

РОЗДІЛ 3.

СОЦІАЛЬНО-ПОЛІТИЧНІ УМОВИ ФОРМУВАННЯ КІБЕРПРОСТОРУ

Логінова Наталія Іванівна

Національний університет «Одеська юридична академія»,
завідувач кафедри інформаційних технологій,
кандидат педагогічних наук, доцент

ІНФОРМАЦІЙНА БЕЗПЕКА В ЕЛЕКТРОННОМУ УРЯДУВАННІ

Електронне урядування є одним з провідних напрямів розвитку інформаційного суспільства сьогодення, що передбачає ефективне використання сучасних інформаційно-комунікаційних технологій та інформаційних ресурсів для забезпечення відкритої взаємодії органів публічної влади та суспільства, надання повного комплексу державних послуг.

Електронне урядування передбачає організацію державної влади за допомогою локальних інформаційних мереж та сегментів глобальної інформаційної мережі інтернет, що дозволяє забезпечити роботу в режимі реального часу, спростити та зробити доступним спілкування громадян з органами державної влади та отримання різних адміністративних послуг [1].

Проблеми інформаційної безпеки електронного урядування в силу специфіки адміністративного процесу управління безпосередньо пов'язані з процесом інформатизації органів державної влади, що здійснюється на основі Концепції розвитку електронного урядування в Україні. Згідно даної Концепції елементами IT-інфраструктури електронного урядування є система електронної взаємодії державних реєстрів, система електронної ідентифікації, електронний кабінет громадянина, вебпортал електронного урядування, спеціальні захищені

мережі передачі даних, захищені центри обробки даних, базові державні реєстри [2].

У зв'язку з цим можна виділити основні загрози та вразливості, які притаманні електронному урядуванню:

- несанкціонований доступ до інформації користувачів та адміністративних інформаційних ресурсів;
- несанкціоноване втручання в програмне забезпечення;
- зараження комп'ютерними вірусами та міжсайтова вразливість адміністративних інформаційних порталів;
- неефективні механізми розмежування доступу до даних користувачів;
- недоступність сервісу або перевищення встановлених законом термінів з надання адміністративних послуг та інше.

Несанкціонований доступ до інформаційних ресурсів сьогодні є найбільш поширеним видом інформаційних загроз. Він полягає в тому, що користувач отримує доступ до об'єкту, на який у нього немає дозволу відповідно до політики безпеки. Для запобігання цій небезпеці в системах електронного урядування необхідно використовувати ідентифікацію та аутентифікацію. Система цифрової ідентифікації громадян є одним з ключових елементів національної програми «Держава в телефоні». Відсутність єдиної системи цифрової ідентифікації в Україні знижує ефективність розвитку електронного урядування.

Втручання в програмне забезпечення пов'язане з несанкціонованим впливом з метою порушення цілісності, конфіденційності та доступності адміністративних інформаційних ресурсів. До них відносяться завантаження підробленої інформації або видалення деяких інформаційних контентів.

Зараження комп'ютерними вірусами відбувається через адміністративні інформаційні портали з метою отримання персональної інформації користувачів, блокування доступу до інформаційних ресурсів, виведення з ладу інформаційних адміністративних порталів.

Адміністративні інформаційні портали часто схильні до атак хакерів та злому. Зламани портали є метою

несанкціонованого отримання персональної інформації користувачів, встановлення шкідливих вірусних програм, шахрайством, проникненням у внутрішню мережу адміністративних установ тощо.

Розмежування доступу сприяє використанню ресурсів інформаційної системи в суворій відповідності до встановлених правил доступу до інформації, в залежності від відповідних ресурсів. Порядок доступу до інформації визначається вимогами, правилами використання, збереження та поширення інформації. IT-інфраструктура інформаційних порталів з надання адміністративних послуг повинна бути доступна не тільки внутрішнім співробітникам (державним службовцям), але й громадянам, які звертаються за певними адміністративними послугами. Відповідно, кількість користувачів, що мають доступ до адміністративної інформації, постійно зростає. Тому одним з основних способів зменшення ризиків витоку інформації є ефективний розподіл повноважень користувачів за допомогою систем управління і контролю доступу.

Недоступність сервісу або перевищення встановлених законом термінів з надання адміністративних послуг пов'язане з перевантаженістю, відсутністю необхідних документів та компетентних співробітників. Для вирішення даної проблеми в листопаді 2020 р. розроблені поправки до Закону України «Про внесення змін до деяких законодавчих актів України щодо оптимізації мережі та функціонування центрів надання адміністративних послуг та удосконалення доступу до адміністративних послуг, які надаються в електронній формі». Зокрема, Закон передбачає моніторинг якості адміністративних послуг, що надаються в електронній формі, спрощення подачі заяв, організація для громадян зворотного зв'язку з пропозиціями та зауваженнями про якість послуг, що надаються на вебпорталах адміністративних органів та інше.

Різноманіття вразливостей і загроз говорить про складність забезпечення інформаційної безпеки електронного урядування. Тому доцільно сформувати умовну концептуальну модель інформаційної безпеки електронного уряду, в

якій треба чітко спланувати розвиток інформаційної безпеки, удосконалити політику безпеки в цій галузі, визначити ризики і загрози інформаційній безпеці, джерела цих загроз, способи та методи їх реалізації. А також удосконалити засоби захисту, що вже існують, і розробити нові, з метою впровадження, експлуатації та розподілу адміністративних інформаційних ресурсів.

Список використаних джерел:

1. Соломко Ю. . Електронне урядування: поняття, сутність, принципи та напрями розвитку. Ефективність державного управління, 2018, ВИП. 2 (55), Ч. 1.
2. Концепція розвитку електронного урядування в Україні: Розпорядження КМУ від 20.09.2017 № 649-р.

Ключові слова: інформаційна безпека, електронне урядування, адміністративні інформаційні ресурси, загрози інформації

Ключевые слова: информационная безопасность, электронное управление, административные информационные ресурсы, угрозы информации

Keywords: information security, e-governance, administrative information resources, information threats

Василенко Микола Дмитрович

Національний університет «Одеська юридична академія»,
в.о. завідувача кафедри кібербезпеки,
доктор фізико-математичних наук, доктор юридичних наук,
професор

Матковська Інга Олексіївна

студентка 4 курсу факультету кібербезпеки
та інформаційних технологій

ДЕЯКІ ПИТАННЯ РИЗИКІВ (ІНФОРМАЦІЙНИХ РИЗИКІВ) В КОНТЕКСТІ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

Відомо, що соціальна інженерія сформувалася в науку і представляє собою вивчення людської поведінки та факторів,