СЕКЦИЯ 2. УПРАВЛЕНИЕ БИЗНЕСОМ В ЦИФРОВОЙ ЭКОНОМИКЕ

УДК 342.72/.73

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В ЦИФРОВОМ ПРОСТРАНСТВЕ

Дворкина К. А., Каленкович Ю. А.
Научный руководитель – к. э. н., доцент Дроздович Л. И.,
ст. преподаватель Янович П. А.
Белорусский национальный технический университет,
a1246860@gmail.com, yanovich@bntu.by

Аннотация. В контексте быстрого развития информационных технологий и все более активного участия людей в цифровой деятельности важным является выявление основных угроз и рисков, обусловленных интенсивным использованием персональных данных в гражданском обороте, а также определением основных принципов защиты личных данных. Это обусловлено тем, что в условиях значительного роста цифровых услуг персональные данные для субъектов рынка являются ценным экономическим ресурсом, позволяющим им не только оценивать потенциал рынка, но и корректировать стратегии развития. Однако учитывая специфический характер таких данных, особо актуальным является правомерное использование таких данных субъектами рынка, не нарушающее их права. Решение данной проблемы возможно только с использованием системного подхода, включая правовые, организационные и технические меры и ограничения, которые обеспечат безопасность и конфиденциальность персональных данных в гражданском обороте. Наиболее опасным видом угрозы для субъектов являются киберпреступления в цифровой среде.

Ключевые слова: персональные данные, конфиденциальные данные, защита персональных данных, Интернет, цифровое пространство, меры по защите персональных данных, Национальный центр защиты персональных данных Республики Беларусь.

В современном мире в ходе быстрого развития информационно-коммуникационных технологий человек проводит большую часть своего времени в сети Интернет и в виртуальном общении. Общаясь с другими людьми, покупая товары, используя социальные сети, оплачивая различные счета через интернет, человек оставляет в сети множество информации, которая его идентифицирует, отличает от других пользователей сети. В правом аспекте совокупность данной информации рассматривают как «персональные данные», что и определяется специальным законом страны.

Согласно ст. 1 Закона Республики Беларусь «О защите персональных данных», под персональными данными понимается «любая информация, относящаяся к идентифицированному физическому лицу или физическому лицу,

которое может быть идентифицировано» [1]. В данном определении достаточно общим рассматривается, по нашему мнению, самый существенный критерий определения личной информации, который позволяет выделять такие данные из огромного массива рыночной информации. Таким критерием является возможность идентификации физического лица с помощью различных персональных данных. И это не случайно, поскольку законодательно содержание и структура личных данных физических лиц не определены. Вместе с тем, с развитием цифровых технологий и переходом взаимодействия субъектов преимущественно в цифровой формат, к персональным данным наиболее целесообразно было бы отнести информацию о самом субъекте, включая законодательно определенную, его фактах из жизни, событиях и обстоятельствах, закрепленная на каком-либо носителе и позволяющая идентифицировать данного субъекта из различных источников. При этом следует учитывать, что в последние годы рост киберпреступлений в финансовой сфере стал возможен только потому, что мошенники и хакеры, выявляя и обладая только частью персональной информации о субъекте способны завладеть средствами клиентов финансовых структур.

В сложившейся ситуации необходимо системное обеспечение безопасности данных со стороны государства, включая формирование специальных организационных структур управления в этой сфере, разработку и принятия специальных законов области противодействия киберпреступности.

С целью надлежащей реализации права на защиту персональных данных в Республике Беларусь был создан специальный уполномоченный орган по защите прав субъектов персональных данных. Данный орган сформирован Указом Президента Республики Беларусь от 28 октября 2021 г. № 422 «О мерах по совершенствованию защиты персональных данных» [2]. Организация получила официальное название как «Национальный центр защиты персональных данных Республики Беларусь».

В условиях цифровизации производственных и управленческих процессов организации, которые используют в своей экономической деятельности анализ и обработку данных о клиентах, должны принимать меры по их защите. Данное требование обусловлено не только необходимостью реализации чисто коммерческой составляющей данной информации для организации, но и мерами безопасности. Для современных инновационных организаций, использующих коммерческую тайну (базы данных клиентов относятся коммерческой информации) такими мерами являются организационно-правовые и технические меры защиты данных как коммерческой информации. При этом программные меры защиты должны быть ориентированы на создание действенных барьеров по снижению основных рисков: внешних и внутренних, которые также называют «инсайдерскими» [3].

Внешние угрозы включают незаконные проникновения в информационную систему организации, например, хакерские атаки. Второй тип угроз – инсайдерские угрозы - встречаются более часто, чем первый тип. Граждане могут раскрывать свою личную информацию, обращаясь в медицинские учреждения

или туристические агентства, в которых зачастую согласия на обработку персональных данных не подписываются. Личные данные гражданина, включая паспортные, информацию о владении недвижимом имуществе, финансах, операциях с банковскими картами, могут оказаться в уязвимом положении, находясь, например, в компьютерных системах, не имеющих базовой защиты. В таких случаях доступ к этой информации может быть получен:

– при прямом проникновении недобросовестного сотрудника агентства в компьютер или к материальным носителям информации [3];

– при хранении данных в облачных сетях, часто на нескольких серверах, которые зачастую находятся за пределами границ Республики Беларусь. Несмотря на требования законодательства о необходимости хранить персональные данные внутри страны, не все провайдеры соблюдают эти правила, зачастую даже не осведомленные о такой обязанности;

– при краже ноутбука или портфеля сотрудника компании, в котором содержится интересующая злоумышленника информация [3].

Рассмотрим подробнее меры по защите персональных данных с учетом различных ситуаций, которые ориентированы на противодействие цифровым правонарушениям и распространение безопасных технологий. Такие меры могут организационные и технические, при этом реальный эффект может принести только системный подход по защите персональных данных.

К организационным мерам относят практики, которые применяются в целях сохранения безопасности, конфиденциальности и целостности данных. Это, например, поддержка руководства, заключающаяся в заинтересованности руководства в защите персональных данных; управление рисками, подразумевающее оценку рисков для безопасности данных и построение стратегии управления рисками в целях минимизации возможных угроз и последствий; управление инцидентами, в рамках которого создается план действий, используемый в тех случаях, когда была нарушена безопасность данных или произошла утечка информации, для быстрой и эффективной реакции на инциденты [4]. Для уменьшения рисков необходимо на постоянной основе контролировать квалификацию работников и обучать их новым способам охраны конфиденциальных данных, а также проводить обучающие программы на темы охраны персональных данных и кибербезопасности.

Технические меры включают разнообразные подходы и инструменты, нацеленные на создание системы, обеспечивающей безопасность, конфиденциальность и целостность данных. К примеру, это может быть шифрование данных, которое не позволяет чужим лицам получить доступ к персональным данным; применение протоколов (например, HTTPS и VPN), необходимых для обеспечения установленного шифрованного канала между пользователем и веб-ресурсом, с целью минимизировать риски, связанные с перехватом и прослушиванием передаваемых данных; управление доступом, обеспечивающее доступ к персональным данным, предоставив его лишь доверенным сотрудникам и менеджерам; использование многофакторной аутентификации для дополнительного уровня защиты данных, которая заключается в том, что

для получения доступа к системе пользователю необходимо предоставить несколько отличающихся между собой методов проверки личности (как, например, пароль и код, полученный по SMS); резервное копирование данных, позволяющее свести к минимуму риск снизить риск потери данных в случае атак или сбоев [4]. Следует также использовать псевдонимизацию, то есть замену реальных имен и фамилий сотрудников на псевдонимы. Все это позволит снизить риск утечки информации, указывающей на конкретного работника. Необходимо постоянно обновлять программное обеспечение, в особенности финансовые программы и защитные программы. Возможно также использовать видео- и аудио-наблюдения, а также средства биометрической идентификации, в частности отпечатки пальцев или распознавания лица.

Таким образом, в современном мире, где информационно-коммуникационные технологии стали неотъемлемой частью нашей жизни, персональные данные о клиентах становятся стратегическим ресурсом, объектом интеллектуальной собственности. В Республике Беларусь защита персональных данных регулируется законодательством, а их обработка требует строгих мер безопасности. Организационные практики, такие как управление рисками и управление инцидентами, важны для обеспечения безопасности данных, включая работу с персоналом при заключении трудовых контрактов. При этом в трудовых контрактах следует полностью определять порядок доступа к конфиденциальной информации, механизм доступа, ответственных лиц за использование такой информации. Технические меры, такие как шифрование, управление доступом и многофакторная аутентификация, играют ключевую роль в защите персональных данных от угроз как изнутри, так и снаружи. Все это содействует обеспечению конфиденциальности, целостности и безопасности данных в цифровом пространстве.

Список использованных источников:

1. О защите персональных данных : Закон Респ. Беларусь, 7 мая 2021 г., № 99-З : в ред. Закона Респ. Беларусь от 01.06.2022 г. // Консультант Плюс : Беларусь [Электронный ресурс] / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. – Минск, 2024. – Режим доступа: https://www.prlib.ru/item/467962. – Дата доступа: 10.05.2024.

2. О мерах по совершенствованию защиты персональных данных : Указ Президента Респ. Беларусь, 28 октября 2021 г. № 422 // Национальный правовой Интернет-портал Республики Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2024. – Режим доступа: https://pravo.by/document/?guid=12551&p0=P32100422. – Дата доступа: 16.04.2024.

3. Утечка персональных данных: последствия [Электронный ресурс]. – Режим доступа: https://searchinform.ru/resheniya /biznes-zadachi/zaschita-personalnykh-dannykh/utechki-personalnyh-dannyh/ posledstviya/. – Дата доступа: 10.05.2024.

4. Защита персональных данных в интернете [Электронный ресурс]. – Режим доступа: https://beseller.by/blog/zashchita-personalnykh-dannykh-belarus/ – Дата доступа: 10.05.2024.