Бібліографічні посилання

1. Про національну безпеку України : Закон України. Документ 2469-VIII, чинний, поточна редакція. Редакція від 01.08.2021, підстава – 1702-IX.
2. Рішення Ради національної безпеки і оборони України від 22 жовтня 2021 року «Про Концепцію реформування Державної служби спеціального зв'язку та захисту інформації України» : Указ Президента України від 22 жовтня 2021 року № 544/2021.
3. Конах В. К. Нормативно-правові засади державної політики України у сфері інформаційно-психологічної безпеки. *Стратегічні пріоритети*. 2012. № 3 (24). С. 152–157.
4. У Комітеті з питань цифрової трансформації відбулися слухання на тему: «Електронна демократія в Україні – дорожня карта для цілі – Україна в ТОП-20». URL: https://thedigital.gov.ua/news/komitet-rozglyanuv-4-zakonoproekti-ta-obgovoriv-praktiku-vikonannya-zakonodavstva-pro-kiberbezpeku-z-derzhavnimi-organami

Калюжна А. О., слухачка
магістратури юридичного факультету
Науковий керівник – Косиченко О. О.,
доцент кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат технічних наук, доцент

РИЗИКИ ВИКОРИСТАННЯ СИСТЕМ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ КОРИСТУВАЧІВ

Біометрія все частіше використовується для ідентифікації громадян у різних сферах життя: для отримання банківських послуг, для складання он-лайн іспитів, оплати проїзду на транспорті тощо [1–3]. Біометричні дані вважаються «надчутливими». При цьому виникають питання довіри до штучного інтелекту стосовно ухвалення остаточних рішень. І збереження паперових копій документів у багатьох випадках має сенс. Тобто є певні ризики використання біометричних даних.

Біометричні дані, на відміну будь-яких інших, що використовуються для ідентифікації, є невід'ємною частиною кожної людини. На відміну від пароля, номера телефону та прізвища, що використовуються зараз, не можна в разі витоку або компрометації даних, змінити своє обличчя, сітківку, фігуру, відбитки пальців тощо. Це надчутливі, але при цьому незмінні дані, які, в принципі, можна вкрасти.

Біометрична інформація та інші, персональні або платіжні дані, що зберігаються в конкретних базах даних, схильні до банальних витоків, кількість яких у всіх сферах життя неухильно зростає. Це відбувається

переважно не через технологічні проблеми, а через людський фактор.

Прихильники біометрії запевняють, що бази даних якось особливо захищені, що впроваджені відповідні криптографічні системи. Насправді немає ніяких особливих способів убезпечити біометричні дані – це звичайні дані, які зберігаються у звичайних базах даних. І працюють з ними ті ж люди, звичайні системні адміністратори, які отримують не звичайні зарплати, при цьому вони самі призначають права доступу – тобто можуть налаштувати собі доступ, куди завгодно та будь-якого рівня. Тут діє старий закон: якщо є можливість для зловживань – то треба вважати, що вони вже є.

Справді, нелегальні послуги «пробивки» людей за особистими даними існують уже давно, чорний ринок інформації бурхливо розвивається. Шахраї дуже винахідливі, тому щойно з'являється новий вид цифрового контенту, вони відразу вигадують, як із цього можна отримати прибуток. Будуть бази біометричних даних – і з них будуть витоки, крадіжки, продаж даних.

Зараз набирає обертів технологія так званої глибокої підробки – Deepfake. В Інтернеті ви можете знайти масу відео із заміною осіб зірок, політиків, відомих людей. Звичайна людина щодня проходить під сотнями камер, її обличчя, хода, голос потрапляють у десятки баз даних різного рівня та різних видів власності, а з баз вони витікають будь-куди. Тести у цій сфері показують гнітючі результати: наприклад, у дослідженні південнокорейських вчених системи біометричної аутентифікації MS Azure та Amazon у 68 % та 78 % випадків відповідно розпізнавали фальшиві особи, з дуже високим ступенем впевненості.

Аудіофейки взагалі зараз виконуються просто ідеально, а авторизацію за голосом зараз уже використовують у реальних банківських додатках. На цей час немає надійних технологій розпізнавання таких фейків.

Тому під час впровадження біометрії головна небезпека полягає в тому, що поки що неясно, як захистити і верифікувати ці дані. Громадяни здають відбитки пальців та фото обличчя, їхні обличчя знімають без їхнього відома та згоди на вулицях, на транспорті, в офісах та торгових центрах. Потім таку інформацію може хтось «злити», вкрасти, перехопити та використати, наприклад, у великих угодах з нерухомістю, пі час управління рахунком у банку, під час проходу на закриті об'єкти тощо.

Висновок: якнайменше здавати біометричні дані, не вестися на «зручність» і уявний виграш. Ці дані гарантовано вкрадуть та продадуть. При цьому той, хто збирає ваші біометричні дані, не вважає за потрібне пояснити, як ці дані планується захищати, у тому числі від своїх співробітників.

Існує думка, що біометрія має спростити ідентифікацію користувачів. Проте ще ніхто з прихильників біометрії не обґрунтував, яку ціну буде сплачено за уявне спрощення ідентифікації. При цьому змінюється рівень інформаційної безпеки на ілюзорний виграш від спрощення ідентифікації користувачів.

Крім того, треба розуміти, що система біометричної ідентифікації – це

система штучного інтелекту, яка не має 100 % якості. Їй завжди властиві помилки першого та другого роду: тобто вона може розпізнати «неправильний» об'єкт як правильний чи не пропустити правильний об'єкт. Тобто завжди залишається ймовірність, що система вас не розпізнає чи розпізнає вас як когось іншого, на кого ви схожі.

Сфера біометричної автентифікації перспективна та швидко розвивається, з кожним роком зростає кількість досліджень та розробок у цій сфері. Однак ці методи недосконалі, і завжди є ймовірність помилок. Варто уважно зважити всі «за і проти», перш ніж ухвалити рішення використати біометрію для захисту своїх конфіденційних даних та коштів. Якщо вкрадений пароль або банківську картку можна замінити, то як замінити вкрадене «обличчя» чи «палець»? Втрачений чи вкрадений біометричний ідентифікатор стає скомпрометованим уже назавжди. Про це слід пам'ятати, погоджуючись використовувати метод біометричної автентифікації. У людей має бути вибір – здавати чи не здавати свої біометричні дані, адже ризики їхнього несанкціонованого використання, як і раніше, залишаються високими.

Бібліографічні посилання

1. Биометрическая идентификация: удобство и риски. URL: https://plus-one.rbc.ru/society/biometricheskaya-identifikaciya-udobstvo-i-riski

2. Биометрия и информационная безопасность. URL: https://safe-surf.ru/users-of/article/659637/

3. Суомалайнен А. Биометрическая защита: обзор технологии. Изд-во ДМК-Пресс, 2019. 99 с.

Касич Є. Ю.,
здобувач 2-го курсу вищої освіти
факультету підготовки фахівців
для органів досудового розслідування
Науковий керівник – Прокопов С. О.,
старший викладач кафедри
економічної та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ

ПОШИРЕННЯ КІБЕРЗЛОЧИННОСТІ В СУЧАСНІЙ УКРАЇНІ, ПРОБЛЕМАТИКА ТА ШЛЯХИ ВИРІШЕННЯ

На сьогодні глобальною проблемою не тільки України, але й усього світу є поширення кіберзлочинів, спроби подолання та звісно статистика даних правопорушень, що значно зросла з періодом усесвітньої пандемії. Кіберзлочини мають різні напрями, що реалізуються у зовсім не схожих