УДК 338.1

Салютина Татьяна Юрьевна
Заведующая кафедрой ЦЭУиБТ
Московский технический университет связи и информатики
Россия, г. Москва
Корчака Владимир Сергеевич
Студент 3 курс
факультет «38.04.01 Экономика»
Московский технический университет связи и информатики
Россия, г. Москва

ЦИФРОВИЗАЦИЯ БИЗНЕСА И РАЗВИТИЕ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ: ВЫЗОВЫ И СОВРЕМЕННЫЕ ТЕНДЕНЦИИ

Аннотация: *В статье рассматриваются основные аспекты цифровизации бизнеса, использования технологий в организациях. Дано описание основных угроз в сфере информационной безопасности. Описано развитие систем защиты информации и актуальность дальнейшего развития данных систем. Подчеркивается необходимость соблюдения правил информационной безопасности в организации.*

Ключевые слова: *информационная безопасность, цифровая безопасность, цифровая экономика, цифровизация, защита информации.*

Annotation: *The article discusses the main aspects of business digitalization and the use of technologies in organizations. A description of the main threats in the field of information security is provided. The development of information protection systems and the relevance of further advancement of these systems are outlined. The necessity of adhering to information security rules within organizations is emphasized.*

Key words: *information security, cybersecurity, digital economy, digitalization, information protection.*

Развитию информационного сообщества сопутствует и цифровая трансформация бизнеса -– во все аспекты деятельности компании сегодня интегрированы технологии. Это улучшает производительность компании, повышает ее эффективность, адаптированность к внешним условиям. Технологии сегодня актуальны не только в IT-сфере, но в любой другой отрасли – при организации операционной деятельности, взаимодействии с контрагентами, партнерами, собственниками, в формировании бизнес-модели.

Цифровая трансформация невозможна без использования новейших технологий: искусственного интеллекта, облачных решений, интернета вещей, автоматизации и Big Data. Однако, использование передовых технологий не только облегчает работу бизнеса, но и создает определенные угрозы его существованию. Так, чем более технологична организация, тем более она уязвима: увеличение цифровизации повышает угрозу несанкционированного проникновения в данные организации, подключения к ее системам, в частности, в условиях использования облачных технологий. Использование большого объема данных ставит под угрозу сохранность этих данных – от личных, до сведений, касающихся производственной деятельности. Серьезно повлиять на деятельность могут и кибератаки: фишинг, вирусные атаки, DDoS-атаки – все это угрозы для современной технологичной компании, последствия от которых могут быть колоссальными.

В современном мире в сводках новостей то и дело мелькают выпуски: «произошла утечка личных данных пользователей в компании N», «в сети были опубликованы пароли тысяч пользователей», «в руки киберпреступников попали номера телефонов N миллионов пользователей». Так, в январе 2024 года в сеть ушла информация с персональными данными полумиллиона владельцев автомобилей KIA в России. В сентябре 2024 года об утечке

сообщила страховая компания «Спасские ворота», в декабре – в отрытом доступе обнаружены данные пользователей САПР «Нанософт». Крупные утечки случались и ранее – «Delivery Club» «потерял» личные данные с 2,2 млн. заказов, у «Geek Brains» более чем у 200 тыс. пользователей были украдены данные имен, номера телефона, адреса электронной почты, «Pikabu» «потеряли» более 1 млн. учетных записей. Кибератакам подверглись и российские компании –«Гемотест», «СДЭК», «Теле2» и пр., и государственные структуры – «Московский метрополитен», «Почта России». Страдают и зарубежные компании: в 2019 году крупная американская социальная сеть потеряла данные 533 млн. пользователей, у компании «Yahoo» хакерская атака затронула все 3 млрд. пользователей [1].

Только в России, за 2024 год в руки мошенников «утекли» 438 млн. номеров телефонов, 227 млн. ед. email-адресов. При этом, Роскомнадзор отмечает, что есть определенный тренд снижения объема утечек данной информации – мошенников сегодня интересует более личная информация пользователя, в том числе данные официальных документов. Кроме того, чаще всего кибератакам подвергаются государственные организации и органы, IT-компании, крупные торговые ритейлы, банковские организации. В целом утечка данных в основном связана с кибератаками, куда реже – с противозаконными действиями сотрудников предприятий, а самыми редкими становятся случайные действия в организации [2].

В экономике сегодня циркулирует огромное количество информации: статистические данные (рынок, компании демография), Big Data (процессы, поведение потребителей), интеллектуальные права и пр. Информация сегодня – критически важный ресурс для компаний. Порядка 90% информации о деятельности компании сегодня хранится именно в цифровом виде.

Следовательно, все это говорит о необходимости уделения внимая не только цифровому развитию, но и цифровой безопасности. Цифровая

безопасность предполагает наличие определенных мер – и на уровне организации, и на уровне законодательства.

Стоит отметить, что сами технологии способствуют и развитию видов защит от угроз информационной безопасности. В свое время были разработаны алгоритмы шифрования данных, антивирусные программы, брандмауэры и средства мониторинга трафика и другие. В начале 2000х были сформированы стандарты в сфере информационной безопасности (ISO/EIC 27001, ISO/IEC 27002, PCI DSS и пр.), имеющие значение как в области мировой безопасности, так и на уровне организаций. В России в 2001 году был принят ГОС Р 34.10 об информационных технология и криптографической защите. С распространением цифровой экономики соблюдение информационной безопасности стало сложнее, и включать не только технические меры, но и соблюдение нормативов, управление рисками и прочие аспекты [3].

Так, перспективным становится использование искусственного интеллекта в совокупности с машинным обучением позволит применять более продвинутые методы обнаружения угроз безопасности, определять аномалии в системе и давать прогноз потенциальных кибератак. Использование современных блокчейн-технологий позволит повысить устойчивость к взломам за счет децентрализации, к тому же, способно повысить уровень безопасности транзакций, что особенно полезно для финансового сектора. Применение биометрии как средства аутентификации становится наиболее безопасным методом по сравнению с паролем для защиты личных данных.

Нужно отметить, что перечисленные технологии стали и основной для проведения кибератак и новых схем – искусственный интеллект способен создавать дипфейки для обмана распознавания лица, генерировать новые вредоносные программы, создавать атакующие алгоритмы.

На законодательным уровне государство также участвует в создании безопасной информационной среды. Так, Министерством цифрового развития

РФ осуществляется нормативное регулирование цифровой среды, в ом числе действуют приказы о необходимости сертификации оборудования связи, определении угроз, информационной безопасности в целом. В 2019-2024 году реализовывался проект «Цифровая экономика», который был выполнен на 95,8%. В рамках проекта выделялись гранты IT-компаниям, поддерживались значимые проекты, разрабатывались новые электронные услуги для граждан и прочие. На его смену пришел проект «Экономика данных», нацеленный на поддержку отечественных компаний, разработок и исследований в том числе в сфере систем защиты информации [4].

Обеспечение информационной безопасности внутри организации предполагает комплексных подход, в рамках которого компания разрабатывает собственную политику безопасности, выбирает технологии шифрования и системы обнаружения и предотвращения вторжений, проводит постоянный мониторинг систем безопасности, обучает сотрудников информационной безопасности и сотрудничает с экспертами по этим вопросам [5].

Подводя итоги, нужно сказать, что цифровизация неизбежна, и сегодня к этому приходят практически все компании – от малых до огромных холдингов. Сложно представить себе сегодня, что база с клиентами хранится в тетради в отделе продаж, а бухгалтерия ведет учет виде записей на бумаге. Цифровизация, с одной стороны, открывает невероятные возможности для компании, но при этом формирует и новые угрозы для бизнеса, которые нельзя оставить без внимания. По этой причине, цифровая безопасность организаций – основа, без которой невозможна цифровизация бизнеса.

Использованные источники:

1. RockYou2024 и еще четыре самых крупных утечки данных в истории: КасперскийДэйли. [Электронный ресурс]. URL: https://www.kaspersky.ru/blog/top-five-data-breaches-in-history/38127/

2. Объем утекших данных российских пользователей вырос на 70%: TADVISER. [Электронный ресурс]. URL: https://www.tadviser.ru/

3. Василенко, Н. В. Информационная безопасность: объекты, этапы развития, факторы усиления угроз в начале XXI века / Н. В. Василенко, Б. Г. Василенко // Ученые записки Международного банковского института. – 2023. – № 4(46). – С. 34-55.

4. Экономика данных: Национальные проекты РФ [Электронный ресурс]. URL: https://xn--80aapampemcchfmo7a3c9ehj.xn--p1ai/new-projects/ekonomika-dannykh/

5. Информационная безопасность как ключевой аспект развития экономики / Д. Н. Асланов, Д. А. Демкин // Вестник науки. 2024. №7 (76). URL: https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-kak-klyuchevoy-aspekt-razvitiya-tsifrovoy-ekonomiki (дата обращения: 29.01.2025).