УДК 004.056

ВОПРОСЫ БЕЗОПАСНОСТИ ПРИ ПРИМЕНЕНИИ ИНФОРМАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

Терентьев Д. Е.

магистрант,

Калужский государственный университет им. К. Э. Циолковского,

Калуга, Россия

Ткаченко А. Л.

к.т.н., доцент,

Калужский государственный университет им. К.Э. Циолковского,

Калуга, Россия

Аннотация

В статье приведены определения цифровой экономики и информационной безопасности. В качестве основных проблем информационной безопасности на предприятии выделены: утечка конфиденциальных данных клиентов, а также данных о предприятии, которые позволяют конкурентам получить засекреченные сведения, характеризующиеся уникальностью. Кроме того, информационная безопасность представляет собой стратегическую задачу государства, поскольку оказывает прямое влияние на национальную безопасность.

Ключевые слова: цифровая экономика, информационная безопасность, национальная безопасность, мошенничество, утечка данных, коммерческая тайна.

SAFETY ISSUES IN THE USE OF INFORMATION SYSTEMS AND TECHNOLOGIES

Terentyev D. E.
master's student,
Kaluga State University named after K. E. Tsiolkovsky,
Kaluga, Russia

Tkachenko A.L.
candidate of Technical Sciences,
Kaluga State University named after K. E. Tsiolkovsky,
Kaluga, Russia

Abstract
The article provides definitions of the digital economy and information security. The main problems of information security at the enterprise are leakage of confidential customer data, as well as data about the enterprise, which allows competitors to obtain classified information characterized by uniqueness. In addition, information security is a strategic task of the state, since it has a direct impact on national security.

Keywords: digital economy, information security, national security, fraud, data leakage, trade secret.

Информационные технологии являются наиболее важной составляющей жизни современного человечества. Без преувеличения можно сказать о том, что в условиях рыночного механизма хозяйствования, информационные и цифровые технологии являются самыми распространенными практически во всех сферах жизнедеятельности общества. Среди таких сфер наиболее крупными являются: экономика, здравоохранение, образование, наука, право и т. д.

Характерной особенностью 21 века является глобальная и полномасштабная цифровизация всех отраслей жизнедеятельности общества. Технологический скачок, произошедший за последние 50–60 лет, существенно

облегчил и усовершенствовал повседневные операции. Если раньше, человеку, чтоб получить ту или иную справку, приходилось лично обращаться в большое количество инстанций, то сейчас, практически любую услугу можно получить, не выходя из дома. Следовательно, цифровизация – это не только экономическая категория, но и всеобщая.

На протяжении последних десятилетий мир является свидетелем глобальной модернизации привычных форм производства, ведения бизнеса, бухгалтерского учета, аудита, менеджмента, маркетинга и прочих крупных экономических дисциплин. Это связано, как уже упоминалось, с развитием информационных технологий во всех социально-экономических сферах.

Цифровизация, как современная тенденция, воспринимается специалистами как последний писк моды. Важно следовать трендам. И одним из главных трендов последнего времени является экономическая цифровизация, которая способствует успешной реализации возможностей как государства, так и общества.

Простыми словами, экономическая цифровизация представляет собой процесс перехода от материальных носителей к нематериальным (цифровым), или переход из офлайна в онлайн. Чаще всего, цифровизации экономики представляет собой электронную коммерцию или электронный бизнес, характерной особенностью которого являются электронные расчеты.

Цифровая экономика - результат процесса инновационного развития экономики, который характеризуется активным применением компьютерных технологий во всех сферах деятельности человека. Особенностью цифровой экономики является трансформация сфер экономики: выдвижение на лидирующую позицию сферы науки и образования как поставщика интеллектуального ресурса в сферы производства цифрового продукта и его потребления [4, с.219].

Информационные технологии обладают рядом бесспорных преимуществ, однако, как и любые другие технологии облают и своими недостатками, которые в первую очередь связаны с безопасностью [2, с. 46].

Как и во всех других сферах и отраслях, расширение возможностей и увеличение потенциала, сопровождается ростом рисков. В это свете главными проблема цифровизации бизнес-среды можно назвать утечку информации и некоторые правовые ограничения. В глобальной экономической цифровизации можно выделить следующие отрицательные составляющие:

1. Увеличение случаев мошенничества. Если до сих пор мошенники были ограничены материально-вещественной основной своей преступной деятельности, то цифровизация «открыла» для них новые горизонты, и, существенно «увеличила» количество интернет-мошенников. Устранение данного минуса, требует большой и планомерной работы по обеспечению информационной безопасности.

2. Несмотря на пропагандируемую тему свободы интернета, данный вопрос имеет обратную сторону. В некотором смысле интернет ограничивает свободу человека, который становится объектом бизнеса, так как его личные данные становятся общедоступными, а его интересы и предпочтения легко отслеживаются различными маркетинговыми службами.

Под информационной безопасностью, по мысли Н. Р. Шевко, понималась защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры [5, с.75].

Таким образом, как можно судить из определения, представленного выше, источниками угрозы информационной безопасности предприятия могут быть как естественные, так и искусственные факторы. Разумеется, на практике чаще всего встречаются воздействие источников искусственного характера,

деятельность которых в современном отечественном законодательстве трактуется как киберпреступность и мошенничество.

Злоумышленники, совершая вышеупомянутые противозаконные действия, преследуют несколько целей, основными среди которых являются следующие:

1. Получение доступа к денежным средствам предприятия и их дальнейшее присвоение.

2. Завладение информацией относительно финансово-хозяйственной деятельности предприятия, представляющей собой коммерческую тайну.

Успешное совершение вышеуказанных преступлений приведет к негативным для предприятия последствиям, которые выражаются в краже денежных средств, фактической утрате реальных шансов на их возмещение, утечке информации, в том числе и персональных данных клиентов, а также получении доступа к маркетинговой, бухгалтерской и прочей информации экономического характера.

Решением вышеуказанной проблемы является покупка качественного и дорогого программного продукта, который обладая набором определенных характеристик, будет гарантировать защиту информационных систем предприятия от хакерских атак.

Учитывая специфику риска угрозы информационной безопасности, важно в процессе функционирования предприятия наладить систему защиты от подобных угроз, которая выражается, в первую очередь, в виде программного обеспечения. Кроме того, в зависимости от размеров предприятия и оборотов его деятельности, важно грамотно укомплектовать персонал, отвечающий за IT-сферу. Ведь никакой программный продукт не будет приносить должного эффекта без квалифицированного участия профессионала.

Рассмотренный нами пример свидетельствует о важности соблюдения мер по информационной безопасности в предприятиях. Однако, данная проблема намного шире и зачастую связан национальной безопасностью, что означает стратегическую важность данного аспекта.

Согласно Стратегии национальной безопасности Российской Федерации, информационной безопасности уделено особое внимание в системе национальной безопасности, поскольку быстро развивающиеся информационные технологии способствуют появлению новых вызовов и угроз. Ввиду этого усиливается роль информационной безопасности в системе национальной безопасности. Вместе с тем национальная безопасность представляет собой безопасность как населения, проживающего на территории страны, так и власти, и окружающей среды в целом. Все это свидетельствует о многоаспектном характере национальной безопасности [3].

Доктрины информационной безопасности Российской Федерации можно выделить следующие особенности национальных интересов: 1) прозрачность и транспарентность деятельности государства в информационной сфере; 2) гарантия защиты конституционных прав и свобод граждан, касающихся информационной безопасности; 3) взаимное и согласованное функционирование государства и гражданского общества, в том числе в рамках укрепления нравственных ценностей общества; 4) обеспечение надлежащего функционирования информационной инфраструктуры как в случае непосредственного влияния информационных угроз, так и в период стабильной мирной обстановки в стране; 5) стимулирование научно-технического прогресса и развития экономических отраслей, способствующих обеспечению информационной безопасности; 6) интеграционное взаимодействие с другими странами для обеспечения международной информационной безопасности и стратегической стабильности [1].

Резюмируя вышеизложенное, можно сделать вывод о том, что информационная безопасность является важнейшей составляющей современного государства и общества как с точки зрения микро, так и с точки зрения макроуровня. Необходимыми действия в данном контексте признаются: разработка качественного программного обеспечения, а так комплектация штата IT-специалистов.

Библиографический список:

1. Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СЗ РФ. 2016. № 50. Ст. 7074.

2. Ашабокова К. А. Плюсы и минусы цифровой трансформации // Научные высказывания. 2024. №3 (50). С. 45–48.

3. Дубень А.К. — Информационная безопасность в системе национальной безопасности: актуальные проблемы информационного права// Вопросы безопасности. – 2023. – № 1. DOI: 10.25136/2409-7543.2023.1.40078 EDN: AOZZYF URL: https://nbpublish.com/library_read_article.php?id=40078

4. Лопатина, Е. Н. Риски в деятельности предприятия: методы оценки и пути снижения / Е. Н. Лопатина, Е. В. Шпак, Т. В. Полякова. — Текст : непосредственный // Молодой ученый. — 2020. — № 18 (308). — С. 111-112. — URL: https://moluch.ru/archive/308/69468/

5. Шободоева, А. В. Развитие понятия «Информационная безопасность» в научно-правовом поле России // Известия БГУ. 2017. №1. URL: https://cyberleninka.ru/article/n/razvitie-ponyatiya-informatsionnaya-bezopasnost-v-nauchno-pravovom-pole-rossii/viewer

Оригинальность 81%