НАЦІОНАЛЬНА БЕЗПЕКА

Котюжинский Е.И., Рожкова А.Л., Каличин Э.В.
магистры,
Одесская национальная академия связи имени А.С. Попова

ПРОБЛЕМАТИКА ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В СЕТИ INTERNET

Персональные данные – это любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных). К такой информации могут относиться фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация. Именно такое расширенное определение дает Закон Украины «О защите персональных данных» [1]. Пользователи часто предоставляют персональные данные, возможно, не обращая на это особого внимания. Взаимодействие с государственными органами и структурами, ведение хозяйственной деятельности, подача деклараций, открытие банковского счета, процедура устройства на работу, взаимодействие с мобильным оператором связи – только некоторые из примеров оперирования персональными данными. Стоит отметить, что мир стремительно «диджитализируется», множество привычных сервисов и услуг уходят в сеть Internet, а за ними уходят и потребители услуг. Как отмечается в [2], со следующего года в государственных органах Украины благодаря продуктам проекта «Дия» от Министерства цифровой трансформации все услуги планируют сделать цифровыми. Но при этом отмечается, что помимо несомненных удобств, есть ряд угроз и рисков, которые стоит учитывать вследствие отсутствия цифровой грамотности и понятия основ безопасности по защите персональных данных у части населения.

Помимо взаимодействия с государством и системными бизнесами, где часто защиту ПД берет на себя сервис или платформа с услугами, граждане ведут активную деятельность в сети Internet, оставляя множество цифровых следов. Как следует с ресурса Википедия, цифровой след (или цифровой отпечаток; англ. digital footprint) – это уникальный набор

действий в сети Internet. Существуют два основных типа цифровых следов: пассивные и активные. Пассивный цифровой след – это данные, которые собираются без ведома владельца. Активный цифровой след появляется, когда пользователь намеренно публикует свои персональные данные, чтобы рассказать о себе в Facebook или Instagram, веб-сайтах, форумах, чатах, группах, тематических площадках и т.д.

Специалистами по OPSEC (операционная безопасность) первым шагом к пониманию факта, какие цифровые следы о субъекте существуют в сети, предлагается идентифицировать чувствительную информацию, используя методы и средства OSINT. На рис. 1 представлены типы приватных (персональных) данных, которые в чаще всего можно обнаружить методами конкурентной разведки.

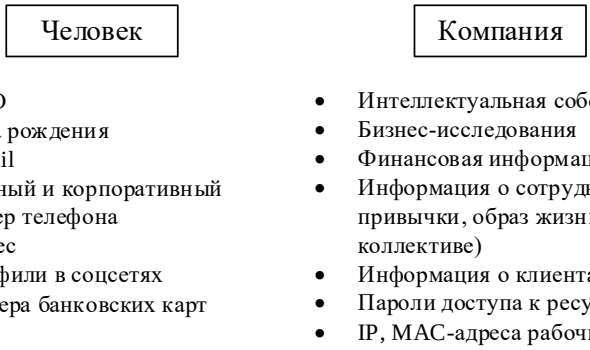

Рис. 1. Основные типы приватных (персональных) данных в сети Internet

Существует несколько классификаций киберпреступлений. Согласно одной из них, преступления разделяются на финансово-ориентированные (фишинг, кибервымогательства, мошенничество), нарушение авторского права, спам, социально или политически-мотивированные, а также киберпреступления, связанные с вторжением в личную жизнь (шпионаж и кража персональных данных). Злоумышленники используют различные инструменты для кражи персональных данных, наиболее известный способ – связка «фишинговая атака + социальная инженерия». Социальная инженерия – это эффективный инструмент получения злоумышленником

информации, в основе которой лежит создание ситуаций, в которых люди сами предоставляют злоумышленникам сведения.

По своей сути, такой сценарий является таргетированной атакой (индивидуальный набор хакерских действий), где за кражей ПД часто стоит монетизация. Помимо этого, сегодня в DarkNet появился новый тренд – продажа цифрового идентификатора и следа пользователя. Риски жертвы, если злоумышленник завладел такой информацией, могут быть значительными, т.к. покупатель получает возможность полностью подменить свой цифровой след на след жертвы.

Для получения доступа к банковским картам пользователя (реквизиты карты, CCV-код на ее обратной стороне и срок действия) злоумышленники применяют как пассивные способы сбора данных (через поддельные сайты), так и активные – методами социальной инженерии, представляясь сотрудниками call-центра. В данном случае среди множества составляющих в системе электронных платежей именно пользователь выступает наиболее уязвимым компонентом.

Защита персональных данных – это комплекс мероприятий, который основан на использовании организационных, правовых, программных, аппаратных методов и средств [3]. Но часто применение базовых методов существенно снижает риски компрометации ПД. Регулярное обновление устройств и ПО на них, оставление данных только на проверенных сайтах, замена скомпрометированных паролей, “табу» на передачу копий паспортов в месенджерах, шифрование паролей – некоторые из них. И самое важное – пользователям стоит внимательно относиться к своим собственным действиям, помня о возможных последствиях.

Список использованных источников:

1. Закон Украины «О защите персональных данных» [Електронний ресурс] // Правовед. – Режим доступу: http://pravoved.in.ua/section-law/193-zuozpd.html

2. Диджитализация в Украине: плюсы и минусы [Електронний ресурс] // Comments.ua. – 2020. – Режим доступу: https://politics.comments.ua/news/domestic-policy/didzhitalizaciya-v-ukraine-plyusy-i-minusy-661623.html

3. Кравцов М.І. Щодо захисту пд в аспекті проблематики кіберзлочинства / Кравцов М.І., Бєлик М.О., Кочетков О.В. // Матеріали 74-ї науково-технічної конференції професорсько-викладацького складу, науковців та студентів ОНАЗ ім. О.С. Попова. – 2019. – С. 153–155.