Цимбаленко Яна Юріївна
кандидат наук з державного управління, доцент
декан факультету соціології і права
КПІ ім. Ігоря Сікорського

Гольцова Ірина Борисівна
аспірант кафедри теорії і практики управління
факультету соціології і права
КПІ ім. Ігоря Сікорського

УПРАВЛІНСЬКІ МЕХАНІЗМИ ЗБЕРЕЖЕННЯ ІНФОРМАЦІЇ В УМОВАХ ДИСТАНЦІЙНОЇ РОБОТИ ПРАЦІВНИКІВ ОРГАНІВ ПУБЛІЧНОЇ ВЛАДИ

Цифрова трансформація публічного управління є відображенням новітніх процесів, що відбуваються у суспільстві та державі. Кіберпростір перетворюються з недосяжного розумінню пересічного громадянина віртуального оточення в повсякденний простір для роботи та відпочинку. Саме кіберпростір є однією з можливостей людини для самореалізації та самоствердження. Виходячи з цього виникає питання щодо достовірності інформації про людину або організацію, або орган влади в кіберпросторі. Викривлення інформації в кіберпросторі, що стосується сектору публічного управління, є таким, що наносить шкоду інтересам держави, громади та підриває авторитет управлінців публічної сфери. Наповнення інформаційного простору величезним обсягом інформації, що має викривлену та небезпечну природу, несе для суспільства та держави загрозу та наслідки, що можуть бути непередбачуваними. Дезінформація та фейковість інформації буде мати найбільший вплив на свідомість людей в тому випадку, коли фейкова інформація буде перемішана з абсолютно правдивою інформацією та достовірними фактами.

На сьогодні в умовах світової пандемії постає питання доцільності та якості проведення реінжинірингу процесів публічного управління. Слушною думкою в умовах обмеженого пересування транспортом, в умовах локдауну є перехід на сучасні та надсучасні інструменти дистанційної роботи. Роботу в дистанційному режимі без доступу на робочі місця та доступ до робочих місць за допомогою віддаленого доступу можна розглядати як часткове вирішення проблеми забезпечення діяльності органів публічної влади в умовах пандемії.

Одним з можливих варіантів вирішення проблеми дистанційної роботи працівників органів публічної влади може виступати цифровізація робочих місць та побудова ефективної інформаційно-телекомунікаційної мережі з розгалуженим доступом до сервісів та віддалених робочих місць. У «цифровому» світі робочі місця перестають бути прив'язаними до фізичних місць – вони стають «цифровими», мобільними, тобто такими, що загалом не потребують постійного перебування працівника на робочому місці [5]. Різноманіття обладнання та інструментів, а також неперервний розвиток цифрових технологій значно розширює можливості роботи в умовах дистанційної віддаленості від традиційного робочого місця. Але «…без конкретизації завдань технологічної модернізації такі проєкти, як засвідчує наша досить тривала практика інформатизації та впровадження електронного врядування, можуть призвести до необґрунтованих витрат часу, збільшення кількості ІТ-персоналу, нецільового використання бюджетних коштів… » [4]. Це не є єдиною проблемою яка постає перед управлінцями публічного сектору. Відділений режим роботи для органів публічної влади є таким, що породжує наступну проблему, яка пов'язана з опрацюванням інформації, її обробкою, збереженням та передачею від працівника до працівника, від працівника до керівника та інше.

Обробка інформації, зокрема з обмеженим доступом, а також необхідність роботи з такою інформацією в умовах віддаленого доступу, або пересилання такої інформації за допомогою інформаційно-телекомунікаційних систем є такою, що ставить під загрозу збереження конфіденційної інформації від несанкціонованого доступу до неї неуповноважених осіб. Отримання доступу до інформації інших осіб може мати за мету пропаганду хибних наративів, хуліганські наміри, маніпуляції з масовою свідомістю для створення негативного іміджу держави, громади або окремої посадової особи органу публічної влади, тощо.

Відповідно до чинного законодавства України обов'язковому захисту інформації підлягає: інформація, що є власністю держави, або інформація з обмеженим доступом, вимоги по захисту якої встановлені законом, зокрема, персональні дані громадян.

Таким чином, функціонування публічної влади в умова світової пандемії та впроваджених локдаунів можливо виключно при наявності системи збереження інформації від несанкціонованого проникнення. Такою системою збереження інформації є комплексна система захисту інформації.

Комплексна система захисту інформації повинна включати комплекс організаційних та інженерно-технічних заходів.

Таким чином, перед управлінцями публічного сектору стоїть завдання створення та впровадження в роботу органу публічної влади системи не тільки інженерно-технічних заходів, що потребують значних витрат коштів, але й насамперед побудову системи управлінсько-організаційних заходів, направлених на забезпечення захисту інформації.

З метою збереження інформації в органах публічної влади в умовах сучасних викликів суспільства повинні бути розроблені та впроваджені організаційні заходи збереження інформації, що є основою інформаційної безпеки в публічному управлінні та в органі публічної влади як суб'єкті інформаційної безпеки.

До таких управлінсько-організаційних заходів захисту інформації в органі публічної влади, зокрема, але не виключно, належить:

1. Створення служби інформаційної безпеки або визначення посадової особи, яка буде забезпечувати побудову організаційної системи захисту інформації;

2. Визначення посадових обов'язків працівників допущених до дистанційної роботи за допомогою віддаленого доступу до робочого місця. Це може відбуватися або шляхом внесення змін до вже існуючої посадової інструкції працівника, або розроблення додаткової посадової інструкції, що буде регламентувати права та обов'язки працівника в період дистанційної роботи, або визначення розпорядчим документом органу публічної влади, також прав та обов'язків працівників які працюють з інформацією за допомогою віддаленого доступу до робочого місця. Крім визначення меж прав та обов'язків працівників органу публічної влади повинно бути визначено відповідальність працівника за порушення вимог законодавства щодо роботи з інформацією. Також з визначеними вище документами працівник повинен бути ознайомлений та йому повинно бути роз'яснено про межі відповідальності під особистий підпис.

3. Розпорядчим документом органу публічної влади повинно бути введено в дію:

a. регламенти та правила адміністрування інформаційної системи, порядок обліку, зберігання, розмноження, знищення носіїв інформації.

b. створення системи ідентифікації працівників органу публічної влади - користувачів інформації органу публічної влади;

c. побудована система доступу до інформації, розмежовані «ролі» працівників органу публічної влади залежно від посади та обсягу повноважень;

d. інструкції та послідовності дій в разі виникнення форс-мажорних обставин, розробка оперативних планів реагування на виявлення спроб несанкціонованого доступу до інформаційних ресурсів системи, виходу з ладу засобів захисту, виникнення надзвичайної ситуації, тощо;

4. Розроблення та проведення навчання працівників правилам інформаційної безпеки органу публічної влади.

Також потребує доопрацювання нормативна база з питань документообігу та реорганізація система діловодства та архівного зберігання документів в органі публічної влади.

Висновки: для забезпечення сталого функціонування органів публічної влади в умовах цифровізації та віддаленого доступу до робочих місць необхідно забезпечити документаційне супроводження заходів із збереження інформації.

Список використаних джерел:

1. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах". URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text 10.11.2021

2. Закон України "Про захист персональних даних". URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text 10.11.2021

3. Постанова Кабінету міністрів України №55 від 17.01.2018 «Деякі питання документування управлінської діяльності». URL: https://zakon.rada.gov.ua/laws/show/55-2018-%D0%BF#Text 10.11.2021

4. Шпига П. С. SMART-підхід до визначення завдань цифровізації робочих місць публічних службовців , Національна академія державного управління при Президентові України. URL: http://academy.gov.ua/infpol/pages/dop/2/files/7bb89df3-d121-4aaf-a6de-4792502589d1.pdf. Переглянуто 10.11.2021

5. Лопушинський І. П. «Цифрові робочі місця» державних службовців як вагома складова електронного урядування в Україні. Теорія та практика державного управління і місцевого самоврядування : електрон. наук. фах. вид. Херсон. нац. техн. ун-ту. 2018. № 1. URL: http://el-zbirn-du.at.ua/2018_1/29.pdf . Переглянуто 10.11.2021