

ПРОБЛЕМИ ВПРОВАДЖЕННЯ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ТРУДОВОМУ І НАВЧАЛЬНОМУ ПРОЦЕСАХ

Мищенко М. Д., студент (гр. КА-43, ІПСА КПІ ім. Ігоря Сікорського)

На сучасному етапі розвитку української економіки починається поступове впровадження сучасних інформаційних технологій, що продемонстрували свою ефективність у інших країнах. Проте управлінці різних рівнів і організацій зазвичай проводять їх впровадження аналогічно прикладам цих країн без урахування вітчизняних реалій. Це стає причиною численних проблем у рядових співробітників і студентів, з якими особа, що приймала таке рішення, зазвичай не стикається.

Ці проблеми можна умовно поділити на три категорії:

- Необхідність передачі персональної інформації третім особам, що не пов'язані із підприємством чи вищим навчальним закладом і не укладали з ними відповідний договір згідно закону України “Про захист персональних даних” (про це далі докладніше).

- Необхідність придбання працівником чи студентом додаткового обладнання чи послуг третіх осіб за власний кошт для продовження своєї трудової чи навчальної діяльності.

- Необхідність придбання працівником чи студентом додаткового обладнання чи послуг третіх осіб для приховання своїх персональних даних і забезпечення інформаційної безпеки своїх комп'ютеризованих пристроїв від третіх осіб, що надають послуги у сфері інформаційних технологій підприємству чи вищому навчальному закладу, а також необхідність здобуття теоретичних знань та практичних навичок у сфері інформаційної безпеки з цією метою.

Розберемо всі три категорії проблем докладно і на прикладах.

Необхідність передачі персональної інформації третім особам виникає, коли від співробітників чи студентів вимагається надати певні данні (пройти анкетування) за допомогою певного онлайн-сервісу чи підтримувати зв'язок із колективом та/або роботодавцем через певну соціальну мережу чи сервіс миттєвих повідомлень.

Наприклад, для обов'язкового збору інформації про наукові досягнення студента часто застосовується сервіс “Google Форми”. Таким чином ці данні потрапляють на сервери компанії Google, яка по відношенню до навчального процесу студента є третьою стороною.

Згідно з визначенням термінів, даним у статті 2 закону України “Про захист персональних даних” [1]:

“володільць персональних даних - фізична або юридична особа, яка визначає мету обробки персональних даних, встановлює склад цих даних та процедури їх обробки, якщо інше не визначено законом;

...

розпорядник персональних даних - фізична чи юридична особа, якій

володільцем персональних даних або законом надано право обробляти ці дані від імені володільця;”

Таким чином у наведеному прикладі володільцем персональних даних виступає вищий навчальний заклад, а розпорядником - компанія Google.

Також згідно частини 4 статті 4 закону України “Про захист персональних даних” *“Володільець персональних даних може доручити обробку персональних даних розпоряднику персональних даних відповідно до договору, укладеного в письмовій формі”*, а згідно ч. 5 ст. 4 того ж закону *“Розпорядник персональних даних може обробляти персональні дані лише з метою і в обсязі, визначених у договорі.”* Такого договору, очевидно, укладено не було.

Далі розглянемо випадки необхідності придбання працівником чи студентом додаткового обладнання чи послуг третіх осіб за власний кошт.

У разі використання підприємством чи ВНЗ сторонніх сервісів може виникнути ситуація, коли наявні у студента чи працівника персональні технічні засоби несумісні з цими сервісами. Зокрема, смартфони із ОС Android версії 2.3 не здатні відображати веб-сторінки зі складним кодом на JavaScript, що унеможлиблює використання таких сервісів, як “Google Форми” та Kahoot, призначеного для проведення тестування. Це змушує студента чи працівника придбати новий смартфон або носити із собою ноутбук із акумулятором із високою ємністю. Враховуючи те, що акумулятори ноутбуків досить швидко деградують, це також призводить до вимушених витрат на їх заміну.

До того ж, може так статись, що у студента чи працівника взагалі немає мобільного телефону, наприклад із ідейних міркувань. Таких осіб автор статті також зустрічав.

Іще однією проблемою є наявність і якість з’єднання з Інтернет у приміщеннях, у яких проводиться навчальний чи трудовий процес. Точніше, відсутність такого з’єднання чи технічні обмеження на одночасну кількість з’єднань. Наприклад, ситуація, коли контрольна робота за допомогою стороннього інтернет-сервісу проводиться у приміщенні, у якому надана студентам Wi-Fi точка доступу здатна надавати з’єднання максимум 30-м пристроям, у той час як самих студентів, що пишуть контрольну, набагато більше. Така невідповідність наявного технічного устаткування поставленим задачам примушує студентів чи співробітників укласти угоду про надання послуг з’єднання з Інтернет із мобільними операторами зв’язку, і навіть це не завжди допомагає. Наприклад, аудиторія може знаходитись на підземному поверсі чи мати товсті стіни, що призводить до поганого покриття безпроводних мереж мобільних операторів або повної його відсутності.

До недавнього часу для надання студентам актуальної інформації щодо навчального процесу та його організація виконувалась через соціальну мережу “ВКонтакте”. Реєстрація аккаунту у цій соціальній мережі, як і в багатьох інших, вимагає його прив’язки до номера мобільного телефону. Як відомо, соціальні мережі часто вдаються до купівлі інформації про своїх користувачів і навіть потенційних користувачів, котрі ще не мають аккаунта в їх сервісах, у сторонніх організацій. Наприклад, відомо [2], що інша популярна соціальна

мережа Facebook скупає різноманітну інформацію про людей: від рівня їх доходів до місць, де вони полюбляють обідати.

Таким чином, вказаного при реєстрації номеру телефону може бути достатньо для того, щоб пов'язати профіль користувача із прямими чи косвенними даними про банківський рахунок, прив'язаний до того самого номера телефону, а також із іншими сервісами, де користувач вказував чи йще вкаже цей номер. Таким чином для збереження приватності персональних даних користувачу соціальної мережі необхідно придбати окрему SIM-картку із окремим номером телефону, призначену лише для роботи з цією соціальною мережею.

Також не треба забувати про інші технічні засоби і способи відслідковування діяльності користувачів у мережі, що здатні пов'язати широкий пласт інформації про працівника чи студента з його аккаунтом у соціальній мережі, створеним виключно для забезпечення його трудової чи навчальної діяльності, і в якому ця діяльність відображена надзвичайно детально і повно.

Захист від цих засобів вимагає глибоких знань щодо принципів роботи і навичок налаштування сучасних комп'ютерних мереж і мережевого програмного забезпечення, у тому числі маршрутизації мережевого трафіку, а також принципів роботи та налаштування браузерів. Також для цього необхідні навички гігієни поведінки з інформацією. Такі знання та навички для працівника чи студента зазвичай не є профільними і їх засвоєння віднімає значну кількість часу і ресурсів, які можна було б використати на виконання своїх безпосередніх обов'язків.

Часто як частина комплексу заходів із забезпечення приватності персональних даних при використанні популярних соціальних мереж і засобів миттєвого обміну повідомленнями, що застосовуються у трудовому чи навчальному процесі, необхідне придбання послуги VPN (віртуальної приватної мережі) для доступу до них із іншої IP-адреси.

Із набуттям чинності Указу Президента України Про рішення Ради національної безпеки і оборони України від 28 квітня 2017 року "Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)" [3], що заборонив Інтернет-провайдером надання послуг з доступу користувачам мережі Інтернет до ресурсу "Вконтакте" (www.vk.com) на три роки, у навчальному процесі почали застосовувати інші засоби миттєвого обміну повідомленнями, що, проте, не вирішило проблему в цілому. Наприклад, сервіс "Google Форми", який продовжують використовувати, вимагає наявності аккаунту Google для заповнення "форми", якщо в налаштуваннях цієї "форми" було вказано, що особа може заповнити її лише один раз. Таким чином, працівнику чи студенту необхідно зареєструвати такий аккаунт, знову ж таки вказавши свій номер мобільного телефону. Більшість сучасних популярних сервісів вимагають його вказання при реєстрації.

Окремо варто розглянемо проблему інформаційної безпеки при застосуванні сторонніх продуктів і сервісів. У сфері інформаційної безпеки за

аксіому традиційно приймається твердження, що користувач не може довіряти програмному забезпеченню, яке написав не він. Якщо програмне забезпечення написав хтось інший, то постає питання про довіру користувача до автора ПЗ. Отримати певну гарантію інформаційної безпеки користувач може лише в двох випадках:

- У разі укладання юридично-правильно оформленого договору із розробником програмного забезпечення, що накладає на нього відповідні обов'язки і не надає йому права на довільний збір, використання та/або розповсюдження інформації користувача.

- У разі повної відкритості коду програмного забезпечення, можливості і права на компіляцію цього коду у готову до використання програму незалежно від будь-якої особи чи організації, відсутності будь-якої форми залежності інфраструктури, необхідної для роботи ПЗ, від будь-якої конкретної особи чи організації, а також неодноразове проведення публічного аудиту коду цього ПЗ.

У всіх інших випадках ПЗ вважається за замовчуванням потенційно небезпечним через можливість помилок, допущених розробником, чи можливу наявність навмисно доданого прихованого функціоналу. Така прискіпливість до ПЗ може здатись надмірною, проте практика показує [4-6] справедливість закону Мерфі у застосуванні до інформаційної безпеки: “все, що може піти не так - піде не так”.

Таким чином, у разі необхідності використання стороннього програмного забезпечення у трудовій чи навчальній діяльності без забезпечення гарантій інформаційної безпеки цього ПЗ перед співробітником чи студентом постає проблема її забезпечення своїми силами. Для цього застосовується комплекс заходів із ізоляції підозрілого ПЗ. Інколи така ізоляція можлива за допомогою спеціалізованого програмного забезпечення, проте це не завжди можливо. Наприклад, при спробі запуску клієнта мережі миттєвого обміну повідомленнями Viber у віртуалізованому середовищі аккаунт цієї мережі автоматично блокується. Також на даний момент не існує засобів віртуалізації мобільних платформ, придатних до практичного застосування. До того ж, ізоляція ПЗ програмними засобами не є повністю надійною. Через це часто єдиним способом забезпечення інформаційної безпеки є запуск підозрілого ПО на окремому пристрої, який не використовується ні для чого іншого.

Висновки

Впровадження сучасних інформаційних технологій - це тривалий, трудомісткий і затратний процес, що включає в себе побудову відповідної інфраструктури, закупку обладнання і укладання відповідних договорів із компаніями, що надають застосовувані сервіси, або розробку цих сервісів за власний кошт, а також аудит якості роботи цих сервісів в умовах підприємства чи ВНЗ. Для вдалого впровадження необхідна кваліфікована оцінка економічної доцільності таких дій, а також робота спеціалістів з інформаційних технологій і юристів для забезпечення ефективної та безпечної роботи цих нововведень, а також забезпечення їх законності. У разі невдалого

впровадження усі проблеми, пов'язані з ним, лягають на плечі співробітників чи студентів.

Науковий керівник: Праховнік Н. А., к.т.н., доцент (каф. ОПЦБ КПІ ім. Ігоря Сікорського)

Література

1. Закон України “Про захист персональних даних”: станом на 1 січ. 2017 р. / Верховна Рада України. - [Електронний ресурс], режим доступу: <http://zakon.rada.gov.ua/go/2297-17>
2. Facebook Privacy: Social Network Buys Data From Third-Party Brokers To Fill In User Profiles [Електронний ресурс]. - Режим доступу: <http://www.ibtimes.com/facebook-privacy-social-network-buys-data-third-party-brokers-fill-user-profiles-2466651>
3. Указу Президента України Про рішення Ради національної безпеки і оборони України від 28 квітня 2017 року "Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)" // Урядовий кур'єр. - 2017. - 17 травня.
4. Virulent Android malware returns, gets >2 million downloads on Google Play [Електронний ресурс] - Режим доступу до ресурсу: <https://arstechnica.com/information-technology/2017/01/virulent-android-malware-returns-gets-2-million-downloads-on-google-play/>
5. The Pwnie Awards 2017 winners: Pwnie for Best Backdoor [Електронний ресурс] - Режим доступу до ресурсу: <https://web.archive.org/web/20170916053153/https://pwnies.com/winners/#backdoor>
6. Facebook Microphone Update: Electronic Surveillance Experts React To Smartphone Mic Data Collection [Електронний ресурс] - Режим доступу до ресурсу: <http://www.ibtimes.com/facebook-microphone-update-electronic-surveillance-experts-react-smartphone-mic-data-1589575>