УДК 004. 056
DOI: 10.31673/2409-7292.2020.044145

**Маслова Ю.Ю. Кушнір І.М.**

# ІНФОРМАЦІЙНА БЕЗПЕКА І ЛЮДСЬКИЙ ФАКТОР

В статті розглянуто проблеми, що можуть виникати під час впровадження і експлуатації систем захисту інформації без належного оцінювання ризиків та можливих недоліків безпосередньо технічних рішень. Певні аспекти впровадження, зазначені найбільш розповсюджені проблеми і ризики, що можуть бути наслідком людського фактору.

**Ключові слова:** людський фактор, ризик, оцінка ризику.

## Вступ

Незалежно від того які системи захисту використовуються, яка кількість та кваліфікація персоналу що залучена до процесу захисту інформації, людський фактор може звести нанівець усі зусилля. Прикладом певних помилок в вихідному коді або в діях персоналу можуть бути декілька наступних прикладів що відбулися на протязі вересня 2020 року. Так експерт в інформаційній безпеці Боб Д'яченко знайшов в відкритому доступі базу даних інтернет магазину Razer, наведена організація займається розробкою професійного ігрового устаткування. База містила ім'я клієнта, адресу електронної пошти, номер телефону, номера замовлень, деталі замовлень, а також білінгові адреси і адреси доставки [1].

Фахівець компанії WizCase виявив бекенд - сервер Bing з відкритим доступним. Сервер зберігав понад 6,5 Тб логів мобільних додатків, що містять 13 000 000 000 записів, отриманих з пошуковика. Виток стався через те, що співробітники Microsoft помилково залишили у відкритому доступі один з бекенд - серверів свого пошуковика Bing [2].

Дослідники vpnMentor виявили відкритий сервер Elasticsearch, де база даних без пароля давала можливість отримати доступ до персональних даних сотень тисяч користувачів, велика частина даних належить сайтам знайомств. Обсяг викраденої інформації - більше 800 ГБ або 300 мільйонів записів. В зазначеній базі також міститися листування користувачів [3].

Зазначене вище доводить що тільки лише технічні елементи управління не зможуть забезпечити достатню інформаційну безпеку на практиці, і створити найбільш економічно-ефективну форму контролю безпеки.

## Недоліки технічних рішень

Найчастіше підприємства, організації та самозайняті особи розглядають тільки певні "технічні рішення" як єдиний засіб захисту активів, мотивуючи свій вибір наявним, вузьким колом знань, про проблеми інформаційної безпеки. Такі інформаційні технології як брандмауери, антивірусне програмне забезпечення, VPN і SIEMS є цінною зброєю в побудові процесу забезпечення інформаційної безпеки [4], але існують серйозні недоліки в технологічному підході:

1. По-перше, технології помиляються. Незважаючи на всі зусилля якісної розробки програмного забезпечення руху, хакерів, тестери і користувачі продовжують знаходити критичні помилки, несподівані виняткові стани, бекдори і інші грубі уразливості в комерційних і в власних розробках програмного забезпечення. У всякому разі, вони в даний час виявляються і експлуатуються більш швидкими темпами, незважаючи на величезний обсяг інвестицій в практику кодування і тестування безпеки системи. Ця проблема посилюється складністю IT систем. Організації, які використовують багатошарову безпеку мають вірне уявлення, але наївно було б припустити, що кожен шар безпеки є ідеальним [5]. Що найменш в тестуванні ПЗ наявне твердження "чим більше програмне забезпечення має строк коду, тим біль можливих помилок в ньому наявне".

2. По-друге, далеко не всі організації дійсно можуть зрозуміти проблеми інформаційної безпеки в достатній мірі, щоб навіть вказати на відповідні технічні рішення. Як правило, вони обирають потрібне для стандартних пакетів ПЗ для забезпечення інформаційної безпеки (наприклад, антивірусне програмне забезпечення), але повне уявлення про вимоги в цілому найчастіше відсутні. Вони сканують листи на наявність

вірусів, але в той же час ігнорують карти пам'яті USB, JavaScript, DNS і інші більш екзотичні атаки. Окрім зазначеного, хтось повинен займатися впровадженням, експлуатацією, управлінням і обслуговуванням всього, що стосується безпеки технологій [5].

3. По-третє, сам термін «технічне рішення» майже завжди має на увазі значні витрати. Зроблені на замовлення технології безпеки обходяться особливо дорого, в той час як стандартні вихідні готові пакети пропонують невеликі конкурентні переваги.

**Метою статті** є аналіз проблем і ризиків, які можуть бути наслідком людського фактору та його впливу на систему керування інформаційною безпекою.

**Економічний аспект впровадження основних або додаткових заходів забезпечення безпеки**

Організації з обмеженими або неефективними заходами безпеки страждають набагато більше і зазнають великих втрат, ніж їх конкуренти з кращими підходом в організації захисту інформації. Придбання та запуск основних або додаткових заходів стає більш дорогим, в ряді випадків вартість впроваджуваних рішень, унаслідок неправильного підходу в оцінці ризиків і безпосередньо в оцінці активів обходяться дорожче, ніж наслідки порушень в безпеці, яких прагнуть уникнути. В деяких, нажаль, рівень заходів не відповідає рівню активів і не здатні до адекватного захисту [5].

Реалізація таких заходів має кілька пов'язаних витрат, деякі з них є очевидними і їх легко виміряти, але багато залишаються прихованими або непомірними:

1. Як правило, доводиться платити авансом, коли ми купуємо щось, будь то продукт (наприклад, брандмауер) або послуги (наприклад, управління безпекою). Ціна покупки може бути одноразовою або періодичною (наприклад, ліцензійні збори, технічне обслуговування). Однак, є і приховані витрати на закупівлі, в тому числі зусилля, необхідні для ідентифікації вимог, вибір відповідних товарів і послуг і завершення угод з купівлі. Внутрішні витрати, як правило, поглинаються в процесі закупівель як накладні витрат у всіх покупках [6].

2. Засоби захисту повинні бути реалізовані і керовані. В цьому випадку час і витрати на управління зміни можуть бути більш значними. Складні технічні елементи управління, такі як виявлення вторгнень і системи запобігання вторгнень, є відносно дорогими в плані реалізації належним чином і бувають упаковані в проекті впровадження, що вимагають конкретних фінансових інвестицій [7]. Навіть послуги мають реалізації та управлінські витрати. Є деяка ступінь руйнування і зміни в якості внутрішніх процесів, пристосованих для поглинання нового обслуговування, і в обох випадках є постійна участь постачальника в питаннях створення і управління [7].

3. Витрати, пов'язані з налаштуванням або використанням засобів захисту.

Передові засоби безпеки істотно більш дорогі у всіх трьох категоріях, ніж високі технології обслуговування або процедурного контролю. Слід зазначити що всі витрати і ефективності варіюються в залежності від видів контролю, що забезпечую певна система.

Як правило, елементи управління, призначені для запобігання або уникнення порушень будуть більш економічно ефективними, ніж ті, які призначені для визначення або виправлення порушень після. Профілактичним і стримуючим фактором управління є зменшення або усунення витрат на вплив від іншого контролю. Не будь-який контроль досить ефективний, так що все ще існує необхідність інвестувати в корегуючи засоби управління, що містять загальні витрати на порушення, які неминуче будуть відбуватися.

Питання в тому, якщо розглядати поліпшення процесів управління в інформаційній безпеки, чи потрібно інвестувати в технології процесів? Не можливо провести просте встановлення по принципу out-of-the-box і ігнорувати інструкцію, процеси налагодження, та загальні рекомендації по забезпеченню безпеки інформації, та потім сподіватися на те, що система буде працювати в повній мірі. Насправді люди і технології доповнюють один одного [7].

**Людський фактор**

Гадаю, майже всі коли-небудь вводили значення в неправильному полі форми, або робили просту помилка в обчисленнях, видаляли не той файл помилково, витягали

неправильну вилку з розетки. Всі припускаються помилок, і здебільшого просто приймаємо такі та подобні помилки як неминуче, а потім робимо все можливе, щоб виявити і усунути проблеми, поки ще не занадто пізно. Відносно контролю технічної безпеки, прості помилки конфігурації можуть залишити мережеві порти відкритими, брандмауери уразливими і системи повністю незахищеними. Насправді людська помилка, куди більш імовірно може привести до серйозних порушень безпеки, ніж технічні уразливості.

Існує область науки, яка називається «Human Factors Engineering», вона прагне вирішити цю проблему. У деяких випадках (наприклад, електростанція системи управління), натискання «не тієї кнопки» може мати катастрофічні наслідки для безпеки. Є система блокування, подвійне управління і автоматичні програмовані відгуки. Цілі групи моніторів стежать і постійно перевіряють систему, її операторів, і динамічний реагування на стані тривоги. Безпека критично важливих систем (то, як вони спроектовані, розроблені, випробувані, експлуатуються і обслуговуються людиною) дуже важлива і досить надійна. І все ж, помилки все ще мають місце. Оператори електростанцій іноді натискають на неправильні кнопки, тим самим виключаючи системи, через що і відбуваються порушення в системах безпеки.

Користувачі вибирають слабкі паролі, і замість того, щоб змінити їх, вони повторно використовують їх в декількох системах. Вони втрачають свої маркери безпеки і смарт-карти. У той час як система контролю безпеки іноді може допомогти як приклад, дотримання довгих букво - цифрових паролів, користувачі як і раніше роблять все по-своєму, наприклад, використовують прості шаблони з клавіатури і вибирають паролі з слів словника [6].

Підводячи підсумки, можна сказати, що інформаційна безпека є одночасно повністю людською та технологічною проблемою.

**Оцінка проблем**

Припустимо, що ваша організація йде в ногу з кращими практиками безпеки. Можливо ви менеджер з інформаційної безпеки або керівник відділу Інформаційної безпеки або група що забезпечення безпеки організації. Адміністрація схвалила набір політик і стандартів в області інформаційної безпеки. Ваші системи вимагають довгих паролів, і ви встановили пристойні брандмауери та антивірусне програмне забезпечення. У вашій організації можливо навіть є система управління інформаційною безпекою, можливо, завірена і відповідна ISO/ IEC 27001. Залишається питання: наскільки система захищена [8].

Для оцінки вищезазначеного розглянемо наступні аспекти докладніше:

1. Наскільки компетентна ваша команда з управління інформаційною безпекою? Чи є вони технічно кваліфікованими в площині управління інформаційною безпекою? Чи є фахівці досить мотивованими, щоб зробити свою роботу добре?
2. Якою мірою відбувається підтримка управління політики інформаційної безпеки організації, цілі та управління? Чи відбувається повідомлення про порушення правил безпеки регулярно з зазначенням серйозності інцидентів ? Коли в останній раз ТОП менеджмент явно підкреслив важливість інформаційної безпеки в засіданні колегії?
3. Чи всі ваші співробітники розуміють і виконують інформаційну політику і стандарти строго? Чи охоплюють політика і стандарти всі вимоги інформаційної безпеки організації? Нові стажисти і тимчасові працівники чи дотримуються тих самих правилами? Чи знають вона які правила і наслідки недотримання?
4. Чи розуміють користувачі необхідність вибору надійних паролів, що потрібно тримати їх в секреті, і часто міняти? Хто-небудь насправді перевіряє, що вони виконують вказівки? А як що до всіх ваших інших політики, стандартів і правил управління? [8]
5. Фахівці, які налаштовують і обслуговують сервера, брандмауери, антивірусне програмне забезпечення і таке інше. тримають в курсі останніх загроз, вразливостей і впливів на всі системах (в тому числі настільні комп'ютери, портативні і мережеві пристрої)? Вони регулярно перевіряють випущені поновлення ПО та патчі безпеки зокрема ? Чи перевіряли вони безпеку нових релізів до задіємня їх на виробничій мережі? Хто-небудь

зможе самостійно і грамотно перевірити ваші системи і мережі, що вони знаходяться в безпеці, і якщо так, наскільки ретельно і як часто? [8]

Ці питання в основному стосуються людей, а не технології. Звичайно, важливо використовувати певні програмні або апаратні комплекси або системи, але, з огляду на, що більшість наявних у продажу засобів розумно функціональні, ще важливіше бути впевненим, що вони налаштовані правильно і підтримується людьми. Такий же аргумент відноситься до антивірусного захисту, IDS / IPS і інших зрілих технологій безпеки. Незважаючи на те, що виробники можуть сказати і як розрекламувати, всі вони досить функціональні, але вони повинні бути правильно налаштовані і йти в ногу з часом і рівнем загроз. Певні системи не можуть задіяти політику і стандарти інформаційної безпеки, люди повинні купувати і налаштовувати системи, включати функцій управління, моніторинг тривоги і використовувати їх. Виходячи з усього цього, можна зробити висновок, що нітрохи не менш важливо інвестувати в людей та їх навчання, як в технології та засоби [9].

**Управління ризиками**

Більшість організацій можуть оцінити свої технології для ризиків інформаційної безпеки, як правило, шляхом оцінки нових продуктів і періодичних випробувань системи, наприклад, тестування pre-релізів і регулярні скани мереж.

З точки зору управління ризиками, люди представляють загрози:

1. Персонал або аутсайдери компанії, які навмисно намагаються порушити безпеку системи управління шляхом явної загрози - типовими прикладами є шахраї, хакери то що. Недбалий і некомпетентний персонал це ще одна форма загрози, вони вводять неправильні дані в вашу систему, що може привести до пошкодження, але навіть сумлінний і дбайливий персонал іноді допускає помилки [7].
2. Співробітники, які вибирають слабкі паролі, ідентифікатори для користувачів, розкривають конфіденційну інформацію, ігнорують помилки, помилки в конфігурації безпеки, відкриті уразливості, які можуть бути використані іншими то що [7].
3. Менеджери і керівники, які не завдали собі клопоту перевірити інформацію, перш ніж надавати дозвіл системі отримати доступ до будь - яких важливих файлів або до файлів та процесів які створюють іншу форму систематичної уразливості.
4. Найчастіше порушення інформаційної безпеки викликані людиною, в результаті організаційних наслідків. Персонал, часом, схильний не довіряти системам, навіть якщо помилки даних є результатом помилок введення даних користувачами. Часом їм складно придумати і запам'ятати гарний, стійкий пароль і вони користуються шаблонами [9].

**Висновок**

Якщо ви серйозно ставитеся до інформаційної безпеки, необхідно вирішувати та прогнозувати для вжиття превентивних заходів фактори, що можуть бути спричинені людиною, так само як і технічні, думати про те, як поліпшити ці обидва аспекти. Вони однаково важливі, не потрібно вибирати. Активне управління ризиками включає в себе оцінку і переоцінку всіх загроз, вразливостей, впливів і послідовного поліпшення заходів контролю. Це ж все робиться не тільки для того, щоб отримати сертифікат 27001 або будь-який інший статус. Інформаційна безпека – це постійний процес управління. Та й коли ваша система в безпеці, а співробітники надійні і уважні, організації чи підприємству немає чого боятися.

**Перелік посилань**

1. Razer data leak exposes personal information of gamers [Електронний ресурс] // -режим доступу: https://www.bleepingcomputer.com/news/security/razer-data-leak-exposes-personal-information-of-gamers/
2. Data Leak: Unsecured Server Exposed Bing Mobile App Data [Електронний ресурс] // -режим доступу: https://www.wizcase.com/blog/bing-leak-research/
3. Report: Popular Marketing Tool Exposes Dating Site Users in Massive Data Leak [Електронний ресурс] // -режим доступу: https://www.vpnmentor.com/blog/report-mailfire-leak/

4. The human factor is key to good security [Електронний ресурс] // -режим доступу: https://www.computerweekly.com/opinion/The-human-factor-is-key-to-good-security

5. Людський фактор та його роль в забезпеченні інформаційної безпеки [Електронний ресурс] // -режим доступу: https://securelist.ru/Chelovecheskiy_faktor_i_ego_rol_v_obespechenii_informatsionnoy_bezopasnosti

6. Информационная безопасность и человеческий фактор [Електронний ресурс] // -режим доступу: http://idmatic.ru/antiinsider/83-antiinsider/342-informacionnaya-bezopasnost-i-chelovecheskij-factor

7. Д'Арси J, Hovav & Galletta DF (2009). Поінформованість. Призначена для користувача Безпека. Контрзаходи і їх наслідки для інформаційних систем зловживання. Стримування. Інформація Systems Research

8. Лейси, Д. (2009). Managing the Human Factor in Information Security, How to win over staff and influence business managers, Chichester, John Wiley & Sons Ltd.

9. Analyzing Human Factors for an Effective Information Security Management System Електронний ресурс] // -режим доступу: https://www.igi-global.com/article/analyzing-human-factors-effective-information/76355

Надійшла: 20.11.2020 Рецензент: д.т.н., професор Вишнівський В.В.