Гончаров С.В., Зборовська Т. В.

Національний фармацевтичний університет, м. Харків

Актуальність побудови інформаційної безпеки в діяльності організацій

t.v.zborovska@gmail.com

Вступ. Для України та всього світу 2023 рік видався важким у багатьох сенсах – зокрема й для глобальної кібербезпеки. Частота та винахідливість кібератак на бізнес, ланцюжки постачання та державні установи постійно зростає. За оцінками IBM, кожен витік даних наносить понад 4,3 млн доларів збитків й потребує щонайменше 200 днів на виявлення й ліквідацію наслідків. Постає питання як забезпечити безпеку у нестабільному цифровому світі? Це питання актуальне, не тільки для великого бізнесу з промисловим виробництвом, але й для навчальних закладів, оскільки вони містять багато інформації про особисті дані здобувачів та педагогічного персоналу. Щоб захиститися, потрібно розглядати умови виконання кроків захисту. Для їх розробки організації широко застосовують принципи та рекомендації, що містить стандарт ISO/IEC 27001.

Мета дослідження. За мету наших досліджень ми беремо визначення сучасних тенденцій щодо світової практики розробки схеми впровадження системи менеджменту інформаційної безпеки в організаціях.

Матеріали та методи. В досліджені ми використовуємо інформаційний метод дослідження літератури та Інтернет-ресурсів.

Отримані результати. Всесвітній економічний форум вніс кіберзлочинність до топ-10 найсерйозніших глобальних ризиків найближчого десятиліття. Свідчення тривожних тенденції можна представити наступним чином: за звітом SonicWall цього року загальна кількість кібератак зросла на 2% у порівнянні з 2022 роком – зафіксовано близько 5,5 млрд епізодів. Контролювати кіберзлочинність дуже важко. Експерти вважають, що глобально в поле зору правоохоронців потрапляють менш ніж 25% від усіх скоєних кіберзлочинів. Ступінь ризиків суттєво виросла через стійкий тренд на

віддалену працю та важке геополітичне середовище, де кібератаки стають важелем економічного і політичного впливу. У світі шириться принцип нульової довіри, який стає фундаментом безпеки у непередбачуваному цифровому середовищі. Його суть полягає в тому, що в організацій більше немає внутрішнього периметра, який можна вважати безпечним. Кожен користувач, кожен процес і кожен пристрій у системі мають ретельно перевірятися. Права доступу до даних слід обмежувати настільки, наскільки це можливо. Тому навчальні заклади також мають його дотримуватися.

На основі проведених досліджень ми пропонуємо універсальну схему реагування на кіберзагрози в першу чергу вірусні атаки в організації (Рис.1).

Рис. 1. Схема реагування на кіберзагрози.

Висновки. Сучасний кіберпростір не можна назвати безпечним місцем, тому ідея нульової довіри актуальна як ніколи. Адже сьогодні корпоративні диджитал-екосистеми виходять далеко за межі власної мережі, охоплюючи віддалену (дистанційну) роботу, партнерські організації та пристрої безконтактного Інтернет зв’язку. Однак використання сучасних технологій та безпекових практик допомагає мінімізувати ризики.