УДК 004.056:338
DOI https://doi.org/10.32782/2663-5941/2022.5/13

Карпович І.М.
Національний університет водного господарства та природокористування

Гладка О.М.
Національний університет водного господарства та природокористування

Калашніков В.І.
Національний університет водного господарства та природокористування

МОДЕЛЮВАННЯ ПРОЦЕСІВ АНАЛІЗУ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЯК СПОСІБ ОПТИМІЗАЦІЇ ВИТРАТ

Статтю присвячено дослідженню кібербезпеки інформаційних систем підприємств в енергетичному секторі. Сьогодні енергокомпанії централізовано через інформаційні системи здійснюють контроль і управління процесами виробництва, передачі та розподілу електроенергії. Розвиток технологій Smart Grid та розумного обліку ведуть до появи численних нових послуг та сервісів, у тому числі і шляхом залучення споживачів, що кардинально змінює архітектуру систем у бік розподіленої автоматизації та змінює принципи управління, доступу і використання інформаційних систем та породжує якісно нові загрози і ризики.

У роботі запропоновано методику графічного моделювання процесу оцінки ризиків кількісним та якісним методом з використанням діаграм діяльності та обчислення ймовірних втрат від реалізації загрози із врахуванням коефіцієнта руйнування. Для проведення аналізу ризиків необхідно: визначити список і цінність активів (ресурсів), що підлягають захисту; ідентифікувати список загроз інформаційній безпеці, актуальних для даної інформаційної системи; оцінити ймовірність реалізації загроз; визначити вразливість активів та розмір потенційних збитків; виконати оцінку ризиків; запропонувати рішення, яке забезпечує необхідний рівень інформаційної безпеки, забезпечити реалізацію і тестування обраних способів захисту та провести оцінку залишкового ризику.

Детально проаналізовано особливості зовнішніх і внутрішніх загроз та вразливостей об'єктів IT-інфраструктури в енергетичному секторі. Основними загрозами для інформаційних систем автоматизації та управління можна вважати: несанкціоноване використання точок доступу до дистанційного технічного обслуговування; мережеві атаки через корпоративну мережу; атаки на стандартні компоненти, що використовуються в мережі ICS; DDoS-атаки; людська помилка або саботаж; проникнення вірусу через знімний носій чи зовнішні пристрої; несанкціонований доступ до ресурсів; атаки на компоненти мережі; технічні збої або форс-мажор.

Узагальнено перелік заходів щодо управління IT-ризиками та способи планування, здійснення і контролю контрзаходів, спрямованих на захист інформаційних систем.

Ключові слова: *аналіз ризику, інформаційна безпека, загрози, мінімізація ризиків, кібербезпека.*

Постановка проблеми. Поняття ризику є ключовим поняттям у сфері безпеки взагалі та інформаційної безпеки (ІБ) зокрема [1]. Ризик інформаційної безпеки, з одного боку, об'єднує спектр питань, пов'язаних із загрозами безпеці інформації, включаючи виявлення джерел загроз та вразливостей інформаційних технологій, визначення способів, ймовірності та можливих наслідків реалізації загроз. З іншого боку, ризик інтегрується у процеси техніко-економічного аналізу та прийняття рішень, пов'язаних із забезпеченням ІБ, створенням засобів та організацією системи захисту інформаційних технологій, визначенням її складу, архітектури та конфігурації.

Аналіз останніх досліджень і публікацій. Проблема кібербезпеки стає все більш актуальною через широке впровадження цифрових технологій промисловими системами автоматизації та управління, зокрема, в енергетичному секторі. Сьогодні процеси виробництва, передачі та розподілу електроенергії істотно залежать від інформаційних систем (ІС), включаючи мережі передачі даних. Енергокомпанії централізовано здійснюють контроль та управління, що породжує якісно нові загрози та ризики, оскільки зовсім недавно ці функції виконувались локально та децентралізовано. Розвиток технологій Smart Grid та розумного обліку ведуть до появи численних нових послуг

та сервісів, у тому числі і шляхом залучення споживачів, що кардинально змінює архітектуру систем у бік розподіленої автоматизації та змінює принципи управління, доступу і використання ІС. Іншими словами, за цих умов кіберзлочинці можуть ставити під загрозу нормальне функціонування енергокомпаній не лише використовуючи віддалені атаки на об'єкти ІТ-інфраструктури енергокомпаній, але і шляхом атаки на споживачів. Аналогічна ситуація спостерігається і в електронній комерції [2]. Зростання вразливості таких систем має компенсуватися використанням нових технологій та засобів захисту.

Стандарт [3] вносить важливе розширення в загальну модель ризику, подаючи ймовірність як суперпозицію «загроз» і «вразливостей» (рис. 1). Це дає можливість аналізувати стан ІБ в граничних випадках: які б не були великі загрози, якщо відсутні вразливості, то ймовірність реалізації ризику дорівнює нулю.

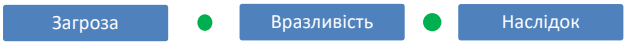

Рис. 1. Загальна модель ризику за стандартом [3]

Формулювання цілей статті. Процес розвитку ризику може бути поданий як послідовний вплив загроз безпеки: на процеси, що протікають в ІС; на результати діяльності як на рівні окремих суб'єктів, так і на рівні сфери діяльності; на процеси управління діяльністю суб'єкта.

На кожній з цих стадій розгортання ризику для його аналізу застосовуються відповідні показники, наприклад: ймовірність виникнення інциденту, показники безпеки інформації (конфіденційність, цілісність, доступність); якість функціонування ІС, можливість виконання інформаційною системою покладених на неї завдань; ймовірність виникнення збитків, можливі збитки суб'єкта від порушення процесу управління його діяльністю.

До характерних особливостей оцінки ризику ІБ належать:

- висока розмірність і пов'язана з цим трудомісткість процесу оцінки, зумовлена великою кількістю потенційних загроз безпеці та вразливості інформаційних технологій, що підлягають захисту;
- необхідність оцінювати ризик на всіх стадіях життєвого циклу інформаційної технології;
- необхідність оцінювати ризик на різних рівнях діяльності з управління інформаційною безпекою, включаючи управління ризиками та аудит ІБ.

Висока розмірність і багаторівневість завдання аналізу ризику зумовлює широке використання якісних методів його вирішення. Проте якісні методи аналізу не повною мірою відповідають сучасній ситуації в інформаційній сфері, що характеризується високою значимістю інформаційної інфраструктури, інтенсивністю інформаційного протистояння та високими ризиками ІБ.

Побудова системи інформаційної безпеки починається з аналізу ризиків. Тобто, перш ніж проектувати систему ІБ, необхідно визначити, які загрози існують для даної ІС, наскільки вони потенційно небезпечні. Кваліфікований облік існуючих загроз і вразливостей ІС та виконаний на цій основі аналіз ризиків закладають основу для вибору рішень із необхідним рівнем ІБ за мінімальних витрат. Аналіз та управління ризиками застосовується для оцінки загроз, вразливостей та ризиків ІС, а також визначення контрзаходів, які забезпечують достатній рівень захищеності цієї інформаційної системи.

Завданням цієї роботи є застосування кількісних методів аналізу ризику, що базуються, зокрема, на результатах формалізації різноманітних процесів, пов'язаних із забезпеченням ІБ в поєднанні з уніфікованою мовою моделювання UML, яка дозволяє графічно описувати об'єкти, їхню взаємодію, процеси функціонування [4]. При цьому найбільш підходящою для поставленої мети є методологія побудови діаграм діяльності, які забезпечують наочне відображення послідовності етапів оцінки та управління ризиками з використанням відповідних розрахунків.

Виклад основного матеріалу. В наш час використовуються два варіанти підходу до аналізу ризиків – базовий та повний. Вибір залежить від оцінки власниками цінності своїх інформаційних ресурсів та можливих наслідків порушення режиму ІБ. У найпростішому випадку (якщо цінність ресурсів з погляду організації не є надмірно високою) власники інформаційних ресурсів можуть не оцінювати ці параметри. Тоді аналіз ризиків проводиться за спрощеною схемою: розглядається стандартний набір найпоширеніших загроз без оцінки їх ймовірності та забезпечується мінімальний або базовий рівень ІБ.

Повний варіант аналізу ризиків застосовується у випадку підвищених вимог до ІБ. На відміну від базового варіанту, тут у тому чи іншому вигляді оцінюються ресурси, характеристики ризиків та вразливостей. Зазвичай, проводиться аналіз співвідношення вартість/ефективність кількох варіантів захисту. В ІС з підвищеними вимогами до інформаційної безпеки при виконанні повного аналізу ризиків доводиться вирішувати низку

складних проблем, які полягають у тому, щоб визначити цінність ресурсів, скласти повний список загроз та оцінити їх параметри, правильно вибрати ефективні контрзаходи.

Таким чином, для проведення повного аналізу ризиків необхідно: визначити список і цінність активів (ресурсів), що підлягають захисту; ідентифікувати список загроз ІБ, актуальних для даної ІС; оцінити ймовірність реалізації загроз; визначити вразливість активів та розмір потенційних збитків; виконати оцінку ризиків; запропонувати рішення, яке забезпечує необхідний рівень ІБ, забезпечити реалізацію і тестування обраних способів захисту та провести оцінку залишкового ризику. Детальніше ці етапи проаналізуємо нижче.

Діаграма діяльності, що ілюструє основні та допоміжні етапи реалізації кількісного та якісного методів оцінки ризиків інформаційної безпеки, подана на рис. 2.

До заходів щодо управління IT-ризиками належать:

- розробка нормативних документів;
- забезпечення фізичної безпеки та безпеки ІС;
- розмежування доступу до ресурсів підприємства;
- контроль за станом корпоративної ІС.

Спочатку визначається об'єкт захисту – проводиться інвентаризація інформаційних активів, оцінюється їх критичність для бізнес-процесів компанії. Потім вирішується, від чого здійснюється захист. Для цього аналізуються властиві системі вразливості, визначається міра їх критичності – ймовірність того, що вони можуть бути реалізовані. На основі цього впроваджуються контрзаходи, аналізується їх результативність і приймається рішення – оптимізувати або залишати працювати.

Щоб своєчасно вносити відповідні корективи, необхідно відстежувати зміни, що відбуваються як в ІС, так і в навколишньому середовищі. Застосування системи заходів захисту, що дозволяють забезпечити прийнятну для організації величину ризику дає можливість мінімізувати або попередити можливі ризики.

Ризик, як відомо, характеризує небезпеку, на яку може наражатися система та організація, що її використовує. Ступінь ризику залежить від цінності активів (ресурсів); імовірності реалізації загроз; простоти використання вразливості для реалізації загроз; існуючих або запланованих до впровадження засобів забезпечення ІБ, які зменшують кількість вразливостей, ймовірність виникнення загроз та можливість негативних впливів.

Приклад класифікації ресурсів та їх вартісна оцінка наведені на рис. 3.

Для кожного класу використовується своя методика визначення цінності елементів, що допомагає

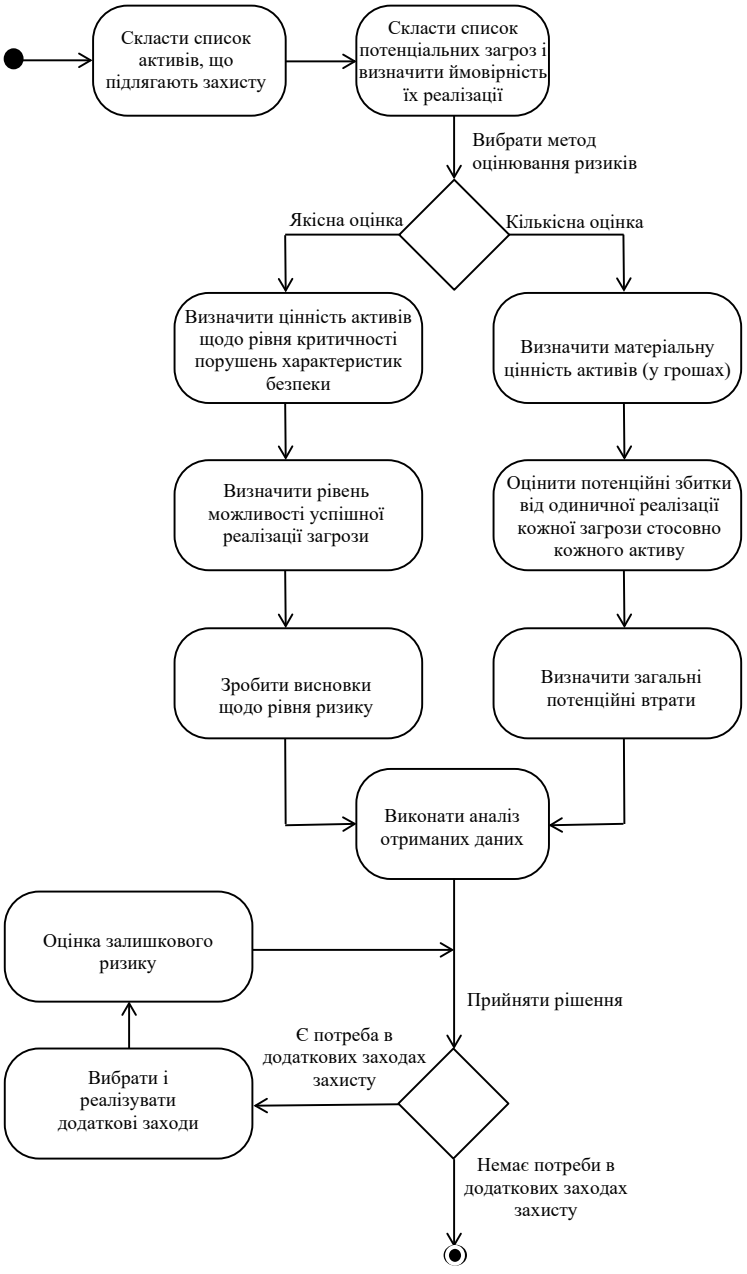

Рис. 2. Діаграма діяльності процесів аналізу ризиків інформаційної безпеки

Рис. 3. Класифікація і визначення цінності активів

вибрати відповідний набір критеріїв. Ці критерії служать для опису потенційної шкоди, пов'язаної з порушенням конфіденційності та цілісності ІС, рівня її доступності. Фізичні ресурси оцінюються за вартістю їх заміни або відновлення їх працездатності. Якісні оцінки вартісних величин потім перетворюються на рангову шкалу, яка може використовуватися і для оцінок інформаційних ресурсів. Програмні ресурси оцінюються тим же способом, що і фізичні, з урахуванням визначення витрат на їх придбання чи відновлення.

Крім критеріїв, що враховують фінансові втрати, комерційні організації можуть застосовувати критерії, що відображають збитки репутації організації; неприємності, пов'язані з порушенням чинного законодавства; збитки для здоров'я персоналу; фінансові втрати від розголошення інформації; втрати, пов'язані з відновленням ресурсів; збитки від дезорганізації діяльності. Процес оцінювання втрат за наведеними критеріями часто має суб'єктивний характер. Крім того, можуть використовуватись і інші критерії в залежності від основної діяльності організації.

Десятки методів, рекомендовані для підтримки процесу оцінки ризику, мають різну застосовність та ефективність на різних стадіях: ідентифікації ризиків, аналізу наслідків, аналізу імовірнісних характеристик, порівняльних оцінок та рівня ризику. Зокрема, для побудови моделі загроз на початковому етапі ідентифікації небезпек та ризику для людей, обладнання, навколишнього середовища успішно використовують методологію дослідження небезпеки та працездатності HAZOP (Hazard and Operability Study). Основна мета цього та схожих методів полягає у систематичній перевірці наявності небезпек. Якщо небезпеки виявлено, такі методи допомагають зрозуміти, як ці небезпеки можуть призвести до негативних наслідків і як цих наслідків можна уникнути шляхом внесення змін до процесу.

Для планування заходів із захисту інформаційних ресурсів вирішальне значення має розуміння видів загроз. Серед основних загроз для інформаційних систем автоматизації та управління, вміщених у рекомендаціях [5], відмітимо наступні: несанкціоноване використання точок доступу до дистанційного технічного обслуговування; мережеві атаки через корпоративну мережу; атаки на стандартні компоненти, що використовуються в мережі ICS; DDoS-атаки; людська помилка або саботаж; проникнення вірусу через знімний носій чи зовнішні пристрої; несанкціонований доступ до ресурсів; атаки на компоненти мережі; технічні збої або форс-мажор.

У загальному випадку, успіх реалізації загрози залежить від мотивації і досвіду порушника, наявного ресурсу, інформованості, часу. Виходячи з цього, можна побудувати орієнтовний перелік характеристик порушників, використовуючи наступну типізацію:

• «Хакер-аматор» – приватна особа, яка намагається знайти можливості та способи зламування технологічних та SCADA-систем, що мають інтерфейси в Інтернеті, за допомогою відомих уразливостей, знайдених з використанням, наприклад, пошукової системи «Shodan»;

• «Інсайдер» (у тому числі, «без злого наміру») – незадоволений співробітник або обслуговуюча персона власної чи сторонніх організацій (постачальники, партнери, налагоджувачі), що має права доступу і знає тонкощі експлуатації систем та способи зберігання конфіденційних даних;

• "Ворог" – злочинні угруповання та іноземні уряди (Cyber Espionage, Cyber Crime, Cyber Activism, Cyber Terrorism, Cyber War тощо).

На практиці поведінка хакерів-аматорів успішно описується мовою ймовірностей, оскільки існує значна кількість статистичних даних щодо частоти та способів таких атак. Тут досить ефективним захистом є відомі спеціалізовані програмні та технічні засоби. Заходи захисту від цієї категорії порушників мають плануватися та виконуватися насамперед.

Інсайдер – найскладніший у моделюванні та нейтралізації тип порушника. Ризики, пов'язані з цим видом порушень, часто недооцінюються. Компенсаційні міри обов'язково повинні включати комплекс організаційно-технічних заходів. Для роботи із внутрішніми порушниками повинні розглядатися і аналізуватися різні типізовані образи, такі як «недбалий», «маніпульований», «ображений», «нелояльний», «впроваджений». Статистичні дані [6], що ілюструють мотивацію внутрішніх порушників, показано на рис. 4. Їх можна використовувати як початкове наближення для формування оцінок та планування заходів щодо профілактики.

Останній із перелічених тип порушника вимагає найскладніших та найдорожчих заходів захисту, які непосильні окремій компанії. В цьому випадку необхідно звернутися за допомогою до компетентних державних органів. Таке звернення повинно бути своєчасним та обґрунтованим, а для подальшого розшуку та покарання винних надана доказова база. З цією метою технічними та організаційними засобами має бути забезпечене виявлення атак, моніторинг стану та надійне ведення журналів подій.

Метою аналізу ризиків, пов'язаних з експлуатацією ІС, є оцінка загроз, тобто умов та факторів, які можуть спричинити порушення цілісності системи, її конфіденційності чи полегшити несанкціонований доступ до неї, та вразливостей – слабких місць у захисті, які роблять можливою реалізацію загрози, а також визначення комплексу контрзаходів, що забезпечує достатній рівень захищеності ІС. Під час оцінювання ризиків враховується ряд факторів: цінність ресурсів, значущість загроз, вразливостей, ефективність наявних та планованих засобів захисту та ін.

Ймовірні втрати від реалізації окремої загрози можна обчислити за методикою, детально описаною раніше в роботі [7], з допомогою формули розрахунку вартості ризику:

$$R_{t_i} = \sum_{k=1}^{k1} \omega_{t_i} p_{t_i} d_{t_i} c(a_k),$$

де $k1$ – кількість активів, на які спрямована загроза $t_i, i = 1,2,3,...,n$; ω_{t_i} – частота виникнення загрози t_i; p_{t_i} – ймовірність реалізації загрози t_i, наприклад, внаслідок успішного використання деякої вразливості; A_{t_i} – набір активів, на які спрямована загроза t_i; $c(a_k)$ – вартість активу $a_k \in A_{t_i}$. Коефіцієнт пошкодження (руйнування) $d_{t_i} \in [0,1]$, що виражає міру руйнівної дії загрози t_i на актив чи активи, може служити критерієм відбору (селектором) тих активів, на які поширюється руйнівна дія загрози t_i.

Процес управління ризиком спрямовано на визначення подій, які можуть вплинути на органі-

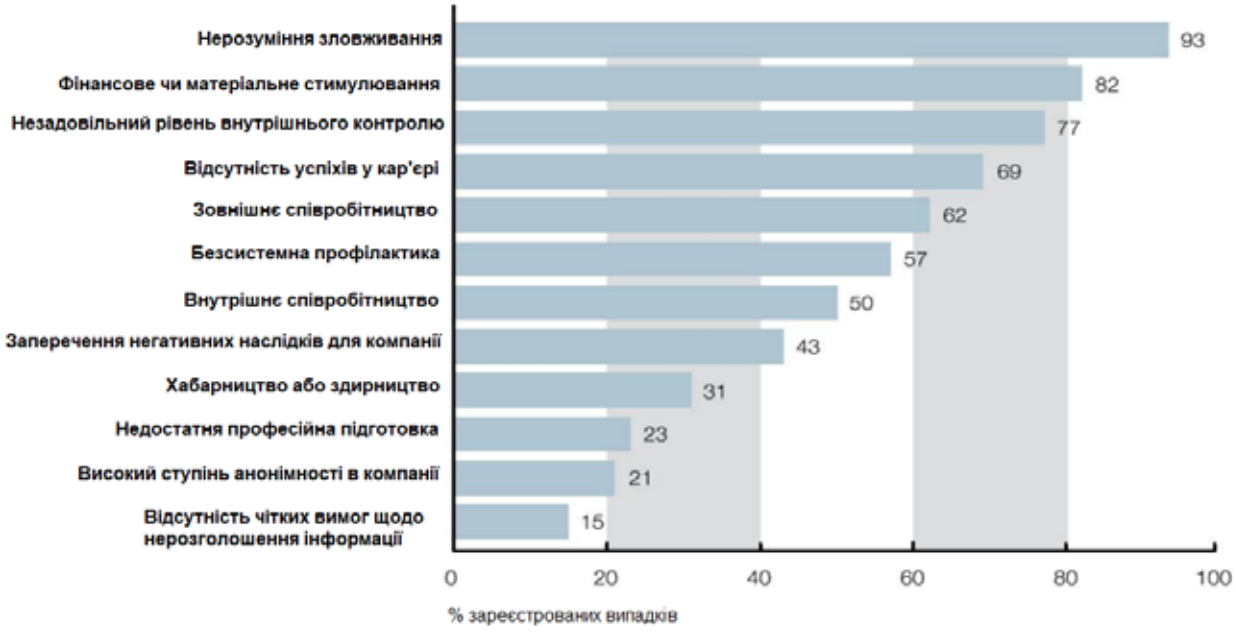

Рис. 4. Мотивація внутрішніх порушників

зацію. При цьому забезпечується контроль допустимого рівня ризику за розумної гарантії досягнення цілей організації. Управління ризиками являє собою неперервний процес, що охоплює всю організацію і здійснюється співробітниками на всіх рівнях.

Планування технічних та організаційних заходів щодо забезпечення ІБ вимагає розв'язання оптимізаційного завдання мінімізації витрат за максимального зниження ризиків. Недопущення критичних ризиків є важливою граничною умовою. У бізнесі неможливо компенсувати всі ризики, оскільки це зробить продукцію фірми та послуги неконкурентноздатними, тому якісь із них необхідно свідомо прийняти. Допустиме навіть прийняття частини критичних ризиків. Головне – не допустити катастрофічних ризиків, за яких виникає загроза втрати бізнесу або пряма небезпека для життя людей.

Висновки. Доцільність та точність визначення необхідності додаткових витрат на заходи щодо забезпечення кібербезпеки залежать від адекватності моделі загроз та правильності розрахунку ризиків. Поняття ризику належить до складних категорій, але в практичному сенсі, ризик – це ймовірність, помножена на наслідки. У нашому випадку, коли йдеться про кіберзагрози, обидві ці складові невідомі або можуть бути оцінені лише приблизно. У частині оцінки ймовірності не можна покладатися на статистику, адже надійної статистики стосовно конкретних систем не існує через ряд об'єктивних і суб'єктивних причин [6]: не всі інциденти фіксуються, а тим більше потрапляють у відкриті звіти; не завжди є можливість достовірно визначити зв'язок технологічних збоїв з діями хакерів; потенційно небезпечні атаки реалізуються рідко або взагалі поки що не були зафіксовані; ймовірність успішної атаки пропорційна мотивації та ресурсу порушника.

Щодо оцінки збитків, то тут ситуація ще складніша. Зокрема, усі енергетичні об'єкти є складними системами, тому порушення функціонування будь-якого елемента закономірно впливає на інші елементи. Через відсутність інформації про способи та види майбутніх атак, міру впливу на інші елементи передбачити складно. Ще більше ускладнює оцінку той факт, що в енергетичному секторі збої можуть спричинити каскадний ефект (або ефект доміно), коли проблеми в одній підсистемі негайно або з невеликою затримкою призводять до збою залежних підсистем.

На основі аналізу ризиків, уразливостей, зловмисників та загроз виконується планування, здійснення та контроль контрзаходів, спрямованих на захист ІС, зокрема, з використанням сучасних методів цифрового обміну даними в умовах сильних перешкод [8]. Детальний перелік заходів щодо забезпечення кібербезпеки підприємства наведений в роботі [9]. Серед них:

- системне адміністрування (SA); мережна безпека (NS); безпека програм (AS); безпека робочих станцій, серверів та пристроїв (ESDS);
- ідентифікація, автентифікація та керування доступом (IAAM);
- захист даних та криптографія (DPC); реагування на інциденти (IP);
- моніторинг, управління виправленнями (MVPM);
- аварійне відновлення та фізичний захист (HADRPP);
- управління активами та управління ланцюгами постачання (AMSC);
- політики безпеки, аудит та навчання персоналу (PAET).

Список літератури:

1. Мохор В., Бакалинський О., Цуркан В. Аналіз способів представлення оцінок ризиків інформаційної безпеки. *Information Technology and Security*. Vol. 6, iss. 1, 2018. P. 75-84. DOI: 10.20535/2411-1031.2018.6.1.153189

2. Карпович І. М., Гладка О. М., Бур'ян Д. Т. Сучасні технології оцінки ризиків інформаційної безпеки в електронній комерції. *Інформаційні технології та комп'ютерна інженерія.* Вінниця: ВНТУ, 2022. № 3(55).

3. ISO/IEC 27032:2012(E). Information technology — Security techniques — Guidelines for cybersecurity. 2012.

4. Martin Fowler. UML Distilled: A Brief Guide to the Standard Object Modeling Language. Third Edition. 2005.

5. Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP) from Terrorist Attacks Focusing on Threats Emanating from Cyberspace. OSCE. 2013.

6. SiFo-Studie 2009/10. Know-how-Schutz in Baden-Württemberg. Steinbeis-Edition Stuttgart, 2010. p.70.

7. Карпович І., Гладка О., Бухало Ю. Технології моделювання і оцінки ризиків інформаційної безпеки. *Технічні науки та технології.* Чернігів: НУ «Чернігівська політехніка», 2021. № 1(23). с. 62-68.

8. Lazarovych, I., Kozlenko, M., Kuz, M., ... Savka, I., Pikuliak, M. Software Implemented Enhanced Efficiency BPSK Demodulator Based on Perceptron Model with Randomization. *IEEE 3rd Ukraine Conference on Electrical and Computer Engineering, UKRCON*. Proceedings, 2021, стр. 221–225. DOI: 10.1109/UKRCON53503.2021.9575458

9. Scott Donaldson, Stan Siegel, Chris Williams, Abdul Aslam. Enterprise Cybersecurity: How to Build a Successful Cyberdefense Program Against Advanced Threats. Apress, 2015. 262 p.

Karpovich I.M., Hladka O.M., Kalashnikov V.I. MODELING OF INFORMATION SECURITY RISK ANALYSIS PROCESSES AS A WAY OF COST OPTIMIZATION

The paper is devoted to the study of cyber security of information systems at an enterprise in the energy industry. Today, energy companies centrally control and manage the production, transmission and distribution of electricity through information systems. The development of Smart Grid technologies and smart accounting lead to the emergence of numerous new services, including through the involvement of consumers, which radically changes the architecture of systems towards distributed automation and changes the principles of management, access and use of information systems and generates qualitatively new threats and risks.

The paper proposes a technique for graphical modeling of the process of risk assessment by a quantitative and qualitative method using activity diagrams and calculation of probable losses from the realization of the threat, taking into account the destruction coefficient. To conduct a risk analysis, it is necessary to: determine the list and value of assets (resources) to be protected; identify a list of threats to information security relevant for this information system; assess the likelihood of threats being realized; determine the vulnerability of assets and the size of potential losses; carry out a risk assessment; to propose a solution that ensures the necessary level of information security, to ensure the implementation and testing of the selected protection methods and to carry out an assessment of the residual risk.

The peculiarities of external and internal threats and vulnerabilities of IT infrastructure objects in the energy sector are analyzed in detail. The main threats to information systems of automation and control can be considered: unauthorized use of access points for remote maintenance; network attacks through the corporate network; attacks on standard components used in the ICS network; DDoS attacks; human error or sabotage; virus penetration through removable media or external devices; unauthorized access to resources; attacks on network components; technical failures or force majeure.

We summarized the list of IT risk management measures and methods of planning, implementation and control of countermeasures aimed at protecting information systems.

Key words: *risk analysis, informational security, threats, risk minimization, cyber security.*