УДК 004.056

Юрій Володимирович БОРСУКОВСЬКИЙ,
кандидат технічних наук,
професор кафедри інформаційної та кібернетичної безпеки
факультету інформаційних технологій та управління
Київського університету ім. Бориса Грінченка;
ORCID: https://orcid.org/0000-0003-1973-2386

МОДЕЛЬ ЗАХИСТУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ ВІД ІНСАЙДЕРСЬКИХ АТАК

Поява і формування інформаційного та кібернетичного просторів сприяло активному впровадженню нових інформаційних технологій в питаннях виявлення, попередження і розслідування кіберзлочинів та злочинів у сфері торгівлі людьми.

З однієї сторони, активні операції в інформаційному і кіберпросторі вимагають переосмислення підходів до захисту конфіденційної інформації від її компрометації і втрат, а з іншої сторони все частіше реєструються випадки інсайдерських атак на таку інформацію всередині об'єктів критично-важливої інфраструктури і правоохоронних органів, що займаються виявленням, попередженням і розслідуванням кіберзлочинів та злочинів у сфері торгівлі людьми.

Одним із напрямків протидії компрометації та втратам конфіденційної інформації може бути створення типової моделі захисту, що дозволить забезпечити організацію заданого рівня безпеки конфіденційної інформації, шляхом створення додаткового рівня криптографічного захисту на локальних та мережних інформаційних ресурсах, а також в ході обміну такою інформацією по каналам зв'язку [1, 2].

Із врахуванням чинного ландшафту інформаційних та кібернетичних загроз, таку модель захисту конфіденційної інформації сьогодні доцільно використовувати для роботи із усіма конфіденційними даними, що стосуються об'єктів критично-важливої інфраструктури і правоохоронних органів, що займаються виявленням, попередженням і розслідуванням кіберзлочинів та злочинів у сфері торгівлі людьми [8].

Зважаючи на вищевказані передумови та те, що модель захисту конфіденційної інформації може також враховувати окремі вимоги служби інформаційної та кібернетичної безпеки, що потребує додаткової формалізації, наведемо у якості прикладу, модель захисту аутентифікаційних даних для доступу до конфіденційної інформації користувача. Мінімальні вимоги до захисту та безпеки конфіденційної інформації можна сформулювати наступним чином:

1. Необхідно забезпечити ефективний захист конфіденційної інформації від несанкціонованого доступу.

2. Повинен бути зручний і оперативний доступ до конфіденційної інформації.

3. Всі аутентифікаційні дані для доступу до конфіденційної інформації (логіни, паролі, URL і т.п.) повинні зберігатися в захищеній базі даних.

4. Всі аутентифікаційні дані для доступу до конфіденційної інформації повинні зберігатися в зашифрованому вигляді, база даних повинна повністю шифруватися.

5. Для зручного доступу до бази аутентифікаційних даних повинен використовуватися майстер-пароль і додаткові апаратні та програмні засоби захисту.

6. Як додатковий елемент захисту, база даних повинна розміщуватися в середовищі, захищеному апаратними та програмними засобами.

7. Вартість рішення повинна бути відносно невисокою.

Це, безумовно, спрощені вимоги до формування моделі захисту конфіденційної інформації і ми також повинні при формалізації моделі враховувати перший закон безпеки "Якщо ви запустили на своєму комп'ютері програму зловмисника, це більше не ваш комп'ютер" [3]. Це вимагає включати в опис моделі додаткові засоби захисту для створення безпекових бар'єрів у випадку здійснення інформаційних, кібернетичних або інсайдерських атак на інформаційні ресурси.

В загальному вигляді модель можна представити таким чином:

$$M_A(CC, FC, MC, SN, GS) = CC(PW_{CC,} C_{KC}, P_{KC}) + FC(PW_{FC}, CP_{AES256}) + MC(PW_{MC}, C_{MC}, P_{MC}) + SN(PW_{SN}, C_{KC}, C_{MC}) + GS(C_{MC})$$

де:

CC – криптографічний контейнер;

FC – USB-флеш диск з апаратним криптографічним захистом;

MC – криптографічний сертифікат;

SN – електронний ключ eToken;

GS – сервіс синхронізації даних;

PWxx – пароль сервісу;

Cxx – секретний ключ сервісу;

Pxx – публічний ключ сервісу;

CP_{AES256} – інтегрований апаратний криптографічний чіп AES256.

Наведемо один з варіантів практичної реалізації представленої моделі. В якості вирішення ми будемо використовувати Open Source менеджер паролів KeePass [4] і USB-флешку з апаратним шифруванням і вбудованим антивірусним захистом Safexs Protector XT [5]. Це працююче рішення, досить гнучке, зручне і перевірене багаторічним використанням в корпоративному секторі і в особистому застосуванні.

KeePass Password Safe - дозволяє зберігати всі паролі користувача, використовуючи один головний майстер-пароль. Додаток підтримує

алгоритми шифрування Advanced Encryption Standard (AES 256-біт, Rijndael і Twofish). Є портативна версія, яку не потрібно встановлювати і можна зберігати на USB-носії, що дозволяє забезпечувати мобільність для нашого рішення. Крім того, є відкритий код програми для його аналізу. KeePass також підтримує експорт бази паролів в різні формати TXT, HTML, PDF і т.п., а також імпорт з різних форматів.

Для додаткового захисту бази конфіденційної інформації користувача KeePass дозволяє використовувати, разом із головним майстер-паролем, додатковий ключовий файл, який в моделі шифрується за допомогою особистого сертифіката (рис. 1).

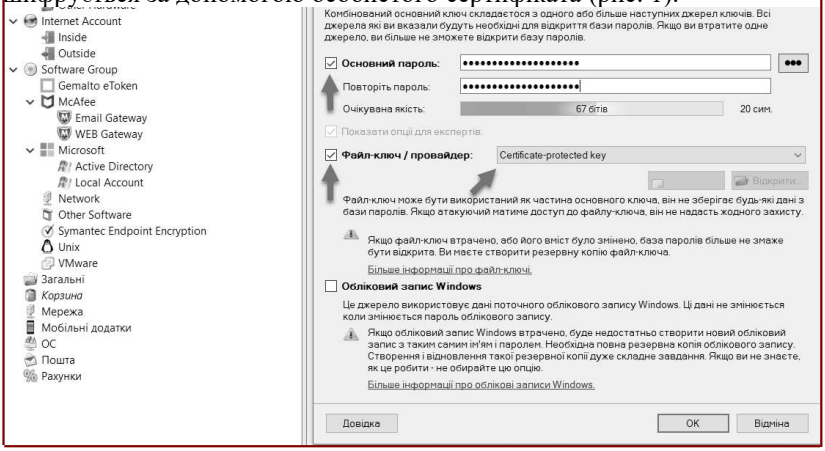

Рис. 1. Приклад структури аутентифікаційних даних

Приклад побудови структури бази аутентифікаційної інформації наведено на рис. 1, де:

Hardware Group – облікові дані обладнання (сервера, комутатори, роутери, маршрутизатори і т.п).

1) підгрупа IBM – облікові дані обладнання виробництва IBM;

2) підгрупа Cisco – облікові дані обладнання виробництва Cisco;

3) підгрупа HP – облікові дані обладнання виробництва HP.

Internet Account – облікові дані інтернет ресурсів. У цій групі зберігаються дані URL, логіни та паролі доступу до інтернет ресурсів, і вони умовно розділені на дві категорії:

1) підгрупа Outside – зовнішні ресурси, які не належать організації;

2) підгрупа Inside – внутрішні ресурси, ресурси всередині організації.

Software Group – облікові дані в різних системах, додатках, сервісах тощо.

Для зберігання секретних ключів сервісів і сертифікатів у наведеній моделі використовуються апаратні електронні ключі SafeNet eToken 5300 [4], що надає додатковий апаратний фактор попередньої апаратної аутентифікації для отримання доступу до конфіденційної інформації.

Реалізація вищенаведеної моделі захисту конфіденційної інформації дозволяє надати:

1) зручний і захищений інструмент для створення і зберігання в зашифрованому вигляді конфіденційної інформації для доступу до файлів, папок, веб-ресурсів, мережевого та серверного обладнання, додатків і сервісів – складні пари (логін, пароль), сертифікат, URL і т.п.;

2) можливість створення унікальних параметрів доступу до конфіденційної інформації для кожного файлу, папки, одиниці обладнання, веб-сервісу, додатків і сервісів;

3) можливість зберігання додаткової конфіденціальної інформації (IP, конфігураційні дані тощо);

4) можливість створення «складних» парольних політик і надання простого і ефективного інструменту для їх виконання;

5) можливість забезпечити мобільність доступу до конфіденційних ресурсів із збереженням багатоступеневого захисту конфіденційної інформації.

Фактично, при реалізації вищенаведеної моделі захисту конфіденційної інформації ми забезпечуємо для користувача наступні рівні апаратного та програмного захисту конфіденційної інформації:

1) апаратний захист бази даних, де зберігаються всі аутентифікаційні дані;

2) криптографічне шифрування конфіденційної інформації в базі даних і на носіях;

3) окремий ключовий файл для доступу до бази даних із шифруванням його індивідуальним сертифікатом;

4) апаратний захист секретних ключів та сертифікатів, що використовуються для доступу до конфіденційної інформації;

5) апаратну аутентифікацію для доступу до бази конфіденційної аутентифікаційної інформації, секретних ключів та сертифікатів.

Таким чином, запропонована модель дозволяє реалізувати багатоступінчатий захист при доступі користувача до своєї конфіденційної інформації (шифрування бази, майстер-пароль, ключовий файл, сертифікат). Така багатоступеневість мінімізує можливість компрометації аутентифікаційних даних користувача, а також надає додаткові можливості для використання унікальних

аутентифікаційних даних при доступі до конфіденційної інформації для кожного окремого файлу, папки, обладнання, сервісу або додатку.

Функціонально модель захисту конфіденційної інформації можна умовно представити у вигляді, що наведено на рис. 2.

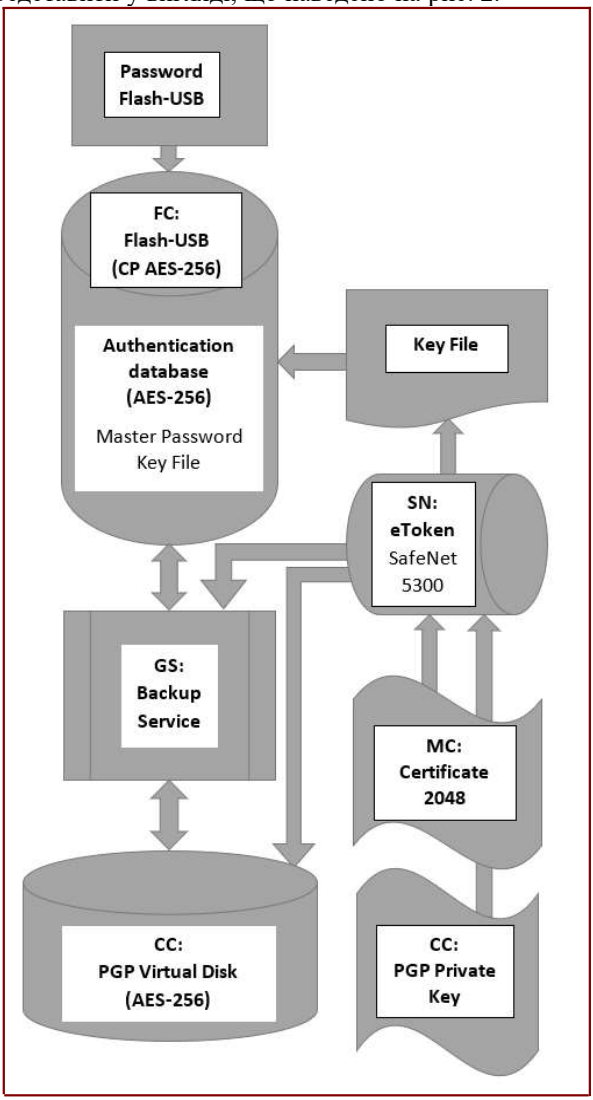

Рис. 2. Функціональний вигляд моделі

Для забезпечення мобільності та збереження резервних копій конфіденційної інформації, ми можемо використовувати криптографічний контейнер з ключами довжиною не менше 2048 біт. Криптографічний контейнер, у нашому випадку, створюється за допомогою відповідного криптографічного сервісу і розміщується, як правило, в захищеному корпоративному середовищі.

Для синхронізації основної і резервної бази конфіденційної інформації користувача використовується сервіс синхронізації GoodSync Enterprise [7] або вбудований в Safexs Protector XT функціонал для безпечного резервного копіювання.

Висновок. Питання ефективної організації захисту конфіденційної інформації переходить сьогодні в розряд найактуальніших питань у цілому світі. Особливо це актуально для підприємств, що відносяться до об'єктів критично-важливої інфраструктури та правоохоронних органів.

Розробка моделі захисту конфіденційної інформації дозволяє надати службам інформаційної безпеки об'єктів критично-важливої інфраструктури та правоохоронних органів інструмент для побудови структурованої системи захисту конфіденційної інформації і стандартизувати вимоги щодо її функціонування.

Наведено приклад використання моделі захисту конфіденційної інформації для створення захищеної і простої у використанні бази аутентифікаційних даних для доступу до конфіденційної інформації користувача. Запропонована модель дозволяє мати кілька ступенів програмного та апаратного захисту, що із однієї сторони спрощує для користувача виконання чинних політик інформаційної і кібернетичної безпеки, зменшує ймовірність дискредитації конфіденційної інформації, а із іншої сторони підвищує ймовірність виявлення зловмисних дій третьої сторони за рахунок багатоступеневої системи захисту. Враховано практичний досвід створення типових моделей захисту конфіденційної інформації для розробки, впровадження та управління сучасними політиками інформаційної безпеки щодо питань використання засобів захисту конфіденційної інформації на підприємствах різних форм власності.

Запропоновану модель імплементовано в структури різних форм власності і навчальні плани підготовки фахівців у сфері інформаційної та кібернетичної безпеки у Київському університеті імені Бориса Грінченка та Державному університеті телекомунікацій. В ході подальших досліджень буде здійснено обробку статистичних результатів, отриманих із зазначених навчальних закладів та внесені корективи в структуру моделі захисту конфіденційної інформації.

Сформовані рекомендації щодо базових елементів при формуванні моделі захисту дають можливість зменшити ризики, що пов'язані з несанкціонованим доступом до конфіденційної інформації, втратою та компрометацією конфіденційних інформаційних ресурсів і т.п.

Подальші дослідження варто зосередити на створенні та впровадженні типових моделей, процедур, регламентів та інструкцій щодо розгортання базових криптографічних засобів захисту конфіденційної інформації та їх експлуатації, тренінгам користувачів, правилам та практикам ефективного використання систем захисту конфіденційної інформації.

Список бібліографічних посилань

1. Управління доступом. TechNet – Microsoft. URL: https://technet.microsoft.com/ru-ru/library/cc770749(v=ws.11).aspx (дата звернення: 21.10.2018).

2. Борсуковський Ю. В., Борсуковська В. Ю. Визначення сучасних вимог щодо політики використання засобів захисту інформації на підприємстві. *Сучасний захист інформації*. 2018. № 1. С. 74–81.

3. Десять непреложных законов безопасности. URL: https://technet.microsoft.com/ru-ru/library/cc722487.aspx (дата звернення: 11.10.2018).

4. KeePass Password Safe. URL: https://keepass.info/ (дата звернення: 11.10.2018).

5. Safexs Protector XT. URL: http://www.safexs.info/products/protector-xt/ (дата звернення: 11.10.2018).

6. SafeNet eToken 5300. URL: https://safenet.gemalto.com/resources/product-brief/data-protection/safenet-etoken-5300 (дата звернення: 11.10.2018).

7. File Synchronization and Backup Software. URL: https://www.goodsync.com/ (дата звернення: 11.10.2018).

8. World Economic Forum. Reports 2018. URL: https://www3.weforum.org/docs/WEF_GRR18_Report.pdf (date of reference: 31 October 2018).

Одержано 31.10.2018

УДК 004.056.2

Володимир Леонідович БУРЯЧОК,
доктор технічних наук, професор,
завідувач кафедри інформаційної та кібернетичної безпеки
Київського університету імені Бориса Грінченка;
ORCID: https://orcid.org/0000-0002-4055-1494;
Володимир Юрійович СОКОЛОВ,
старший викладач кафедри інформаційної та кібернетичної безпеки
Київського університету імені Бориса Грінченка;
ORCID: https://orcid.org/0000-0002-9349-7946

ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ ОБ'ЄКТИВНОГО КОНТРОЛЮ ЗАХИЩЕНОСТІ КОРПОРАТИВНИХ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ І МЕРЕЖ

Історія розвитку інформаційного суспільства тісно переплетена, як відомо, з інформаційними операціями. Останнім часом це призводить до того, що заходи по маніпуляції інформацією, дезінформації конкуруючих сторін і/або введення їх один одного в оману є невід'ємною частиною внутрішньої і зовнішньої політики