УДК 004.062

ЛЮДСЬКИЙ ФАКТОР В ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ

Химуля А. В., здобувач вищої освіти гр. КБ-171
Науковий керівник: **Гур'єв В. І.,** к.т.н., професор
Національний університет «Чернігівська політехніка»

Рік за роком експерти і аналітичні компанії, що спеціалізуються в області інформаційної безпеки (ІБ), відзначають одну і ту ж глобальну тенденцію: кількість кібератак збільшується, вони стають все витонченішими і призводять до все більш тяжких наслідків

Існує багато різного програмного захисту, наприклад фаєрволи, системи виявлення вторгнень, антивіруси і т. д., кожне з яких виконує певні функції і спрямоване на вирішення певних завдань. Однак ми можемо використовувати найкраще ПЗ, в якому застосовуються самі передові технології, криптостійкі алгоритми, але при цьому не можна бути впевненим на всі 100%, що наша система невразлива. Тому що в реалізації всіх рішень та застосування їх на практиці беруть участь люди, а людям властиво помилятися. Людина, будучи частиною системи, була і залишається найбільш вразливим місцем в системі безпеки.

Питання інформаційної безпеки на підприємствах було піднято не так давно. У 1983 році завод «АвтоВАЗ» був атакований хакерами. Це була одна з перших атак в Союзі, але найцікавіше в тому, що злочинець був співробітником заводу.

Навіть для зовнішніх атак в переважній більшості випадків зловмисники використовують інсайдерів - співробітників, які знають компанію зсередини. Ними маніпулюють за допомогою фішингу, шантажу, підкупу, соціальної інженерії. Кіберзлочинці поки не знайшли більш простого способу пробити захист підприємства, ніж використовувати конкретного користувача і атакувати конкретний ПК.

Одна з найнебезпечніших груп ризику - люди, які поділяють екстремістські, ортодоксальні переконання. Як правило, навіть «співчуваючі» серед співробітників - це ризик для роботодавця. Співробітник може поширювати свої переконання в колективі, зробити диверсію, стати інформатором для подільників за межами підприємства.

До інших груп ризику відносяться боржники, любителі азартних ігор, люди з серйозними захворюваннями. Звичайно, сам факт іпотеки у співробітника, любові до ігор або наявності серйозної хвороби - не привід для його звільнення. Це просто фактори, які роблять їх більш уразливими перед обличчям життєвих обставин: їх легше шантажувати, підкупити, ними простіше маніпулювати. Зазвичай таких співробітників просто беруть під більш пильний контроль.

Окрема категорія ризику - мстиві, схильні до саботажу співробітники. Ситуація ускладнюється, якщо така людина потрапляє під звільнення. Так сталося в 1992 році в нафтовій компанії Chevron. Звільнений співробітник відключив систему оповіщення фірми, зламавши комп'ютери в Нью-Йорку і Сан-Хосе, переналаштував їх. Вандалізм був виявлений, коли система не змогла використовуватися для повідомлення сусіднього міста про викид шкідливих речовин. Протягом десяти годин тисячі людей в 22 штатах і шести районах Канади піддалися ризику зараження.

Людський фактор з найбільшою ймовірністю проявляється при наступних умовах: недостатня оснащеність програмно-апаратними засобами, недолік фахівців інформаційної безпеки(ІБ), недостатньо високий професійний рівень фахівців ІБ і непоінформованість рядових співробітників і керівників компанії в сфері ІБ.

Програмно-апаратні засоби захисту інформації можна умовно розділити на кілька типів:

- антивірусне ПЗ,

- аналізатори трафіку,
- системи резервного копіювання,
- системи захисту інформації від несанкціонованого доступу, в тому числі засоби шифрування,
- системи розмежування доступу і авторизації.

Кожен тип з перерахованих відповідає за своє коло завдань, вимагає відповідної настройки і інтеграції в загальну інфраструктуру підприємства. Реалізувати глобальне завдання з вибудовування програмно-апаратної частини ІБ корпорації під силу спеціалізованим компаніям.

Найкращий ефект досягається за рахунок поєднання програмних рішень для запобігання інцидентів безпеки, тому що інакше тримати під контролем складну розподілену структуру майже неможливо.

Для вирішення комплексу ІБ-задач необхідно:

1. Контролювати місця зберігання і маршрути руху інформації по всіх каналах зв'язку, які використовуються в компанії (пошта, Skype, месенджери, форуми, хмарні сховища та ін.)
2. Виявляти дані в мережі підприємства в будь-який момент часу. Аналізувати дані будь-якого формату: текстового, графічного, аудіо.
3. Фіксувати дії співробітників, їх активність на підприємстві, за робочими ПК і поведінку в колективі.
4. Відстежування небезпечних рис характеру. Як правило, фахівці з безпеки роблять це «вручну», що вкрай важко на величезних підприємствах. Але на ринку з'являються IT-рішення, які дозволяють автоматизувати цю роботу. Це робить автоматизований профайлинг, наприклад. Він показує цінності і характер людини, схильності до авантюризму, наприклад, демонструє в динаміці, якщо в особистостях людини відбуваються значні зміни.

Список використаних джерел

1. Роль людського чинника у питаннях захисту інформаційних систем [Електронний ресурс] 2. Режим доступу до ресурсу: http://www.vestipb.ru/articles8561.html

3. Роль людського фактора {Електронний ресурс} – Режим доступу до ресурсу: http://softline.rbc.ru/page/rol-chelovecheskogo-faktora/

4. Людський фактор та інформаційна безпека підприємства {Електронний ресурс] – Режим доступу до ресурсу: http://softline.rbc.ru/page/rol-chelovecheskogo-faktora/

УДК 004.855.5

МЕТОДИКА ПРОТИДІЙ СИНТЕЗУ ЗОБРАЖЕННЯ, ЗАСНОВАНА НА ШТУЧНОМУ ІНТЕЛЕКТІ (DEEPFAKE)

Чулінда О. С., здобувач вищої освіти, гр. МКБп-201
Науковий керівник: **Ткач Ю. М.**, д.пед.н., проф.
Національний університет «Чернігівська політехніка»

На даний момент в мережі настає велика проблема підробки відео, тобто підставлення або анімація обличчя людини. Це здійснюється за допомогою штучного інтелекту. Також за допомогою штучного інтелекту обробляються і підміняються не лише відео файли а і фотографії, на яких звичайна людина не може розпізнати підробку.

Методика синтезу зображення або ще називають діпфейки (deepfake), заснована на штучному інтелекті, використовується для з'єднання і накладення існуючих зображень і відео на вихідні зображення або відеоролики[4]. Що може призвести до шантажу або розповсюдженні злоякісної інформації від людини яка не подавала цю інформацію.