УДК 004.7.056.5

Дмитро Володимирович Швець,
кандидат педагогічних наук, доцент, ректор Харківського національного університету внутрішніх справ

Механізми забезпечення кібербезпеки в інформаційному просторі

Для забезпечення національних інтересів та їх захисту на міжнародному рівні виняткового значення набуває обґрунтування ефективних механізмів забезпечення кібербезпеки держави. В Україні ці механізми все ще знаходяться на етапі становлення. Деякі з них потребують удосконалення, а окремим елементам більшості з них не вистачає концептуального обґрунтування.

Актуальність зазначеної теми зумовлена необхідністю подолання суперечностей між стрімким зростанням важливості кібербезпекової проблематики та частковою готовністю України відповісти на новітні кібербезпекові виклики, а також нагальною потребою визначення ключових стратегічних проблем і шляхів їх вирішення для розбудови ефективних механізмів забезпечення кібербезпеки України.

Кібербезпека – це захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі [1].

Одним із пріоритетних напрямків інформатизації українського суспільства є впровадження електронного управління. Механізми забезпечення кібербезпеки в інформаційному просторі є технологічною основою застосування електронного управління, вони є захистом доступу осіб, підприємств, установ та організацій до електронних послуг в інформаційному просторі.

Взаємодія між компонентами будь-якої системи, описується, насамперед, поняттям доступу суб'єктів до об'єктів. Суб'єктом може бути користувач або процес (задача, трансакція, запущена програма або сервіс), а об'єктом – логічний або фізичний ресурс системи (файл, набір

даних, програма, сервіс, база даних, канал передачі даних тощо). Базовою характеристикою доступу є те, що в результаті його створюється потік інформації від об'єкта до суб'єкта шляхом виконання таких операцій, як читання, запис, модифікація, пошук тощо.

Управління доступом є ключовим механізмом забезпечення кібербезпеки в інформаційному просторі. Механізми управління доступом можуть бути класифіковані: за рівнями реалізації механізмів безпеки та за етапами роботи і компонентами.

За рівнями реалізації виділяють три категорії механізмів кібербезпеки: адміністративно-правові, програмно-технічні та фізичного захисту.

Механізми кібербезпеки за етапами роботи і компонентами, які реалізують підсистему управління доступом, поділяють на механізми ідентифікації, автентифікації, авторизації та моніторингу.

На етапі ідентифікації визначаються та перевіряються ідентифікатори суб'єкта й об'єкта системи. При автентифікації перевіряється достовірність суб'єкта – чи дійсно він той, за кого себе видає. Якщо суб'єкт автентифікований і має відповідні права на об'єкт, він буде авторизований, тобто йому буде надано доступ до запрошеного ним об'єкта. Моніторинг передбачає протоколювання йаналіз подій безпеки.

Під час опису систем управління доступом, як правило, відзначають базові властивості системи інформаційної кібербезпеки: конфіденційність, цілісність, доступність, підзвітність. Підзвітність характеризує те, що всі події та дії суб'єкта в системі інформаційної безпеки ідентифікуються, реєструються й можуть бути перевірені. Властивість підзвітності в системі реалізується чотирма методами: ідентифікацією, автентифікацією, авторизацією і аудитом.

Серед нормативно-правових актів Європейського Союзу, які визначають основні засади законодавства у сфері електронної ідентифікації слід відзначити регламент ЄС № 910/2014 Європейського Парламенту та Ради Європи «Про електронну ідентифікацію та довірчі послуги для електронних трансакцій на внутрішньому ринку» [2]. Цей регламент спрямований на підвищення рівня безпеки електронних трансакцій на внутрішньому ринку шляхом надання загальної основи для безпечної та цілісної електронної взаємодії між підприємствами, громадянами і державними органами, тим самим підвищуючи ефективність державних і приватних онлайн-послуг, електронного бізнесу й електронної торгівлі в ЄС. Він робить вагомий внесок у побудову єдиного цифро-

вого ринку шляхом створення умов для взаємного крос-кордонного визнання ключових компонентів, таких як електронна ідентифікація, електронні документи, електронні підписи та електронні послуги, а також для сумісності послуг електронного управління на території ЄС.

Згідно з європейським регламентом засоби електронної ідентифікації в контексті схеми електронної ідентифікації позділяються на три рівні безпеки (гарантії) та відповідні засоби їх забезпечення: обмежений (низький), суттєвий, вищий (високий).

Кожен рівень гарантії повинен належити до засобів електронної ідентифікації в контексті схеми електронної ідентифікації, які забезпечують відповідний ступінь безпеки до ідентичності особи, про яку заявляється або стверджується, і характеризуються відповідними технічними специфікаціями, стандартами та процедурами, пов'язаними з ними, в тому числі з технічними засобами контролю, метою яких є зниження ризику зловживання або підміни ідентичності.

При цьому встановлено мінімальні технічні характеристики, стандарти та процедури стосовно низького, суттєвого та високого рівнів гарантії, які повинні бути застосовані для засобів електронної ідентифікації.

Аналіз загального стану впровадження інфраструктури електронної ідентифікації в державах – членах ЄС свідчить про неоднорідність прийнятих у різних країнах політик у цій сфері, використання різних технологій ідентифікації та автентифікації, які відповідають різним рівням довіри електронної ідентифікації.

Архітектура інфраструктури електронної ідентифікації має передбачати можливість використання декількох інструментів електронної ідентифікації. Це буде сприяти поширенню послуг на базі електронної ідентифікації серед громадян.

Упровадження електронної ідентифікації в Україні призвело до ситуації, коли в інформаційних системах різного призначення та масштабу часто використовуються засоби електронної ідентифікації користувачів без урахування таких основних принципів, як кібербезпека, захист персональних даних, достовірність ідентифікації, інтероперабельність і комфортність використання [3].

Таким чином, відсутність єдиної нормативної та технічної політики використання і захисту ідентифікаційних даних користувачів, загальних процедур і алгоритмів автентифікації та захисту інформації в системах, забезпечення їх інтероперабельності й ефективної взаємодії

інформаційних систем стає стримуючим чинником для ефективного забезпечення кібербезпеки в Україні.

Список бібліографічних посилань

1. Про основні засади забезпечення кібербезпеки України : закон України від 05.10.2017 № 2163-VIII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 30.10.2019).
2. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014. URL: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG (дата звернення: 30.10.2019).
3. Національна стратегія електронної ідентифікації України. Біла книга з електронного урядування / під ред. О. Потія та Ю. Козлова. 145 с. URL: https://cdn.regulation.gov.ua/8d/f3/4c/32/regulation.gov.ua_File_196.pdf (дата звернення: 30.10.2019).

Одержано 01.11.2019