ЗАБЕЗПЕЧЕННЯ ПРОМИСЛОВОЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СУЧАСНОМУ СВІТІ

Тригуб О. М.
Науковий керівник – ст. викл. Хондак І. І.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки, 14, каф. Охорони праці)
E-mail: olha.tryhub@nure.ua

Nowadays, information security is an important problem for all firms or campaigns. As the dynamics of the growth of the number of cyberattacks is growing rapidly, it is necessary to ensure the necessary protection of internal data. However, most firms prefer to save on the protection of their information space, which is why they are becoming victims of hackers. Therefore, it is very important not to delay and pay attention to the protection of information security, because the damage after a cyberattack can be more serious than the cost of protection.

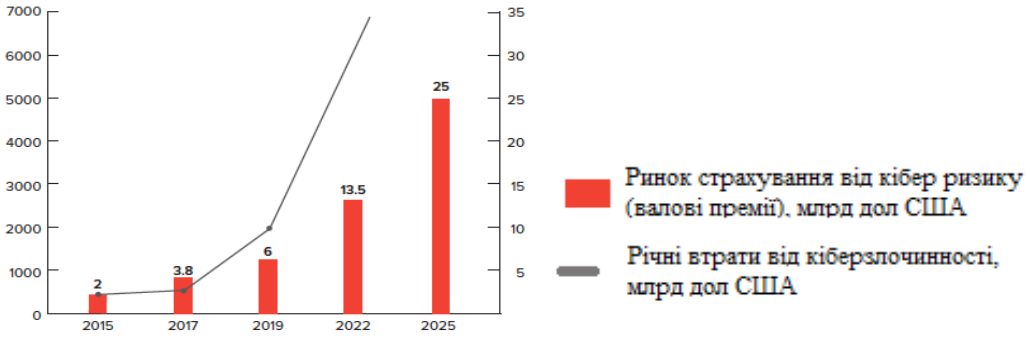
У зв'язку з розвитком виробництва ускладнюються і завдання забезпечення промислової безпеки. Це пов'язано з впровадженням у виробництво нових технологій і матеріалів, ускладненням технологічного процесу, збільшенням інформаційного навантаження. Відповідно і все більша кількість даних переноситься з паперового в електронний вигляд. Але в цей же час хакери можуть спробувати отримати доступ до них.

Наочним прикладом останнього, є атака українських підприємств вірусом «Petya.A». В результаті цих дій була заблокована діяльність багатьох підприємств, в які входять наступні: аеропорт «Бориспіль», ЧАЕС, Укртелеком, Укрпошта, Ощадбанк, Укрзалізниця. Атакам також піддалися сайт Кабінету Міністрів України, телеканал «Інтер», медіахолдинг ТРК «Люкс», різні інтернет-видання, а також сайти Львівської міської ради , Київської міської державної адміністрації та Служби спецзв'язку України. Після чого, влітку 2017 року, економіка України зазнала збитків в 0,4-0,5% річного ВВП. Внаслідок подібних дій людина може зазнати різного виду шкоди. Через вторгнення вірусом «Petya.A» в систему Ощадбанку, підприємство запрацювало у звичному режимі лише через тиждень. Під час атаки вірусом та її наслідків велика кількість транзакцій Ощадбанку не були завершені. Тобто достатній обсяг грошей просто зник з рахунків відправників і не перевівся на рахунки отримувачів. Другим вірусом по серйозності збитків є вірус «WannaCry». «Поки не зрозуміло скільки комп’ютерів було уражено, але, наприклад, збитки від WannaCry склав привлизно 4 млрд. дол.» – таким був коментар радіостанції Voice of America в перші дні після страту роботи «WannaCry».

Також кібератаки проводяться з метою отримання конфіденціальної інформації. У подальшому хакери можуть шантажувати розповсюдженням серед ваших друзів і родичів таких данних, яких би їм не варто було б зна-

ти. Подібні дії завдадуть неабиякої моральної шкоди. Проте, може бути й інший варіант. Якщо хакери розкриють якусь суперсекретну інформацію суперсектетної державної служби всьому світу, може розпчатися паніка серед населення. У цьому випадку наслідки схожі, але вже більш глобальні. З цього можна зробити висновок, що віруси завдають величезної матеріальної і моральної шкоди як працівникам так і їх клієнтам. Внаслідок страждає репутація цих підприємств.

Деякі кампанії, фірми чи підприємства намагаються отримати якомога більший прибуток і тому економлять на витратах на оновлення обладнання, на захист свого кібепростору. Важливо провести професійну оцінку вашої системи з точки зору потенційно уразливих місць, а потім розробити і впровадити безпечну мережеву архітектуру. Установка засобів безпеки на нижні рівні мережевий архітектури дозволить запобігти обмін шкідливими даними між пристроями і забезпечить захист від випадкових конфігурацій обладнання. Сьогодні більш, ніж коли-небудь, необхідно пам'ятати про подібні загрози кібератак, яким піддається ваше виробництво. Нижче наведена діаграма зі статті «Як компанії страхують кіберризики в україні»[1], де показана динаміка зростання кіберстрахуванння і кіберзлочинності у світі вцілому.



Як видно зі схеми, хоч розвиток кіберзлочинності і не стоїть на місці, але, за прогнозами експертів, збиток після атак з роками буде все більше якщо підприємства будуть недоооцінювати хакерів. Для захисту застарілого обладнання і результативної боротьби з внутрішніми і зовнішніми загрозами сьогодні життєво необхідна ефективна стратегія забезпечення безпеки, що включає роботу сучасних захисних засобів.

Список використаних джерел

1. Как компании страхуют киберриски в Украине [Електронний ресурс] – Режим доступа: https://delo.ua/special/kak-kompanii-strahujut-kiber-riski-v-ukraine-346724/ (дата звернення 22.02.19).

2. Пономаренко Д.В., Лесных В.В., Бочков А.В. Современные подходы к мониторингу состояния промышленной безопасности опасных производственных объектов.