обеспечение защиты корпоративных данных на должном уровне в условиях стремительного развития цифровых инструментов в экономике.

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.

Активное внедрение цифровых технологий на предприятиях всех отраслей экономики вносит изменения и в систему выявления, оценки и минимизации рисков и угроз экономической безопасности, в современных условиях возникновение угроз сохранности цифровых данных становится одним из основных направлений обеспечения безопасности. В настоящее время атаки на системы хранения данных становятся всё более сложным и частым явлением, поэтому вопросы обеспечения кибер- безопасности должны выступать приоритетной задачей в обеспечении экономической безопасности предприятия.

Библиографический список

1. Абаимова К.В., Арутюнян Э.Р. Проблемы экономической безопасности предприятия в современных условиях // Экономика и бизнес: теория и практика. – 2015. – №4. – С. 4-8.

2. Асаул В.В., Михайлова А.О. Обеспечение информационной безопасности в условиях формирования цифровой экономики // Теория и практика сервиса: экономика, социальная сфера, технологии. – 2018. – № 4 (38). – С. 5-9.

3. Самочкин В.Н., Барахов В.И. Экономическая безопасность промышленных предприятий // Известия ТулГУ. Экономические и юридические науки. – 2014. – № 3-1. – С. 342-352.

4. Ablyazov T., Asaul V. On competitive potential of organization under conditions of new industrial base formation // SHS Web of Conferences. – 2018. – Vol. 44.

5. Попов Е.В., Семячков К.А. Проблемы экономической безопасности цифрового общества в условиях глобализации // Экономика региона. – 2018. – № 4. – С. 1088-1101.

6. Официальный сайт газеты Washingtonpost. – URL: https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/?noredirect=on&utm_term=.e651fc6cd41f

7. Сетевое издание РИА Новости. – URL: https://ria.ru/20170908/1502040513.html

8. Рейтинг 100 самых дорогих глобальных брендов (BRANDZ Global Top 100). – URL: http://online.pubhtml5.com/bydd/rxhd/#p=4

9. Отчет DBT Center «Цифровой водоворот, или Как цифровая революция реформирует промышленность» (Digital Vortex: How Digital Disruption is Redefining Industries). – URL: https://www.cisco.com/c/dam/en/us/solutions/collateral/industry-solutions/digital-vortex-report.pdf

10. Официальный ежегодный отчет о киберпреступности за 2019 год Herjavec Group (ведущей мировой консалтинговой фирмы по кибербезопасности). – URL: https://www.herjavecgroup.com/the-2019-official-annual-cybercrime-report/

11. Официальный сайт компании HeadHunter. – URL: https://hh.ru/search/vacancy?text=Экономическая+безопасность&area=1&from=suggest_post