УДК 004.056.5

К ВОПРОСУ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ФИЗИЧЕСКИХ ЛИЦ, ИСПОЛЬЗУЮЩИХ ИНФОРМАЦИОННУЮ ИНФРАСТРУКТУРУ

О. В. Босько

Институт информационных технологий УО «Белорусский государственный университет информатики и радиоэлектроники»,
ул. Петруся Бровки 6, Минск, 220013, Беларусь

Статья посвящена анализу и систематизации рисков, которым подвергаются участники информационного обмена, а также вопросу обеспечения безопасности персональных данных физических лиц, использующих информационную инфраструктуру в личных целях.

Ключевые слова: информационная инфраструктура, информационный обмен, персональные данные, безопасность, риски.

TO THE QUESTION OF ENSURING THE SECURITY OF PERSONAL DATA OF INDIVIDUALS USING INFORMATION INFRASTRUCTURE

O. V. Bosko

Institute of Information Technologies
Belarusian State University of Informatics and Radioelectronics,
6 Petrusya Brovki street, Minsk, 220013, Belarus

The article is devoted to the analysis and systematization of the risks to which the participants of information exchange are exposed, as well as the issue of ensuring the security of personal data of individuals using the information infrastructure for personal purposes.

Keywords: information infrastructure, information exchange, personal data, security, risks.

Использование информационной инфраструктуры для информационного обмена имеет неоспоримые преимущества, среди которых экономия, функциональность, эффективность и целый ряд других. Однако помимо положительных сторон есть риски, которым подвергается как информация, так и сами участники информационного обмена.

Для передаваемой информации существует угроза перехвата, изменения либо подделки и утери информации. В связи с этим основными целями информационной безопасности является сохранение:

- конфиденциальности информации (ее доступности только ограниченному кругу пользователей информационной системы);

- целостности информации (обеспечения защиты от случайного или преднамеренного искажения или разрушения);

- доступности информации.

Опасность перехвата данных особенно велика при использовании сети Интернет. Интернет является открытой системой, предназначенной для свободного обмена информацией. Злоумышленники часто предпринимают попытки несанкционированного доступа к информации. Их действия представляет постоянную угрозу, в том числе для сетей, подсоединенных к Интернету.

При информационном обмене существует риск, что канал обмена данными может быть использован для проведения кибератак. Участник обмена не может в полной мере быть уверен в защищенности других сторон взаимодействия и безопасности передаваемой ими информации. Файлы могут содержать компьютерные вирусы любого типа, червя, троянскую программу или вредоносную программу другого типа, которые могут нанести серьезный урон, привести к повреждению или даже полной утрате информации, содержащейся на компьютере получателя. Еще одним риском для участников информационного обмена является угроза безопасности их персональных данных. В соответствии с Законом Республики Беларусь «О защите персональных данных» персональные данные – любая информация, относящаяся к идентифицированному физическому лицу или физическому лицу, которое может быть идентифицировано [1].

Таким образом, исходя из определения, которое дает закон, персональные данные, – это любая информация, с помощью которой можно прямо или косвенно идентифицировать человека. К такой информации можно отнести паспортные данные (ФИО, пол, дата рождения, серия и номер паспорта, личный номер, адрес регистрации и проживания); биометрические данные (отпечатки пальцев, ладоней, радужная оболочка глаза, характеристики лица и его изображение, описание внешности); генетические данные (ДНК, группа крови); специальные персональные данные (расовая либо национальная принадлежность, политические взгляды, членство в профсоюзах, религиозные или другие убеждения, здоровье, привлечение к административной или уголовной ответственности) и т.д.

Закон Республики Беларусь «О защите персональных данных» регулирует отношения, связанные с защитой персональных данных при их обработке, и не распространяется на отношения, касающиеся случаев обработки персональных данных физическими лицами в процессе исключительно личного, семейного, домашнего и иного подобного их использования, не связанного с профессиональной или предпринимательской деятельностью.

В связи с тем, что физические лица часто используют информационную инфраструктуру и становятся участниками информационного обмена в личных целях, безопасность их персональных данных не всегда может быть обеспечена в процессе таких коммуникаций.

Если рассматривать информацию в качестве объекта, который может быть уничтожен, изменен или похищен, то граждане чаще всего подвергаются следующим видам атак [2]: а) вирусы, трояны, иные вредоносные программы, наносящие урон целостности компьютерных систем; б) программы-вымогатели, занимающие весь экран устройства и не исчезающие до выплаты мошенникам определенной суммы; в) фишинг или хищение информации о банковских картах и счетах путем социальной инженерии, когда физическое лицо добровольно выдает мошеннику, представившемуся сотрудником банка, требуемую информацию, или путем подмены сайта магазина или кредитного учреждения на его подобие; г) кража персональных данных для последующего использования с целью получения каких-либо преференций от имени пострадавшего.

Персональные данные физических лиц, полученные в процессе личного информационного обмена, могут быть использованы злоумышленниками для иных целей (побуждение к совершению преступлений, вовлечение в экстремистскую деятельность и др.).

Таким образом, в результате проведенного анализа определены риски, которые возникают в процессе информационного обмена и использования информационной инфраструктуры: риски для конфиденциальности, целостности и доступности информации (как передаваемой, так и содержащейся на компьютерах участников информационного обмена), а также риски для сохранности персональных данных участников информационного обмена.

В связи с тем, что персональные данные физических лиц могут быть использованы для противоправной деятельности, обосновано разработать комплекс мер, направленных на обеспечение безопасности персональных данных физических лиц, использующих информационную инфраструктуру в рамках информационного обмена, осуществляемого в личных целях.

Библиографический список

1. О защите персональных данных [Электронный ресурс] : Закон Респ. Беларусь, 7 мая 2021 г., № 99-З // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

2. Свойства безопасности информации [Электронный ресурс] // Информационная безопасность. – Режим доступа: https://searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/osnovnye-aspekty-informatsionnoj-bezopasnosti/svojstva-bezopasnosti-informatsii/. – Дата доступа: 04.10.2022.