УДК 004.056.53
Зайко Т.А.[1], Колесникова М.В.[2]
[1]канд. техн. наук, доц. НУ «Запорізька Політехніка»
[2]студ. гр. КНТ-128 НУ «Запорізька Політехніка»

МІЖНАРОДНІ СТАНДАРТИ КІБЕРБЕЗПЕКИ

У сьогоденні, як ніколи швидко розвиваються всі сфери життя людини. Основними напрямками такої еволюції побуту є автоматизація та діджиталізація. Як результат – виникнення нової сучасної проблеми – кіберзлочинності. Уряд, бізнес, та пересічні громадяни потребують захисту пристроїв, програм, особистої та комерційної інформації від шкідливого втручання ззовні. З цього постає необхідність прийняття заходів, щодо захисту мереж, систем, пристроїв та даних, попередження та відбиття кібер-атак. Цим і займається кібербезпека.

Зважаючи на еволюцію кіберзагроз, що можуть катастрофічно вплинути на важливу інфраструктуру держави, спеціалісти з питань безпеки були змушені звернутися до стандартів заснованих на ризиках. Достовірність оцінки ризиків залежить від кількісного аналізу загроз, вразливостей і їх наслідків, що передбачає збір і вивчення величезних обсягів інформації. Цей процес є вартісним, трудомістким і тривалим. Через це, організації не займаються власною розробкою, а спираються у своїй стратегії та політиці безпеки на існуючі міжнародні стандарти кібербезпеки.

Стандарти кібербезпеки - це твердження, які описують, що має бути досягнуто з точки зору результатів безпеки, щоб виконати заявлені цілі безпеки підприємства. Зараз у світі існує безліч стандартів, якими користуються різні провідні країни, наступні з них є найбільш поширеними на міжнародному рівні:

Сімейство стандартів ISO 27000. Набір стандартів безпеки, випущених Міжнародною організацією зі стандартизації (ISO), які набули широкого поширення у всьому світі. Вони включають у себе документи: ISO/IEC 27001 – вимоги до систем менеджменту інформаційної безпеки (СМІБ); ISO/IEC 27000 – огляд та словник термінів, що стосуються СМІБ; ISO/IEC 27003 та

ISO/IEC 27004 – керівництво та вимірювання ефективності СМІБ; ISO/IEC 27006 – вимоги до органів, що здійснюють аудитів та сертифікацію, ISO/IEC 27007 – керівництво до проведення аудиту СМІБ.

Існують також інші стандарти ISO: ISO/IEC 27032 до: 2012 – інформаційні технології та методи безпеки, настанови щодо кібербезпеки; ISO/IEC 15408 - інформаційні технології та методи безпеки, критерії оцінки IT-безпеки; ISO 22301 – вимоги до соціальної безпеки та системи менеджменту безперервності бізнесу; ISO/IEC 27035 – інформаційні технології та методи безпеки, управління інцидентами інформаційної безпеки та ін.

NIST SP 800 розроблено для задоволення і підтримки вимог безпеки і конфіденційності інформації та інформаційних систем уряду США та Канади. Ці стандарти налічують 800 публікацій, що містять керівництва та довідкову інформацію на безліч різних тем, наприклад: SP 800-184 – посібник з відновлення подій кібербезпеки, SP 800-53 Rev. 5 контроль безпеки та конфіденційності для інформаційних систем та організацій, SP 800-40 – керування вразливостями, SP 800-81-2 посібник із розгортання системи безпечних доменних імен (DNS). Всі статті є у вільному доступі на сайті організації NIST.

Британський стандарт BS 7799 регламентує управління інформаційною безпекою організації незалежно від сфери її діяльності. На його основі було розроблено міжнародний стандарт ISO/IEC 17799 проте його початковим виданням і досі керуються у 27 країнах світу.

ISA/IEC 62443 стандарт з кібербезпеки, що розроблений як національний стандарт США, проте поширений і у країнах Європейського союзу. Визначає вимоги до захисту промислових автоматизованих систем керування.

General Data Protection Regulation (GDPR) - обов'язкові законодавчі норми, що базуються на конфіденційності для підприємств, які обробляють або контролюють приватні персональні дані, що належать громадянам ЄС.

PCI DSS – це стандарт безпеки даних платіжних карток. Він є обов’язковим для більшості підприємств, які збирають, обробляють та зберігають дані платіжних карток, таких як Visa чи Mastercard.

Деякі цих стандартів регулюються законодавчими органами (GDPR, PCI DSS), а деякі носять рекомендативний характер. Проте, якщо організація розгортає діяльність на міжнародному рівні, дотримання стандартів кібербезпеки є обов’язковою умовою співпраці багатьох провідних країн світу.

Отже, використання стандартів кібербезпеки є невід’ємною частиною політики безпеки підприємств критичної інфраструктури. Але незважаючи на різноманіття стандартів, необхідно вибирати найостанніші, ті, що

повністю задовольняють вимогам до безпеки і конфіденційності конкретної організації. Основними мірами підтримки захищеності є дотримання, регулярне вимірювання ефективності прийнятих стандартів та впровадження нових. Така стратегія призведе не лише до зменшення ризиків зовнішнього втручання, а й до збільшення довіри зацікавлених сторін, а отже й принесе нові інвестиції.