ЗАСІБ МОНІТОРИНГУ ВИТОКУ ЕЛЕКТРОННИХ ДОКУМЕНТІВ

Главчев М.І., Главчева Ю.М., Філоненко А.М.
Національний технічний університет "Харківський політехнічний інститут", м. Харків

У сучасному світі цифрових технологій питання безпеки інформації є надзвичайно актуальним. Збільшення обсягів електронних документів, що циркулюють у межах організацій, призводить до зростання ризиків їхнього несанкціонованого доступу, копіювання або передачі. Сучасна комп'ютерна злочинність включає не лише класичні форми зловмисних дій у кіберпросторі, а й нові типи загроз, спричинені активним проникненням цифрових технологій у бізнес, науку, освіту та державне управління.

Законодавча база у сфері інформаційної безпеки не завжди встигає за стрімким розвитком технологій. У зв'язку з цим на перший план виходять технічні засоби, що здатні забезпечити ефективний захист конфіденційної інформації, незалежно від правового супроводу. Одним із важливих напрямів є розробка засобів, що дозволяють виявляти факти витоку документів шляхом безперервного моніторингу активності користувачів.

Метою даного дослідження є створення ефективного засобу для виявлення витоків електронних документів шляхом запровадження системи контролю доступу до них. Об'єктом дослідження виступає система контролю за дотриманням політики безпеки у роботі з документами, а предметом – механізми моніторингу, реалізовані з використанням файлів-агентів.

Розроблений програмний засіб базується на ідеї вбудованих агентів у електронні документи, які фіксують усі дії користувача: відкриття, копіювання, пересилання, друк тощо. Ці агенти здатні передавати сигнали на сервер моніторингу, що дозволяє в режимі реального часу аналізувати потенційно небезпечні дії. Система підтримує ведення журналу подій, створення звітів, а також реалізацію механізмів попередження при виявленні підозрілої активності.

У процесі дослідження було проаналізовано існуючі технології виявлення витоків даних, виявлено їхні переваги та обмеження, запропоновано архітектуру власного рішення, що не потребує глибокої інтеграції у наявну інфраструктуру підприємства.

Практичне значення розробки полягає у створенні адаптивного засобу моніторингу, що може бути застосований у корпоративних середовищах для захисту критично важливої інформації. Система дозволяє своєчасно виявляти спроби порушення політики доступу до документів, що є важливою складовою комплексної стратегії кіберзахисту організації.

Література:

1. Главчев М. І., Баленко О. І. Формування програмного комплексу захисту комерційного програмного забезпечення персонального використання //Системи управління, навігації та зв'язку. – 2016. – №. 4. – С. 63-66.