к.т.н. Козубцова Л.М.

Військовий інститут телекомунікацій та інформатизації імені Героїв Крут

Обґрунтування структури методики планування заходів кібербезпеки об'єктів критичної інформаційної інфраструктури організації

Постановка завдання. Кібернетична безпека (кібербезпека) – стан захищеності критичних об'єктів національної інформаційної інфраструктури та окремих її складових, за якого забезпечується їх стале функціонування і розвиток, своєчасне виявлення, запобігання і нейтралізація кібернетичних загроз в інтересах людини, суспільства, держави. На підставі положень Стратегії національної безпеки України, Воєнної доктрини України та Концепції розвитку сектору безпеки і оборони України визначено оперативну ціль «1.5. Удосконалення системи кібербезпеки та захисту інформації» [1, с. 33], Закону України "Про основні засади забезпечення кібербезпеки України" [2]; Стратегії кібербезпеки України [3]; Рішення Ради національної безпеки і оборони України від 10.07.17 "Про стан виконання рішення Ради національної безпеки і оборони України від 29 грудня 2016 року" "Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації" [4] встановлено, що на даний час, на існуючих об'єктах критичної інфраструктури (ОКІІ) організацій відсутня методика планування заходів забезпечення їх кібербезпеки. Тому, на підставі [1-4] виникає об'єктивне наукове завдання щодо необхідності обґрунтування методики планування заходів забезпечення кібербезпеки об'єктів критичної інфраструктури організацій.

Мета доповіді. Апробувати структуру методики планування заходів, забезпечення кібербезпеки ОКІІ організацій на основі удосконалення NIST Special Publication 800-53 Revision 4 шляхом корегування та доповнення окремих етапів.

Результат дослідження. Розглянем ключові методології планування. На рис. 1 наведено структуру процесів забезпечення кібербезпеки за так званою схемою PDCA (Plan, Do, Chek, Akt), тобто (Планування заходів з безпеки, Впровадження заходів, Перевірка їх ефективності, Покращення заходів). Циклічність повторюється як (1+N), тобто як бачимо, забезпечення та управління кібербезпекою є безперервним циклічним процесом.

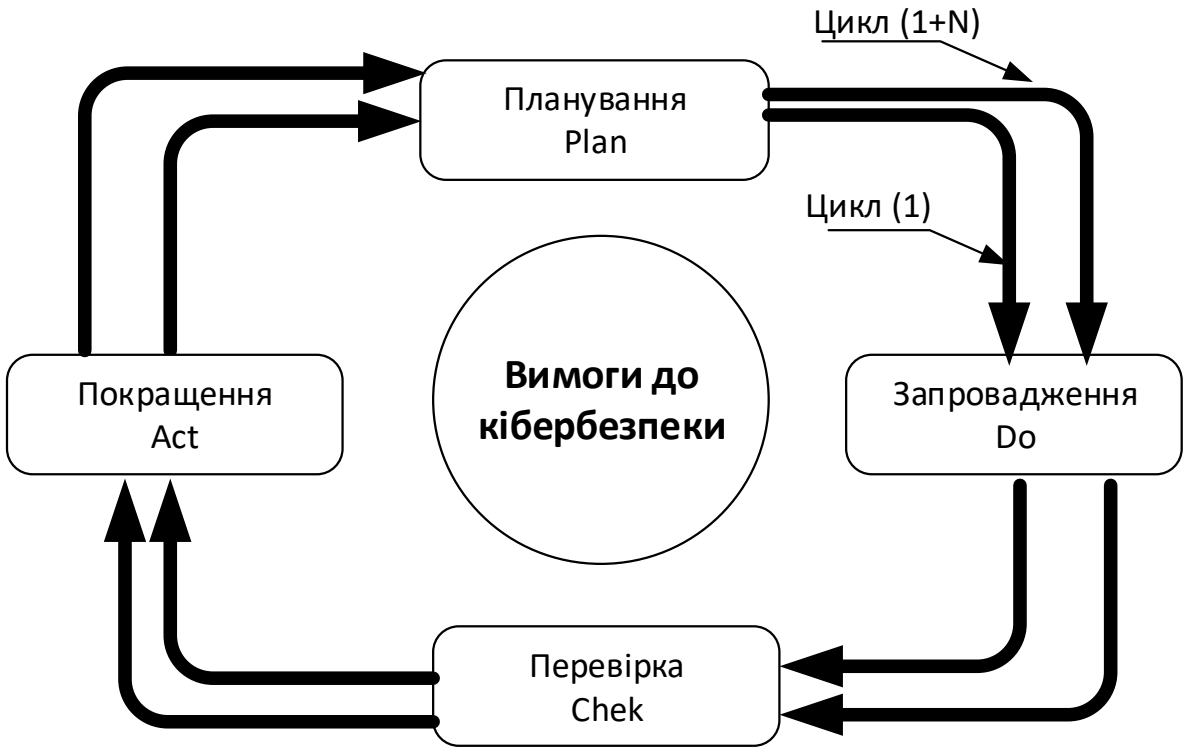

Рис. 1. Структура процесів забезпечення кібербезпеки за схемою PDCA

Перевагами процесного підходу є простота і прозорість, ефективне використання ресурсів, єдине розуміння на всіх рівнях. Недоліки ж пов'язані з труднощами впровадження цього підходу, із складністю визначення чіткої інтеграції процесів в єдину систему з-за значної їх кількості, проблематичністю дотримання інтересів всіх учасників ланцюжка процесів, різними тлумаченнями й розумінням стандарту у різних консультантів (експертів).

Досвід вказує, що процесний підхід «запрацює» тільки в умовах створення системи збалансованих показників в галузі безпеки. Але це дуже не просто, особливо з огляду на те, що система управління (менеджменту) інформаційної безпеки поки знаходиться більше в області теорії й концепції, а не успішної

практики.

Тому у відповідності до постановки завдання, методика планування заходів кібербезпеки ОКІІ організацій включає наступні фази та етапи:

Фаза 1 Планування заходів забезпечення кібербезпеки ОКІІ організації.

Етап 1 З'ясування предмета та об'єкту планування.

Етап 2 Вибір конкретної організації, як об'єкту дослідження, з подальшим для якого формуватиметься матриця заходів забезпечення кібербезпеки.

Етап 3 З'ясування, які саме ОКІІ є у розпорядженні (на балансі) обраної організації.

Етап 4 Реалізація заходів з категоріювання та декомпозиції ОКІІ організації на компоненти, які вразливі до ДІВ.

Етап 5 Формування комплексу заходів, спрямованих на забезпечення кібербезпеки ОКІІ організації.

Фаза 2 Впровадження заходів кібербезпеки ОКІІ організації.

Етап 6 Реалізація відібраних заходів забезпечення кібербезпеки ОКІІ організації.

Етап 7 Складання акту (доповіді) щодо реалізованих заходів, спрямованих на забезпечення кібербезпеки ОКІІ організації станом на момент часу T_0.

Фаза 3 Перевірка (аудит) заходів забезпечення кібербезпеки ОКІІ організації.

Етап 8 Аудиторська перевірка рівня досягнення реалізованості заходів, спрямованих на забезпечення кібербезпеки ОКІІ організації

Етап 8.1 Аудиторська перевірка рівня досягнення реалізованості заходів, спрямованих на забезпечення кібербезпеки ОКІІ організації по контрольному вибірковому або по всім заходам станом на момент часу $T_{пер.(пас)}$.

Етап 8.2 Аудиторська перевірка рівня досягнення реалізованості заходів, спрямованих на забезпечення кібербезпеки ОКІІ організації із застосуванням активного кібервпливу станом на момент часу $T_{пер.(актив)}$.

Етап 9 Оцінювання ефективності виконання заходів, спрямованих на забезпечення кібербезпеки ОКІІ організації.

Етап 10 Складання та надсилання аудиторського звіту зацікавленій стороні організації.

Фаза 4 Покращення заходів спрямованих на забезпечення кібербезпеки ОКІІ організації. Метою даної фази є посилення або зміни раніше обраних заходів кібербезпеки ОКІІ організації.

Етап 11 Перегляд обраних раніше заходів спрямованих на забезпечення кібербезпеки ОКІІ організації. Посиленні вимог.

В дійсному досліджені пропонується до обговорення запропоноване рішення щодо надання подальшого розвитку структури методу моніторингу кіберстійкості інформаційної системи [5], окремі етапи методики аудиту інформаційної безпеки, які рекомендовані в NIST Special Publication 800-53 Revision 4 [6]. Слід відзначити, що в початковому вигляді [6] методика аудиту кібербезпеки інформаційної системи непридатна до рішення наукової задачі дослідження, оскільки вона не передбачає здійснювати прогнозування заходів спрямованих на забезпечення кібербезпеки ОКІІ організації. Тому в ході подальших досліджень нами переосмислено окремі кроки (етапи) існуючої методики [5].

Дійсне дисертаційне дослідження є самостійним логічним продовженням перспективного напрямку означеного в [5].

Висновки.

1. Вперше пропонується до обговорення формалізована структура методики планування заходів кібербезпеки на об’єктах критичної інформаційної інфраструктури організацій, на засадах циклічної моделі «plan-do-check-act».

2. Запропонована структура методики планування заходів забезпечення кібербезпеки на об’єктах критичної інформаційної інфраструктури організацій має логічну структура і забезпечуватиме єдиний підхід до планування заходів кібербезпеки.

3. Представлене дослідження не вичерпує всіх аспектів зазначеної проблеми. Теоретичні та практичні результати, що одержані в процесі

наукового пошуку, становлять підґрунтя для подальшого її вивчення в такому напрямі, як обґрунтування методики оцінювання ефективності реалізації заходів кібербезпеки ОКІІ організації.

Наукова новизна одержаного результату. Запропоновано подальше удосконалення NIST Special Publication 800-53 Revision 4 шляхом корегування та доповнення окремих етапів, що в сукупності дозволять вирішити науково-технічну задачу з планування заходів, спрямованих на забезпечення кібербезпеки на ОКІІ організацій.

Список використаних джерел

1. Петренко А.Г. План дій щодо впровадження оборонної реформи у 2016 – 2020 роках (дорожня карта оборонної реформи). Затверджено Міністром оборони України від 15.08.2016 р. К.: ДВПСП та МС МО України, 2016. 210 с.

2. Закон України “Про основні засади забезпечення кібербезпеки України”. URL: https://zakon.rada.gov.ua/laws/show/2163-19.

3. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року “Про Стратегію кібербезпеки України”, затверджена Указом Президента України від 15.03.16 № 96/2016. URL: https://zakon5.rada.gov.ua/laws/show/96/2016.

4. Рішення Ради національної безпеки і оборони України від 10.07.17 “Про стан виконання рішення Ради національної безпеки і оборони України від 29 грудня 2016 року” “Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації”, введеного в дію Указом Президента України від 13.02.17 №254/2017. URL: https://zakon.rada.gov.ua/laws/show/n0006525-17.

5. Козубцова Л.М. Удосконалення методів моніторингу кіберстійкості інформаційної системи спеціального призначення : дисертація кандидата технічних наук: 05.13.05 – “Комп’ютерні системи та компоненти” : Захищена 22.09.2020: Затв. 26.11.2020. К.: Відкритий міжнародний університет розвитку людини «Україна», 2020. 222 с.

6. NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems.