УДК 004.056.5

Клим В.Ю., канд. техн. наук, доцент
Жульковська І.І., канд. техн. наук, доцент
Університет митної справи та фінансів, м. Дніпро, v0123klim@gmail.com
Жульковський О.О., канд. техн. наук, доцент
Дніпровський державний технічний університет, olalzh@ukr.net

ПИТАННЯ УПРАВЛІННЯ ДОСТУПОМ В ІНФОРМАЦІЙНИХ СИСТЕМАХ ЕЛЕКТРОННОГО УРЯДУ ПІД ЧАС НАДЗВИЧАЙНИХ СИТУАЦІЙ

На сьогодні організація діяльності органів державної влади розвинутих країн світу неможлива без роботи національних інформаційних систем (ІС) електронних урядів (ЕУ). Метою роботи таких ІС є забезпечення якісного рівня доступу, оперативності та отримання фізичними або юридичними особами державних послуг та інформації про діяльність державних органів. До складових національної інфраструктури ЕУ відносять наступні: Єдиний портал державних та муніципальних послуг; Єдина система міжвідомчої електронної взаємодії; Національна платформа розподіленої обробки даних; Єдина система ідентифікації та аутентифікації в інфраструктурі, яка забезпечує інформаційно-технологічну взаємодію ІС, що застосовують для надання державних послуг в електронній формі; Інформаційна система центрального засвідчувального органу [1, 2]. З лютого 2022 року державні органи України працюють в умовах воєнного стану і тому робота ІС електронного уряду зазнає більшого навантаження разом із підвищенням вимог кібербезпеки.

Управління доступом як механізм контролю, нагляду та спостереження за доступом до інформаційних ресурсів в комп'ютерних системах та мережах набуває пріоритетного значення в умовах надзвичайних ситуацій. Виникнення форс-мажорних обставин зазвичай супроводжується багатьма факторами, які впливають на роботу ІС і до яких відносять наступні: збій енергопостачання, припинення або відсутність мобільного зв'язку, фізичне ушкодження або знищення апаратного обладнання. Наслідки впливу визначених факторів також мають різний масштаб та характер. З боку користувача це відсутність доступу до об'єкту ІС через звичні гаджети – ноутбуки, смартфони, телефони, планшети, збій в роботі встановленого програмного забезпечення, веб-додатків, он-лайн доступу до віддалених баз даних, компонент ІС тощо. Основні проблеми внутрішнього стану ІС складають відновлення працездатності технічного обладнання, програмного забезпечення за мінімальний інтервал часу та перевірка на непошкодженість цілісності та повноти інформаційних ресурсів. Зрозуміло, що робота електронного уряду в умовах надзвичайних ситуацій та воєнного стану на окремих територіях країни особливо важлива для населення, коли порушені певні ланки логістичного сполучення або коли люди вимушені знаходитись поза межами країни. Таким чином, для електронного уряду головною метою у визначених випадках є забезпечення дистанційного постійного захищеного якісного доступу до актуальних державних послуг для більшості верст населення, незалежно від місця знаходження, а також гарантування надійного зберігання національних інформаційних ресурсів, тобто їх цілісності, актуальності, конфіденційності [3, 4, 5].

Одним з основних питань щодо вирішення поставленої задачі постає боротьба із несанкціонованим доступом, як зовнішнім так і внутрішнім, до мережевих ресурсів державних ІС. До прикладів інцидентів зовнішнього несанкціонованого доступу відносять заволодіння сторонніми особами комп'ютерами, ноутбуками, смартфонами, планшетами та (або) вилучення сторонніми особами в усній або електронній формі інформації із логінами та паролями із подальшим використанням для входу до ІС як користувачів. Інцидентами внутрішнього несанкціонованого доступу можна назвати заволодіння сторонніми особами серверами, підключення сторонніми особами до комп'ютерних мереж технічними та

програмними засобами, вилучення сторонніми особами в усній або електронній формі інформації про логіни та паролі адміністратора ІС (комп'ютерної мережі) із подальшим використанням для входу до управління доступом ІС.

Саме через механізми управління доступом визначається рівень авторизації після успішного проходження аутентифікації. Високий ступінь ризику щодо несанкціонованого доступу до конфіденційної інформації суб'єкта під час надзвичайних ситуацій обумовлює встановлення багатофакторного процесу перевірки особистості користувача – аутентифікації [5, 6].

Крім того, для високої вірогідності виникнення форс-мажорних обставин ефективним методом запобігання втрати інформації, як для об'єктів так і для суб'єктів ІС, є застосування резервного копіювання та реплікації інформаційних ресурсів із збільшеним значенням частоти виконання процесу [6, 7, 8]. Це відноситься не тільки до великих обсягів даних, які входять до ІС, наприклад, державні реєстри платників податків, виборців, судових рішень і таке інше, але й до даних про логіни та паролі користувачів. Для фізичних осіб резервне копіювання логінів та паролів можливо виконати не тільки в електронному вигляді, але й на паперовому носії. Для юридичних осіб також роздруківка важливих баз даних та фінансової звітності стане важливим підґрунтям у випадку вирішення спірних питань із контрагентами та податковими органами в умовах форс-мажору та прискорить відновлення діяльності організації в штатному режимі.

Отже, реалізація зазначених вище запобіжних заходів з безпеки інформації підвищує рівень захищеності управління доступом до ресурсів державних ІС, допомагає його скорішому відновленню у робочому режимі, дозволяє суттєво знизити ризики щодо несанкціонованого доступу до конфіденційної інформації суб'єкта та об'єкта, цілісності та повноти інформаційних ресурсів ІС електронного уряду під час надзвичайних ситуацій за мінімальних фінансових витрат.

Список посилань

1. Жекало Г. І., Заяць М.Я., Вакун О. В. Сутність та зміст електронного урядування : концептуальний вимір. Державне управління: удосконалення та розвиток. 2020. №8. [Електронний ресурс]. – Режим доступу: http://www.dy.nayka.com.ua/pdf/8_2020/54.pdf (дата звернення 04.04.2023).

2. Положення про Міністерство цифрової трансформації України, затвердженого постановою Кабінету Міністрів України від 18 вересня 2019 року № 856. [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/856-2019-%D0%BF#n73 (дата звернення 25.03.2023).

3. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України" [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/96/2016 (дата звернення 25.03.2023).

4. Закон України «Про основні засади забезпечення кібербезпеки України» №°2163-VIII від 05.10.2017 р. Голос України. 2017. №208.

5. Клим В.Ю. Електронне голосування: умови проектування та технології створення національної інформаційної системи. / В.Ю. Клим // Технічні науки та технології. – 2022. – №°1(27). – С.°142°–°151. DOI: https://doi.org/10.25140/2411-5363-2022-1(27)-142-151

6. Жованік М.О. Концепція управління та розмежування доступу до інформаційно-технічних ресурсів у сучасній ІТ-інфраструктурі. / М.О. Жованік // Молодий вчений. – 2017. – № 4 (44). – С. 527 – 532.

7. НД ТЗІ 3.6 -004-21 Порядок впровадження системи безпеки інформації в державних органах, на підприємствах, організаціях, в інформаційно-комунікаційних системах яких обробляється інформація, вимога щодо захисту якої встановлена законом та не становить державної таємниці. Київ, 2021.

8. НД ТЗІ 2.3-025-21. Т.2. Методика оцінювання заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем. Київ, 2021.