цінностей Українського народу; розвиток медіа-культури суспільства і соціально відповідальної медіа-середовища; формування ефективної правової системи захисту особистості, суспільства і держави від деструктивних пропагандистських впливів; створення на базі норм міжнародного права системи і механізмів захисту від негативних зовнішніх впливів, перш за все, пропаганди; розвиток інформаційного суспільства [4, с.9].

1. Боднар І.Р. Інформаційна безпека як основа національної безпеки [Електронний ресурс].– Режим доступу: https://core.ac.uk/download/pdf/141443493.pdf

2. Закон України. Про інформацію / [Електронний ресурс].– Режим доступу: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2657-12.

3. Залєвська І. І., Удренас Г. І. Інформаційна безпека України в умовах російської військової агресії [Електронний ресурс].– Режим доступу: http://www.sulj.oduvs.od.ua/archive/2022/1-2/6.pdf

4. Панченко О. Інформаційна складова національної безпеки [Електронний ресурс]. – Режим доступу: https://www.rdc.org.ua/download/stati/Informational-warehouse.pdf

5. Почепцов, Г. Інформаційна політика: навч. посібник [Текст] / Г. Г. Почепцов. – К.: Знання, 2006. – 663 с.

6. Супрун, В. М. Інформаційний суверенітет як один з елементів інформаційної безпеки держави: І. Р. Боднар. Інформаційна безпека як основа національної безпеки Механізм регулювання економіки, 2014, № 1 теоретико-правовий аспект [Електронний ресурс]. – Режим доступу : http://www.nbuv.gov.ua/portal/natural/vkhnu/Pravo/2009 .

7. Ярочкін, В. Система безпеки фірми [Електронний ресурс]. – Режим доступу : http://www.nbuv.gov.ua.

8. Скиба, Е. Роль філософії права в формуванні свідомості суспільства сучасної формації. Науково-теоретичний альманах Грані, 2020. *23*(5), 64-76. https://doi.org/10.15421/172054

УДК 004+351
DOI: 10.31733/17-03-2023-578-579

Ілля ЖЕЛНОВАЧ
курсант факультету №4
Харківського національного
університету внутрішніх справ

СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Інформація, а також процеси, системи та мережі, які її обробляють, є важливими активами кожної організації, як у державному, так і в приватному секторі. Інформаційна безпека має гарантувати конфіденційність, цілісність і доступність інформації та систем, які її обробляють.

Система управління інформаційною безпекою включає в себе необхідну організаційну структуру (ролі та комітети) та процедурну організацію (процеси безпеки), а також необхідні інструкції (процедури та правила). постійно визначати, управляти, контролювати, підтримувати та покращувати інформаційну безпеку в організації на основі підходу до управління ризиками.

Управління інформаційною безпекою - це безперервний процес, стратегії та концепції якого повинні постійно переглядатися на предмет їх ефективності та результативності, а також оновлюватися за необхідності [1].

Хоча СУІБ призначена для створення цілісної системи управління інформаційною безпекою, цифрова трансформація вимагає від організацій постійного вдосконалення та розвитку їхніх політик безпеки та засобів контролю. Структура та межі, визначені СУІБ, можуть застосовуватися лише протягом обмеженого періоду часу, і на початкових етапах співробітникам може бути складно прийняти їх. Завдання організацій полягає в тому, щоб розвивати ці механізми контролю безпеки в міру того, як змінюються їхні ризики, культура та ресурси.

Стратегія управління інформаційною безпекою організації може бути зумовлена багатьма різними факторами. Програма може бути натхненна внутрішньою політикою або вимагатися зовнішніми силами. Обидва ці потенційні чинники мають відповідні стандарти та вимоги до дотримання.

У деяких випадках внутрішні політики безпеки та бізнес-цілі організації можуть

вимагати впровадження систем управління інформаційною безпекою. Наприклад, ISO 27001, міжнародний стандарт, що описує найкращі практики безпеки, вимагає впровадження системи управління інформаційною безпекою. Компанії, які хочуть пройти сертифікацію на відповідність стандарту ISO 27001, повинні його впровадити. Програма управління безпекою організації також може бути зумовлена зовнішніми факторами. Наприклад, багато організацій працюють відповідно до одного або декількох нормативних актів про захист даних інформації на всіх рівнях організації. Така архітектура повинна включати в себе різні складові, такі як технічні заходи, політики та процедури, навчання та свідомості працівників і т.п. Консолідована архітектура безпеки також дозволяє зменшити дублювання заходів та забезпечити єдиний підхід до управління безпекою інформації в організації [2].

Для ефективного моніторингу та управління безпекою інформації важливо розробити процеси та процедури, які дозволяють ідентифікувати та аналізувати ризики, приймати рішення щодо їхнього зниження або усунення, а також реагувати на інциденти безпеки. Для цього можуть використовуватися різні інструменти, такі як системи управління інформаційною безпекою, системи моніторингу та аналізу журналів подій, системи контролю доступу та інші.

Найважливішим елементом впровадження консолідованої архітектури безпеки є залучення всіх працівників організації до процесу управління безпекою інформації. Це можна здійснити шляхом навчання працівників правилам безпеки, проведення свідомості про безпеку, включення їх у процеси аудиту та відстеження виконання правил безпеки. Такий підхід допоможе забезпечити високий рівень безпеки інформації в організації та знизити ризики її втрати або пошкодження.

Крім того, для успішного впровадження консолідованої архітектури безпеки необхідно розробляти та виконувати регулярні оцінки ризиків, щоб ідентифікувати потенційні загрози та оцінювати їх вплив на бізнес-процеси. Ці оцінки допоможуть визначити пріоритетні напрямки розвитку безпеки інформації та визначити необхідні ресурси для їх впровадження.

Також, управління безпекою інформації повинно бути вбудоване в бізнес-процеси організації, щоб забезпечити максимальну ефективність та ефективність заходів безпеки. Це означає, що безпека інформації повинна бути врахована при плануванні бізнес-процесів, розробці нових продуктів та послуг, прийнятті рішень про інвестиції

Важливо також забезпечити постійний моніторинг та аналіз ефективності заходів безпеки, щоб вчасно виявляти та усувати можливі вразливості. Це допоможе забезпечити стабільність та безпеку інформаційних систем організації на довгострокову перспективу

Висновки: консолідована архітектура безпеки та інтегрована стратегія безпеки дозволяють забезпечити ефективне управління безпекою інформації в організації та захистити її від потенційних загроз. Для досягнення цієї мети необхідно залучити всіх працівників організації та впроваджувати регулярні оцінки ризиків, забезпечити постійний моніторинг.

---

1 Informationssicherheits-Managementsystem (ISMS) aufbauen und steuern // вебсайт. URL: https://www.uimc.de/leistungen/informationssicherheit/aufbau-eines-isms (дата звернення: 24.02.2023).

2. The Importance of Information Security Management // вебсайт. URL: https://www.checkpoint.com/cyber-hub/network-security/what-is-security-management/what-is-information-security-management/ (дата звернення: 25.02.2023).