Додаток 3
до Методичних рекомендацій щодо
здійснення базових заходів кіберзахисту
(пункт 7 розділу III)

Приклад опису рекомендованих базових кроків для створення переліку кіберризиків

Для формування переліку кіберризиків, як правило, враховують таксономію кіберінцидентів, а також ризики, які можуть мати місце та визначені оператором об’єкта критичної інфраструктури або іншим власником об’єкта кіберзахисту. Приклад таких ризиків для кібербезпеки може містити:

1. Ризики, пов’язані з хмарними сервісами:
   - неправильна конфігурація хмарних ресурсів;
   - витік даних через хмарні сервіси;
   - залежність від постачальників хмарних послуг.
2. Ризики, пов’язані з Інтернетом речей (IoT):
   - вразливості в IoT-пристроях;
   - недостатній захист даних, що передаються через IoT.
3. Ризики, пов’язані з мобільними пристроями:
   - втрата або крадіжка мобільних пристроїв;
   - вразливості мобільних додатків.
4. Ризики, пов’язані із соціальними мережами:
   - витік конфіденційної інформації через соціальні мережі;
   - фішинг через соціальні мережі.
5. Ризики, пов’язані з постачальниками та партнерами:
   - вразливості в системах постачальників;
   - недостатній контроль безпеки у партнерів.
6. Ризики, пов’язані з новими технологіями:
   - вразливості в блокчейн-технологіях;
   - ризики, пов’язані з використанням штучного інтелекту.

7. Ризики, пов’язані з регуляторними змінами:
   - невідповідність новим вимогам законодавства;
   - штрафи та санкції за порушення регуляторних норм.
8. Ризики, пов’язані з людським фактором:
   - недостатня обізнаність співробітників щодо кібербезпеки;
   - інсайдерські загрози.
9. Ризики, пов’язані з фізичною безпекою:
   - несанкціонований доступ до серверних приміщень;
   - крадіжка обладнання.

Врахування цих ризиків допоможе забезпечити більш комплексний підхід до кібербезпеки об’єкта критичної інфраструктури або іншого об’єкта кіберзахисту.

Щоб зіставити кіберризики з допустимим рівнем ризику та залишеним ризиком, можна скористатися такими кроками:

1. Визначення допустимого рівня ризику:
   допустимий рівень ризику – рівень ризику, який організація готова прийняти для досягнення своїх цілей. Визначте, які ризики є прийнятними, а які – ні. Це може бути зроблено через консультації з керівництвом та заінтересованими сторонами.

2. Оцінка ризиків:
   використовуйте реєстр кіберризиків для оцінки ймовірності та впливу кожного ризику. Це допоможе зрозуміти, які ризики є найбільш критичними для об’єкта кіберзахисту.

3. Зіставлення з допустимим рівнем ризику:
   порівняйте оцінені ризики з допустимим рівнем ризику. Якщо ризик перевищує прийнятний рівень, необхідно вжити заходів для його зниження.

4. Розробка планів реагування:
   для ризиків, які перевищують допустимий рівень ризику, розробіть плани реагування. Це можуть бути заходи з пом’якшення, уникнення, передачі або прийняття ризику.

5. Оцінка залишеного ризику:
   залишений ризик – ризик, який залишається після впровадження заходів з пом'якшення. Оцініть, чи відповідає залишений ризик допустимому рівню ризику організації. Якщо залишений ризик все ще перевищує прийнятний рівень, необхідно переглянути та посилити заходи з пом'якшення.

6. Моніторинг та перегляд:
   регулярно переглядайте та оновлюйте реєстр ризиків, допустимий рівень ризику та залишений ризик. Це допоможе забезпечити актуальність та ефективність заходів з управління ризиками.

Приклад таблиці для зіставлення ризиків з допустимим рівнем та залишеним ризиком:

Ризик	Ймовірність	Вплив	Допустимий рівень ризику	Залишений ризик	Заходи щодо зниження ризику
1	2	3	4	5	6
Шпигунське та шкідливе ПЗ	Висока	Високий	Середній	Низький	Регулярне оновлення антивірусного ПЗ, резервне копіювання даних, навчання персоналу
Фішинг	Висока	Середній	Середній	Низький	Навчання співробітників, впровадження багатофакторної автентифікації
Атаки на кінцеві точки	Середня	Високий	Середній	Низький	Використання EDR (Endpoint Detection and Response), політика BYOD (Bring Your Own Device)
Витік даних	Низька	Високий	Низький	Низький	Шифрування даних, контроль доступу, регулярні аудити безпеки
DDoS атаки	Середня	Середній	Середній	Низький	Використання захисту від DDoS, резервні канали зв'язку
Вразливості в ПЗ	Середня	Високий	Середній	Низький	Регулярне оновлення ПЗ, проведення тестування на проникнення.

Продовження додатка 3

1	2	3	4	5	6
Соціальна інженерія	Висока	Середній	Середній	Низький	Навчання співробітників, впровадження політики безпеки інформації
Ненадійні постачальники	Низька	Середній	Низький	Низький	Оцінка постачальників, укладання договорів з вимогами до безпеки
Втрати пристроїв	Низька	Середній	Низький	Низький	Використання шифрування, віддалене блокування пристроїв
Інсайдерські загрози	Низька	Високий	Низький	Низький	Контроль доступу, моніторинг активності, навчання персоналу
Неправильна конфігурація хмарних ресурсів	Середня	Високий	Середній	Низький	Регулярні аудити конфігурацій, навчання персоналу
Витік даних через хмарні сервіси	Середня	Високий	Середній	Низький	Шифрування даних, контроль доступу
Залежність від постачальників хмарних послуг	Низька	Середній	Низький	Низький	Оцінка постачальників, резервні плани
Вразливості в IoT-пристроях	Середня	Високий	Середній	Низький	Регулярне оновлення ПЗ, контроль доступу
Недостатній захист даних в IoT	Середня	Високий	Середній	Низький	Шифрування даних, контроль доступу
Втрата або крадіжка мобільних пристроїв	Середня	Середній	Середній	Низький	Використання шифрування, віддалене блокування пристроїв
Вразливості мобільних додатків	Середня	Високий	Середній	Низький	Регулярне оновлення ПЗ, тестування на проникнення

Продовження додатка 3

1	2	3	4	5	6
Витік конфіденційної інформації через соціальні мережі	Висока	Середній	Середній	Низький	Навчання співробітників, контроль доступу
Фішинг через соціальні мережі	Висока	Середній	Середній	Низький	Навчання співробітників, впровадження багатофакторної автентифікації
Вразливості в системах постачальників	Середня	Високий	Середній	Низький	Оцінка постачальників, укладання договорів з вимогами до безпеки
Недостатній контроль безпеки у партнерів	Середня	Високий	Середній	Низький	Оцінка партнерів, укладання договорів з вимогами до безпеки
Вразливості в блокчейн-технологіях	Низька	Високий	Середній	Низький	Регулярне тестування на проникнення, оновлення ПЗ
Ризики, пов’язані з використанням штучного інтелекту	Середня	Високий	Середній	Низький	Оцінка ризиків, впровадження заходів безпеки
Невідповідність новим вимогам законодавства	Середня	Високий	Середній	Низький	Регулярний моніторинг законодавства, навчання персоналу
Штрафи та санкції за порушення регуляторних норм	Низька	Високий	Середній	Низький	Впровадження заходів відповідності, регулярні аудити
Недостатня обізнаність співробітників щодо кібербезпеки	Висока	Середній	Середній	Низький	Навчання співробітників, регулярні тренінги
Інсайдерські загрози	Низька	Високий	Низький	Низький	Контроль доступу, моніторинг активності, навчання персоналу

Продовження додатка 3

1	2	3	4	5	6
Несанкціонований доступ до серверних приміщень	Низька	Високий	Низький	Низький	Фізична охорона, контроль доступу
Крадіжка обладнання	Низька	Середній	Низький	Низький	Використання шифрування, фізична охорона