ЮРИДИЧНІ НАУКИ

УДК 34

ПРОБЛЕМА ОБІГУ ПЕРСОНАЛЬНИХ ДАНИХ В МЕРЕЖІ ІНТЕРНЕТ

Виноградов С.С.
Навчально-науковий інститут інформаційної безпеки
Національної академії Служби безпеки України

Досліджені питання обігу персональних даних в мережі Інтернет та актуальні проблеми їх захисту. Розглянуті варіанти застосування превентивних заходів щодо протидії незаконного привласнення персональних даних в мережі. Детально висвітлені правові та технічні можливості забезпечення охорони персональних даних. Крім того, проаналізовані проблеми між правовим регулюванням обігу персональних даних та реальною ситуацією в мережі.
Ключові слова: персональні данні, правове регулювання обігу, превентивні заходи, технічні можливості охорони, мережа Інтернет.

Постановка проблеми. Мережа Інтернет, як і більшість інформаційних технологій, є дуже популярними на теперішній час, тому зараз важко уявити людство до масового впровадження інтернету до цивільного сектору. Завдяки мережі Інтернет у людини є можливість придбання важливих для життя речей (їжа, одяг, побутова техніка) використовуючи тільки персональний комп'ютер, заробляти гроші в мережі знаходячись будь-де, тощо. Платою за такі можливості є – вимога надати персональні дані для реалізації можливостей, що надає мережа.

Будь-який сайт, для надання повноцінних можливостей користувачу, вимагає пряму реєстрацію – із зазначенням персональних даних, або авторизацію, що використовує профілі соціальних мереж, що належать користувачу, де всі необхідні дані вже вказані.

Кожен з веб проектів має тенденцію та реалізований функціонал відстеження дій користувача на сайті з метою маркетингових досліджень. Іншими словами усі дії користувача на сайті, а також IP адреса, версія операційної системи, назва та версія Інтернет браузера, який використовується, час, який користувач перебував на сайті, фіксується у записах на сервері та може бути використаним власником Інтернет ресурсу на свій розсуд.

Реєстрація скриньки електронної пошти вимагає від користувача залишити персональні дані: ПІБ, дата народження, номер телефону, інакше процес реєстрації електронної пошти не може бути завершеним.

З часом роботи в мережі, у будь-якого досвідченого користувача виникають питання: як залишатися анонімним в мережі? Як захистити себе від відстеження та зберегти персональні дані від несанкціонованого доступу?

Аналіз останніх досліджень і публікацій. Правові механізми обігу та охорони персональних даних викладені у доступній формі в законі України про «Захист персональних даних» [1]. Крім того існують директиви Європейського парламенту і Ради, що регулюють це питання на міжнародному рівні: Директива 95/46/ЄС «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» [2], Директива 97/66/ЄС «Про обробку персональних даних і захист прав осіб у телекомунікаційному секторі» [3]. Т. Обуховська у своїй статті: «Захист персональних даних в умовах розвитку інформаційного суспільства: Передумови, принципи та міжнародне законодавство» [6] аналізує базові принципи, міжнародні правові акти, що регламентують відносини у сфері захисту персональних даних та загальновизнані, міжнародні стандарти щодо захисту персональних даних, у тому числі «Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних» № 108 від 28 січня 1981 р. [8]. К.С. Мельник у своїй статті «Обробка та захист персональних даних в соціальних мережах» також висвітлює актуальні питання обробки та захисту персональних даних в соціальних мережах» [7], здійснює аналіз проблемних аспектів забезпечення приватності в соціальних мережах, але ці публікації висвітлюють теоретичну частину обігу персональних даних у мережі Інтернет, без практичної її складової, тобто без реалій користувачів та взаємовідносин між ними.

Виділення невирішених раніше частин загальної проблеми. В Україні на законодавчому рівні ця проблема регулюється законом «Про захист персональних даних», який зобов'язує повідомляти всіх суб'єктів персональних даних про факт обробки або передачі персональних даних третім особам. Впровадження в мережу цього закону відбувається слабо, тому, що Інтернет є фактично безконтрольний кіберпростір, що надає можливість робити що завгодно кожному користувачу, без наслідків нести за противоправні дії юридичну відповідальність.

У світі інформаційних технологій, існують негласні домовленості між власниками Інтернет бізнесів про обмін інформацією та користувачів, що відвідали інтернет ресурси. Кожна з компаній, яка працює в мережі, має певну клієнтську базу, ретельно зібрану за час існування компанії. Для подальшого ефективного існування, компанії необхідно знаходитись на першій сторінці пошукових систем, по запитах користувачів, стосовно того ринкового сегмента, в якому працює компанія.

Головною умовою перебування на перших сторінках Google, Yandex, Yahoo та інших пошукових системах є факт посилання на інтернет ресурс зі сторонніх веб сайтів. Це означає, що кількість посилань зі сторонніх Інтернет ресурсів на компанію, прямо пропорційна рейтингу компанії у позиціях пошукової системи за заданими ключовими словами пошуку. Найпростіший спосіб отримати посилання зі сторонніх ресурсів, не витрачаючи значні кошти – це домовленість з власниками Інтернет ресурсів, схожими з тематикою компанії, про обмін персональними даними клієнтів. Це можуть бути портали, каталоги, тематичні форуми, розважальні журнали. Для більшості веб проектів обмін клієнтською базою є вигідним, на відміну від суб'єктів «електронної комерції» (e-commerce).

Отже, є закон, який намагається регулювати обмін персональними даними, а з іншого боку – негласні домовленості Інтернет бізнесу, дотримання яких власникам Інтернет ресурсів є більш важливим, ніж встановлена законодавством України відповідальність за незаконне поширення персональних даних.

Мета статті. Метою цієї статті є комплексний аналіз наявних реалій обігу персональних даних в мережі Інтернет. Висвітлення проблем між законодавством регулюючим цей обіг та внутрішніми законами безконтрольного кіберпростору. Узагальнення цієї проблеми та пошук можливих шляхів вирішення.

Виклад основного матеріалу. Нині стосовно регулювання обігу персональних даних в мережі існує три загальні проблеми, це:

1. збереження анонімності;
2. захист користувачів від відстеження дій;
3. захист персональних даних від несанкціонованого доступу.

Інтернет гіганти, такі як Google, Microsoft, Yahoo, а також російський Yandex вирішують проблему анонімності, надаючи користувачам можливість користуватися їх ресурсами знеособлено. Однак для повноцінного користування ресурсами, наприклад того ж Google, користувачеві необхідно зареєструватися. Привілеї значні: 15 Гб дискового простору на серверах Google, захищену від злому електронну пошту, повну синхронізацію зі смартфоном та багато чого ще. Кожен інтернет магазин, оформлені замовлення вимагає від користувача реєстрації, де має бути вказано, ПІБ, номер телефону, адреса електропошти. Реєстрація необхідна для підтвердження замовлення через e-mail користувача та формування рахунку фактури на певний товар. У деяких випадках потрібно вказати адресу проживання (для оформлення доставки). Зрозуміло, що збирання персональних даних необхідно для здійснення організованого процесу продажу товарів, або послуг у мережі Інтернет, але водночас зростає і ризик. Існує вірогідність, що зібрані персональні дані «розпорядники» використовують для протиправних діянь у мережі. Наприклад: «маркетингові дослідження» в мережі, дуже часто є збором персональних даних користувачів, які потім використовуються для розсилок електронної реклами, або спаму. В іншому випадку персональні дані можуть бути викраденими зловмисниками, для продажу баз даних користувачів мережі на нелегальних форумах, для отримання прибутку. Потрібно усвідомлювати, що Інтернет магазини створюються для отримання прибутку власником, а не для забезпечення схоронності персональних даних клієнтів. Вимога безпеки завжди присутня в технічному завданні на створення Інтернет магазину, і навіть створюється механізм захисту персональних даних, але цей функціонал, має ціну, що іноді перевищує бюджет всього проекту, тому належної уваги механізму захисту не приділяється. Мається на увазі, що створюючи максимальний комфорт для клієнтів у мережі, зростає ризик поширення персональних даних людей третім особам, без згоди на розпорядження персональними даними та можливості контролювати цей процес.

Відомо, що користувачі в мережі здійснюють дії від перегляду стрічки новин до користування сервісами електронної комерції. Кожна дія фіксується в історії переглядів Інтернет браузера та у записах веб сайту, що зберігаються на сервері й постійно оновлюються. Потрібно знати, що сервіси фіксації дій користувача потрібні для пошукової оптимізації, аналізу сторінок входу – сторінка, з якої користувач потрапив на сайт, сторінок виходу – сторінок, з яких користувач покинув веб ресурс. Крім того, ця інформація використовується для аналізу часу, який клієнт перебував на веб сайті та на кожній його сторінці. Ці дані використовують веб майстри та інтернет маркетологи. Компанія Google надає потужний сервіс для реалізації функціоналу дослідження дій користувача – Google Analytics. Ідея інструменту полягає в оптимізації розвитку Інтернет бізнесу, але може бути використана зловмисниками для реалізації шахрайських схем – фішингу. Сенс таких схем у зборі переваг користувача та інтересів, і створення моделі його поведінки. Далі користувача направляють на сторінку-клон популярного сайту, де клієнт залишає персональні дані, не замислюючись про наслідки. Після цього користувача перенаправляють на сторінку оригінального web-сайту, щоб приховати факт незаконного збору персональних даних. Як відомо, існує закон, який забороняє незаконний збір персональних даних та юридична відповідальність у кримінальному кодексі за ці протиправні дії, але основна ідея шахрайських схем в тому, що людина добровільно залишає персональні дані на сайтах-клонах. В Україні, ще не має юридичної практики патентування дизайну веб сайтів, це означає, що людина, опонувавши програмування, має можливість повністю скопіювати структуру, функціонал та кольорову гаму будь-якого сайту, наприклад, для заробітку на рекламі або банальних хвастощів.

Розуміючи суть того, що персональні дані не знаходяться під надійним контролем у мережі, поряд з тим, що захист персональних даних регулюється як з правової, так і з технічної сторони, постає питання: як саме убезпечити персональні дані? Однозначної відповіді на це питання досі немає ні у юристів, які намагаються правовими нормами захистити персональні дані в мережі, ні в інженерів з безпеки комп'ютерних мереж. Причина явна: «Те, що створюється людиною, людиною і руйнується».

Тому для захисту персональних даних, необхідно виконувати певні правила при роботі у ме-

режі, унеможливлюючи можливість потраплян-ня персональних даних до зловмисників:

1. Для перегляду сайтів бажано використовувати режим інкогніто Інтернет браузера з включеним режимом захисту від відстеження. Така дія дозволяє не зберігати історію переглядів. Включений режим захисту від відстеження дає можливість не залишати у записах серверів технічної інформації про персональний комп'ютер, яка може бути корисною для зловмисників.

2. Використання протоколу https для перегляду Інтернет сторінок. Цей протокол шифрує вихідний трафік користувача і не дає можливість його перехоплення та подальшого розшифрування. У вихідному трафіку зберігається найбільш важливі для зловмисників персональні дані користувача (дані авторизації, паролі від електронної пошти, IP адреси). Доступ до такої інформації, повинен бути обмежений для сторонніх осіб. Всі Інтернет браузери, від Internet Explorer від Microsoft, до Safari від Apple надають можливість шифрування з'єднання по протоколу https.

Для браузерів: Opera, Firefox та Chrome, існує додаток HTTPS Everywhere, що перенаправляє користувача на https версію сайту.

3. Необхідно уважно перевіряти адреси популярних сайтів. Це пов'язано з тим, що зловмисники використовують різні схеми, щоб змусити користувачів залишити свої персональні дані у схожій за адресою сторінці соціальної мереж або клонованому Інтернет-магазині. В іншому випадку кіберзлочинці використовують електронні листи, що містять посилання на клоновані сайти. Тому потрібно уважно перевіряти зміст електронної пошти.

Технічні рекомендації спеціалістів з інформаційної безпеки, допомагають користувачам зберегти персональні дані в мережі, а методи правового регулювання запобігають незаконному поширенню персональних даних та забезпечують гарантії безпеки в інтернеті на поточному етапі: Закон «Про Захист Персональних Даних», Стаття 32 Конституції України «Ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України» і заходи відповідальності, за недотримання законності: Стаття 182 Кримінального кодексу України «Порушення недоторканності приватного життя». В майбутньому, правова база забезпечення захисту персональних даних в інтернеті буде повністю доопрацьована і впроваджена в інформаційно-телекомунікаційний простір.

Де-факто проблема обігу персональних даних у мережі, є глобальною, і охоплює всі групи користувачів мережі Інтернет, від користувачів до професійних кіберзлочинців. Право вибору є у кожного користувача в мережі, використовувати сервіси та механізми для забезпечення анонімності та повного збереження персональних даних, або залишати персональні дані всюди, не замислюючись про наслідки. Крім того є категорія користувачів, що активно користується помилками людей у мережі, з метою особистого збагачення або підняття власного ЕГО. Правове регулювання «Захисту персональних даних» з часом буде реалізовано і впроваджено в мережу Інтернет на належному рівні й користувачам не потрібно буде користуватися технічними засобами забезпечення анонімності в мережі. А наглядовим органам буде повністю передана функція стеження за дотриманням законності при передачі, обробці та поширенню персональних даних суб'єктів.

Висновки і пропозиції. Використання комбінованих методів захисту персональних даних в інтернеті, має позитивний результат. Причиною тому є тенденція розвитку захисту інформації користувача використовуючи норми правового регулювання обігу персональних даних в мережі Інтернет. Необхідно зазначити, що інтернет корпорації також зацікавлені у співробітництві з користувачами мережі та збереження персональних даних на власних серверах. У той самий час стрімко розвивається напрямок кіберзлочинності, спрямований на незаконне збирання та використання персональних даних користувачів глобальної мережі інтернет, використовуючи лазівки, як в законодавстві, так і пролом у захисті інформації на серверах, персональних комп'ютерах і смартфонах. Однак стрімкий розвиток напрямку захисту інформації та свідомість користувачів, які прагнуть конфіденційності, призведе до виродження кіберзлочинності як явища. Цей факт, у свою чергу, дозволить людям насолоджуватися перевагами інтернет технологій у повному обсязі, не турбуючись про збереження своїх персональних даних. А повноцінний захист, що буде реалізовано на державному рівні, дозволить швидко вирішувати суперечливі питання, завдяки законодавчій базі стосовно обігу персональних даних в мережі інтернет.

Список літератури:

1. Про захист персональних даних [Електронний ресурс]: Закон України № 2297-VI від 1 черв. 2010 р. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/2297-17.
2. Про захист осіб у зв'язку з обробкою персональних даних та вільним обігом цих даних [Електронний ресурс]: Директива 95/46/ЄС Європейського парламенту та Ради від 24 жовт. 1995 р. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/994_242.
3. Про обробку персональних даних і захист прав осіб у телекомунікаційному секторі [Електронний ресурс]: Директива 97/66/ЄС Європейського парламенту та Ради від 15 груд. 1997 р. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/994_243.
4. Лайфхакер «Как защитить свои персональные данные в интернет» [Електронний ресурс]. – Режим доступу: https://lifehacker.ru/2016/06/06/protecting-your-personal-data.
5. Офіційний блог лабораторії Касперського: «Хотите знать, что известно о вас Google» [Електронний ресурс]. – Режим доступу: https://blog.kaspersky.ru/google-privacy/9819.
6. Обуховська Т. І. «Захист персональних даних в умовах розвитку інформаційного суспільства: Передумови, принципи та міжнародне законодавство» [Електронний ресурс] / Обуховська Т. І. – Режим доступу: http://visnyk.academy.gov.ua/wp-content/uploads/2014/05/2014-1-17.pdf.

7. Мельник К. С. «Обробка та захист персональних даних в соціаль-них мережах» [Електронний ресурс] / Мельник К. С. – Режим доступу: http://ippi.org.ua/sites/default/files/14mksdsm.pdf.
8. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних [Електронний ресурс]: Конвенція Ради Європи № 108 від 28 січ. 1981 р. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/994_326.

Виноградов С.С.
Учебно-научный институт информационной безопасности
Национальной академии Службы безопасности Украины

ПРОБЛЕМА ОБОРОТА ПЕРСОНАЛЬНЫХ ДАННЫХ В СЕТИ ИНТЕРНЕТ

Аннотация
Исследованы вопросы оборота персональных данных в сети Интернет. А также актуальные проблемы охраны персональных данных. Рассмотрены вопросы применения превентивных мер касательно противодействия незаконного присвоения персональных данных в сети. Детально освещены правовые и технические возможности обеспечения охраны персональных данных. Кроме того, проанализированы проблемы между правовым регулированием оборота персональных данных и реальной ситуацией в сети.
Ключевые слова: персональные данные, правовое регулирование оборота, превентивные меры, технические возможности охраны, сеть Интернет.

Vynohradov S.S.
Educational Scientific Institute of Information Security
National academy of Security service of Ukraine

THE PROBLEMS OF THE TURNOVER OF PERSONAL DATA ON THE INTERNET

Summary
The issues of the turnover of personal data on the Internet are investigated. And also actual problems of protection of personal data. Questions of application of preventive measures concerning counteraction of illegal appropriation of personal data in a network are considered. The legal and technical possibilities of securing the protection of personal data are described in detail. In addition, the problems between the legal regulation of the turnover of personal data and the real situation in the network have been analyzed.
Keywords: personal data, legal regulation of turnover, preventive measures, technical security capabilities, the Internet.