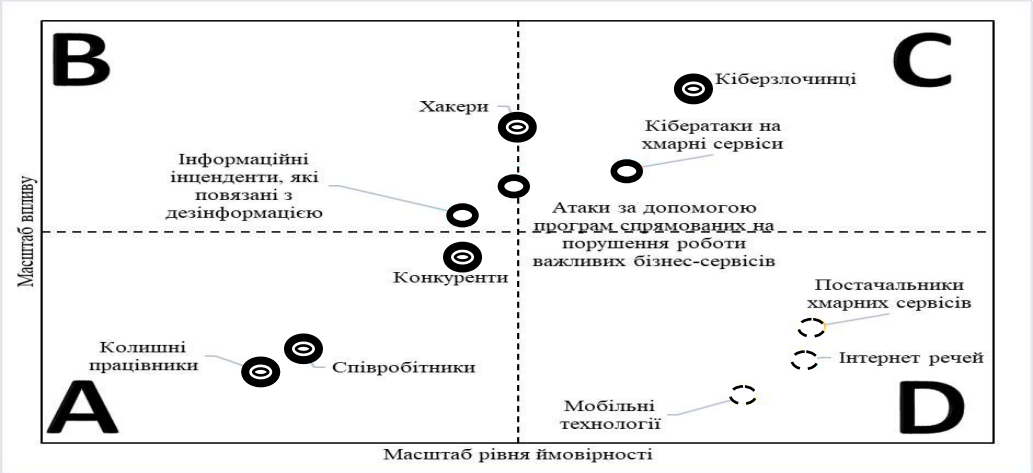

Рис. 1. Карта впливу кіберзагроз на підприємство

Примітка: - потенційні загрози на 2022 р.; - потужні і успішні атаки потенційних загроз; - прогноз інцидентів на 2022 р.

Джерело: розраховано авторами за даними анкетного опитування 217 респондентів 45 підприємств України у грудні 2021 р.

Таким чином, встановлено, що нова ера кібербезпеки вимагає цілком нових підходів до управління підприємством та його ресурсами, зокрема інформаційними. Успіх таких змін значною мірою залежить від того, як гнучко організовані бізнес-процеси на підприємстві, а також як імплементуються нові моделі та методи роботи. Через недоліки в організаційній роботі та невміння управляти змінами підприємства відчувають наслідки кібер-ризиків, а тому вважаємо доречним дотримання кібергігієни за умов COVID-реальності

Список використаних джерел

1. Про рішення РНБО України від 14.05.2021 р. «Про Стратегію кібербезпеки України» від 26.08.2021 р. № 447/2021.: Указ Президента України. URL: https://www.president.gov.ua/documents/4472021-40013

***Букраба О.М.**, аспірант*
Одеський національний економічний університет
aleksandrbukraba@gmail.com

ПРОЕКТ СИСТЕМИ ЕЛЕКТРОННОГО ГОЛОСУВАННЯ НА ОСНОВІ ТЕХНОЛОГІЇ БЛОКЧЕЙН

Україна впевнено тримає курс на цифровізацію. Її мета полягає у тому аби реформувати усі процеси в нашій державі та об’єднати всі відомства в єдину зручну й дієву систему за допомогою інформаційних технологій. Це дозволить органам влади завжди мати актуальні дані для ухвалення ефективних рішень, спростить та зробить прозорим надання державних послуг громадянам та бізнесу, що призведе до зниження рівню корупції. Цифровізація має торкнутися не тільки галузі надання адміністративних послуг та електронного урядування, а й галузей освіти, охорони здоров’я, транспорту, судів, питань демократії тощо. Так, наразі, створений проект Електронна демократія (е-Демократія), який

полягає у запровадженні інструментів цифрової демократії: електронних петицій, опитувань, обговорення проектів нормативно-правових актів та громадського бюджету [1].

Запровадження системи електронного голосування на основі технології блокчейн для проведення виборів державного та місцевого рівнів може стати ключовою складовою проекту е-Демократія та важливим кроком у цифровізації України, оскільки таке рішення має наступні переваги:

1. Ймовірність виникнення помилок та порушень під час голосування та підрахунку голосів зводиться майже до нуля, оскільки усі внутришні процеси автоматизовані.

2. Гарантується цілісність результатів голосування завдяки використанню технології блокчейн та розподіленого збереження даних на пристроях користувачів.

3. Виборці отримають змогу голосувати за допомогою смартфона або комп'ютера з будь-якої точки світу, завдяки чому зросте залученість громадян до виборчого процесу.

4. Згодом буде досягнуте суттєве скорочення витрат на проведення виборів та спрощення процесу їх організації, завдяки скороченню кількості виборчих дільниць.

Основні вимоги до системи електронного голосування полягають у забезпеченні таємниці голосування у відповідності зі статтею 71 Конституції України [2], неможливості голосування під чужим ім'ям, неможливості зміни результатів голосування, здатності системи безвідмовно працювати в умовах високого навантаження, стійкість до DDoS та інших видів атак, можливість голосування за допомогою смартфону чи комп'ютера та інтуітивно-зрозумілий інтерфейс користувача. Також виборець повинен мати змогу перевірити те, що його голос був доданий до бази даних та зберігається там без змін. Вихідний код системи електроного голосування має бути оприлюднений. Це дозволить зробити систему прозорою та збільшіть довіру громадян до неї.

Пропонується інтегрувати клієнтську частину системи електроного голосування з застосунком Дія. Це дозволить використовувати вже реалізовану та перевірену часом функціональність: механізм ідентифікації громадянина та цифровий підпис. Використання існуючих рішень у новій системі дозволить скоротити витрати та час на розробку системи електронного голосування.

Результати голосування мають зберігатися у розподіленій базі даних, реалізованій на основі технології блокчейн. Ця технологія дозволяє зберігати дані у вигляді ланцюжку блоків. Кожен блок складається з заголовку та списку транзакцій. Заголовок блоку містять інформацію, хеш суму попереднього блоку, хеш-суму транзакцій, які увійшли у цей блок, свою хеш суму та час створення блоку. Перший блок в ланцюжку називають первинним блоком і розглядають як окремий випадок, оскільки він не має попереднього блоку [3]. Завдяки такій структурі збереження даних не можливо змінити чи видалити дані у якомусь певному блоці. Потрібно змінювати усі наступні блоки. Для того щоб новий блок був прийнятим іншими користувачами мережі, він має задовольняти певним вимогам, які варіюються у залежності від обраного протоколу консенсусу. Найбільш поширеними протоколами консенсусу є доказ виконання роботи (Proof of Work (PoW)) та доказ долі власності (Proof of Stake (PoS)) [4]. В Україні з 2017 року технологія блокчейн використовується в оновленій системі електронних торгів конфіскованим майном СЕТАМ та в інформаційній системі державного земельного кадастру [5]. Оскільки технологія блокчейн є захищеною за дизайном та відповідає вимогам задачі візантійських генералів [6], то для того щоб змінити результати голосування зловмисники мають виконати атаку 51 відсотка. Така атака може бути проведена шляхом змови більшості виборців, що є майже недосяжною задачею, або завдяки масовому злому облікових записів виборців, який неможливо виконати через високу обчислювальну складність.

Стійкість системи до DDoS атак буде забезпечуватися за рахунок розподіленості системи. Відсутність єдиного центру обробки інформації значно збільшує захищеність системи від DDoS атак.

Збереження таємниці голосування буде забезпечено завдяки використанню двох окремих баз даних: у базі bulletinDB будуть зберігатися аналоги відривних частин бюлетенів підписані ЕЦП виборця, а у базі даних votesDB будуть зберігатися лише голоси виборців та

унікальні хеш суми, за допомогою яких виборець буде мати змогу ідентифікувати свій голос серед інших.

Надійність ЕЦП полягає у високій обчислювальній складності знаходження зворотньої функції до функції шифрування. Складність знаходження зворотньої функції полягає у факторизації великого цілого числа n на прості множники. Загальний метод решета числового поля, який є найшвидшим алгоритмом факторизації на сьогоднішній день, дозволяє виконати розкладання k-бітного цілого числа на множники зі швидкістю, яка обраховується за формулою (1) [7]:

$$\exp((c+o(1))k^{\frac{1}{3}}\log^{\frac{2}{3}}k), \text{ для } c<2. \quad (1)$$

При правильно обраній довжині ключа цифрового підпису ця швидкість є доволі низькою, що не дозволяє зловмисникам масово підробити ЕЦП виборців і таким чином проголосувати від їх ім'ені.

Список використаних джерел

1. Цифрова держава. – Режим доступу: https://plan2.diia.gov.ua/.
2. Конституція України. – Режим доступу: https://www.president.gov.ua/documents/constitution/.
3. Офіціальний сайт Blockchain technology «Advantages & disadvantages of blockchain technology». – Режим доступу: https://blockchaintechnologycom.wordpress.com/2016/11/21/advantages-disadvantages/.
4. Офіціальний сайт Blockchain Labs «What Are Consortium Blockchains?». – Режим доступу: https://www.blockchainlabs.asia/news/what-are-consortium-blockchains/.
5. Офіціальний сайт Міністерства аграрної політики та продовольства України. Державний земельний кадастр перейшов на технологію Blockchain. Режим доступу: http://minagro.gov.ua/node/24722/.
6. Blockchains, Digital Assets, Smart Contracts, Decentralized Autonomous Organizations / Ethereum. Вид. CreateSpace Independent Publishing Platform. – 2016. – 360 с.
7. The Mathematics of Ciphers: Number Theory and RSA Cryptography / S.C. Coutinho. A K Peters/CRC Press; 1 edition. – 1999. – 198 с.

Науковий керівник: Гострик О.М., к.е.н., доцент

Буряк С. Ю., доцент
Український державний університет науки і технологій
ser.buryak@gmail.com
Гололобова О. О., асистент
Український державний університет науки і технологій
Gololobova_Oksana@i.ua

ВИКОРИСТАННЯ ЛІТІЙ-ІОННИХ АКУМУЛЯТОРІВ НА ЗАЛІЗНИЦІ

Акумуляторні батареї використовуються на рухомому складі протягом багатьох десятиліть, проте донедавна вони служили головним чином для живлення допоміжних споживачів або як резервне джерело енергії, призначеного для забезпечення переміщення поїзда на невеликі відстані у разі перебоїв у подачі електроенергії. На сьогодні тягові акумуляторні батареї стають реальною альтернативою електрифікації та дизельному паливу. Поряд із біопаливом та воднем, перспективною альтернативою традиційному дизелю у потягах є акумульована електроенергія. В даний час у світі успішно експлуатується велика кількість моделей гібридних тепловозів та електровозів, а провідні машинобудівні компанії активно проводять розробки повністю рухомого акумуляторного складу. Залежно від того, які параметри акумулятора є найбільш важливими в конкретній техніці, для неї буде оптимальним застосування цілком певного різновиду літій-іонного акумулятора. Більше