Секція 2.
Реформування правоохоронної і судової систем: український і зарубіжний досвід

Section 2.
Reforming of law enforcement and judicial systems: Ukrainian and foreign experience

Золотий А.
студент групи ПР-14
юридичного факультету
Західноукраїнського
національного університету

Науковий керівник:
к.е.н., доцент
кафедри безпеки та правоохоронної
діяльності ЗУНУ
Колесніков А. П.

ЦИФРОВА БЕЗПЕКА ЮРИСТА В УМОВАХ ІНФОРМАЦІЙНОЇ ВІЙНИ

Від початку повномасштабної війни українці зустрілися з глобальними проблемами про які раніше мовчав весь світ. Окрім фізичного протистояння рф застосовує методи інформаційної війни для розсіювання уваги та пошкодження персональних даних. Війна ведеться не лише на полі бою, а й у кіберпросторі, тому діяльність юриста вимагає пильної уваги до правил цифрової безпеки. За даними Інституту цифрової безпеки, у 2022 році на Україну чекає безпрецедентна ескалація кібератак з боку росіян на громадянське суспільство та державний сектор, починаючи від цілеспрямованого фішингу зі шкідливим програмним забезпеченням і закінчуючи перенаправленням інтернет-трафіку через росію.

На сьогодні існує низка проблем, які породжують неприємні наслідки для юристів, що стосується їхнього персонального простору. Наприклад це відсутня ефективна система забезпечення захисту даних в органах державної влади, органах місцевого самоврядування та володільцях і розпорядниках персональних даних, які обробляють персональні дані. У багатьох випадках доступ до реєстрів має

необмежене коло осіб. Відсутнє належне матеріально-технічне забезпечення тих, хто працює з базами даних, а це означає, що дані легко копіюються на інші носії, держава часто не забезпечує комп'ютерами своїх співробітників, а ноутбуки з даними використовуються не лише на робочому місці, але й у закладах громадського харчування та вдома. Низький рівень кваліфікації та оплати праці працівників, відповідальних за кібербезпеку в державних установах, організаціях/компаніях та органах місцевого самоврядування. Співробітників "легко купити", тобто вони можуть розкрити інформацію за певну плату. Їх некомпетентність також може призвести до випадкового витоку даних. Відсутня культура поваги до права на приватність і захист персональних даних. Українцям часто бракує навичок цифрової гігієни. Відсутня ефективна система державного контролю за захистом персональних даних. [2]

Навіть зараз, коли почалося повномасштабне вторгнення, цілі Міністерства цифрової трансформації залишаються незмінними: оцифрувати 100% державних послуг, розвивати цифрову економіку та інтернет-інфраструктуру, навчати людей цифровій грамотності. Однак війна додала нові пріоритетні напрямки, наприклад, військові технології. Технології відіграють важливу роль на передовій і роблять перемогу більш доступною.

Чи можна сьогодні обійтися юристам без використання Інтернету? Я вважаю, що кожен з нас не може уявити своє повсякденне життя на роботі без інтернету. Ми вже давно користуємося електронними підписами, використовуємо електронну пошту замість листів у конвертах і не чекаємо на "живі" підписи. Ми надсилаємо документи через месенджери та проводимо зустрічі в онлайн-конференціях. Навчання, робота, дозвілля - все онлайн. І завдяки інтернету ми можемо повноцінно спілкуватися і продовжувати працювати в період карантину - як ми могли собі це уявити 10 років тому? [3,с.253]

Технології принесли нам нові можливості, але також і нові пастки. Основними "пристроями" для підключення до інтернету є комп'ютери, планшети та смартфони. І те, наскільки захищені наші персональні дані (не лише наші, а й наших клієнтів) і наскільки ми непомітні, напряму залежить від того, наскільки ми вміємо поводитися з цими пристроями.

Безпека персональних даних - це не та концепція, яка покладається виключно на правила, встановлені законом чи підзаконними актами. Вона вимагає ретельного та послідовного підходу не лише в той момент, коли витік даних має негативний вплив. Ігнорування потенційних ризиків, поки не станеться найгіршого, не є найкращою стратегією. Ми повинні визнати, що не тільки наше майбутнє, але особливо зараз наша фінансова та фізична безпека залежить від того, наскільки ми цифрово грамотні. Якщо ми розголошуємо CVV-коди наших банківських карток, ми втрачаємо гроші, втрачаємо доступ до месенджерів та електронної пошти, втрачаємо роботу, випадково публікуємо документи клієнтів або

пишемо про них образливі коментарі в Інтернеті, шкодимо власній репутації тощо. [4]

По-перше, кожен має усвідомити, що жоден пристрій не може захистити себе від загроз, якщо нехтувати правилами використання та зберігання інформації. Чомусь навіть у професійному середовищі юристів існує думка, що можна працювати безпечно, якщо регулярно вживати антивірусних заходів і не встановлювати сумнівне програмне забезпечення. На думку експертів, така поведінка може зробити вас мішенню для хакерів.

Наслідки кібератак дуже різняться залежно від цілей кіберзлочинців. Зазвичай це або прямі фінансові втрати (наприклад, крадіжка банківських рахунків або онлайн-гаманців), або непрямі фінансові втрати (в цьому випадку гроші не викрадені, але не витрачені через атаку). Наприклад, вірус Petya-A завдав шкоди третині економіки України за один день, або близько 3-3,5 мільярдів гривень. Підприємства були зупинені майже на три дні, тому не вироблялася продукція і не надавалися послуги. Таким чином, непрямі фінансові збитки, завдані вірусом, склали близько 10 мільярдів гривень. Атаки також можуть завдати репутаційної шкоди. Наприклад, якщо зламати сайт Президента, то гроші не будуть втрачені, але репутація Президента може постраждати (зокрема, через публікацію компрометуючих фактів). [4,с.120]

Проаналізувавши усі можливі види кіберзлочинності, можна навести декілька порад для юристів, як не стати жертвою кіберзлочинності.

1. Оновіть програмне забезпечення на мобільних телефонах, планшетах, ноутбуках та комп'ютерах. Не встановлюйте програмне забезпечення з сумнівних джерел і встановлюйте програмне забезпечення лише з офіційних магазинів або веб-сайтів виробників (принаймні на пристрої, що використовуються для роботи). Також важливо постійно оновлювати антивірусне програмне забезпечення, хоча це лише невелика перешкода для шпигунських програм [5,с.29].
2. Двофакторна автентифікація. Ускладнює доступ до важливих даних, таких як електронна пошта, соціальні мережі та онлайн-банкінг.
3. Завжди робіть резервні копії важливих документів. Зберігайте дані на окремому пристрої або в хмарі.
4. Не відкривайте вкладення або посилання в електронній пошті чи соціальних мережах, якщо ви не впевнені, що вони адресовані вам.
5. Шифруйте важливу інформацію як на пристрої, так і під час надсилання, використовуючи зашифровані контейнери або закриті архіви. При використанні публічних бездротових локальних мереж використовуйте зашифровані канали зв'язку (SSL/HTTPS/VPN) [6, с. 32].

Отже, в умовах повномасштабної війни виникає досить поширена проблема кіберзлочинності , що порушує особисті кордони юристів та широкого кола осіб. Для протидії порушення цифрової безпеки перш за

все варто знати про види та способи ведення інформаційної війни.

Відсутня ефективна система забезпечення захисту даних в органах державної влади, органах місцевого самоврядування та володільцях і розпорядниках персональних даних, які обробляють персональні дані, у багатьох випадках доступ до реєстрів має необмежене коло осіб породжують негативні наслідки для юристів. Для протидії інформаційній війні потрібно знати засоби захисту та дотримуватися простих порад для створення безпечних умов праці юриста та захисту персональних даних клієнтів.

Список використаних джерел

1. Шемчук В.В. Роль і значення інформаційної функції держави у сучасних умовах. The scientific heritage. 2019. No 33. URL: file:///C:/Users/user/Downloads/1602489241118224.pdf (Угорщина)
2. Шемчук В.В. Механізм забезпечення інформаційної безпеки держави: теоретично-методологічні основи. Філософські та методологічні проблеми права. 2019. № 1. С. 51–59. URL: http://nbuv.gov.ua/UJRN/Fmpp_2019_1_8.
3. Шемчук В.В. Економічна та інформаційна безпека держави: правові аспекти співвідношення. Актуальні проблеми держави і права. 2019. Вип. 83.Одеса. С. 253–259.
4. Шемчук В. В. Кіберзлочинність як перешкода розвитку інформаційного суспільства в Україні. Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: «Юридичні науки». 2018. Т.29 (68). № 6. С. 119– 124. URL: http://nbuv.gov.ua/UJRN/UZTNU_law_2018_29(68)_6_23.
5. Шемчук В.В. Концептуальні підходи розуміння інформаційної війни в сучасному світі. Вчені записки Таврійського національного університету ім. В.І.Вернадського. Серія: «Юридичні науки». Том 30 (69). № 3. 2019. С.29–35.
6. Шемчук В.В. Інформаційна безпека та інформаційна оборона в контексті розвитку вітчизняної доктриний законодавчої основи. Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: «Юридичні науки». 2019. Т. 30 (69). № 4. С. 31–37. URL: http://nbuv.gov.ua/UJRN/UZTNU_law_2019_30(69)_4_8.
7. Шемчук В.В. Забезпечення інформаційної безпеки як функція сучасних держав: порівняльний аналіз: монографія: Київ: Ліра-К, 2020. С.351.