МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
імені ВОЛОДИМИРА ДАЛЯ

КОНСПЕКТ ЛЕКЦІЙ

з курсу:
Кібербезпека в аспекті інформатизації та діджиталізації суспільства

для здобувачів вищої освіти,
усіх спеціальностей та рівнів підготовки

(електронне видання)

Затверджено
на засіданні кафедри
"Інформаційних технологій та програмування"
Протокол № 07 від 14.03.2025

Київ 2025

УДК 004.01

Конспект лекцій з курсу «Кібербезпека в аспекті інформатизації та діджиталізації суспільства» для здобувачів вищої освіти, усіх спеціальностей та рівнів підготовки (електронне видання) / Розр: О.І. Захожай. – Київ: Вид-во СНУ ім. В. Даля, 2025. – 53 с.

Містяться теоретичні відомості по темам, які є актуальними для широкого колу користувачів сучасних інформаційних систем та технологій для забезпечення безпечної взаємодії в цифровому світі.

Розробник	О.І. Захожай, зав. кафедри, д.т.н.
Відп. за видання	О.І. Захожай, зав. кафедри, д.т.н
Рецензент	Д.М. Марченко, професор, д.т.н.

1 БЕЗПЕЧНИЙ ДОСТУП ДО СЕРВІСІВ ДЕРЖАВНОЇ І МІСЦЕВОЇ ВЛАДИ

1.1 Огляд державних сервісів та інструментів взаємодії з ними

Електронна послуга (або е-послуга) – це адміністративна або інша публічна послуга, що надається громадянину або юридичній особі в електронній формі. Завдяки цьому, громадянин має змогу отримати послугу від держави (оформлення ліцензії, соціальної допомоги, особистого документу тощо) без особистого відвідування органів влади.

Е-послуги надаються через Інтернет, тож доступні з дому чи офісу 24 години на добу та сім днів на тиждень. Таким чином, вони є зручнішими та швидшими за особисті візити та мінімізують ризики корупції. Електронні послуги надаються через систему електронних сервісів державної і місцевої влади.

З 2001 року Організація Об'єднаних Націй досліджує стан світового розвитку електронного урядування, зокрема надання електронних послуг, вивчаючи здобутки у розбудові цієї сфери 193 країн-членів ООН. Кожні два роки ООН оновлює інформацію і викладає отримані результати дослідження у аналітичних звітах. Останнє дослідження розвитку електронного урядування в світі датоване поточним 2018-м роком [1]. Серед останніх оглядів тенденцій розвитку електронних державних сервісів можна відокремити [2].

Це дослідження проводилося комплексно за різними показниками та може використовуватися як база для розуміння проблем електронного урядування в світі.

Загальноприйнятим показником зрілості е-уряду в тій або іншій державі є E-Government Development Index (EGDI) – комплексний індекс, що базується на наступних трьох компонентах:

– Індекс онлайн сервісів (Online Service Index), що визначає міру розвиненості веб-послуг з боку електронного уряду, він в свою чергу включає багато компонентів: доступ до інформації про послуги, можливість отримати послугу онлайн та доступ по послуг з допомогою мобільних додатків.

– Індекс телекомунікаційної інфраструктури (Telecommunication Infrastructure Index), що оцінює міру оснащеності громадян засобами ІКТ, розвиток цих засобів у країні відповідно до новітніх розробок та розвитку мережу передових країнах світу.

– Індекс людського капіталу (Human Capital Index) – це індекс, що показує, наскільки високий рівень освіти у громадян, чи готові вони користуватися інформаційними послугами.

Завдяки цьому міжнародному дослідженню можна простежити динаміку розбудови електронного урядування в Україні. Однак, оскільки в Україні перші серйозні кроки щодо забезпечення надання державою електронних сервісів були зроблені у 2014 році, цікаво відзначити, як змінювалися тенденції у досліджуваній сфері за останні 4 роки.

Згідно з результатами дослідження ООН 2014 року (United Nations E-government Survey 2014) [3] щодо розвитку електронного урядування (E-Government

Development Index) Україна посіла 87 місце серед 193 країн, втративши 19 позицій за останні 2 роки та 33 позиції за останні чотири роки. При цьому, найбільш низьку оцінку – 0,2677 Україна отримала за компонентом «Онлайн послуги», яка удвічі нижча відповідного показника 2012 року (0,4248), тобто регрес був відчутним.

За 2014-2016 роки ситуація значно покращилася. Україна у 2016 [4] році виправила негативну тенденцію втрати своїх позицій у світовому рейтингу електронного уряду (E-Government Development Index, United Nations), піднявшись на 25 позицій – з 87 позиції у 2014 році на 62 у 2016 році. Оцінка за компонентом «Онлайн послуги» склала 0,5870. Загальна оцінка за індексом E-Government Development Index (EGDI) склала 0,6076.

У останньому дослідженні ООН від 2018 (E-government Survey 2018), присвяченому розвитку електронного урядування у світі, Україна посіла 82 місце у рейтингу, тобто знов рейтинг держави знизився, так само як трохи знизилася оцінка за компонентом «Онлайн послуги», яка склала 0,5694. Однак, незважаючи на падіння рейтингу, загальна оцінка за індексом E-Government Development Index (EGDI) становила 0,6165 і, таким чином Україну, як і раніше, віднесено до числа країн з високим рейтингом розвитку електронного урядування (відповідно 0,5–0,75). Всього існує чотири групи індексів: найвищий, високий, середній, низький. Індекс онлайн сервісів (Online Service Index) станом на 2018 рік дещо знизився [1].

Відмітимо, що за 2014–2016 роки Україна зробила суттєвий ривок у становленні е-уряду, про що окремо зазначено у звіті ООН за 2016 рік [4, с. 60–61], однак в період 2016–2018 років динаміка розвитку була не такою вражаючою і навіть погіршилася. Зараз знову спостерігається підвищення активності щодо процесів цифровізації суспільно-політичних, економічних процесів.

Індекс онлайн сервісів (Online Service Index – показник, який засвідчує розвиненість електронних сервісів в державі, він обчислюється за кількома критеріями, в тому числі і в залежно від стадій розвитку електронних послуг. Фахівцями ООН у своїх періодичних дослідженнях електронного урядування розроблено підхід до визначення стадій розвитку електронних послуг. З 2010 року пропонується виокремлювати чотири стадії розвитку електронних послуг [Цит. за 5, с. 10–11]:

– Стадія 1: Нові інформаційні послуги: веб-сайти уряду надають інформацію з публічної політики, управління, законів, нормативів, відповідної документації та видів державних послуг. Громадяни мають можливість легко отримувати інформацію про нове в діяльності національного уряду та міністерств, а також можуть переходити за посиланнями до архіву інформації.

– Стадія 2: Розширені відомості про послуги: на урядових веб-сайтах надана можливість посиленої односторонньої або простої двосторонньої електронної комунікації між урядом і громадянином, таких як завантажуванні форми для державних послуг і додатків. Сайти мають аудіо та відеоможливості та багатомовний інтерфейс.

– Стадія 3: Транзакційні послуги: на урядових вебсайтах є можливість, двостороннього зв'язку уряду з громадянами. Необхідна в тій чи іншій формі

електронна автентифікація громадянської ідентичності для успішного завершення обміну. На урядових вебсайтах присутня можливість обробки фінансових транзакцій, а також електронного голосування, завантаження форм, застосування електронних ключів для онлайн податків, ліцензій і дозволів.

– Стадія 4: Підключені послуги: урядові веб-сайти повністю змінили спілкування уряду зі своїми громадянами за допомогою Web 2.0 та інших інтерактивних інструментів. Інформація, данні та знання передаються від урядових установ через інтегровані програми. Уряди країн перейшли від уряд центричного підходу орієнтованого на громадянина, до діалогового підходу орієнтованого на громадян через життєвий цикл подій і сегментовані групи, щоб забезпечити індивідуальний підхід. Уряди країн створюють навколишнє середовище, що розширює можливості громадян приймати більш активну участь у діяльності уряду, таким чином, щоб мати право голосу в прийнятті рішень.

Як зазначається в літературних джерелах [2], «e-government не слід зводити тільки до використання Інтернету в роботі органів влади. Прозорість структур державного управління, яка є метою концепції e-government, не досягається лише завдяки підключенню до мережі Інтернет або створенню інформаційного web-сайта. Он-лайн доступ є обов'язковим елементом e-government, проте не завжди он-лайн уряд буде вважатися e-government. Останній вимагає більш глибокої перебудови традиційних форм функціонування, характеризується прозорістю управління, моніторингом, контролем над виконавчою дисципліною, прийнятими рішеннями та ін. Без структурної реформи системи влади, вироблення концептуально нового підходу до організації надання адміністративних послуг, впровадження ІКТ не призведе до підвищення ефективності роботи, а буде виглядати як спроба навчити старого собаку новим трюкам» [6, с. 282–283].

В Україні з 2016 по 2020 роки відбувається реалізація Концепції розвитку системи електронних послуг в Україні [7], одним з напрямом реалізації Концепції закріплено визначення та планування стадій розвитку системи електронних послуг. Аналіз комплексу заходів з цього напряму свідчить про їх відповідність підходу, запропонованому у дослідженнях ООН щодо стадій розвитку електронних послуг.

Вказаним документом запропоноване наступне визначення електронної послуги: електронна послуга – адміністративна та інша публічна послуга, що надається суб'єкту звернення в електронній формі за допомогою засобів інформаційних, телекомунікаційних, інформаційно-телекомунікаційних систем.

Надання адміністративних послуг в електронній формі та доступ суб'єктів звернення до інформації про адміністративні послуги з використанням мережі Інтернет забезпечуються через Єдиний державний портал адміністративних послуг, який є офіційним джерелом інформації про надання адміністративних послуг в Україні, у тому числі через інтегровані з ним інформаційні системи державних органів та органів місцевого самоврядування (ч.1 ст. 17, ч.1 ст. 9 Закону України «Про адміністративні послуги») [9].

Концепцією передбачено перелік пріоритетних послуг, які запроваджуються в електронній формі першочергово, причому встановлено, що ці послуги мають

відповідати третій, четвертій стадії розвитку. У зазначений перелік входять 45 послуг. На сьогодні більша частина з них надаються повністю в електронному вигляді – напроти такої послуги на Єдиному державному порталі адміністративних послуг є відмітка «онлайн». Для зручності на порталі є окрема сторінка «Послуги онлайн» [10].

Однак, є послуги, які можна замовити онлайн, але отримати їх результат можна лише особисто у паперовому вигляді. І є послуги, замовити які можна лише прийшовши до Центру надання адміністративних послуг або безпосередньо до суб'єкта надання відповідних послуг. Згідно з ч. 1 ст. 12 Закону України «Про адміністративні послуги» центр надання адміністративних послуг – це постійно діючий робочий орган або структурний підрозділ місцевої державної адміністрації або органу місцевого самоврядування, що зазначений у частині другій цієї статті, в якому надаються адміністративні послуги через адміністратора шляхом його взаємодії з суб'єктами надання адміністративних послуг.

Підсумуємо, що частиною 1 ст. 9 Закону України «Про адміністративні послуги» закріплено три способи звернення особи до суб'єкта надання адміністративних послуг для отримання адміністративної послуги, а саме:

– безпосередню (суб'єкт звернення напряму звертається до суб'єкта надання адміністративних послуг);

– через центри надання адміністративних послуг (далі – ЦНАП) (взаємодія між суб'єктом звернення та суб'єктом надання адміністративних послуг відбувається через адміністратора ЦНАП);

– через Єдиний державний портал адміністративних послуг (взаємодія між суб'єктом звернення та суб'єктом надання адміністративних послуг здійснюється в електронній формі з використанням мережі Інтернет).

ЦНАП так само як і Єдиний державний портал адміністративних послуг буквально не належать до суб'єктів надання адміністративних послуг. Вони не надають адміністративні послуги безпосередньо, а забезпечують організацію надання адміністративних послуг шляхом взаємодії з суб'єктами надання адміністративних послуг. Отже, центри надання адміністративних послуг та Єдиний державний портал адміністративних послуг є альтернативними каналами звернення за адміністративними послугами.

І лише частиною 4 статті 13 Закону України «Про адміністративні послуги» передбачено можливість здійснювати надання адміністративних послуг адміністратору ЦНАП у випадках, передбачених законом. При цьому Закон визначає, що надання адміністративних послуг безпосередньо адміністратором ЦНАП можливе лише за умови якщо відповідні повноваження будуть закріплені у спеціальному законі. Тобто у цьому випадку адміністратор ЦНАП виступатиме суб'єктом надання адміністративних послуг.

Основними завданнями ЦНАП є:

1) організація надання адміністративних послуг у найкоротший строк та за мінімальної кількості відвідувань суб'єктів звернень;

2) спрощення процедури отримання адміністративних послуг та поліпшення якості їх надання;

3) забезпечення інформування суб'єктів звернень про вимоги та порядок надання адміністративних послуг, що надаються через адміністратора [11].

Перелік адміністративних послуг, які надаються через центр, визначається органом (посадовою особою), що прийняв рішення про його утворення.

Перелік адміністративних послуг, які надаються через центр, суб'єктами надання яких є органи виконавчої влади, визначається органом (посадовою особою), що прийняв рішення про його утворення, та включає адміністративні послуги органів виконавчої влади, перелік яких затверджується Кабінетом Міністрів України.

Крім адміністративних послуг, за рішенням органу, що утворив ЦНАП, у такому центрі також можуть надаватися і неадміністративні послуги, зокрема, укладення договорів і угод представниками суб'єктів господарювання, які займають монопольне становище на відповідному ринку послуг та які мають соціальне значення для населення (водо, тепло, газо, електропостачання тощо.

Важливою умовою отримання результатів послуг в форматі онлайн є наявність у суб'єкта звернення електронного цифрового підпису або іншого інструменту, який підтверджує електронну ідентифікацію фізичної, юридичної особи. Якщо у особи немає електронного цифрового підпису, то згідно з правилами роботи чинних державних електронних сервісів вона може або (1) замовити послугу онлайн, але отримати її результат онлайн не вийде і їй необхідно буде завітати до відповідного органу влади для особистого підписання документів; (2) зареєструватися як користувач на веб-порталі адміністративних послуг, але не зможе засвідчити свою особу і таким чином скористається лише тими сервісами (їх меншість), які не вимагають ідентифікації.

Оскільки електронні адміністративні послуги є частиною електронного урядування, крім згаданої Концепції розвитку електронних послуг, правове регулювання цієї сфери здійснюється також Стратегією сталого розвитку «Україна-2020» [12], схваленої указом Президента України від 12 січня 2015 року № 5/2015, Стратегією реформування державного управління України на 2016-2020 рр. [13], затвердженої розпорядженням КМУ від 24 червня 2016 р. № 474-р, Концепцією розвитку електронного урядування в Україні [14], схваленої розпорядженням КМУ від 20 вересня 2017 р. № 649-р, Законом України «Про адміністративні послуги» від 6 вересня 2012 року № 5203-VI, Законом України «Про електронні документи та електронний документообіг» [15] від 22.05.2003 № 851-IV, Законом України «Про електронні довірчі послуги» від 5 жовтня 2017 р. № 2155-VIII [16].

Зокрема, основними завданнями в рамках даного напряму реформи державного управління, що передбачено реалізувати до 2020 р., є:

– завершення переходу органів виконавчої влади на електронний документообіг та їх інтеграція до системи електронної взаємодії органів виконавчої влади (всі центральні органи виконавчої влади та 80 % місцевих органів виконавчої влади);

– створення та вдосконалення відкритих державних реєстрів;

– цифровізація адміністративних послуг – не менше 80 електронних адміністративних послуг третьої стадії розвитку, та 40 – четвертої стадії розвитку); розвиток відкритих даних – збільшення кількості наборів відкритих даних та покращення їх якості [12].

2016–2017 роки, як бачимо, позначилися розвитком нормативно-правової бази з питань електронного урядування та електронних послуг, що варто оцінити позитивно, однак прийняті нормативні документи мають окремі неузгодженості між собою.

Так, План заходів з реалізації Стратегії реформування державного управління України на 2016–2020 роки передбачає розроблення переліку з 80 пріоритетних послуг в електронній формі [13], а Концепція розвитку електронних послуг в Україні до 2020 р. містить перелік лише з 45 таких послуг.

До того ж зазначені нормативно-правові акти визначають різні строки здійснення оптимізації процедур надання адміністративних послуг. Так, Планом заходів з реалізації Стратегії реформування державного управління України на 2016–2020 рр. передбачено проведення оптимізації процедур надання 15 найбільш популярних адміністративних послуг протягом 2017–2020 рр. Концепцією розвитку електронних послуг в Україні оптимізацію процедури надання пріоритетних адміністративних послуг планується завершити до кінця 2017 р., а решти адміністративних послуг – у 2018–2019 рр.

Отже, у державній політиці з розвитку електронних послуг є неузгоджені моменти щодо кількості електронних адміністративних послуг, що підлягають цифровізації до 2020 року, та строку здійснення такої цифровізації. Плутанина на рівні програмних документів може привести до зниження ефективності запропонованих заходів, оскільки заважає здійсненню чіткої і послідовної державної політики в сфері електронного урядування і, зокрема, електронних послуг. Саме тому вкрай важливо нормативноправову базу з питань електронного урядування узгодити з нормативними актами, що регламентують надання електронних адміністративних послуг.

Надалі наводиться огляд впровадження електронних адміністративних послуг в Україні на державному рівні.

1. Електронні адміністративні послуги Державної служби з геодезії, картографії та кадастру України.

Через Публічну кадастрову карту (e.land.gov.ua) [16] можна отримати 15 електронних послуг, однак для отримання 7 з них необхідна авторизація в особистому електронному кабінеті, 5 електронних послуг доступні без авторизації, окремо виділені 3 електронні послуги для сертифікованих інженерів землевпорядників.

Авторизація на порталі Державної служби з геодезії, картографії та кадастру України можлива за допомогою кількох інструментів ідентифікації на вибір: ідентифікація з використанням ЕЦП, ідентифікація з використанням BankID Приватбанку (платна), ідентифікація з використанням Mobile ID KS, ідентифікація з використанням BankID НБУ, через Email та пароль.

Електронні послуги, доступні після авторизації в особистому електронному кабінеті:

– відомості Державного земельного кадастру;

– витяг з технічної документації про нормативну грошову оцінку; відомості про права власності на земельні ділянки;

– інформація про осіб, що переглядали відомості щодо прав власності на земельну ділянку; довідка з державної статистичної звітності про наявність земель та їх розподіл;

– подання заяви з надання дозволу на розроблення документації із землеустрою;

– запит на отримання документації із землеустрою з Державного фонду документації із землеустрою.

Електронні послуги, доступні без авторизації:

– витяг з Державного реєстру сертифікованих інженерів-геодезистів;

– витяг з Державного реєстру сертифікованих інженерів-землевпорядників;

– дублікат кваліфікаційного сертифіката інженера-землевпорядника; отримання кваліфікаційного сертифіката інженера-землевпорядника;

– витяг з Державного реєстру оцінювачів з експертної грошової оцінки земельних ділянок.

Електронні послуги для сертифікованих інженерів-землевпорядників:

– заява про державну реєстрацію земельної ділянки;

– подання на погодження проекту землеустрою; заява про внесення виправлених відомостей до Державного земельного кадастру.

2. Електронні адміністративні послуги Державної архітектурно-будівельної інспекції України.

Станом на листопад 2021 року через веб-сайт edabi.gov.ua [21] підприємці та громадяни вже можуть скористатися 14 електронними адміністративними послугами:

– повідомлення про початок виконання підготовчих робіт;

– повідомлення про зміну даних у повідомленні про початок виконання підготовчих робіт;

– повідомлення про початок будівельних робіт щодо об’єктів, будівництво яких здійснюється на підставі будівельного паспорту;

– повідомлення про зміну даних у повідомленні про початок будівельних робіт щодо об’єктів, будівництво яких здійснюється на підставі будівельного паспорту;

– повідомлення про початок будівельних робіт щодо об’єктів, що за класом наслідків (відповідальності) належать до об’єктів з незначними наслідками (СС1);

– повідомлення про зміну даних у повідомленні про початок будівельних робіт щодо об’єктів, що за класом наслідків (відповідальності) належать до об’єктів з незначними наслідками (СС1);

– декларація про готовність до експлуатації об’єкта, будівництво якого здійснено на підставі будівельного паспорта;

– внесення змін до декларації про готовність до експлуатації об'єкта, будівництво якого здійснено на підставі будівельного паспорта;

– декларація про готовність до експлуатації об'єкта, що за класом наслідків (відповідальності) належать до об'єктів з незначними наслідками (СС1);

– внесення змін до декларації про готовність до експлуатації об'єкта, що за класом наслідків (відповідальності) належать до об'єктів з незначними наслідками (СС1);

– декларація про готовність до експлуатації самочинно збудованого об'єкта, на яке визнано право власності за рішенням суду;

– внесення змін до декларації про готовність до експлуатації самочинно збудованого об'єкта, на яке визнано право власності за рішенням суду;

– отримання ліцензії із будівництва об'єктів, що за класом наслідків (відповідальності) належать до об'єктів з середніми та значними наслідками;

– внесення змін до переліку видів робіт ліцензії із будівництва об'єктів, що за класом наслідків (відповідальності) належать до об'єктів з середніми та значними наслідками.

Умовою використання електронних послуг Державної архітектурно-будівельної інспекції України є наявність особистого ключа та чинного посиленого сертифіката, які в процесі подання будуть використовуватися для накладання електронного цифрового підпису на форму із декларацією (повідомленням). На поточний момент сервіс підтримує також сертифікати видані центром сертифікації ключів інформаційно-довідкового департаменту Міністерства доходів і зборів України [22].

3. Електронні адміністративні послуги Міністерства екології та природних ресурсів України.

Через веб-портал e-eco.gov.ua [23] надаються 2 електронні адміністративні послуги: подання декларації про відходи та отримання дозволу на відходи (працює в тестовому режимі).

Для подання декларації про відходи необхідно мати ключі для накладання електронного цифрового підпису.

4. Електронні адміністративні послуги Міністерства економічного розвитку і торгівлі України.

Єдиний державний портал адміністративних послуг (poslugy.gov.ua) запрацював у кінці 2015 замість запланованої дати 1 січня 2014 року, його обслуговує Міністерство економічного розвитку і торгівлі України. На сьогодні через Єдиний державний портал адміністративних послуг можна отримати електронні адміністративні послуги не тільки в сфері діяльності Міністерства економічного розвитку і торгівлі України, а у будь-якій сфері життя: громадянство, міграція, переїзд, реєстрація (Реєстри), соціальний захист, природні ресурси та екологія, енергетика, енергозбереження, сім'я, зовнішньоекономічна діяльність, безпека та захист, освіта та культура, нерухоме майно, транспорт, дорожнє господарство, перевезення, фінансові послуги, податки та декларування та інші.

Отже, як уже згадувалося вище, Єдиний державний портал адміністративних послуг є офіційним джерелом інформації про надання адміністративних послуг в Україні. Цілями Порталу є:

– впорядкування та надання вичерпної інформації про адміністративні послуги;

– надання адміністративних та інших публічних послуг в електронному вигляді.

Надання послуг в електронному вигляді через вказаний веб-портал передбачає [9]:

– послідовне впровадження послуг в електронному вигляді (по мірі готовності суб'єктів надання);

– розширення способів ідентифікації одержувачів послуг;

– впровадження механізмів сплати за послуги.

Для роботи з порталом необхідно пройти процедуру реєстрації в персональному кабінеті та ідентифікації, що має на меті засвідчити автентичність фізичної або юридичної особи за допомогою електронного цифрового підпису та системи ідентифікації Національного банку України Bank ID.

5. Електронні адміністративні послуги Міністерства юстиції України.

На сьогодні кількість електронних сервісів, які надаються Міністерством юстиції України, є найбільшою у порівнянні з іншими міністерствами та центральними органами виконавчої влади. Через Кабінет електронних сервісів Міністерства юстиції України (kap.minjust.gov.ua) [24] відвідувачам пропонується:

– отримання документів з державних реєстрів Міністерства юстиції України в режимі онлайн;

– реєстраційні дії у державних реєстрах України в електронному вигляді;

– пошук інформації у державних реєстрах України;

– користування електронними системами звітності для тих осіб, які здійснюють спеціалізовану професійну діяльність;

– участь в електронних торгах арештованим майном тощо.

У Кабінеті електронних сервісів Міністерства юстиції України є можливість скористатися такими державними реєстрами, інформаційними системами та електронними послугами:

1) На порталі «Звернення у сфері державної реєстрації актів цивільного стану» (https://dracs.minjust. gov.ua/) [25] реалізовані можливості: запису на прийом до відділу ДРАЦС у зручний час, задавання питання в онлайн режимі, подання заяви на реєстрацію актів цивільного стану. Однак, отримати результат послуги можна лише особисто.

2) На порталі реалізована можливість доступу до реєстрів, які обслуговує Міністерство юстиції України: державний реєстр речових прав на нерухоме майно, Єдиний реєстр підприємств щодо яких порушено провадження у справі про банкрутство, Єдиний державний реєстр юридичних осіб та фізичних осіб-підприємців, Реєстр громадських об'єднань, Державний реєстр друкованих ЗМІ та інформаційних агентств як суб'єктів інформаційної діяльності, Єдиний реєстр

громадських формувань, Єдиний реєстр арбітражних керуючих, Єдиний державний реєстр судових рішень, Електронний реєстр апостилів, Єдиний державний реєстр осіб, які вчинили корупційні правопорушення, Єдиний державний реєстр осіб, щодо яких застосовано положення Закону України «Про очищення влади», Єдиний державний реєстр нотаріусів.

Щоб отримати інформацію (довідки, витяги) з перелічених реєстрів необхідно бути зареєстрованим користувачем Кабінету електронних сервісів (mail.gov.ua). Додатково певні сервіси Кабінету передбачають надання інформації лише тим користувачам, які підтвердили свою особу за допомогою ЕЦП.

3) «Електронний суд» надає можливість сплати судового збору онлайн, отримання інформації щодо стадій розгляду судових справ, доступу до Єдиного державного реєстру судових рішень, надсилання процесуальних документів електронною поштою учасникам судового процесу, надсилання судової повістки у вигляді SMS-повідомлень, оприлюднення відомостей у справах про банкрутство.

4) «Електронний цифровий підпис»: реалізована можливість замовлення електронного цифрового підпису.

5) «Інформаційні системи» надає можливість пошуку законодавчих документів українського та міжнародного законодавства, проектів нормативно-правових актів, а також пошук і завантаження шаблонів документів (заяв, договорів, інших юридичних документів).

6) Прийом громадян у режимі відеоконференції (працює у тестовому режимі). Кабінет електронних сервісів надає можливість громадянам зустрітися з керівництвом державних установ та відомств України за допомогою відеоконференції: передбачені спілкування з посадовою особою в режимі реального часу, обмін за необхідності документами, файлами, аудіозаписами та будь-якою іншою інформацією у цифровому форматі.

7) Електронна торгівля. Передбачено можливість проведення он-лайн аукціонів з продажу арештованого майна. На час написання статті сервіс не працює. Для повноцінного користування електронними сервісами Міністерства юстиції України необхідно зареєструватися на відповідному сайті, таким чином створюється особистий обліковий запис. Увійти в особистий Кабінет електронних сервісів можна також з використанням ЕЦП, а в майбутньому і за допомогою BankID.

Аналіз електронних сервісів Міністерства юстиції України дозволяє зробити такі висновки:

– для користування певними послугами (наприклад, отримання документів з державних реєстрів Міністерства юстиції України в режимі on-line) достатньо створення особистого облікового запису, але отримання інших послуг вимагає підтвердження особи за допомогою ЕЦП;

– електронні адміністративні послуги, що надаються Міністерством юстиції України, можна отримати і на Єдиному державному порталі адміністративних послуг (poslugy.gov.ua), який відсилає до Кабінету електронних сервісів.

8. Електронні сервіси Державної фіскальної служби України. Державна фіскальна служба України одна з перших в Україні розпочала розвивати електронні

послуги та сервіси для платників податків. Електронні сервіси, що надаються Державною фіскальною службою України, поділяються на:

– електронні сервіси, розміщені на офіційному веб-порталі ДФС sfs.gov.ua;

– електронні сервіси, які надаються через «Єдине вікно подання електронної звітності;

– електронну звітність [26].

До електронних сервісів, розміщених на офіційному веб-порталі ДФС sfs.gov.ua, належать: загальнодоступний інформаційнодовідковий ресурс» (ЗІР), «Електронний кабінет платника податків», «Дізнайся більше про свого бізнеспартнера», «Перевірка свідоцтва платника єдиного податку», «Електронна звітність», «Реєстр страхувальників», «Анульована реєстрація платників ПДВ2», сервіс «Пульс» (Можливість цілодобового повідомлення про неправомірні дії або бездіяльність працівників ДФС), «Декларування online», «Митна статистика», «Акредитований центр сертифікації ключів», «Електронна митниця», Дані Реєстрів волонтерів АТО.

Електронні сервіси, які надаються через «Єдине вікно подання електронної звітності, охоплюють:

– перелік із 14 сервісних запитів на отримання відомостей з Реєстру платників ПДВ, Єдиного реєстру податкових накладних тощо;

– електронні сервіси для платників податків в системі електронного адміністрування ПДВ (10 сервісних запитів);

Крім цього запроваджено:

– укладання договорів з територіальними органами ДФС «Про визнання електронних документів» в електронній формі;

– опрацювання електронних повідомлень про відкриття/закриття рахунків платників податків у банках та інших фінансових установах;

– інформаційні повідомлення про заборгованість з податків та зборів (обов'язкових платежів);

– інформаційні повідомлення про заборгованість за іноземними кредитами, залученими державою або під державні гарантії, бюджетними позичками;

– інформаційні повідомлення про настання терміну сплати розстроченої (відстроченої, реструктуризованої) суми грошових зобов'язань (податкового боргу);

– повідомлення щодо допущених помилок у податкових розрахунках за формою 1ДФ;

– електронне повідомлення про результати електронної обробки (звірки) податкової інформації з податку на додану вартість. – повідомлення про прийняття працівника на роботу.

Згідно з інформацією офіційного вебсайту Державної фіскальної служби України, більше 90 % платників ПДВ та майже 80 % платників Єдиного соціального внеску звітують в електронній формі.

9. Електронні послуги Пенсійного фонду України.

Електронні послуги, які може отримати користувач на вебпорталі електронних послуг Пенсійного фонду України (portal.pfu.gov.ua) [27] після реєстрації:

– послуга надання електронних документів (довідка про доходи пенсіонера для субсидії;

– довідки про доходи пенсіонера;

– індивідуальні відомості про застраховану особу (довідка ОК-5);

– витяг з Реєстру застрахованих осіб (РЗО). Результатом отримання послуги є надсилання образу документу у вигляді pdf-довідки та електронного документу, підписаний ЕЦП ПФУ, який, згідно з чинним законодавством, є аналогом паперового документу, підписаного відповідальною особою в органі ПФУ.

– перегляд електронної пенсійної справи. На перегляд надаються такі дані з електронної пенсійної справи: основні дані (номер пенсійної справи/особового рахунку, дата відкриття особового рахунку, вид пенсії, орган ПФУ призначення пенсії, дата призначення); адресні дані (адреса реєстрації та адреса фактичного місця проживання); довідка по зарплаті, що врахована при призначенні/перерахунку пенсії; довідка про стаж, врахований для визначення права на пенсію; довідка про стаж, врахований для розрахунку пенсії.

– отримання відомостей про себе з Реєстру застрахованих осіб ПФУ (РЗО);

– перегляд даних страхувальника з Єдиного реєстру страхувальників; перегляд звернень, поданих особою до органів ПФУ;

– перегляд страхувальником власних звітних даних;

– запис на прийом до органів ПФУ;

– можливість подання скарг;

– подання заяв на призначення, перерахунок пенсії;

– запит на підготовку паперових документів;

– запит на отримання документів.

Для отримання низки електронних послуг достатньо зареєструватися на веб-порталі Пенсійного фонду України, однак для більшості послуг умовою є наявність ЕЦП.

За відсутності електронного цифрового підпису для реєстрації на порталі необхідно звернутися до територіального органу Пенсійного фонду та оформити заяву на реєстрацію (її теж можна роздрукувати з порталу, заповнити вдома і принести територіальному органу Пенсій-ного фонду), маючи при собі паспорт та ідентифікаційний код.

За наявності електронного цифрового підпису візит до територіального органу Пенсійного фонду не потрібен, реєстрація здійснюється через портал.

Слід відзначити, що на порталі електронних послу Пенсійного фонду України передбачено, що у майбутньому можна буде здійснити вхід до свого особистого кабінету не лише з використанням ЕЦП, але й за допомогою електронного пенсійного посвідчення і токена.

До речі, цифрові технології та онлайн сервіси поширюються не лише на центральному рівні, місцева влада також опікується питаннями впровадження smart-

технологій у життя регіонів. Так, в світі давно відома концепція «розумного міста», яка є найбільш прогресивним способом організації та розвитку міського простору.

«Smart city» передбачає використання цифрових технологій, які надають доступ до різноманітних показників у місті. Головний тренд в удосконаленні міста – використання Big Data. Здійснюючи постійний моніторинг, влада виявляє проблемні місця, і визначає можливості покращення умов існування в місті і підвищення комфорту життя всіх мешканців.

Наприклад, у Харкові, Дніпрі, Рівному зараз активно запроваджуються smart-технології до всіх сфер суспільного життя: насамперед, реалізується низка проектів в категоріях «Smart-транспорт», Smart-energy, E-medicine, «Безпечне місто», «Екологія», «Утилізация сміття», E-government, «Туризм». Усього запроваджується більше 20 проектів для розвитку smart-міста [28].

Проведений аналіз стану розвитку електронних адміністративних послуг дозволив зробити низку висновків.

1. Підходи до впровадження електронних послуг, закріплені у Концепції розвитку електронних послуг в Україні, відповідають міжнародним підходам, розробленим фахівцями ООН, в галузі державних електронних сервісів. За даними останнього дослідження ООН від 2018 (E-government Survey 2018) Україну віднесено до числа країн з високим рейтингом розвитку електронного урядування. Однак, з часу минулого дослідження 2016 оцінка за компонентом «Онлайн послуги» трохи знизилася, так само як і загальний рейтинг держави в сфері електронного урядування (82 місце проти 65 в 2016 році), що може свідчити про необхідність змін у підходах до державної політики розвитку електронного урядування та електронних послуг.

2. Державна політика розвитку електронних послуг характеризується неузгодженістю у визначенні основних її засад, в тому числі, щодо кількості електронних адміністративних послуг, що підлягають електронізації до 2020 року, та строків здійснення такої електронізації.

3. Умовою отримання результатів послуг в форматі онлайн, крім обов'язкової реєстрації на відповідному поталі електронних сервісів, є наявність у суб'єкта звернення інструменту, який підтверджує електронну ідентифікацію фізичної, юридичної особи. В основному таким інструментом є електронний цифровий підпис. На деяких державних електронних сервісах реалізована можливість альтернативних способів автентифікації з використанням Bank ID Приватбанку або Національного банку України, Mobile ID KS, через Email та пароль. Для отримання електронних сервісів Пенсійного фонду України додатково передбачена можливість ідентифікації за допомогою електронного пенсійного посвідчення та токена, однак на цей час ці способи ідентифікації особи не працюють.

4. Створений в Україні Єдиний державний портал адміністративних послуг є централізованим ресурсом, який інтегрує онлайн-сервіси усіх органів державної влади для надання публічних послуг в єдиному інформаційному просторі. Він є по суті інтегрованим офісом всіх запроваджених електронних послуг в країні і працює за принципом відсилання до веб-порталу відповідного державного органу. Для отримання електронної послуги можна також відвідати відповідний веб-портал

органів державної влади і замовити онлайн-послугу. Таким чином, наразі існує дублювання надання електронних сервісів через Єдиний державний портал адміністративних послуг та через окремі веб-портали електронних послуг органів державної влади. Вважаємо, що надання адміністративних послуг в електронній формі за допомогою окремих вебпорталів і одночасне надання електронних адміністративних послуг через Єдиний державний портал адміністративних послуг заважає процесу інтеграції процедур надання адміністративних послуг в електронній формі, створює передумови для розпорошеності інформації про електронні адміністративні послуги, тягне за собою додаткові витрати бюджетних коштів на створення нових веб-ресурсів, що забезпечують їх надання, викликає необхідність у додатковій електронній ідентифікації споживачів послуг.

5. Через Єдиний державний портал адміністративних послуг надаються лише державні електронні послуги: скористатися електронними сервісами місцевого рівня на цьому порталі не можна.

6. Популяризація цифрових сервісів, які вимагають додаткових інструментів ідентифікації особи, такі як ЕЦП, Bank ID, Mobile ID KS, Email та пароль, NFC та ін., створює додаткові виклики та кіберзагрози. Для мінімізації таких ризиків потрібне планомірне навчання населення методам і засобам попередження кіберзагроз, а також мінімізації наслідків кібератак та електронного шахрайства.

1.2 Комплекс заходів щодо безпечного доступу до державних сервісів

1.2.1 Вразливості QR-кодів та сценарії безпечного користування

QR-коди використовуються як ключовий інструмент для спрощення безконтактної взаємодії та введення даних, в тому числі інтернет-посилань. Це особливо важливо в у мовах пандемії, коли зменшується кількість точок дотику та безпосередньої взаємодії, що забезпечує зручний і безконтактний обмін даними. Вони не є небезпечними за своєю суттю, але можуть бути відкритими для використання кібер-зловмисниками.

Коди швидкого реагування (QR) можна розглядати як послуги скорочення URL-адрес – вони забезпечують миттєвий доступ до такої інформації, як веб-сайти та контактна інформація. Вони також можуть дозволити користувачам входити в мережу Wi-Fi без пароля. Вони все частіше використовуються в усіх сферах життя, що також призводить до підвищення зацікавленості до них з боку кіберзлочинців.

Технологія QR-коду сама по собі безпечна, але, в міру зростання залежності від неї, кіберзлочинці звертають на це увагу. Ці коди можуть запропонувати вхід для потенційних кібератак, оскільки вони не забезпечують видимість веб-сторінки, програми тощо. Натомість вони автоматично перенаправляють користувачів на веб-сторінки, магазини додатків для завантаження програм, здійснення платежів тощо, що дає кіберзлочинцям можливість включитися в процес. Під час пандемії Unit 42, команда розвідки загроз Palo Alto Networks, спостерігала за кіберзлочинцями на підпільних онлайн-форумах, які обговорювали способи зловживання QR-кодами та націлювання на повсякденного споживача. В інтернет-ресурсах також знаходяться

інструменти з відкритим вихідним кодом та відеоуроки, які пропонують навчання, як проводити атаки за допомогою QR-кодів.

Ще в 2018 році Juniper Research передбачало чотирикратне збільшення використання QR-кодів до 2022 року, так як функція сканування QR вбудована в камери багатьох мобільних пристроїв. Ймовірно, пандемія спричинила ще один сплеск використання цієї технології, тому потрібно бути обережними щодо того, що ми скануємо.

Сценарії використання QR-кодів кіберзлочинцями.

Існує кілька сценаріїв, якими кіберзлочинці можуть використовувати QR-коди для власних зловмисних цілей. Одним з них є злам веб-сайту та заміна наявного там QR-коду своїм власним (підміна QR-коду). Оскільки QR-коди виглядають дуже схожими, заміну практично малоймовірно помітити. Сканування цього коду може автоматично спрямовувати нічого не підозрюючих споживачів на фішингову URL-адресу, де кіберзлочинці можуть запитати облікові дані користувача, а потім, наприклад, взяти під контроль електронну пошту або облікові записи соціальних мереж. Це також може привести користувачів до незаконного магазину додатків, де вони можуть несвідомо завантажити шкідливий додаток, що містить вірус, шпигунське програмне забезпечення, троян або інший тип зловмисного програмного забезпечення, що може призвести до викрадення даних, порушення конфіденційності (викрадення координат геолокації або списку контактів, дзвінків, перехоплення повідомлень), вимагання засобами програм-вимагачів або до тіньового криптомайнінгу.

Ще один кіберзлочинний сценарій – це honeypot. Зловмисники можуть створити небезпечну мережу WiFi, обіцяючи безкоштовний доступ до Інтернету всім, хто сканує їхній QR-код. Коли пристрій під'єднано, хакери можуть підслуховувати або перехоплювати дані, які передаються, а також викрасти ідентифікаційну інформацію, конфіденційну ділову інформацію, облікові дані онлайн-банкінгу та дані кредитної картки.

Тому треба бути дуже обережними, коли скануємо QR-коди.

Способи захисту від небезпечних QR-кодів.

Неозброєним оком неможливо визначити, чи кіберзлочинці зловживають QR-кодом, але є багато запобіжних заходів, які можна вжити, щоб не стати жертвою.

Власники бізнесу та IT-адміністратори повинні регулярно перевіряти цілісність своїх сайтів і додатків, щоб переконатися, що код і посилання, які вони надають, є справжніми. Вони можуть робити це, регулярно скануючи код, щоб перевірити, чи правильне посилання в QR-коді. Їм потрібно перевірити як веб-версію, так і версію мобільного браузера, оскільки, як відомо, кіберзлочинці компрометують лише останню, щоб зменшити ймовірність виявлення.

Роботодавці також повинні надавати персоналу тренінги з кібербезпеки, щоб вони усвідомлювали ризики як для організації, так і для них самих. Вони включають використання надійних та унікальних паролів як для особистих, так і для робочих облікових записів, налаштування багатофакторної автентифікації та виявлення фішингових електронних листів, а також небезпечних віртуальних середовищ.

Оскільки багато співробітників продовжують працювати з некорпоративних середовищ, тренінги з кіберобізнаності забезпечать віддалених працівників знаннями та обізнаністю, щоб приймати розумні рішення, не даючи зловмисникам отримати доступ до будь-яких особистих та корпоративних мереж, пристроїв і даних.

Усіх нас навчили «думати, перш ніж натиснути» на підозріле посилання або електронний лист, але тепер настав час переглянути це для QR-кодів, тому подумайте, перш ніж сканувати. Не скануйте QR-код, якщо ви не знаєте, куди він приведе, і переглядайте веб-сайт і доменне ім'я, щоб переконатися, що саме туди, куди ви очікуєте бути спрямовані. Існує багато безпечних програм для сканування QR-кодів, які дозволяють користувачам переглядати веб-сайти перед їх відвідуванням. Багато веб-переглядачів також дозволяють користувачам вимкнути автоматичне переспрямування на веб-сайти, щоб можна було перевірити домен URL-адреси, та вирішити, чи заслуговує він довіри, щоб отримати додаткову інформацію, перш ніж вживати заходів.

Треба переконатися, що ви завантажуєте програми лише з надійних джерел, таких як Apple App Store або Google Play Store. І постійно оновлювати всі розумні пристрої, щоб скористатися найновішими засобами захисту.

Таким чино можна зробити наступні висновки:

1) Треба уважно подумати, перш ніж сканувати;
2) Після сканування не використовувати автоматичний перехід за посиланням, а уважно передивитися його, на який сервер він спрямований
3) Треба бути обізнаними та пильними.

Як і у випадку з будь-якою технологією, яка все частіше використовується, імовірно, у найближчі часи ми побачимо зростання спроб кіберзлочинців зловживати QR-кодами, тому важливо знати про ризики, щоб мати можливість вжити правильних запобіжних заходів. QR-коди і надалі відіграватимуть важливу роль, оскільки ми починаємо одужувати від пандемії COVID-19, але ми не можемо бути задоволеними. Добре подумайте до, під час і після сканування QR-кодів, щоб максимально збільшити шанси захисту ваших пристроїв і даних.

1.2.2 Безпека парольного доступу

На сьогодень, найпоширенішим засобом авторизації користувачів у різноманітних електронних сервісах та службах є парольний доступ. При такому доступі використовується дві складові: логін і пароль.

Логін – це ім'я користувача в електронній системі, необхідне для ідентифікації та авторизації. Обов'язковою умовою до логіну є те, що в системі не може бути двох чи більше користувачів з одним логіном. Таким чином, логін дозволяє однозначно ідентифікувати користувача системи. Така сама умова унікальності покладається на адреси електронної пошти, тому дуже часто, в різноманітних системах, в якості логінів використовується адреса електронної пошти користувача. Однак, зважаючи на те, що адреси електронної пошти, як правило, не є конфіденційними, існує ймовірність, що одна людина може зареєструватися в сервісі з логіном, що співпадає з адресою електронної пошти іншої людини. Для виключення такої ситуації, підчас

реєстрації з логіном-адресою електронної пошти сервіс додатково здійснює перевірку того, що вказаний поштовий акаунт знаходиться в доступі особи, що реєструється. Це відбувається через направлення відповідного автоматичного електронного листа з посиланням підтвердження реєстрації на цю адресу електронної пошти. Якщо користувач має доступ до поштового акаунту – він зможе завершити реєстрацію, якщо ні – процес реєстрації скасовується.

В якості логіну може використовуватися, як правило, довільна послідовність символів латиниці, арабських цифр, а також символів, що не є буквами чи цифрами (символи підкреслення, дефісу тощо). В переважній більшості систем не дозволяється в логіні використовувати не латинські символи. Це пов'язано з відмінністю кодувань таблиць символів і використання символів, наприклад, кирилиці може призвести до помилок авторизації на сервісі.

З розвитком мобільного зв'язку, дедалі частішим стає використання в я кості логіну-ідентифікатору користувача в системі – його номер мобільного телефону. Це також, пов'язано з тим, що кожен номер в мобільних мережах є унікальним та не повторюється (з урахуванням коду держави та коду оператора). Таким чином, кожен номер є унікальним ідентифікатором в межах усього світу. Крім цього, використання в якості логінів телефонних номерів автоматично забезпечує коректний формат кодової послідовності – використовуються тільки арабські цифри, та знак +. У випадку використання номеру телефонну як логіну, в системах також використовується додаткова перевірка повної доступності цього номеру, а також виключення можливості реєстрації на «чужий» номер. Ця процедура, по аналогії з адресами електронної пошти, здійснюється шляхом надсилання SMS або автоматичного дзвінка на цей номер з подальшими діями, які може виконати тільки особа, яка володіє цим номером. У випадку відсутності у користувача доступу до пристрою, який закріплений за вказаним номером телефона, реєстрація скасовується.

Пароль – це додаткова кодова послідовність символів, яка необхідна для однозначного підтвердження того, що вхід до системи здійснює саме та особа, яка проводила реєстрацію (відповідно, це та сама людина, яка цей пароль створювала при реєстрації, або змінювала пізніше в процесі роботи з акаунтом сервісу). Таким чином, якщо навіть логін стає доступний іншій особі, то відсутність в неї пароля – не дозволить авторизуватися в системі від імені власника логіну. Очевидно, що пароль є основним елементом обмеження доступу до сервісу іншим особам та не повинен розголошуватися.

Для забезпечення безпеки акаунтів у сервісах потрібно притримуватися певних правил поводження з паролями. Створення унікальних комбінацій для входу кожен раз при реєстрації нового акаунта вимагає додаткових зусиль та часу, проте використання простої ключової фрази несе значні ризики – від потрапляння особистої інформації в мережу, до викрадення коштів з онлайн-рахунків.

Для забезпечення надійного захисту особистих даних треба дотримуватися простих правил під час створення безпечного пароля:

– треба уникати часто вживаних слів, використовувати, анприклад, фрази або декілька слів, які несумісні в одному реченні.

– не треба використовувати занадто прості та передбачувані комбінації (Дослідження показують, що в більш як 23,2 мільйона облікових записів використовувався пароль “123456”. Другою поширеною комбінацією є “123456789” в 7,7 мільйона користувачів);

– треба використовувати спеціальні знаки, при цьому, більшість людей використовують спеціальні символи в кінці або на початку комбінації, що спрощує роботу кіберзлочинців. Рекомендується розміщувати спеціальні символи в середині певної фрази або слова;

– категорично не рекомендується використовувати особисті дані в тексті пароля. Ключові фрази для входу, які містять ім’я користувача, легко відгадати за допомогою спеціальних програм;

– бажано створювати унікальну комбінацію для кожного акаунта. Таким чином витік одних облікових даних не поставить під загрозу інші і, можливо, більш цінні акаунти.

Створення надійного паролю ще не забезпечує безпеки персональних даних. Для цього слід дотримуватися певних правил зберігання та використання паролів:

– нікому не передавайте пароль (це стосується навіть друзів і членів сім’ї);

– ніколи не надсилайте пароль електронною поштою, у миттєвому повідомленні або за допомогою інших засобів зв’язку, які не гарантують надійного захисту.

– використовуйте унікальний пароль для кожного веб-сайту. Якщо зловмисники отримали відомості облікового запису з одного сайту, вони намагатимуться використовувати ці облікові дані на сотнях інших відомих веб-сайтів, таких як банківські послуги, соціальні мережі або покупки в Інтернеті, сподіваючись, що пароль повторно використовується в іншому місці. Ця атака є дуже поширеною;

– ніколи не слід записувати нагадування паролів, особливо, коли їх можуть побачити інші особи;

– рекомендується використовувати менеджери паролів. Однією з причин слабкості більшості комбінацій, є те, що користувачі просто не мають можливості запам’ятовувати складні ключові фрази для входу, і тому створюють прості, які легко запам’ятати. Для таких випадків і призначена функція менеджер паролів, яка допомагає створювати та зберігати складні комбінації, а не тримати їх в голові. В таких системах усі паролі зберігаються в спеціальному сховищі паролів – файлі чи файлах, доступ до яких обмежується спеціальним майстер-паролем. Самі файли надійно шифруються, що унеможливлює доступ до їх вмісту навіть, якщо самі файли потрапляють в руки зловмисників. При цьому, користувачу залишається запам’ятати тільки майстер-пароль, який, звичайно, повинен відповідати усім наведеним вище рекомендаціям.

У зв’язку з удосконаленням інструментів зловмисників рекомендується користувачам бути обережними при роботі в Інтернет-мережі, а також використовувати надійні рішення для ефективного захисту конфіденційних даних та особистої інформації, наприклад, такі як двохфакторна аторизація.

Також одним з варіантів витоку конфіденційних даних (зокрема, паролів) може бути візуальне спостереження іншими особами процедури введення паролів. З цією метою, поля введення паролів, як правило, робляться такими, що не відображають символів, що вводяться. Але, розкриття парольної комбінації також можливе через візуальну фіксацію послідовності натискання клавіш на клавіатурі (або сенсорному екрані). Для зниження небезпеки розкриття паролів не рекомендується вводити його в людних місцях, де є прямий візуальний контакт з іншими особами, а також використовувати такі комбінації, які можуть вводитися дуже швидко, що ускладнює візуальну фіксацію.

Також додатковим заходом з захисту паролів є його заміна. Раніше існувало поширене правило, що регулярна зміна паролів захищає від несанкціонованого доступу, але з часом дослідження та приктичні спостереження показали, що це не так. Щотижня, щомісяця чи раз на пів року міняти пароль сенсу немає. Люди починають забувати ці паролі, записувати, додавати при кожній зміні прості комбінації, що є найгрубішим порушенням конфіденційності (див. рисунок 1).

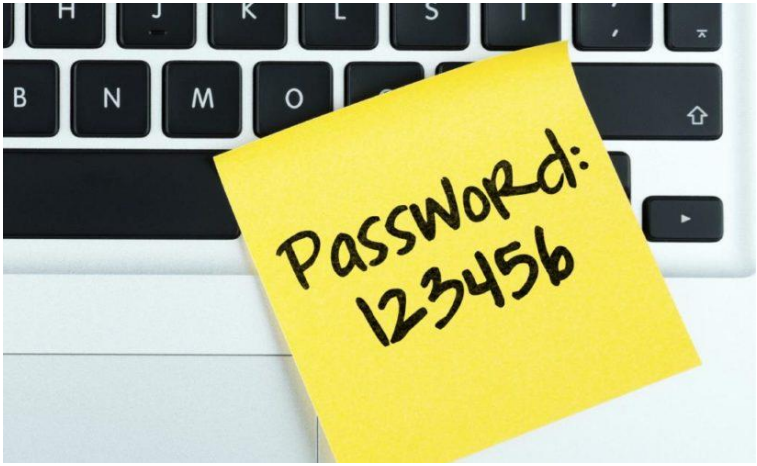

Рисунок 1 – Записування нагадувань паролів є найгрубішим порушенням безпеки особистих даних

Звичайно, можна постійно міняти пароль, але такого правила вже немає. Зараз сучасний підхід дещо інший. Вважається, якщо спочатку був встановлений хороший, надійний пароль, який не використовується глобально для всіх акаунтів, його потрібно міняти в тому випадку, якщо з'являються підозри, що його вкрали. Наприклад, коли пароль вводився в публічному місці або на чужому комп'ютері. Якщо пароль складний, унікальний, без персональної інформації й ви використовуєте новий пароль для кожного акаунту і зберігаєте його в надійному місці, міняти його потрібно тільки в випадку, якщо стався якийсь витік і ваш пароль опинився у відкритому доступі

1.2.3 Двофакторна (двоетапна) авторизація

Останнім часом для підвищення безпеки акаунтів та персональних даних користувачів все частіше використовується двофакторна (багатофакторна) авторизація. Іноді використовується термін двоетапна (багатоетапна) авторизація.

1.2.4 Доступ з використанням апаратних ключів

В окремих випадках, коли безпекові питання носять критичний характер, та є загроза цілеспрямованих хакерських атак, можуть використовуватися спеціальні пристрої – паратні ключі захисту (рисунок 2).

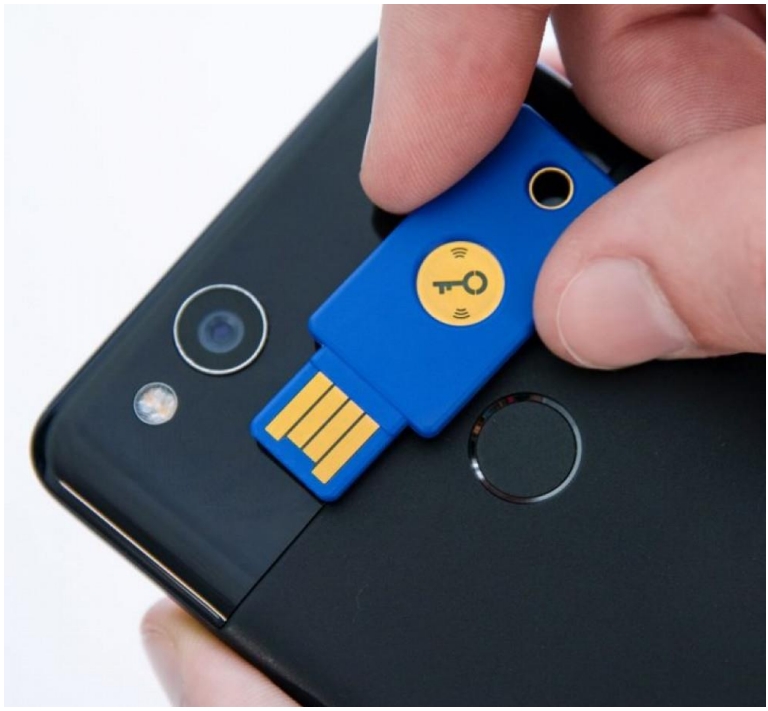

Рисунок 2 – Вигляд апаратного колюча захисту доступу до акаунту

Як правило, такі ключі використовують для доступу до систем критичного застосування, таких як акаунти державних діячів, журналістів, банківських службовців, акаунтів що містять дані з ознаками державної таємниці тощо. Такі акаунти є першочерговою мішенню хакерських атак та вимагають додаткового підвищеного захисту.

Апаратні ключі на кшталт того, який наведений на рис. 2, містить спеціальний код (токен) який повинен бути зчитаний в момент індентифікації користувача в сервісі. Фактично, цей засіб авторизації є розвитком багатофакторної авторизації.

Таким чином, навіть якщо кіберзлочинець отримає у власне розпорядження логін і пароль користувача, він не зможе авторизуватися в системі без апаратного ключа.

Такі апаратні ключі бувають дротові, бездротові та комбіновані. Дротові ключі використовують як правило з'єднання по інтерфейсу USB. Бездротові, в основному, використовують інтерфейси Bluetooth та NFC. Останнього часу, перевага надається NFC-пристроям, так як безконтактне зчитування ключа може відбуватися тільки на маленькій відстані від термінала (5-10 см). Це дозволяє зменшити ймовірність зчитування пристрою сторонніми терміналами зловмисників. Комбіновані ключі мають к дротовий інтерфейс так і бездротовий. Саме такий пристрій проілюстровано на рис. 2. Переваги бездротових ключів пов'язані з універсальністю використання з портативними пристроями, які не мають відповідного типу апаратного інтерфейсу, але найвищий ступінь захисту забезпечують саме дротові ключі, в яких не використовується трансляція кодової послідовності радіохвилями, які можуть бути перехоплені. Звичайно, зменшення ефективної відстані зчитування ключа підвищує його безпечність та ускладнює задачу зловмисників у скануванні секретного коду (токену).

1.2.5 Доступ з використанням електронного цифрового підпису

Іншим варіантом надійної ідентифікації користувача та його авторизації в системі є використання електронного цифрового підпису, який є перевіреним унікальним ідентифікатором особи або установи у світовому інформаційному просторі.

Електронний цифровий підпис (або скорочено – ЕЦП) за правовим статусом прирівняний до власноручного підпису або печатки. Фактично, він представляє дані в електронній формі, отримані за результатами криптографічного перетворення, які додаються до інших даних або документів і забезпечують їх цілісність та ідентифікацію автора.

За допомогою послуг ЕЦП можна підписувати електронні документи, користуватися електронними послугами, реєструватися на державних порталах тощо. Документи, підписані за допомогою ЕЦП, мають таку саму юридичну силу, як і звичайні.

Так як електронний цифровий підпис однозначно ідентифікує особу та забезпечує передачу персональних даних в шифрованому вигляді, він є достатньо надійним засобом ідентифікації на різних віддалених мережевих ресурсах.

Фактично шифрувальна система електронного цифрового підпису складається з трьох складових:

1) відкритого ключа (сертифіката відкритого ключа);

2) закритого (приватного) ключа;

3) пароля до закритого (приватного) ключа.

Відсутність або некоректність хоча б однієї з цих складових не дозволяє виконати коректну криптографічну задачу та використати ключ для ідентифікації користувача.

Відкритий ключ (сертифікат відкритого ключа) генерується підчас творення цифрового підпису авторизованим центром надання цифрових довірчих послуг. Цей

центр і надалі забезпечує обслуговування ключа, поновлення сертифікатів та забезпечення криптографічних процедур. Сертифікати відкритого ключа є у відкритому доступі та публікуються відповідними центрами з надання цифрових довірчих послуг. Вони використовуються як в процесі підписання, так і перевірки підпису (в тому числі підчас автентифікації користувача).

Відкритий ключ використовується для перевірки ЕЦП одержуваних документів (файлів). Відкритий ключ працює тільки в парі з особистим ключем. Відкритий ключ міститься в Сертифікаті відкритого ключа, і підтверджує приналежність відкритого ключа ЕЦП певній особі. Крім самого відкритого ключа, Сертифікат відкритого ключа містить в собі персональну інформацію про його власника (ім'я, реквізити), унікальний реєстраційний номер, термін дії Сертифікату відкритого ключа. З метою забезпечення цілісності представлених у Сертифікаті даних він підписується особистим ключем Центру сертифікації ключів.

Закритий ключ ЕЦП формується на підставі абсолютно випадкових чисел, що генеруються давачем випадкових чисел, а відкритий ключ обчислюється з особистого ключа ЕЦП так, щоб одержати другий з першого було неможливо.

Закритий ключ ЕЦП є унікальною послідовністю символів довжиною 264 біти, яка призначена для створення Електронного цифрового підпису в електронних документах. Працює закритий ключ тільки в парі з відкритим ключем. Закритий ключ необхідно зберігати в таємниці, адже будь-хто, хто дізнається його, зможе підробити електронний цифровий підпис (якщо, звичайно, цей ключ не захищений паролем).

Закритий (приватний ключ) формується в одному екземплярі центром надання цифрових довірчих послуг та надається власнику підпису для зберігання та використання. У будь-яких випадках, закритий ключ не передається іншим особам та повинен безпечно зберігатися власником підпису.

Пароль до закритого (приватного) ключа – це кодова послідовність яка вказується підчас використання цифрового підпису та є додатковим безпековим заходом від несанкціонованого використання цифрового підпису. У випадку заволодіння закритим (приватним) ключем, використання його не можливо без знання паролю. До пароля закритого (приватного) ключа пред’являються ті самі вимого, що були вказані вище у пункті 1.2.2.

Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа. За правовим статусом він прирівнюється до власноручного підпису (печатки). Електронний підпис не може бути визнаний недійсним лише через те, що він має електронну форму або не ґрунтується на посиленому сертифікаті ключа.

За умови правильного зберігання власником закритого (приватного) ключа його підробка неможлива. Електронний документ також не можливо підробити: будь-які зміни, не санкціоновано внесені в текст документа, будуть миттєво виявлені.

Автентифікація користувача за допомогою ЕЦП вимагає вказання центру надання електронних довірчих послуг, який видав цей підпис, шляху де розміщується закритий (приватний) ключ, а також паролю цього ключа. Слід

зазначити, що з метою безпеки передавання паролю, слід використовувати веб-сервіси, які взаємодіють з клієнтським програмним забезпеченням по шифрованих каналах і захищеному протоколу HTTPS.

Велика кількість державних сервісів, серед варіантів автентифікації, пропонують до використання саме ЕЦП: портал пенсійного фонду України, особистий кабінет платника податків на сайті ДПС України, портал державних послуг ДІЯ, портал проходження іспитів на знання державної мови та ін, а також особисті кабінети фінансових установ. В якості прикладу, нижче розглянута процедура авторизації на порталі дія з використанням електронного цифрового підпису.

На рис. 3 показана вкладка автентифікації користувача саме через використання ЕЦП. Для цього, треба в пунктирному полі вказати шлях до файлу закритого приватного ключа, потім нижче вказати який Кваліфікований надавач електронних довірчих послуг генерував цей ключ (або залишити «Визначити автоматично») та нижче ввести в полі «Пароль» пароль для закритого (приватного) ключу.

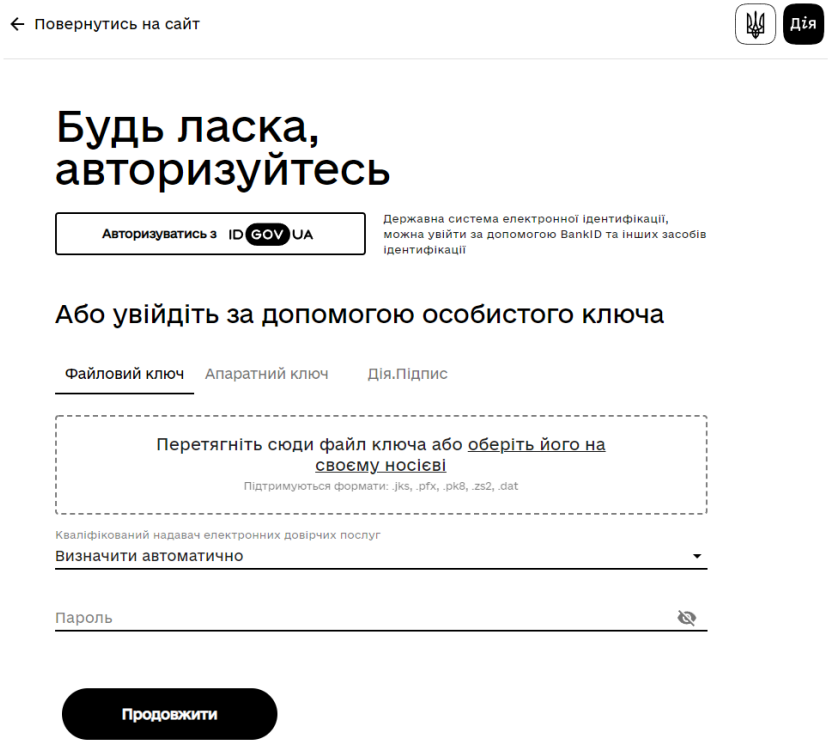

Рис. 3 – Варіанти автентифікації користувача на порталі ДІЯ

Після натискання кнопки «Продовжити» ключ буде зчитаний та перевірений. У випадку позитивного результату перевірки буде здійснена авторизація в особистому кабінеті порталі ДІЯ. Для інших порталів та сервісів процедура автентифікації за ЕЦП аналогічна.

У випадку зберігання ключа ЕЦП на спеціальному захищеному носієві, при автентифікації треба обрати вкладку «Апаратний ключ» (згідно рис. 3), а якщо на персональному смартфоні встановлений додаток ДІЯ та доступна і включена функція «ДІЯ.Підпис», то для автентифікації можна використати третю вкладку на рис. 3.

2 БЕЗПЕКА ПЕРСОНАЛЬНИХ ДАНИХ В РОЗРІЗІ ДІДЖІТАЛІЗАЦІЇ

2.1 Е-профіль громадянина в сучасному ІТ світі

Сьогоднішня можливість отримувати доступ до всього, що підключено до інтернету, це розкіш, яку ми не можемо дозволити собі втратити. Проте чим більше людей використовують онлайн системи, тим більше кіберзагроз.

Витік інформації вже зараз впливає на геополітичні процеси і стає міцною зброєю в руках конкурентів, у тому числі політичних. Проте у віртуальному онлайн світі звичайній людині можна нашкодити цілком реально, як і у реальному житті.

Зловмисники можуть роздобути ваші персональні дані, історію хвороби, приватні переписки у месенджерах, проникнути у смартфон вашої дитини і почати спілкування з нею, отримати доступ до ваших рахунків та онлайн-банкінгу або до ваших гаманців із криптовалютами.

Якщо озирнутись навколо себе, то одними з найвразливіших місць віртуального світу є мобільний телефон із доступом до соціальних мереж, месенджерів, та десятків мобільних додатків часто невідомого походження, де люди з легкістю діляться приватною інформацією, яка, на перший погляд, не є критичною.

При цьому, треба чітко розуміти, що в ІТ-світі нічого не буває безкоштовним. Будь-яка інформація є товаром, на який обов'язково знайдеться покупець. Якщо ми не платимо за якийсь товар і він є безкоштовним для нас (ті ж самі соціальні мережі), то в цьому випадку ми і є товаром, а точніше наші персональні дані. При чому, ми самі ділимося нашими даними, вважаючи їх не критичними, але при певній обробці та систематизації ці дані можуть мати комерційну цінність. Профайли, які збираються на всіх користувачів в соціальних мережах або інших онлайн ресурсах, досить добре монетизуються власниками таких додатків.

Інколи проблема конфіденційності персональних даних з'являється в дуже неочікуваних ситуаціях. Так, наприклад, постінг світлин, що ілюструють аспекти нашого життя можуть містити зображення інших персон і публікація таких зображень без відповідних дозволів призводить до порушення конфіденційності персональних даних.

Наприклад, останнім часом в наше життя все більше входить таке поняття як шерентінг. Шерентінг – новий термін, утворений від англійських слів parenting (виховувати) і to share (ділитися, розміщувати в інтернеті). Це поняття описує дуже поширене явище, коли батьки викладають у соцмережі фотографії своїх дітей і публічно розповідають про ситуації з їхнього життя. Іронія в тому, що за правилами більшості соцмереж, діти не мають права створювати власні акаунти, поки їм не виповниться 13 років. Це означає, що ті діти, які слідують цим правилам, навіть не знають, що коїться в них за спиною. А після реєстрації у соцмережах вони можуть бути неприємно здивовані від того, як багато фотографій їхні батьки оприлюднили. Таким чином, наш цифровий е-профіль у глобальному інформаційному середовищі може починати формуватися ще до того, як ми стаємо повноправними учасниками цифрового світу та інтернет-спільноти.

Іншим прикладом неправомірних дій через соціальні мережі є функція надсилання подарунків від користувачів мережі TikTok своїм улюбленим кліп-мейкерам. Так, відомі факти, коли на деяких ресурсах в TikTok користувачів спонукали до надсилання «цифрового подарунку» вартістю до 48,99 фунтів задля отримання телефона улюбленої зірки соціальної мережі. Такі дії класифікуються як вимагання. Ситуація також ускладняється тим, що серед постраждалих в основному були діти, які за віком на досягли 13 років, та в загалі не повинні припускатися до реєстрації у соціальних мережах. Регуляторний орган США вже оштрафував TikTok на 5,7 млн доларів після звинувачень в зборі особистих даних дітей молодше 13 років без згоди батьків.

Достатньо розповсюдженими також є відомості про те, що спеціальні служби різних держав стежать за користувачами в інтернеті, що також є порушенням прав на приватне життя.

Таким чином, е-профіль громадянина, як сукупність відомостей про нього в різних цифрових ресурсах, починає формуватися ще до того, як цей громадянин стає користувачем цих сервісів. Також, слід пам'ятати, що будьт які наші дії в інтернет ресурсах залишають відомості про нас, які можуть як бути корисними для нас, так і стати джерелом проблем. Тому, на будь якому етапі користування електронними сервісами та ресурсами треба зважувати переваги і можливі ризики та визначати доцільність тих чи інших дій. У будь-якому разі, треба пам'ятати одне найголовніше правило: ми самі створюємо умови для того, щоб даними нашого е-профілю могли скористатися інші особи і тільки ми визначаємо доцільність висвітлення таких даних.

Використання е-профілів громадян в різних інтернет ресурсах може мати як позитивні так і негативні наслідки. Так, наприклад, якщо хтось має повну історію хвороби людини за декілька років, він може вирішити багато питань у боротьбі з вірусами у медичній сфері, але також може бути елементом маніпуляцій і шантажу зі сторони зловмисника, якщо ці дані не були надійно захищені і потраплять йому в руки.

Хакерів та зловмисників в інтернеті цікавить будь-хто, навіть якщо ви не публічна людина. Вас можуть зламати для атаки на ваших колег, керівництво, родичів, або навіть просто випадково.

Для того, щоб не стати жертвою, потрібно іноді виконувати прості вправи та підтримувати так звану кібергігієну. Треба замисліться та проаналізувати, яку інформацію могли б використати проти вас потенційні зловмисники, і спробуйте максимально унеможливити такий сценарій.

Кібергігієна – це, перш за все, самооцінка своїх ризиків. Так само, як мити руки перед їжею, важливо дотримуватись простих правил, що наведені нижче.

– Не підключатись до публічного, неперевіреного WiFi. В цьому випадку краще використовувати мобільний інтернет. Якщо, все ж таки існує потреба підключення, то краще це робити із використанням VPN (не безкоштовного), який дозволяє надсилати дані по шифрованим каналіам.

– Не переходьте за посиланнями, які вам невідомо чому присилають, навіть якщо це ваші знайомі зі знайомих акаунтів. Часто зловмиснику потрібно від вас тільки один клік за посиланням, щоб отримати доступ до вашого профілю.

– Не додавайте незнайомих людей у друзі в соціальних мережах, бо вони можуть відправляти інформацію про вас іншим особам вже у статусі вашого друга.

– Не забувайте про менеджмент паролів, правила якого вже наводилися раніше у п. 1.2.2, використовуйте різні складні паролі, які важко вирахувати, та двофакторну автентифікацію не через SMS, а через додаток.

– Завжди встановлюйте автоматичні оновлення версій програмного забезпечення. Якщо вже вийшло оновлення, цілком можливо, що у старій версії є вразливості.

– Робіть регулярні бекапи важливої інформації, сегментуйте дані, не зберігайте все в одному місці та за одним акаунтом.

– Перевіряйте, щоб сайт, яким ви користуєтесь, працює за шифрованим протоколом HTTPS, а не звичайним HTTP.

– Хоча б раз на кілька років ходіть на тренінги з кібербезпеки. Запросіть туди своїх дітей-підлітків та колег по роботі.

2.2 Джерела персональних даних в IT середовищі

Спробуйте "загуглити" своє ім'я і подивіться, скільки відкритої інформації про вас є в інтернеті. Де і з ким ви відпочивали, як звати ваших батьків, яке дівоче прізвище вашої мами, або навіть як звати ваших домашніх улюбленців.

Персональні дані, наразі - найцінніше, що є у віртуальному цифровому світі. Перед тим, як завантажувати будь-який додаток, бажано дізнатись, хто розробники, як вони зберігають ваші дані і як використовують.

Надалі розглянуто основні джерела та методи отримання персональних даних в IT-середовищі.

2.2.1 Онлайн серфінг

Коли ми відвідуємо якийсь сайт, наш комп’ютер повідомляє йому свої IP-адресу, тип і розмір екрану.

Також сайт бачить, звідки ми на нього прийшли: з якої сторінки чи за яким запитом в пошуковику. А зіставивши нашу IP-адресу з іншими даними, можна визначити і місце нашого перебування.

Якщо виходити в Інтернет з комп’ютерної мережі на роботі, зацікавлена особа легко вирахує нашого роботодавця. Це повністю автоматизований процес який підтримується великою кількістю інтернет сервісів, хоча самої лише IP-адреси ще не досить, щоб гарантовано встановити особу користувача, так як IP-адреса нашого комп’ютерного пристрою може регулярно змінюватися. Тому багато інтернет ресурсів містять лише ймовірні, приблизні дані про тих, хто їх відвідує.

В теорії інтернет-провайдер може бачити все, що робить користувач в Інтернеті, наприклад на які сторінки він заходить. Але, як правило, провайдери не

фіксують звітів про діяльність своїх клієнтів, бо в цьому немає жодної економічної потреби.

З іншого боку, багато інтелектуальних функцій веб ресурсів, які направлені на зручність нашого користування ними несуть потенційну загрозу конфіденційності даних. Серед таких функцій можна назвати найпопулярніші: кастомізація реклами, відправлення звітів про відмови програмного забезпечення, статистику використання сервісів, дані рукописного та голосового введення, дані геолокації, дані персональних хмарних сховищ, що підтримуються, наприклад, в операційних системах від Microsoft; дані геопозиціонування зі співставленням їх на супутникових картах, хмарні сервіси, інтелектуальний пошук та обробка пошукових запитів, що мають місце в рішеннях від Google. Інші IT-компанії також використовують подібний функціонал, який в певних випадках носять загрозу конфіденційності даних.

Багато хто чув про так звані "кукі" (Від англ. cookie). Якщо ми натискаємо десь на рекламу автомобіля, система це запам'ятовує і на іншому сайті нам покажуть рекламу аналогічного змісту (тек звана контекстна реклама). Такі ресурси як Amazon запам’ятовують не тільки усі наші комерційні операції, а й те, які книги ми переглядали, але не купили. А туристичні сайти пам’ятають про авіаквитки, які ми зарезервували, але не придбали. Ці дані зберігаються щонайменше півроку і можуть бути використані у будь який момент як для нашої користі, так і в нашу шкоду.

Теоретично, наприклад, новинний сайт за допомогою кукі може виявити, що хтось з користувачів переглядаєте багато матеріалів про тероризм і це могло би зацікавити служби безпеки. Також, існують системи кластеризації потоків повідомлень в інтернет-форумах і чатах, які дозволяють виділяти тренди та визначати спрямованість дискусій, що може бути використано як в комерційних, маркетингових цілях, так і в безпекових аспектах.

Але, слід пам’ятати, якщо ми щоразу чистимо кукі, завершуючи інтернет серфінг, стежити за нами вже значно складніше.

2.2.2 Пошукові сервіси

Сучасні пошукові системи, на кшталт Google, запам'ятовують запити користувачів, для підвищення релевантності отриманих даних. Запам’ятовуються навіть зроблені помилки в запитах, для того щоб після визначення можливих закономірностей, враховувати це при формування search-листу. В цьому випадку, теоретично, спецслужби, на основі переліку запитів користувача, можуть запідозрити його в тероризмі, тому що в його пошукові запити стосуються вибухівки, навіть якщо це проста цікавість без жодної задньої думки.

Але, слід зазначити, що можливості пошуковиків не такі бездоганні. Наприклад, якщо чистити за собою кеш браузера і кукі, то той же Google буде пам'ятати наші пошуки, але не зможе пов’язати їх з нами.

Слід зазначити, що хоч компанії, що розробляють пошукові системи і прагнуть дізнатися про нас більше, їх, все ж таки, стримує громадська думка і закони про захист приватного життя. Пошуковики зацікавлені тільки в тій інформації, яка

допомагає їм персоналізувати рекламу, а для цього не потрібно зберігати історію пошуків і встановлювати особу користувача.

2.2.3 Електронна пошта

Більшість «безкоштовних» поштових сервісів, в тому числі й найбільш популярні в світі: Gmail і Yahoo, сканують електронну пошту користувачів, а потім показують їм рекламу, пов’язану зі змістом їхніх листів.

В компаніях кажуть, що це роблять машини, а не люди і що це нікому не шкодить: мовляв, ідеться тільки про те, щоб збільшити віддачу від реклами.

Але дехто вважає, що хто б не виконував цю роботу, вона порушує нашу приватність. Так Едвард Сноуден, викривач Prism, стверджував, що Агентство національної безпеки побудувало інфраструктуру, здатну перехопити "практично будь-яку інформацію". "Ця система автоматично перлюструє переважну більшість наших розмов і листів. Якби я хотів залізти до вашої електронної пошти або телефону, то мав би лише скористатись системою перехоплення. Я можу отримати доступ до вашої електронної пошти, кредитної картки, паролів і записів телефонних розмов", - каже він.

Деякі експерти припускають, що державні спецслужби справді мають технічні можливості, щоб вести пошук за ключовими словами у величезних масивах даних. Крім того, провайдери мають певні зобов'язання перед державою. Так, Директива Євросоюзу «Про збереження даних» вимагає від провайдерів зберігати інформацію про електронні листи й дзвінки протягом 6-24 місяців. Зокрема, дані про відправника, одержувача, час або тривалість дзвінків, але не зміст повідомлень або розмов.

2.2.4 Додатки та електронні книги

Чимало додатків для мобільних пристроїв визначають місце перебування людини – наприклад, програми для велосипедистів чи бігунів, які відстежують їхній маршрут і середню швидкість.

Всі ці дані передаються на сервер власника додатку і ми не знаємо, що робить з ними розробник програми. Швидше за все, нічого, але ризик існує. Людина зазвичай вмикає подібні програми на порозі свого будинку, тож з їх допомогою можна, наприклад, вирахувати її адресу.

Електронні книжки також можуть розповісти про свого власника. Щоразу, як ми підкреслюємо якісь фрази в своєму Kindle, він відправляє ці дані на Amazon. Так, наприклад, відомий професор інституту інтернету Оксфордського університету Віктор Майр-Шонберґер каже, що йому, як автору видань, вкрай цікаво, що виділяють його читачі.

2.2.5 Соціальні мережі

В соцмережах люди з власної волі діляться інформацією з друзями та знайомими. Але використання цієї інформації в комерційних цілях є дуже спірним питанням. Ми щодня повідомляємо мережі щось про себе. Ці подробиці можуть здаватися дріб’язковими, але якщо їх зіставити – наслідки можуть бути разючі.

Наприклад, якщо написали повідомлення в соцмережі, що йдете випити кави в конкретний парк, це може навести когось на вашу адресу. Маючи поштовий індекс

парку і ваше прізвище, можна отримати доступ до вашої реєстраційної інформації: домашньої адреси, номера мобільного чи адреси електронної пошти.

Крім того, соцмережа може автоматично визначати наше місцеперебування. Ця функція може відключатися, але багато хто забувають про це не приділяють цьому ніякої уваги. Як наслідок – соціальна мережа завжди має відомості про наше поточне положення.

Також, соціальні мережі реєструють та запам'ятовують кожен наш лайк. Дослідження, яке було проведено в Кембриджському університеті, показало, що за лайками можна з 88%-ю точністю відрізнити чоловіка від жінки, з 95%-ю – афро-американця від європейця, і з 85%-ю точністю – республіканця від демократа.

Тому шкідливість розголошення окремої інформації має набагато менший рівень, ніж розголошення інформації, яка може бути консолідована та використана для визначення нових відомостей.

2.2.6 Телефон

Багато хто вважає свій телефон чимось більш приватним, аніж комп'ютер. Але це зовсім не відповідає дійсності. Встановити місце перебування людини за допомогою телефону можна трьома різними способами. Навіть якщо ми нікому не дзвонимо, фахівці можуть простежити, від якої щогли мобільного зв'язку наш телефон отримуєте сигнал. Це не те саме, що точне місце перебування, але, наприклад, у багатьох кримінальних розслідуваннях і цього було достатньо.

А якщо ваш телефон використовує мережу Wi-Fi або GPS, наші точні координати – також не секретом.

З боку прослуховування розмов все також не є однозначним. На зважаючи на запевнення мобільних операторів щодо повної конфіденційності розмов, треба брати до увагу існуючу вимогу з боку держави реєструвати та протягом півроку зберігати на серверах мобільного оператора відомостей про усі телефонні дзвінки та повідомлення. Ця інформація може надаватися силовим структурам за відповідним запитом. Також, не слід забувати про можливий виток інформації з цих серверів. Звичайно, влада може дізнатися лише номери наших телефонів, серійні номери пристроїв, хто і кому дзвонив, а також час і тривалість дзвінка. А от зміст розмов чи фінансову інформацію оператор не повідомляє. Хоча треба враховувати і можливість хакерських атак.

2.2.7 Транспорт

Транспортні магнітні картки також накопичують дані про нас. Наприклад, коли ми розплачуєтесь в метро карткою, інформаційна система метрополітену отримує інформацію про нашу поїздку. В ній фіксується, де і коли ми скористалися карткою, причому це стосується не тільки метро, а й інших видів транспорту, тим більше, що безконтактні електронні платежі у громадському транспорті стають дедалі популярнішими в Україні. Звичайно транспоті компанії кажуть, що дані лишаються прив'язані до конкретної картки протягом певного періоду (як правило 2-х міфсяців), а далі стають анонімними і використовуються для досліджень. Звичайно, такі компанії діють в рамках закону "Про захист персональних даних і не передають ці дані третім особам для використання у комерційних цілях. Але може статися що

завгодно. Теоретично, існує можливість стеження за людиною за допомогою транспортних карток та безконтактних платежів.

Якщо мати на руках дані із транспортних карток і зіставити їх з записами камер спостереження, можна відстежити пересування суб'єкта.

2.2.8 Покупки

Не для кого не є секретом, що супермаркети вивчають купівельні звички людей за допомогою карток лояльності (дисконтних карток). Таким чином магазин намагається підвищити ефективність маркетингу.

Коли ми підписуємось на картку торгових мереж, то погоджуємось на використання даних про вас. В анкетах ми добровільно вказуємо персональні дані: прізвище, ім'я, дату народження, особистий номер телефонної пошти та електронну адресу тощо. На основі цих даних ретейлери надсилатимуть нам адресні пропозиції, рекламу та інформацію, яка може нас зацікавити.

Також, торгівельні площадки, які не мають карток лояльності, мають можливість відстежувати звички своїх клієнтів. Це робиться на основі аналізу нашого споживчого кошик, за номером банківської картки, якою ми розраховуємося, щоправда без використання імені. При цьому, існує можливість співставлення номеру банківського рахунку та прізвища його власника. При цьому, аналіз наших покупок робиться в хронологічній послідовності, у прив'язці до сезону і навіть часу купівлі.

Стосовно користувачів інтернет-магазинів такий аналіз стає ще більш детальним. Коли ми передивляємось якісь товари, кожен наш клік по посиланням на групах товарах, або конкретних пропозиціях фіксується для визначення наших уподобань та зацікавленості. Таким чином фіксується не тільки кінцеві зроблені покупки, а й усі товари та групи товарів, які викликали в нас зацікавленість, при чому також в прив'язці до сезону, часу та ін.

Сукупний аналіз цих даних дозволяє власникам торгівельних майданчиків визначати динаміку попиту на різні групи товарів та окремі позиції, відслідковувати сезонний попит, а також розробляти маркетингові заходи щодо стимулювання купівельної активності.

2.2.9 Камери спостереження

Камери відеоспостереження стають дедалі доступнішими за причини значного зниження їх вартості. Кількість таких камер дедалі зростає в усьому світі. При цьому різноманіття таких камер дуже велике: це і камері загального використання з дротовою або бездротовою передачею відеоданих, а також спеціального призначення для особливих у мов спостереження як відкритого так і прихованого.

Слід зазначити, що поки що ці пристрої не сполучені між собою, в глобальні системи сховища відеоданих, і ніхто примусово не збирає отриману інформацію в єдину картину. Але такий час глобалізації, все ж таки наближується. При чому, ми самі надаємо таку інформацію добровільно до відкритого доступу, публікуючи відео ролики у різноманітних відео каталогах, на кшталт YouTube, або роблячи стрімінгові трансляції у популярних сервісах на кшталт Twitch.

Технології розпізнавання облич зараз також на підйомі, тож не виключено, що одного прекрасного дня "можна буде відстежити всі наші пересування хоч в межах рідного міста, хоч в межах усього світу.

Записи з камер спостереження підпадають під дію закону "Про захист персональних даних". Це означає, що ми маємо право знайомитися з уривками, на яких фігуруємо особисто або фігурує інформація про нас, наприклад номерні знаки наших авто. Але як довго можуть зберігатись ці записи, закон не визначає.

Низка країн, зокрема Великобританія та Сполучені Штати Амераки увели норми щодо відеоспостереження. Вони зокрема зобов'язують місцеві органи влади та поліцію регулярно робити ревізію камер і вирішувати, чи є вони необхідними, ефективними та рівномірно розташовані. Але, при цьому, правила для відеокамер, розташованих на підприємствах і приватній власності, не є повністю врегульованими і власним має право визначати особисто політику використання корпоративних систем відеоспостереження.

2.2.10 Водіння транспорту

На транспорті, враховуючи підвищену небезпеку життю та здоров'ю людей, особливий контроль даних учасників дорожнього руху є однією з найважливіших задач.

Поліція вже тривалий час використовує камери, здатні автоматично визначати номерні знаки транспортних засобів.

В усьому світі вже сьогодні забезпечений відеоконтроль усіх основних ділянок транспортних магістралей. Камери фотографують номерні знаки транспортних засобів і реєструють дату, час і місце зйомки. У фокус потрапляє передня частина машини, тож на фото можуть потрапити і водій з пасажиром.

Далі обладнання сканує номерні знаки і перевіряє їх по кількох базах даних. Система автоматичного розпізнавання номерних знаків зчитує номерні знаки щосекунди. Таким чином, можна в режимі реального часу вистежити авто, які становлять інтерес, наприклад, для поліції.

У деяких випадках камери можуть здіймати тревогу, помітивши машину з конкретними номерами. Наприклад, коли в 2005 році озброєна банда убила в Бредфорді (Великобританія) поліцейську Шерон Бешенівскі і спробувала втекти, система моніторингу щоразу подавала сигнал, коли авто підозрюваних проїжджало повз камери. Це дозволило поліції оперативно затримати вбивць.

Систему автоматичного розпізнавання номерних знаків також використовують податківці, митники, інші державні установи.

Схожою технологією, тільки у значно скромніших масштабах, користуються і приватні компанії, наприклад супермаркети чи паркінги. Так вони визначають клієнтів, які порушили правила паркування або поїхали не заплативши.

2.2.11 Кредитно-інформаційні служби

Агентства кредитних історій – це фірми, які збирають фінансову інформацію про особу, зокрема дані про його кредитні картки, банківські рахунки, іпотеку та борги.

Послугами цих агентств користуються банки, оператори мобільного зв'язку і навіть комунальні підприємства. Вони надають агентствам інформацію про клієнтів для аналізу їхньої кредитоспроможності.

В своїй діяльності такі агентства використовують чимало різних даних – від національного реєстру виборців до виплат по кредитних картках. В їхньому статуті закріплено, що кожен має право переглянути власну кредитну історію.

В типовій кредитній історії перераховані кредитні рахунки особи, дати їхнього відкриття, кредитні ліміти чи суми кредиту, а також інформація про затримки виплат. Крім того, там містяться особисті дані: ім'я, дата народження, поточна і попередня адреси проживання особи.

Діяльність таких агентств стає дедалі важливішою в руслі зростання кількості випадків шахрайства з отриманням кредитних послуг, що оформлюються на підставних осіб, або на третіх осіб без їхнього відома. Ці агентства можуть надавати інформацію за запитами правоохоронних органів.

Наприклад, підчас отримання пільгових сервісів, таких як іпотека або субсидія, особа вдає, що живе сама, бо для таких громадян передбачена пільги. Місцеві органи влади можуть попросити кредитне агентство перевірити, чи не значаться за цією адресою інші люди – наприклад у реєстрі виборців чи в рахунках за телефон.

Всі подібні агентства наголошують, що діють суворо в рамках закону і поважають право на приватність громадян.

2.2.12 Державні реєстри

Українці зобов’язані реєструватись у національному списку виборців, хоча багато людей цього не роблять і їх не карають. У підсумку формується єдиний реєстр – відкритий документ з адресами громадян. Вже багато років він є золотою жилою для торговців, журналістів і розповсюджувачів реклами.

Зараз на вимогу громадянина його ім’я можуть прибрати з загальнодоступного списку – воно залишиться тільки в закритій версії, яку використовує влада. Однак, кредитно-інформаційні агентства теж домоглися доступу до закритої версії. Крім того, нею можуть користуватися політичні партії та депутати.

Якщо ми не реєструємося у виборчих списках, перед нами зачиняються двері всіх кредитних установ.

Загальнодоступну версію реєстру може придбати будь-хто для будь-яких цілей, зокрема прямих продажів. Фактично, виборчі списки відображають історію ваших переїздів і місць проживання.

Нині на рівні держави також запущено багато цікавих, корисних електронних сервісів: E-health, ДІЯ та інші. Приємно розуміти, що ми одні з небагатьох країн світу, хто запустив і продовжує запроваджувати такі послуги онлайн.

Гарна мета – покращення нашого життя та зменшення бюрократичних і корупційних складових. Проте, треба розуміти, що саме питання кібербезпеки є ключовим для довіри громадян та використання онлайн сервісів.

Якщо ваші дані просять надати державні органи, потрібно також цікавитись, якими є стандарти зберігання і де їх будуть тримати.

Коли держава запускає глобальні рішення, бажано публічно заявляти розробника, а також відповідального за кібербезпеку (зазвичай це окрема компанія).

В розвинених країнах розробники із задоволенням говорять про кіберзахист. У такий спосіб вони акцентують увагу на турботі про своїх користувачів. Надійний захист персональних даних, безперечно, є конкурентною перевагою, тому що споживач на це вже звертає увагу.

2.3 Ознаки порушення приватності персональних даних при е-взаємодії та сценарії протидії

«Кожен має право на повагу до свого приватного та сімейного життя, до свого житла і кореспонденції», — закріплено у ст. 8 Європейської конвенції про захист прав людини і основоположних свобод. Однак чи не є право на приватність лише декларацією в умовах глобалізації? Наразі ми маємо дві діаметрально різні позиції стосовно поняття приватності. Перша позиція переконує, що приватність з часом зникне, з огляду на обсяги персональних даних, які щодня збираються про кожного з нас. Друга позиція, навпаки, наголошує на абсолютній цінності права на повагу до приватного життя, потреба в якій зростає в еру технологій, коли є можливість заробити на витоку персональних даних, а отже, політика держави щодо підвищення безпеки даних набуває першочергового значення.

До травня 2018 р. європейці дотримувалися рамочної Директиви про захист персональних даних 95/46/ЕС від 24.10.1995 р. Потім 25.05.2018 р. набув чинності Загальний регламент із захисту персональних даних №2016/679 (далі — GDPR, Регламент). Важливим нюансом GDPR є екстериторіальний принцип дії нових європейських правил обробки персональних даних, який не обговорювали останні два роки лише ліниві. Тому деяким українським компаніям варто уважно поставитися до вказаних правил, особливо якщо їхні послуги орієнтовані на європейський чи міжнародний ринок.

Загальний регламент із захисту персональних даних №2016/679 спрямований не лише на захист споживача, але й на захист бізнес-середовища. GDPR надає резидентам ЄС інструменти для пильного контролю за своїми персональними даними, запроваджує універсальний підхід до обробки та збору даних (насамперед, на основі «згоди»), встановлює детальні та єдині для всіх процедури щодо захисту

персональних даних і розслідування фактів їх порушення, передбачає штрафи до 20 млн євро або 4% від річного доходу компанії.

Україна, в особі Кабінету Міністрів України, 25.10.2017р. самостійно визначила для себе завдання імплементувати GDPR у національне законодавство до 25.05.2018 р. Постановою Кабінету Міністрів України від 25.10.2017 р. №1106, якою був затверджений План заходів з виконання Угоди про асоціацію між Україною та ЄС, а також строк приведення законодавства у відповідність до GDPR продовжено до 25.05.2020 р. Відповідальність за виконання вказаних положень покладено на Уповноваженого Верховної Ради України з прав людини, Мін'юст, Мінфін, Мінекономіки, МВС. 12.11.2019 р. при Секретаріаті Уповноваженого ВРУ з прав людини була створена міжвідомча робоча група щодо розробки законодавчих пропозицій у сфері захисту персональних даних.

Розробка та подання на розгляд Кабінету Міністрів України законопроекту щодо внесення змін до Закону України «Про захист персональних даних», ухваленому ще 01.06.2010 р. за зразком чинної на той час Директиви ЄС №95/46/ЕС — це завдання, що залишається актуальним вже не один рік, до якого активно долучилися представники центральних органів виконавчої влади та інших державних органів, правники, міжнародні експерти.

Загальний регламент із захисту персональних даних №2016/679 передбачає широке тлумачення терміну «персональні дані». Персональні дані — це не лише інформація, яка прямо ідентифікує особу, але й інформація, яка в сукупності з іншими даними може бути використана для ідентифікації особи (наприклад, ім'я, номер паспорта, номер посвідчення водія, домашня адреса, фотографія, адреса електронної пошти, банківські реквізити, медична інформація, IP-адреса комп'ютера тощо).

Згідно з GDPR, є дві особи, відповідальні за обробку персональних даних — контролер та процесор. Контролером називають особу (фізичну чи юридичну) або орган державної влади, які визначають ціль та мету обробки персональних даних. Процесором є особа чи орган державної влади, що здійснює обробку персональних даних відповідно до мети та цілей, встановлених контролером. Саме контролер і процесор несуть солідарну відповідальність у випадку порушень GDPR та зобов'язані повідомляти контролюючі органи, а в окремих випадках і суб'єктів даних, про будь-які порушення (витік, викрадення, несанкціонований доступ), пов'язані з персональними даними, протягом 72 годин після встановлення такого порушення.

Частина 1 ст. 82 Регламенту встановлює, що будь-яка особа, яка зазнала матеріальної чи нематеріальної шкоди в результаті порушення положень цього Регламенту, має право на отримання компенсації від контролера чи процесора за завдану шкоду. Відповідальність за допущені порушення необов'язково повинна бути у вигляді адміністративного штрафу, також це може бути попередження, ультиматум, обмеження чи заборона діяльності. Однак якщо мова все ж таки доходить до накладення штрафу, наглядовий орган у кожному конкретному випадку повинен гарантувати, що штраф буде ефективним, співмірним та стримувальним (ч. 1 ст. 83 Регламенту).

За незначні порушення GDPR розмір матеріальної відповідальності може сягнути максимум 10 млн євро або 2% від річного обігу компанії за попередній фінансовий рік, залежно від того, яка сума буде більшою. За значні порушення, пов'язані з недотриманням основних принципів захисту персональних даних, розмір матеріальної відповідальності може сягнути максимум 20 млн євро або 4% від річного обігу компанії за попередній фінансовий рік, залежно від того, яка сума буде більшою.

В українському законодавстві одразу кілька законів регулюють питання надання інформації про фізичних та юридичних осіб. Це і Закон «Про інформацію», що регулює відносини щодо одержання і поширення інформації, і Закон «Про захист персональних даних», що визначає захист і обробку персональних даних, і Закон «Про доступ до публічної інформації», який надає право на отримання інформації, що знаходиться у володінні розпорядників.

Одні й ті ж визначення у цих Законах не ідентичні, а подеколи частково суперечать один одному, чим створюють проблеми із реалізацією особою свого права на інформацію.

2.3.1 Інформація про особу та персональні дані

Інформація про особу – це будь-які відомості, що стосуються фізичної особи, як то біографічні дані, її вподобання (наприклад, улюблена книга чи колір), погляди тощо. Це дуже широкий обсяг інформації. Та чи є будь-яка інформація про фізичну особу її персональними даними?

Закон України «Про інформацію» ототожнює ці два поняття. У статті 11 цього Закону міститься таке визначення: «інформація про фізичну особу (персональні дані) – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована…». Аналогічне визначення персональних даних закріплено у статті 1 Закону «Про захист персональних даних»: «персональні дані – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована». Проте у цьому Законі прямо не сказано, що вся інформація про особу – це її персональні дані.

Ключовим є розуміння того, яка особа є ідентифікованою, або такою, що може бути ідентифікована. Не виникає, як правило, питань щодо таких відомостей, як ім’я, адреса проживання, індивідуальний податковий номер. Ці дані окремо або в сукупності дають змогу володарю цих даних чітко ідентифікувати конкретну особу. Ситуація є трохи складнішою з даними, що ідентифікують особу опосередковано. Наприклад, ми купуємо в магазині певні продукти і використовуємо дисконтну картку. Сама по собі інформація про куплені продукти не є персональними даними, хоча і стосуються фізичної особи. Адже будь-хто міг купити такі ж самі продукти в цьому або іншому магазині.

Та якщо ми купили і використали дисконтну картку – це дає змогу продавцеві ідентифікувати конкретну особу, а отже ваша історія покупок у поєднанні з інформацією про картку стає персональними даними. Так, ми можемо говорити, що персональними даними будуть відомості про номер картки, ім’я її власника, дата і

час покупки, її вартість, а також інформація про куплені речі. І ці дані будуть захищатись відповідно до законодавства та повинні збиратись із законною метою.

Тобто, якщо певна інформація дає змогу володільцю виділити із групи людей конкретну особу, то її можна вважати персональними даними. Тому, дані, які самі по собі не є персональними даними, за певних обставин (коли вони дають змогу ідентифікувати особу) ними стають.

Проте, якщо сукупність певних даних не дає змогу ідентифікувати особу, то їх обробка не захищається Законом «Про захист персональних даних». Слід звернути увагу, що така ж позиція викладена і в вище згаданому Регламенті Європейського Парламенту і Ради (ЄС) 2016/679. Так, у пункті 26 цього Регламенту сказано, що «принципи захисту даних, відповідно, не можна застосовувати до анонімної інформації, зокрема інформації, що не стосується фізичної особи, яку ідентифіковано чи можна ідентифікувати, або персональних даних, що стали анонімними у такий спосіб, що суб'єкта даних неможливо чи більше неможливо ідентифікувати. Таким чином цей Регламент не стосується опрацювання такої анонімної інформації, у тому числі, для статистичних або дослідницьких цілей».

Персональні дані – це інформація про фізичну особу. Не вся інформація про особу є її персональними даними. Все залежить від того, чи дає змогу ця інформація ідентифікувати особу.

Варто також наголосити, що не вся інформація за бажанням особи може бути віднесена до розряду конфіденційної. Є багато випадків, коли різними законами передбачено відкритість певної інформації, наприклад, про займану посаду і робочі контакти, розпорядження бюджетними коштами, відомості із відкритих реєстрів тощо. Отже, законами може бути заборонено будь-кому обмежувати доступ до певної інформації. Фактично особа, якої стосується інформація, не має права визначати режим доступу до такої інформації.

На основі вище наведеного, можна зробити висновок, що:

– конфіденційною є інформація про фізичну або юридичну особу, крім суб'єктів владних повноважень, яка обмежена у доступі цією особою, а також попередньо обмежена законодавством до моменту, поки особа не відкриє таку інформацію за власним бажанням;

– така інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом;

– законодавством може бути заборонено віднесення певної інформації до обмеженої у доступі, зокрема і конфіденційної.

2.3.2 Персональні дані та конфіденційна інформація

Вкрай важливим є усвідомлення того, що персональні дані – це завжди інформація про фізичну особу, при чому лише живу особу. Відповідно до статей 24 і 25 Цивільного кодексу України людина, як учасник цивільних відносин, вважається фізичною особою. Її цивільна правоздатність виникає в момент народження і припиняється в момент смерті. Тому, враховуючи положення Закону «Про захист

персональних даних» і Цивільного кодексу, інформація про померлу особу не є її персональними даними.

Однак, до конфіденційної може відноситись також інформація про юридичну особу, наприклад, “комерційна таємниця”. Відповідно до статті 505 Цивільного кодексу України це можуть бути відомості технічного, організаційного, комерційного, виробничого та іншого характеру (за винятком тих, які відповідно до закону не можуть бути віднесені до комерційної таємниці) і щодо яких ця юридична особа вжила заходи щодо збереження секретності. До конфіденційної юридичною особою може бути віднесена також і інша інформація.

В той же час законодавством може бути заборонено віднесення певних персональних даних фізичної особи до конфіденційної інформації. Відкритою є, наприклад, така інформація:

– прізвища, імена, по батькові фізичних осіб, які отримали бюджетні кошти, отримали у володіння, користування чи розпорядження державне та/або комунальне майно (частина п’ята статті 6 Закону «Про доступ до публічної інформації»);

– персональні дані, що стосуються здійснення особою, яка займає посаду, пов’язану з виконанням функцій держави або органів місцевого самоврядування, посадових або службових повноважень (частина друга статті 5 Закону «Про захист персональних даних»);

В обох випадках прізвища, імена, по батькові фізичних осіб, які отримали бюджетні кошти або займають певну посаду, є їх персональними даними, адже ці відомості дають змогу ідентифікувати конкретну особу. Проте будь-які дії із відкритими персональними даними, наприклад, збирання, поширення тощо, не підпадають під регулювання Закону «Про захист персональних даних». І хоча це прямо не закріплено у цьому Законі, проте таке розуміння логічно випливає із його положень, адже всі дії щодо обробки (збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання і поширення (розповсюдження, реалізація, передача), знеособлення, знищення персональних даних, у тому числі з використанням інформаційних (автоматизованих) систем) спрямовані на захист саме тих персональних даних, які є конфіденційною інформацією. Інакше, на володільця покладався б надмірний тягар обов’язків (наприклад, повідомляти суб’єкта персональних даних про зміну, видалення чи знищення його персональних даних відповідно до статті 21 Закону «Про захист персональних даних»), які неможливо було б виконати на практиці. Це фактично паралізувало б роботу будь-яких володільців таких даних.

Ці дані є відкритими у доступі відповідно до законодавства і не можуть бути віднесені до конфіденційної навіть за бажанням відповідної особи. Будь-хто може обробляти їх без обмежень.

Варто також додати, що відповідно до судової практики, до конфіденційної не може бути віднесено і іншу інформацію про посадових чи службових осіб (наприклад, дані про освіту, досвід роботи, знання іноземної мови, відсутність судимості тощо), якщо до посади, пов’язаної з виконанням функцій держави або

органів місцевого самоврядування, встановлені відповідні кваліфікаційні чи інші обов'язкові для займання цієї посади вимоги (п. 5.8 Постанови Пленуму ВАСУ № 10 від 29.09.2016р. «Про практику застосування адміністративними судами законодавства про доступ до публічної інформації»).

Таким чином, не всі персональні дані є конфіденційною інформацією. У випадках, встановлених законодавством, деякі персональні дані є відкритою інформацією. Водночас, конфіденційна інформація включає в себе не тільки персональні дані.

2.3.3. Розголошення персональних даних

З'ясувавши як співвідносяться між собою всі ці поняття, варто також розібратись чи може поширюватись така інформація і в якому порядку.

Слід зазначити, що вільно поширюватись може та інформація про фізичну, юридичну особу, яка є відкритою відповідно до законодавства. Це також стосується інформації, яка раніше була правомірно оприлюднена розпорядником (частина третя статті 6 Закону «Про доступ до публічної інформації»).

Також поширюватись може конфіденційна інформація про особу, її персональні дані, якщо ця особа надала свою згоду на поширення або самостійно поширила її серед необмеженого кола осіб, наприклад, розповіла про певні факти свого життя в прямому ефірі телеканалу, опублікувала її у соціальних мережах без обмеження режиму доступу.

В деяких випадках така інформація може поширюватись без згоди особи. Відповідно до частини другої статті 14 Закону «Про захист персональних даних» поширення персональних даних без згоди суб'єкта персональних даних або уповноваженої ним особи дозволяється у випадках, визначених законом, і лише (якщо це необхідно) в інтересах національної безпеки, економічного добробуту та прав людини. До таких законів ми можемо віднести, наприклад, податкове чи кримінально-процесуальне законодавство, що надають право відповідним органам отримувати обмежену у доступі інформацію для виконання своїх функцій.

Одним із законів, що дозволяє поширювати такі дані є Закон «Про доступ до публічної інформації». У ньому закріплено загальну конструкцію, що регулює поширення обмеженої у доступі інформації – трискладовий тест (частина друга статті 6 цього Закону).

Трискладовий тест зобов'язує розпорядників інформації, розглядаючи запит на публічну інформацію або вирішуючи чи оприлюднювати інформацію на сайті, з'ясовувати:

1) чи обмежується доступ до інформації на підставі закону в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя? У випадку із конфіденційною інформацією таким інтересом скоріш за все буде захист репутації або прав інших людей, або запобігання розголошенню

інформації, одержаної конфіденційно. Доступ до такої інформації може бути обмежено Законом «Про захист персональних даних» або іншими законами.

2) чи може розголошення інформації завдати істотної шкоди цим інтересам? Розпорядник повинен з'ясувати чи настануть для особи, якої стосується конфіденційна інформація, негативні наслідки через поширення цієї інформації. Якщо поширення інформації не матиме значний негативний вплив, то інформація може поширюватись. Якщо розголошення завдасть істотної шкоди, то розпорядник повинен перейти до наступного пункту.

3) що переважає: шкода від оприлюднення такої інформації чи суспільний інтерес в її отриманні, що полягає в інтересах національної безпеки, економічного добробуту та прав людини? Іншими словами, розпорядник інформації повинен у конкретній ситуації оцінити, збалансувати та вирішити, який інтерес має більший пріоритет. Якщо переважає інтерес суспільства – надати інформацію, а якщо інтерес захисту приватності – відмовити. При цьому, розпорядник зобов'язаний врахувати вимоги частини сьомої статті 6 Закону «Про доступ до публічної інформації», а саме: надати сам запитуваний документ (якщо запитувач просив надати документ), вилучивши з нього ці конфіденційні відомості.

На відміну від інших видів обмеженої у доступі інформації, розпорядники конфіденційної інформації за відсутності згоди суб'єкта персональних даних можуть поширити таку інформацію лише в інтересах національної безпеки, економічного добробуту та прав людини.

2.3.4 Методи та сценарії забезпечення приватності особистих даних при е-взаємодії

На основі вище наведеного було встановлено, що більшість випадків безкарного оприлюднення персональних даних пов'язано з прямою або опосередкованою згодою особи-власника цих даних. То му, звичайно, треба чітко розуміти наслідки, які можуть бути у випадку особистого оприлюднення персональних даних, або надання дозволу на їх оприлюднення.

Всі ці дані можуть використати проти вас. Потрібно привести до ладу таку публічну інформацію, налаштувавши персональні параметри у соцмережах, і періодично перевіряти це.

Як захистити свої персональні дані?

Використовувати для листування лише шифровані месенджери. Наприклад, «Вотсап», «Месенджер» (застосунок для листування в соцмережі «Фейсбук») тощо. Не користуватися для комунікації СМС, месенджери, соцмережі «ВКонтакте», «Телеґрам» тощо.

Застосовувати двофакторну автентифікацію скрізь, де це можливо.

Використовувати електронний цифровий підпис.

Застосовувати активацію пристроїв і застосунків через біометричні дані (наприклад, через відбиток пальця тощо).

Використовувати складні паролі, різні для різних сервісів. Регулярно замінювати паролі.

Не вводити однотипного пароля для різних платформ.

Не встановлювати на смартфон сумнівних і ненадійних застосунків. Частина експертів зараховує до таких і українські державні онлайн-сервіси.

Ніде й ніколи не вводити логін і пароль від електронної пошти, крім самої електронної пошти. Те ж саме стосується соцмереж, банківських та інших важливих застосунків.

Після купівлі комп'ютера чи смартфона користуватися ними лише після оновлення програмного забезпечення.

Не скачувати піратський контент і контент із торентів.

Скаржитися на акаунти чи сайти, які нелегально поширюють персональні дані громадян, а також долучатися до їхнього блокування.

3 ЕЛЕКТРОННІ ПОСЛУГИ ФІНАНСОВИХ УСТАНОВ

Зупинімося детальніше на BankID як способу верифікації громадян через українські банки для надання адміністративних та інших послуг через Інтернет. Ідентифікація через BankID нічим не відрізняється від перевірки документів в банках в очному режимі. Ідентифікація з використанням BankID для громадян відрізняється від ідентифікації за допомогою електронного цифрового простотою використання і популярністю, оскільки здебільшого ЕЦП поширені серед юридичних осіб, а кожна фізична особа на сьогодні володіє банківською карткою.

Правовою основою використання BankID для адміністративних послуг на сьогодні становлять: Закон України «Про адміністративні послуги», Постанова Кабінету міністрів України «Про затвердження Порядку ведення Єдиного державного порталу адміністративних послуг» [18], Положення про систему BankID Національного банку України, затверджене постановою правління Національного банку України від 30.08.2016 № 378 [19].

Наразі до єдиної національної системи електронної дистанційної ідентифікації фізичних і юридичних осіб BankID НБУ підключені «Ощадбанк» та «Радабанк», низка банків знаходиться на різних стадіях підготовки, тестування та підключення до системи [20].

Крім системи BankID НБУ, існує проект Приватбанку, який впроваджує власну систему BankID. Однак, ідентифікації за допомогою BankID Приватбанку недостатньо для відкриття банківського рахунку або проведення інших фінансових операцій, оскільки НБУ дозволив здійснювати банківські операції за допомогою BankID лише у власній системі BankID НБУ. Детальніше про надання банками послуг в мережі Інтернет можна подивитися у правовій літературі [21].

4 ЕЛЕКТРОННЕ ШАХРАЙСТВО В СУЧАСНОМУ ЦИФРОВОМУ СВІТІ

4.1 Телефонне шахрайство

Телефонне шахрайство – це вид шахрайства, коли шахрай телефонує і переконує жертву повідомити особисту, фінансову чи конфіденційну інформацію або переказати гроші. Виманювати платіжні дані зловмисник може з будь-якого приводу: “родич потрапив у ДТП”, “Ви виграли мільйон!”, “Ваша картка заблокована”. Навчіться розпізнавати обман за допомогою порад, які наведені у статті.

Шахрая цікавлять реквізити Вашої платіжної картки, паролі, коди банків та мобільних операторів, кодові слова. Усе це зловмиснику потрібно, аби зняти залишки коштів на карті або переконати жертву здійснити переказ коштів на свою користь.

Шахрай може назватися будь-ким – працівником банку, працівником НБУ, Пенсійного фонду, Фіскальної служби, працівником поліції, комунальних служб, мобільного оператора, покупцем вашого товару тощо.

Якщо запитують термін дії картки, тризначний номер на звороті картки, паролі, коди банків та мобільних операторів, негайно треба припиняти розмову.

Шахрай може обіцяти “легкі” гроші, наприклад, несподіваний виграш, може намагатися керувати у телефонній розмові вашими діями – направляти до терміналу чи банкомату, може попросити сфотографувати та переслати/надати фото платіжної картки, залякувати, що Ваша картка заблокована, а злочинці зламали рахунок, чи попросити перейти за посиланням та зазначити всі персональні дані та реквізити платіжної картки. Усі зазначені дії співрозмовника є прямими ознаками шахрайства.

Три типових сценарії телефонного шахрайства.

Сценарій “Ваша картка заблокована”. Шахрай маскується під працівника банку і просить надати інформацію: реквізити картки, одноразові паролі. Також під час розмови шахрай може переконувати здійснити перерахунок коштів, зняти ліміт по картці. При цьому сценарії треба пам’ятати – працівники банку ніколи не телефонують, щоб дізнатись зазначену інформацію. Якщо є сумніви, шахрай чи працівник, передзвоніть на офіційний номер телефону банку, який зазначеній на картці.

2) Сценарій “Мамо, я в поліції або у лікарні”. Вночі телефонує нібито представник правоохоронних органів і повідомляє, що Ваш родич в поліції за бійку, ДТП, крадіжку тощо. Щоб його визволити вам необхідно сплатити кошти (перерахувати грошову компенсацію постраждалому/слідчому/лікарю чи судді тощо). Для переконливості шахрай передає слухавку нібито родичеві, який жалібним голосом пояснює, що сталася біда. Перед тим, як віддавати, сплачувати чи переказувати кошти, треба зателефонувати своєму родичу та запитати, як у нього справи.

3) Сценарій “Ви виграли автомобіль, квартиру, мільйон тощо”. Жертві надходить SMS-повідомлення щодо виграшу, більше деталей на сайті або за телефоном. Особа, передзвонює за вказаним номером, де їй пояснюють, щоб отримати свій приз, необхідно сплатити податок у розмірі 1% від його вартості. Для переконливості шахраї можуть створити сайт, на якому є вся інформація щодо “акції” та відгуки попередніх переможців. Треба пам’ятати, що податки не сплачує отримувач виграшу, вони утримуються з суми виграшу через її зменшення на суму податків.

4.2 Інтернет шахрайство та шкідливе програмне забезпечення

Цей вид шахрайства є одним з найдавніших та спостерігається з часів коли активно почали використовуватися комп'ютерні мережі. Комп’ютерні віруси є різновидом шкідливого програмного забезпечення.

Комп'ютерний вірус - різновид комп'ютерних програм або шкідливий код, відмінною особливістю яких є здатність до розмноження (самореплікації). На додаток до цього віруси можуть без відома користувача виконувати інші довільні дії, у тому числі які завдають шкоди користувачеві та/або комп'ютеру.

Навіть якщо автор вірусу не програмував шкідливих ефектів, вірус може призводити до збоїв комп'ютера через помилки, невраховані тонкощі взаємодії з операційною системою та іншими програмами. Крім того, віруси зазвичай займають деяке місце на накопичувачах інформації та відбирають деякі інші ресурси системи. Тому віруси відносять до шкідливого програмного забезпечення.

В даний час не існує єдиної системи класифікації та іменування вірусів (хоча спробу створити стандарт було здійснено на зустрічі CARO у 1991 році).

Прийнято розділяти віруси:

– по об'єктах, що уражаються (файлові віруси, завантажувальні віруси, скриптові віруси, макровіруси, віруси, що вражають вихідний код програмного забезпечення);

– за враженими операційними системами і платформами (DOS, Microsoft Windows, Unix, Linux, Android, iOS і т.д.);

– за технологіями, що використовуються вірусом (поліморфні віруси, стелс-віруси, руткіти);

– за мовою програмування, якою написаний вірус (асемблер, високорівнева мова програмування, скриптова мова та ін);

– за додатковою шкідливою функціональністю (бекдори, кейлоггери, шпигуни, ботнети та ін).

Антивірусна програма (антивірус) — будь-яка програма для виявлення комп'ютерних вірусів, а також небажаних (вважаються шкідливими) програм взагалі та відновлення заражених (модифікованих) такими програмами файлів, а також для профілактики — запобігання зараженню (модифікації) кодом або операційним кодом.

На даний момент антивірусне програмне забезпечення розробляється в основному для ОС сімейства Windows від компанії Microsoft, що викликано великою кількістю шкідливих програм саме під цю платформу (а це, у свою чергу, викликане великою популярністю цієї ОС, також як і великою кількістю засобів розробки, в тому числі безкоштовних і навіть «інструкцій щодо написання вірусів»). На даний момент на ринок виходять продукти і під інші платформи настільних комп'ютерів, такі як Linux і Mac OS X. Це викликано початком поширення шкідливих програм і під ці платформи, хоча UNIX-подібні системи завжди славилися своєю надійністю.

Крім ОС для настільних комп'ютерів і ноутбуків, також існують платформи і для мобільних пристроїв, такі як Windows Mobile, Symbian, iOS Mobile, BlackBerry, Android, Windows Phone та ін. Деякі розробники антивірусних програм випускають продукти для таких пристроїв.

Класифікувати антивірусні продукти можна відразу за декількома ознаками, такими як:

– технології антивірусного захисту, що використовуються;

– функціонал продуктів;

– цільові платформи.

За технологіями антивірусного захисту поділяють:

– класичні антивірусні продукти (продукти, що застосовують тільки сигнатурний метод детектування);

– продукти проактивного антивірусного захисту (продукти, що застосовують тільки проактивні технології антивірусного захисту);

комбіновані продукти (продукти, що застосовують як класичні, сигнатурні методи захисту, так і проактивні).

За функціоналом продуктів поділяють:

– антивірусні продукти (продукти, що забезпечують лише антивірусний захист);

– комбіновані продукти (продукти, що забезпечують не тільки захист від шкідливих програм, але й фільтрацію спаму, шифрування та резервне копіювання даних та інші функції);

За цільовими платформами бувають:

– антивірусні продукти для операційних систем сімейства Windows;

– антивірусні продукти для операційних систем сімейства *NIX (до цього сімейства відносяться ОС BSD, Linux, Mac OS X та ін.)

– антивірусні продукти для мобільних платформ (Windows Mobile, Symbian, iOS, BlackBerry, Android, Windows Phone та ін.)

Антивірусні продукти для корпоративних користувачів також можна класифікувати за об'єктами захисту:

– антивірусні продукти для захисту робочих станцій;

– антивірусні продукти для захисту файлових та термінальних серверів;

– антивірусні продукти для захисту поштових та Інтернет-шлюзів;

– антивірусні продукти для захисту віртуалізації серверів (в тому числі для data-центрів).

У 2009 році почалося активне поширення так званих лжеантивірусів – програмного забезпечення, яке не є антивірусним, тобто не має реального функціоналу для протидії шкідливим програмам, але видає себе за таке. По суті, лжеантивіруси можуть бути як програмами для обману користувачів та отримання прибутку у вигляді платежів за «лікування системи від вірусів», так і звичайним шкідливим програмним забезпеченням.

Перелік найпоширенішого антивірусного програмного забезпечення:

– антивірус Касперського – продукт для захисту вашого ПК, чия ефективність перевірена мільйонами користувачів у всьому світі. Програма включає основні інструменти для захисту комп'ютерних систем.

– ESET – забезпечує виявлення та блокування вірусів, троянських програм, черв'яків, шпигунських програм, рекламного програмного забезпечення, фішинг-атак, руткітів та інших інтернет-загроз, що становлять небезпеку для компаній та приватних користувачів. Незважаючи на мінімальну потребу в ресурсах, це рішення забезпечує достатній рівень проактивного захисту, практично не знижуючи продуктивність комп'ютера.

– розроблена компанією Symantec, програма Norton AntiVirus є однією з найпопулярніших антивірусних засобів. Ця програма автоматично видаляє віруси, інтернет-хробаків та троянські компоненти, не створюючи перешкод для роботи користувача. Norton AntiVirus дозволяє протистояти загрозам найсучасніших spyware- та adware-програм і блокує роботу таких програм ще до того моменту, як користувач перенаправляється на інший сайт.

– антивірус Dr.Web перевіряє всю оперативну пам'ять навіть зараженого комп'ютера. Доктор Веб проводить повну антивірусну перевірку пам'яті комп'ютера та здатний зупинити вірусний процес. Важливим показником якості роботи антивірусної програми є не лише її здатність знаходити віруси, а й лікувати їх, не просто видаляти інфіковані файли разом із важливою для користувача інформацією, а й повертати їх у початковий "здоровий" стан.

– Avast! Professional Edition увібрав у себе всі високопродуктивні технології для забезпечення однієї мети: надати найвищий рівень захисту від комп'ютерних вірусів. Цей продукт є ідеальним рішенням для робочих станцій на базі Windows. Нова версія ядра антивірусу avast! забезпечує високий рівень виявлення разом з високою ефективністю, що гарантує 100% виявлення вірусів "In-the-Wild" і високий рівень виявлення троянів з мінімальним числом помилкових спрацьовувань. Механізм антивірусного ядра сертифікований ICSA, що постійно бере участь у тестах VirusBulletin і отримує нагороди VB100%.

– BitDefender Antivirus – потужна антивірусна програма з різноманітними можливостями, що дозволяють оптимально захистити персональний комп'ютер. BitDefender Antivirus захищає від комп'ютерних вірусів із застосуванням технологій ICSA Labs, Virus Bulletin, Checkmark, CheckVir та TUV. Модуль B-HAVE наслідує дійсного (віртуального) "комп'ютера в комп'ютері". Ця BitDefender-технологія представляє новий рівень безпеки, виявляючи та знешкоджуючи навіть рідкісні віруси або вірусний код, для якого ще не вийшли нові бази записів вірусів.

– Panda Antivirus є найпростішим та інтуїтивно зрозумілим у використанні рішенням безпеки для домашнього ПК. Після встановлення програми користувач може забути про віруси, програми-шпигуни, руткіти, хакери, онлайн-шахраї і більше не турбуватися про збереження конфіденційної інформації. Panda Antivirus має прості налаштування, легкий і зрозумілий інтерфейс, автоматичне оновлення (після встановлення відразу шукатиме оновлення), здійснює контроль на рівні TCP/IP. Panda Antivirus є досить надійним антивірусом підійде в першу чергу для домашнього користування.

– продукт McAfee VirusScan здійснює сканування файлових серверів та робочих станцій за розкладом та за запитом користувача, здатний виявляти та знешкоджувати віруси-трояни та програми-хробаки. Крім того, системні адміністратори отримують можливість надавати програмам і процесам той чи інший ступінь пріоритетності, відповідно до якого вони скануватимуться антивірусом, що дозволяє економити ресурси корпоративних мереж.

– Avira AntiVir – популярний антивірус німецького розробника. Цю програму завжди відрізняли якість роботи та швидка реакція на появу нових вірусів. Вона включає резидентний монітор, сканер і програму оновлення. AntiVir може постійно стежити за файлами та архівами, які можуть бути потенційними переносниками вірусів. Шукаються також і макроси, які впроваджуються в офісні документи. Програма невибаглива до ресурсів і показує хороші результати у роботі за швидкістю та якістю пошуку.

– Trend Micro Internet Security дозволяє дуже просто захистити ваш комп'ютер, ваші приватні персональні дані та вашу онлайн-активність. Продукт забезпечує захист як від існуючих вірусів, програм-шпигунів та крадіжки даних, так і від майбутніх веб-загроз. Користуйтеся електронною поштою, інтернет-магазинами, онлайн-банкінгом, обмінюйтесь цифровими фотографіями та не турбуйтесь про безпеку вашої приватної інформації.

5 НАВЧАЛЬНО-МЕТОДИЧНЕ ТА ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ НАУКОВО-ДОСЛІДНОЇ ПРАКТИКИ

1. 1. The United Nations E-Government Survey 2018: Gearing E-Government to Support Transformation towards sustainable and resilient societies URL: https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-GovernmentSurvey-2018.

2. Кохан В.П., Єгорова-Луценко Т.П. Стан розвитку електронних адміністративних послуг: огляд впровадження на державному рівні. Право та інноваційне суспільство, 2018, №2 (11) 12 с. URL: http://apir.org.ua/wp-content/uploads/2018/12/Kokhan_Egorova-Lutcenko11.pdf.

3. The United Nations E-Government Survey 2014: E-Government for the Future We Want. URL: https:// publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2014.

4. The United Nations E-Government Survey 2016: E-Government in Support of Sustainable Development. URL: https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2016.

5. Полярна В.Л., Рябець В.В. Європейські практики надання електронних послуг в правоохоронній діяльності та перспективи їх провадження в Україні, 36 с. URL:http://ktpu.kpi.ua/wp-content/uploads/2017/02/Ryabets_ Polyarna_Derzhavne-upravlinnya.pdf.

6. Правове регулювання відносин у мережі Інтернет : монографія /[А. П. Гетьман, Ю. Є. Атаманова, В. С. Мілаш та ін.] ; за ред. С. В. Глібка, К. В. Єфремової. Харків : Право, 2016. 360 с.

7. Про схвалення Концепції розвитку системи електронних послуг в Україні: розпорядженням Кабінету Міністрів України від 16.11.2016 р. № 918-р. Офіційний вісник України. 2016 р. № 99. Стор. 259. Стаття 3234.

8. Про адміністративні послуги: Закон України від 6.09.2012р. № 5203-VI. URL: http://zakon.rada.gov.ua/laws/ show/5203-17.

9. Єдиний державний портал адміністративних послуг. URL: https://poslugy.gov.ua.

10. Про затвердження Примірного положення про центр надання адміністративних послуг: постанова Кабінету міністрів України від 20.02.2013 р. № 118. URL: http://zakon.rada.gov.ua/laws/show/118-2013-%D0%BF.

11. Про Стратегію сталого розвитку «Україна – 2020»: Указ Президента України від 12.01.2015 р. № 5/2015. URL: http://zakon2.rada.gov.ua/laws/show/5/2015.

12. Деякі питання реформування державного управління України»: розпорядження КМУ від 24.06.2016 р. № 474 р. URL: http://zakon.rada.gov.ua/laws/show/474-2016-%D1%80.

13. Про схвалення Концепції розвитку електронного урядування в Україні: Розпорядження КМУ від 20.09.2017 р. № 649-р. URL: http://zakon.rada.gov.ua/laws/show/649-2017-%D1%80.

14. Про електронні документи та електронний документообіг: Закон України від 22.05.2003р. N 851-IV. URL: http://zakon.rada.gov.ua/laws/show/851-15.

15. Про електронні довірчі послуги: Закон України від 5.10.2017 р. № 2155-VIII. URL: http://zakon.rada.gov.ua/ laws/show/2155-19.

16. Веб-ресурс електронних послуг Державної служби України з питань геодезії, картографії та кадастру. URL: https://e.land.gov.ua.

17. Про затвердження Порядку ведення Єдиного державного порталу адміністративних послуг: постанова КМУ від 3.01.2013 р. № 13. URL: http://zakon.rada.gov.ua/laws/show/13-2013-%D0%BF.

18. Про затвердження Положення про Систему BankID Національного банку України: постанова правління Національного банку України 30.08.2016 р. № 378. URL: http://zakon.rada.gov.ua/laws/show/v0378500-16.

19. НБУ розширив можливості системи BankID. URL: https://www.epravda.com.ua/news/2018/10/10/641481/.

20. Glibko S. Problems of legal provision of innovative banking. European political and law discourse. Vol. 3. Issue 3. 2016. 168–173.

21. Електронна система здійснення декларативних процедур у будівництві. URL: https://e-dabi.gov.ua/.

22. Інструкція з отримання електронної послуги. URL: https://e-dabi.gov.ua/images/dabi_instr.pdf.

23. Електронні адміністративні послуги Міністерства екології та природних ресурсів України URL: e-eco.gov.ua.

24. Кабінет електронних сервісів Міністерства юстиції України. URL: https://kap.minjust.gov.ua.

25. Веб-портал «Звернення у сфері державної реєстрації актів цивільного стану». URL: https://dracs.minjust.gov. ua.

26. Електронні сервіси Державної фіскальної служби України. URL: http://sfs.gov.ua/diyalnist-/elektronnyi-servisi.

27. Портал електронних послуг Пенсійного фонду України. URL: https://portal.pfu.gov.ua.

Навчальне видання

КОНСПЕКТ ЛЕКЦІЙ

з курсу «Кібербезпека в аспекті інформатизації та діджиталізації суспільства» для здобувачів вищої освіти, усіх спеціальностей та рівнів підготовки (електронне видання)

Укладач:
Захожай Олег Ігорович

Редактор О.*І. Захожай*
Техн. редактор *О.І. Захожай*
Оригінал - макет *О.І. Захожай*

Підписано до друку _____
Формат $60 \times 84\ 1/16$. Папір типограф. Гарнитура *Times*.
Друк офсетний. Ум. друк. арк.___. Обл.-вид.арк._____.
Тираж ___ прим. Вид. №_____. Замовл. №_____. Ціна договірна.

Видавництво Східноукраїнського національного університету імені Володимира Даля

Свідоцтво про реєстрацію: серія ДК № 1620 від 18.12.03 р.
Адреса університету: вул. Іоанна Павла II, 17,
м. Київ, 01042, Україна
e-mail: vidavnictvoSNU.ua@gmail.com.