Дяків Назар Валерійович
здобувач наукового ступеня доктор філософії
Вінницького державного педагогічного університету
імені Михайла Коцюбинського

Дякова Людмила Валеріївна
здобувачка ступеня вищої освіти магістр
Вінницького державного педагогічного університету
імені Михайла Коцюбинського

КІБЕРБЕЗПЕКА ДЕРЖАВНОГО СЕКТОРУ: ЗАХИСТ АДМІНІСТРАТИВНИХ ПРОЦЕСІВ В УМОВАХ ВІЙНИ

Повномасштабна війна, розв'язана Російською Федерацією проти України, супроводжується безперервним тиском не лише на фронті, а й у цифровому середовищі. Кіберпростір став ареною, де ведеться не менш запекла боротьба. Зокрема, об'єктами атак дедалі частіше стають цифрові сервіси держави, серед яких особливу вразливість мають державні реєстри. Саме ці системи забезпечують доступ до ключових адміністративних послуг — від реєстрації бізнесу до фіксації народження чи смерті. Їх порушення або знищення може паралізувати значну частину державних функцій. Цей аналіз спрямований на вивчення характеру кіберзагроз для реєстрів у період 2024–2025 років, оцінку наслідків конкретних атак, а також виявлення основних напрямів захисту [1].

За період війни обсяг кібератак, спрямованих на українські державні органи, значно зріс. Лише у 2023 році, згідно з даними Держспецзв'язку, було зафіксовано понад тисячу кіберінцидентів, що на третину більше, ніж у попередньому році [2]. Сотні спроб вторгнення до державних інформаційних систем щотижня блокуються фахівцями з кіберзахисту. У центрі уваги — спроби отримати несанкціонований доступ до чутливої інформації, дестабілізувати роботу держорганів, а також викрасти розвіддані, зокрема щодо військової інфраструктури.

Переважна більшість атак приписується спецслужбам РФ, проте фіксуються й операції з боку інших країн. Наприклад, один із найбільш резонансних випадків у 2023 році стосувався діяльності хакерів із Китаю, які зуміли проникнути в урядові IT-системи. Серед найчастіше вживаних методів — розсилка шкідливих програм (вайперів, троянів), викрадення паролів через фішинг, атакування через уразливості програмного забезпечення, а також масовані DDoS-атаки. З'являється й новий тип загроз — атаки з використанням мобільних шкідників та автоматизованих систем збору доступів. [3]

Попри широке коло цілей, державні реєстри особливо привабливі для зловмисників. Це пояснюється їхньою критичною роллю у функціонуванні держави: реєстр юридичних осіб, база нерухомого майна, записи актів цивільного стану — всі ці системи формують основу електронного

управління [4]. Злам однієї з них здатен не лише зупинити окремі послуги, а й спричинити правовий хаос.

Найгучнішим епізодом останнього часу стала атака 19 грудня 2024 року. За офіційною інформацією Міністерства юстиції, ціллю хакерів стали інформаційні ресурси ДП «НАІС» та сам Мін'юст. Фахівці одразу пов'язали атаку з діяльністю спецслужб Росії, зважаючи на її складність і масштаби. Внаслідок втручання було припинено роботу всіх основних державних реєстрів, включно з реєстром нерухомості, ЄДРПОУ, реєстром актів цивільного стану тощо. [5]

Платформа «Дія» та низка онлайн-сервісів оголосили про тимчасову недоступність частини функцій. Відновлення реєстрів відбувалося поступово: перші сервіси були підключені лише через два тижні після інциденту, а повноцінна стабілізація — наприкінці січня 2025 року. Упродовж усього цього періоду користувачі державних послуг стикались із труднощами, зокрема неможливістю зареєструвати бізнес, оформити спадщину або провести правочини через нотаріуса. [6]

Інший тривожний інцидент стався вже у січні 2025 року, коли CERT-UA виявила скоординовану спробу компрометації нотаріусів. Хакерська група, ймовірно пов'язана з тією ж атакою грудня, розсилала листи із шкідливим ПЗ, замасковані під офіційну кореспонденцію Мін'юсту. Ціллю було отримання доступу до систем державної реєстрації через легітимні облікові записи. Використовуючи інструмент віддаленого управління DarkCrystal RAT, зловмисники отримували контроль над пристроями нотаріусів, що могло дозволити зміну даних у реєстрах. [7]

Попри складність цієї атаки, фахівцям вдалося запобігти найгіршому сценарію — виявити зараження та локалізувати загрозу до того, як відбулися зміни в системах. Цей випадок підкреслює новий тип ризику — атаки через «довірених» користувачів зсередини системи, де технічні засоби захисту працюють не завжди ефективно.

Висновок: сукупність наведених прикладів підтверджує, що державні реєстри залишаються однією з найвразливіших мішеней у кіберпросторі. Їхній захист – не лише технічна, а й політична задача. З кожним інцидентом зростає розуміння того, що критична інфраструктура в цифровому вимірі — не менш важлива, ніж електростанції чи транспорт.

Список використаних джерел

1. Державна служба спеціального зв'язку та захисту інформації України. Про діяльність у сфері кіберзахисту у 2023 році. URL: https://cip.gov.ua/news/u-2023-roci-na-obiekti-kritichnoyi-infrastrukturi-ukrayini-zdijsneno-majze-1700-kiberatak—derzspzvyazku

2. Міністерство юстиції України. Повідомлення про кібератаку на державні реєстри 19 грудня 2024 року. URL: https://minjust.gov.ua/news/main/reestri-buli-prizupineni-cherez-kiberataku

3. CERT-UA. Звіт про фішингову кампанію UAC-0173 проти українських нотаріусів. URL: https://cert.gov.ua/article/4847523

4. Служба безпеки України. Про розслідування кібератак проти державних ресурсів. URL: https://ssu.gov.ua/novyny
5. Microsoft Digital Defense Report 2023. URL: https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report
6. National Cyber Security Coordination Centre при РНБО України. Про співпрацю з ENISA. URL: https://www.rnbo.gov.ua/ua/NKCK.html
7. NATO CCDCOE. Ukraine on the path to joining the NATO cyber defence centre. URL: https://ccdcoe.org/news/2023/ukraine-to-join-nato-

Ємець Ольга Іванівна,
кандидат економічних наук,
доцент кафедри підприємництва, торгівлі та прикладної економіки
Прикарпатського національного університету імені Василя Стефаника

Бойчук Іванна Володимирівна
студентка ОПП "Підприємство, торгівля та біржова діяльність"
Прикарпатського національного університету ім. Василя Стефаника
м. Івано-Франківськ, Україна

ВПЛИВ ДОБРОЧЕСНОСТІ ТА КОМПЛАЄНС-МЕНЕДЖМЕНТУ НА ЕФЕКТИВНІСТЬ БІЗНЕСУ В УМОВАХ КРИЗИ

В умовах сучасної нестабільності, зумовленої економічними, політичними та громадськими кризами, бізнес має адаптувати свої стратегії для збереження конкурентоздатності та лояльності зацікавлених сторін. Одним з ключових факторів, які допомагають компаніям долати труднощі, є дотримання етичних норм та ефективне впровадження комплаєнс-менеджменту. Ці аспекти забезпечують стабільність, знижують ризики та сприяють довготерміновому розвитку підприємств.

Доброчесність є не лише етичним стандартом, але й потужним інструментом, що сприяє побудові стійкої корпоративної культури. Підприємства, які послідовно дотримуються принципів відкритості, чесності та відповідальності, мають значно вищі шанси на подолання кризових ситуацій. Відсутність корупційних схем, прозорість ведення бізнесу та справедливе ставлення до партнерів і співробітників допомагають уникнути репутаційних ризиків і правових санкцій [1].

Комплаєнс-менеджмент є надзвичайно важливим як система внутрішнього контролю, що має на меті зменшити ризики недотримання вимог законодавства та корпоративних правил. Особливе значення він має в періоди криз, коли існує велика потреба в ефективному контролі фінансових операцій, ретельній перевірці партнерів і якісній оцінці ризиків. Варто зазначити, що цьому сприяє використання аналітичного інструменту YouControl [3].