УДК 004[681.518]
Петро Сергійович КЛІМУШИН,
кандидат технічних наук, доцент,
доцент кафедри інформаційних технологій факультету № 4
Харківського національного університету внутрішніх справ
ORCID: https://orcid.org/0000-0002-1020-9399

МЕХАНІЗМИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ В ІНФОРМАЦІЙНОМУ ПРОСТОРІ

Взаємодія між компонентами будь-якої системи характеризується передусім поняттям доступу суб'єктів до об'єктів. Суб'єктом може виступати користувач або процес (завдання, трансакція, запущена програма або сервіс), а об'єктом – логічний або фізичний ресурс системи, такої як файл, набір даних, програма, сервіс, база даних, канал передавання даних тощо. Базовою характеристикою доступу є те, що в результаті його створюється потік інформації від об'єкта до суб'єкта, шляхом виконання операцій, таких як читання, запис, модифікація, пошук та ін.

Управління доступом є ключовим механізмом безпеки в інформаційному просторі. Механізми управління доступом можуть бути класифіковані [2] за рівнями реалізації механізмів безпеки, механізми безпеки – за етапами роботи і компонентами.

За рівнями реалізації виділяють три категорії механізмів безпеки:

– *адміністративні механізми* включають політики, плани, процедури, заходи, що визначені політикою безпеки організації;

– *технічні механізми безпеки* – програмні або апаратні засоби, підсистеми і сервіси інформаційної безпеки;

– *механізми фізичного захисту* – фізичні бар'єри, екрани і засоби контролю доступу.

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

На етапі ідентифікації визначаються і перевіряються ідентифікатори суб'єкта й об'єкта системи. При автентифікації перевіряється достовірність суб'єкта, чи дійсно він той, за якого себе видає. Якщо суб'єкт автентифікований і має відповідні права на об'єкт, він буде авторизований, тобто йому надається доступ до запрошеного ним об'єкта. Моніторинг передбачає протоколювання й аналіз подій безпеки [1].

Описуючи системи управління доступом, виділяють базові властивості системи інформаційної безпеки: конфіденційність, цілісність, доступність та підзвітність. Властивість підзвітності характеризує те, що всі події та дії суб'єкта в системі інформаційної безпеки ідентифікуються, реєструються і можуть бути перевірені. Властивість підзвітності в системі реалізується чотирма механізмами: ідентифікацією, автентифікацією, авторизацією і аудитом.

Серед нормативно-правових актів ЄС, які визначають основні засади законодавства у сфері електронної (е-) ідентифікації, перш за все слід назвати регламент ЄС № 910/2014 Європейського парламенту та Ради "Про електронну ідентифікацію та довірчі послуги для електронних трансакцій на внутрішньому ринку". Цей регламент спрямовано на підвищення рівня безпеки е-трансакцій на внутрішньому ринку шляхом надання загальної основи для безпечної та цілісної е-взаємодії між підприємствами, громадянами і державними органами, тим самим підвищуючи ефективність державних і приватних онлайн-послуг, е-бізнесу та е-торгівлі в ЄС.

Зазначений регламент робить вагомий внесок у побудову єдиного цифрового ринку шляхом створення умов для взаємного кроскордонного визнання ключових компонентів, таких як е-ідентифікація, е-документи, е-підписи та е-послуги, а також для сумісності послуг е-урядування на території ЄС.

Також важливим правовим аспектом, визначеним регламентом, є те, що держави-члени залишають за собою право використовувати та вводити в дію ті або інші засоби е-ідентифікації для доступу до онлайн-послуг, приймати рішення, чи слід залучати приватний сектор до надання таких засобів, мати вибір, чи повідомити про всі, деякі або не повідомляти про жодну зі схем е-ідентифікації, що використовуються на національному рівні для доступу до громадських онлайн-послуг або особливих послуг.

До окремого значущого розділу вимог регламенту слід віднести визначення того, що рівні гарантій е-ідентифікації повинні характеризувати ступінь безпеки засобу е-ідентифікації під час встановлення ідентичності людини, забезпечуючи тим самим гарантію того, що особа, яка потребує ідентифікації, насправді є людиною, для якої було встановлено дану ідентичність. Встановлюється, що

рівень гарантії залежить від ступеня впевненості в тому, що засіб е-ідентифікації забезпечує підтвердження заявленої ідентичності або ствердження про ідентичність людини з урахуванням процесів (наприклад, підтвердження і перевірка справжності особи, автентифікація), діяльності з управління (наприклад, організацією, що надає засоби е-ідентифікації, процедурами надання таких засобів), а також упровадженого технічного контролю.

Відповідно до європейського регламенту засоби е-ідентифікації в контексті схеми е-ідентифікації поділяють за трьома рівнями безпеки (гарантіями) та відповідними механізмами їхнього забезпечення: *обмежений* (низький), *суттєвий*, *вищий* (високий).

Кожний рівень гарантії повинен відноситись до засобів е-ідентифікації в контексті схеми е-ідентифікації, які забезпечують відповідний ступінь безпеки щодо ідентичності особи, про яку заявляється або стверджується, та які характеризуються відповідними технічними специфікаціями, стандартами та процедурами, пов'язаними з ними, у т. ч. 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 до засобів е-ідентифікації.

Одним із найважливіших аспектів міжнародної та європейської нормативної бази сфери е-ідентифікації слід назвати підхід до визначення архітектури управління послугами е-ідентифікації, функціональних вимог до обміну інформацією та захисту інформації в інфраструктурі е-ідентифікації.

Окремо варто наголосити, що на рівні міжнародних стандартів та рекомендацій чітко визначено коло суб'єктів, залучених до інфраструктури е-ідентифікації, описано їхні діяльність та роль.

Аналіз загального стану упровадження інфраструктури е-ідентифікації в державах – членах ЄС свідчить про неоднорідність прийнятих у країнах політик у цій сфері, використання різних технологій ідентифікації та автентифікації відповідно до різних рівнів довіри е-ідентифікації. Їх можна згрупувати в такі основні концептуальні підходи [3]:

1. Максимально спрощених механізмів ідентифікації та автентифікації для кінцевого користувача в інформаційних системах на основі використання пари "логін – пароль".

2. Більш надійні механізми автентифікації у системах надання онлайн-сервісів на основі одноразових паролів із варіаціями генерування їх за допомогою списків, надсилання коротких текстових повідомлень та спеціальних програмно-апаратних генераторів паролів.

3. Найбільш надійні механізми автентифікації в системах надання онлайн-сервісів на основі використання криптографічних перетворень, тобто найбільш надійних механізмах довіри з використанням електронних цифрових підписів (ЕЦП). Такі механізми ґрунтуються на застосуванні та розвитку інфраструктури довіри, що базується на інфраструктурі відкритих ключів (Public Key Infrastructure – PKI), та використовують різновиди програмної та апаратної реалізації засобів е-ідентифікації. Апаратні засоби реалізовано у варіантах засобів кваліфікованого е-підпису та старт-карток. Також використовуються засоби е-ідентифікації на основі SIM-карток для послуг мобільної ідентифікації (mobileID).

Архітектура інфраструктури е-ідентифікації має передбачати можливість використання декількох механізмів е-ідентифікації. Це сприятиме поширенню послуг на базі е-ідентифікації серед громадян. У багатьох європейських країнах паралельно доступні декілька механізмів е-ідентифікації.

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

Таким чином, відсутність єдиної нормативної та технічної політики використання та захисту ідентифікаційних даних користувачів, загальних процедур та алгоритмів автентифікації та захисту інформації в системах, механізмів забезпечення інтероперабельності та ефективної взаємодії інформаційних систем стає чинником, що стримує розвиток систем надання онлайн-послуг і не сприяє зміцненню довіри громадян до таких послуг та до цифрових технологій взагалі. Необхідність подолання таких перешкод вимагає зваженого комплексного підходу до створення в Україні єдиної інфраструктури е-ідентифікації, інтегрованої до систем е-урядування.

Список бібліографічних посилань

1. Клімушин П. С. Стратегії та механізми електронного урядування в інформаційному суспільстві: монографія. Харків: Вид-во ХарРІ НАДУ «Магістр», 2016. 524с.

2. Марков А. С.. Цирлов В. Л. Безопасность доступа: подготовка к CISSP. *Вопросы кибербезопасности*. 2015. Вып. 2 (10). С. 60–68.

3. Національна стратегія електронної ідентифікації України. Біла книга з електронного урядування / під редакцією О. Потія та Ю. Козлова. URL : https://cdn.regulation.gov.ua/8d/f3/4c/32/regulation.gov.ua_File_196.pdf.

Одержано _____.2018