УДК 004.05:338.3

В. О. Панченко

МЕХАНІЗМ ПРОТИДІЇ ІНСАЙДЕРАМ У СИСТЕМІ КАДРОВОЇ БЕЗПЕКИ

Запропоновано механізм протидії інсайдерам у системі кадрової безпеки для суб'єктів підприємницької діяльності та сформульовано перелік рекомендацій (як одного з механізмів захисту) щодо підвищення стійкості паролів і поліпшення їх запам'ятовування. Аргументовано, що це у комбінації з наведеними раніше підходами автора надасть змогу отримати первинну інформацію, необхідну для подальшої побудови моделі роботи інсайдерів для суб'єктів підприємницької діяльності.

Ключові слова: *кадрова безпека, інсайдер, економічна безпека, статистичний аналіз.*

Постановка проблеми. Сьогодні на сучасному етапі розвитку, в епоху стрімкого розвитку ІТ- та інших технологій, їх впровадження в економіку суб'єктів підприємницької діяльності, особливо актуальним стає питання забезпечення кадрової безпеки суб'єктів підприємницької діяльності під час небажаних (незаконних) дій своїх співробітників. Однією з таких категорій є інсайдери – звичайні співробітники суб'єктів підприємницької діяльності, що володіють закритою інформацією (наприклад, комерційною таємницею) і надають її (за яких-небудь умов: за гроші, шантаж, особисте незадоволення керівництвом та ін.) стороннім особам. Відповідно до економічного словника, інсайдер (англ. *Insider*, від *inside* – буквально всередині) – це особа (співро-

бітник), яка через свій службовий чи сімейний стан має доступ до конфіденційної інформації суб'єктів підприємницької діяльності; це посадові особи, директори, основні акціонери суб'єктів підприємницької діяльності з широким володінням акцій і їхні найближчі родичі. До цієї групи також належать особи, які видобувають конфіденційну інформацію про діяльність суб'єктів підприємницької діяльності та використовують її з метою особистого збагачення. Такі суб'єкти підприємницької діяльності найчастіше є конкурентами на ринку. Саме так і організовується один з каналів витоку закритої інформації. Тут слід обумовити, що ця категорія співробітників діє цілеспрямовано у переданні інформації конкурентам-суб'єктам підприємницької діяльності.

Стан дослідження. Над проблемами в цій сфері працюють відомі фахівці і вчені: В. П. Верин, А. А. Кириченко, Ю. А. Кудрявцев, Е. А. Олейников, М. О. Кизим, Т. С. Клебанова, Е. В. Раєвнєва, М. П. Гуров, М. В. Куркін, С. М. Шкарлет, С. В. Кавун та ін. [1–7]. В їхніх працях досліджено питання систематичного підходу для усунення загроз інформаційній та економічній безпеці (зокрема й кадровій), але більшою мірою ці розвідки стосуються зовнішніх загроз. Не повністю вирішеним є й питання внутрішніх загроз, і, як наслідок, питання роботи (або протидії їх діям) інсайдерів у системі кадрової безпеки суб'єктів підприємницької діяльності.

Наприклад, у своїх працях С. В. Кавун виробив [2; 4] концептуальну модель системи економічної безпеки, що нагадує «соту», тому автор запропонував назвати її «стільниковою» концептуальною моделлю СЕБ. Крім того, така «стільникова» модель надасть змогу побачити і оцінити (а значить, і вжити всіх необхідних заходів) усі сторони наявних аспектів кадрової безпеки. Представлені значення показників були отримані аналітичним шляхом і не є категоричними в плані їх оцінок. Надалі автор запропонував для підвищення ступеня об'єктивності використовувати експертні оцінки, здобуті за допомогою розробленої експертної системи. Також ці публікації є продовженням авторського напряму досліджень [8–11].

Метою статті є наочне представлення можливих механізмів або схем реалізації дій інсайдерів для керівників різних рангів і окреслення планових заходів щодо усунення каналів витоку закритої інформації (комерційної таємниці) суб'єктів підприємницької діяльності.

Виклад основних положень. Проведений порівняльний аналіз джерел статистичної інформації (Computer Security Institute, CSI) показав стійку тенденцію зростання втрат різних ресурсів суб'єктів підприємницької діяльності від діяльності інсайдерів. Свідченням цього

є показник перевищення в 2007 році рівня інцидентів суб'єктів підприємницької діяльності, пов'язаних з інсайдерами, порівняно з вірусними зараженнями.

Все це свідчить про виниклі потреби в професійних співробітників у сфері кадрової безпеки та захисту інформації на суб'єктах підприємницької діяльності. У найближчі три роки, за дотримання темпів розвитку ІТ-інфраструктури, суб'єкти підприємницької діяльності повинні будуть більшість фінансових та інших видів витрат спрямовувати на реалізацію заходів (наприклад, побудову системи кадрової безпеки) та придбання відповідних засобів забезпечення кадрової безпеки та захищеності інформації.

За даними ООН, вже сьогодні збитки, що завдаються комп'ютерними злочинами від діяльності інсайдерів на суб'єктах підприємницької діяльності, можна порівняти з доходами від незаконного обігу наркотиків та зброї. Тільки у США щорічний економічний збиток від таких злочинів становить близько 100 млрд дол. Причому багато втрат не виявляються або про них не повідомляють.

У своїй діяльності інсайдери використовують або відомі канали витоку інформації (наприклад, електронну пошту, копіювання на зовнішні носії, отримання паперових копій документів, сканування), або створюють власні (наприклад, «зомбування» власного ПК для можливості віддаленого доступу, надання автентифікаційних даних стороннім особам, використання завідомо слабких паролів, неякісне знищення паперових носіїв).

Перелік використовуваних програмних і апаратних засобів сьогодні настільки великий і різноманітний, що його перелік займе доволі багато місця. Одне лише варто обумовити обов'язково – труднощів у знаходженні та придбанні таких засобів сьогодні не існує жодних.

Які ж механізми роботи інсайдерів використовуються на суб'єктах підприємницької діяльності? Всі інсайдери працюють за тими самими алгоритмами, відмінність може залежати тільки від специфіки самих корпорацій або компаній. Для початку всю кількість інсайдерів необхідно класифікувати за деякими ознаками. Оскільки основним об'єктом, на який спрямована діяльність інсайдерів, є інформація (причому закрита: комерційна, банківська, персональна, службова, автентифікаційна, фінансова та ін.), то однією з ознак класифікації є рівень доступності даних для інсайдерів. Автор пропонує такі типи інсайдерів за ознакою рівня доступності даних: 1) співробітники, які вже володіють цією інформацією; 2) співробітники, які мають доступ до цієї інформації; 3) співробітники, які бажають отримати валід-

ний доступ до цієї інформації; 4) співробітники, які хочуть отримати невалідний доступ до цієї інформації.

Автор навмисне використав поняття «інформація», а не «дані», оскільки перше поняття набагато ширше, а дані можуть бути окремим випадком формалізованого представлення інформації, придатним для використання в будь-якому бізнес-процесі суб'єктів підприємницької діяльності. Наведемо декілька прикладів детального опису введених відмінностей в табличній формі (див. табл.).

Таблиця

Приклади варіантів використання понять

Бізнес-процес	Дані	Інформація
Набір спеціалістів	Рекламні оголошення	Представлення нової послуги
Підготовка до випуску нової продукції	Специфікації, рецепти, формуляри, дистрибутив, первинні коди	Рівень готовності продукту, технічні характеристики, строки виходу
Представлення нової послуги (банківської, юридичної, комерційної, промислової)	План реалізації, технічний опис, модель	Розширення сфери впливу на ринок, вихід на дещо вищий конкурентний рівень, залучення більшої кількості клієнтів

З огляду на наведену авторську класифікацію типів інсайдерів за ознакою рівня доступності даних, можна з достатнім ступенем впевненості виокремити категорії співробітників суб'єктів підприємницької діяльності, які можуть бути або стати потенційними інсайдерами: 1) менеджери; 2) керівники молодших рангів (у старших керівників є стимули, зацікавленості, приводи); 3) співзасновники, які володіють меншою частиною капіталу; 4) пересічні співробітники суб'єктів підприємницької діяльності, що мають за родом своєї діяльності доступ до закритої інформації (комерційної, банківської, персональної, службової, автентифікаційної, фінансової та ін.) і не задоволені обсягами наданих ресурсів (посадою, грошовими винагородами, преміями, тимчасовими винагородами: відгулами, відпустками).

До речі, діями інсайдерів на суб'єктах підприємницької діяльності можуть бути не тільки «несанкціонована передача» інформації, але й, наприклад, навмисне псування, зміна або знищення інформації (даних), що є навмисною загрозою функціонування суб'єктів підприємницької діяльності. І за всім цим також стоять (хоча і менші)

ресурсовтрати: грошові, часові, фінансові, статистичні, банківські та ін. Маючи надані висновки та авторські рекомендації, пропонуємо множину можливих механізмів діяльності інсайдерів на суб'єктах підприємницької діяльності:

1) співробітник (інсайдер) може здійснити навмисний або ненавмисний винос інформації або даних;

2) співробітник (інсайдер) може здійснити навмисне або ненавмисне спотворення інформації або даних;

3) співробітник (інсайдер) може здійснити навмисне або ненавмисне псування інформації або даних;

4) співробітник (інсайдер) може здійснити навмисне або ненавмисне знищення інформації або даних.

При звичайному розрахунку загальна кількість всіх варіантів механізмів складе 16 з урахуванням всіх можливих комбінацій.

Подальші організаційні заходи щодо виявлення (запобігання деструктивній діяльності) і ліквідації наслідків є основними і можуть бути представлені як відповідна авторська методика так:

1. Посилення правил використання та складання паролів або інших механізмів автентифікації суб'єктів підприємницької діяльності.

2. Впровадження та ретельне дотримання відомих (світових) стандартів, внутрішніх інструкцій, законодавчих актів, норм, правил, законів.

3. Чітке розмежування прав доступу і уважний вибір об'єкта для делегування поточних прав іншим співробітникам суб'єктів підприємницької діяльності.

4. Введення на суб'єкті підприємницької діяльності власної служби кадрової безпеки, а також групи залагодження інцидентів з комп'ютерної (кадрової) безпеки.

5. Планове (щотижневе, квартальне, піврічне, річне, позапланове) обстеження суб'єкта підприємницької діяльності на предмет виявлення відомих (і невідомих або скритих) каналів витоку інформації.

6. Використання системи масштабного «логування» (запису в файл всіх операцій, дій, транзакцій) для найбільш вразливих місць системи і критичних ресурсів суб'єкту підприємницької діяльності.

Цей перелік можна нескінченно продовжувати і вводити нові рекомендації, а надто при сучасному рівні розвитку IT-технологій. Однак збільшення їх кількості може дати зворотний ефект, коли в гонитві за кількістю реалізацій захисних функцій буде істотно втрачати якість. Водночас зростає складність, що також вплине на якість їх реалізації в підприємницькій діяльності. Тому представлена кількість, вважаємо, є «золотою серединою» і оптимальною множиною для

початкового впровадження на суб'єкті підприємницької діяльності. Додатково пропонуємо перелік рекомендацій (як один з механізмів захисту) щодо підвищення стійкості паролів і поліпшення їх запам'ятовування. Його застосування дозволить значною мірою покращити якість запам'ятовування паролів, що вводяться без зменшення їхньої довжини.

Основні рекомендації:

1. Використання транслітерації – прийом вводу даних (символів пароля), за якого знаки розміщені в одній розкладці, наприклад, англійській, а саме слово (або частина його) вводиться з іншої розкладки. Наприклад, слово українською мовою «фортеця» реально буде виглядати як «rhtgjcnm». Цей прийом дасть змогу деякою мірою ускладнити використання візуального каналу знімання інформації або звичайного підглядання під час введення пароля.

2. Впровадження спочатку / в середині / в кінці пароля символа (більше одного призводить до ускладнення запам'ятовування) із змінним регістром, тобто якщо пароль вводиться малими символами, то використання в зазначених місцях літери (це додаткове натискання клавіші Shift під час вводу, що можна зробити непомітно за допомогою мізинця) збільшує його криптостійкість або стійкість до злому, не зменшуючи здатності до запам'ятовування. Цей прийом ґрунтується на психологічній характеристиці людини, за якої доволі легко можна запам'ятати символ і його місце розташування. Відтак запроваджений пароль може виглядати так: «Фортеця» або «ФортецЯ».

3. Використання в тих же місцях (див. п. 2) цифр, але не більше двох, тому що більшу кількість вже буде помітно при вводі. Цей прийом також ускладнює процес підглядання під час вводу пароля. Наприклад, запроваджений пароль може виглядати так «Фортеця» або «Фортеця78».

4. Під час вводу осмислених літературних слів (це не раціонально з погляду криптостійкості та можливості атаки по словнику) рекомендується підбирати слова, що складаються з букв, що на клавіатурі знаходяться поруч (мається на увазі встановлена розкладка клавіатури – QWERTY). Це дозволить, не володіючи достатньою швидкістю набору, ввести пароль з необхідною швидкістю, що також зменшить ймовірність підглядання під час вводу пароля. Запропонований пароль, приміром, може виглядати так «фортеця».

5. Використання зворотного порядку вводу осмислених слів – для оволодіння цього прийому необхідні відповідні навички, що може не кожен користувач. Крім того, не варто забувати про подібні можливості в програмах аудиту (злому) захисту, наприклад, SAMInside

або L0phtCrack 6. Відтак, запроваджений пароль може виглядати так «яцетроф».

6. Використання ASCII-кодів другої половини таблиці (водночас код є тризначною цифрою). Цей прийом ефективний, якщо вводиться пароль, який є цифровим кодом достатньої довжини, наприклад, номер стільникового телефону з кодом оператора. Тоді послідовність буде нерозривною при вводі і, отже, непомітною. Методика вводу: правою рукою на цифровій панелі вводиться цифрова послідовність, а лівою рукою непомітно натискаються відповідні клавіші (Shift + Alt) при вводі альтернативного коду. Тож запроваджений пароль може виглядати так «+34657**156**457683**210**456», де жирним кольором показані альтернативні коди – 156 і 210. Крім того, цим способом можна отримати достатню довжину пароля.

7. Використання властивості «буденності» фрази, що призводить до значного збільшення довжини пароля, тобто в якості пароля використовується відома, буденна фраза, словосполучення, пропозиція, афоризм, прислів'я, вірші, рядки пісні.

8. Використання властивості «незвичайності або неординарності», що є протидією методу соціальної інженерії: коли зломщик, стежачи за власником пароля, складає індивідуальний словник користувача (його звички, слова-паразити, жаргон, сленг, клички тварин, дати, скорочення, абревіатури), який потім буде використовувати для атаки. Тоді, застосовуючи це правило, користувач використовує як пароль цілком незвичне для нього слово, фразу або словосполучення.

Слід також зауважити на можливості захисту від програм, іменованих KeyLogger, які записують скан-коди всіх клавіш на клавіатурі, що взагалі позбавляє сенсу використання будь-яких прийомів і правил підвищення криптостійкості парольного захисту, тому що символи зчитуються ще до моменту їх використання в паролі. Деякі такі програми можна ще й добре заховати від можливості візуального виявлення. Ці ж функції перехоплення скан-кодів можуть бути реалізовані й апаратно – у вигляді невеликого пристрою, що підключається в роз'єм клавіатурного кабеля. Якщо функції перехоплення реалізовуються програмним способом, то такі програми мають бути попередньо впроваджені в систему.

Висновки. На основі запропонованих механізмів можна отримати первинну інформацію, необхідну для подальшої побудови моделі роботи інсайдерів у підприємницькій діяльності, для суб'єктів підприємницької діяльності.

Наукову новизну статті забезпечує формування цілісного механізму протидії інсайдерам у системі кадрової безпеки для суб'єктів

підприємницької діяльності та переліку рекомендацій (як одного з механізмів захисту) щодо підвищення стійкості паролів і поліпшення їх запам'ятовування і запропонованих раніше підходів.

Як подальший напрям дослідження можна рекомендувати розробку математичної інтерпретації завдання виявлення інсайдерів у системі кадрової безпеки для суб'єктів підприємницької діяльності, а також проведення аналізу економічного ефекту використання пропонованої моделі та можливих наслідків дій інсайдерів.

1. Верин В. П. Преступления в сфере экономики. М.: Дело, 2002. 215 с.
2. Кавун С. В. Жизненный цикл системы экономической безопасности предприятия. *Управління розвитком*. 2008. № 6. С. 17–21.
3. Кавун С. В., Сорбат И. В. Инсайдер – угроза экономической безопасности. *Управління розвитком*. 2008. № 6. С. 7–11.
4. Кавун С. В., Сорбат И. В. Математическая интерпретация задачи выявления инсайдеров в организации (предприятии). *Научный журнал «Экономика: проблемы теории и практики».* Днепропетровск: Руснаука, 2009. Т. 246. № 4. С. 862–869.
5. Олейников Е. А. Экономическая и национальная безопасность: учебник для вузов. М.: Экзамен, 2005. 768 с.
6. Геєць В. М., Кизим М. О., Клебанова Т. С., Черняк О. І. Моделювання економічної безпеки: держава, регіон, підприємство: монографія. Х.: ХНЕУ, 2006. 240 с.
7. Гуров М. П., Кудрявцев Ю. А. Теневая экономика и экономическая преступность в вопросах и ответах: учебное пособие. СПб.: Санкт-Петербургский университет МВД России, 2002. 237 с.
8. Кавун С. В., Панченко В. А. Модель інтелектуального управління системою кадрової безпеки підприємства. *Науковий вісник. Серія економічна:* збірник наукових праць Львівського державного університету внутрішніх справ. Львів: ЛьДУВС, 2017. Вип. 2. С. 190–198.
9. Кавун С. В., Панченко В. А. Аналіз категоріального апарату у сфері кадрової безпеки. *Ефективна економіка*. Дніпро: Дніпровський державний аграрно-економічний університет, 2017. № 1. URL: http://www.economy.nayka.com.ua/?op=1&z=6150.
10. Кавун С. В., Панченко В. А. Класифікація індикаторів управління кадровою безпекою підприємства. *Информационная экономика: этапы развития, методы управления, модели:* колективна монографія / за ред. В. С. Пономаренко, Т. С. Клебановой. Х.: ВШЭМ–ХНЭУ им. С. Кузнеца, 2018. 668 с. С. 482–502.
11. Кавун С. В., Панченко В. А. Підхід до оцінювання кадрової безпеки підприємства з позицій релевантних функцій управління персоналом. *Сучасні проблеми моделювання соціально-економічних систем*: матеріали X міжнародної науково-практичної Інтернет-конференції (5–6 квітня 2018 р.). Х.: ВШЕМ–ХНЕУ ім. С. Кузнеця, 2018. 224 с. С. 73–77.

Panchenko V. A. The mechanism of insider incident in the system of personnel safety

The formation of a mechanism for countering insiders in the personnel security system for business entities and a list of recommendations (as one of the protection mechanisms, its application will greatly improve the quality of the memory of entered passwords, while not reducing its length.) to increase the stability of passwords and improve their memorization, combined with the author's previously proposed approaches will provide the primary information necessary for the further construction of the work model insiders for business entities.

Having the above conclusions and author's recommendations, the set of possible mechanisms of activity of insiders on subjects of entrepreneurial activity is offered. It is determined that the problem of internal personnel security of business entities should take a worthy place in the development of world corporations and companies and receive all necessary resources (human, organizational, financial, etc.) for the implementation, implementation and observance of the requirements of personnel security of the subjects of management. This will offer a mathematical interpretation of the task of identifying insiders in the personnel security system of business entities, as well as analyze the economic effect of using the proposed model and the possible consequences of insider actions.

A holistic understanding of the functioning of any subject of business activity is impossible without the official presentation of its economic model. As a suggested direction of further research, we can propose the development of a mathematical interpretation of the task of identifying insiders in the personnel security system for business entities, as well as conducting an analysis of the economic effect of using the proposed model and the possible consequences of the actions of insiders.

Key words: *personnel security, insider, economic security, statistical analysis.*

Стаття надійшла 22 травня 2018 р.