УДК 004.05 DOI:10.30837/rt.2024.1.216.03

О. І. ПЕЛЮХ, М. В.ЄСІНА, канд. техн. наук, Д.Ю. ГОЛУБНИЧИЙ, канд. техн. наук

СУЧАСНІ ЗАГРОЗИ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИМ СИСТЕМАМ ТА МЕТОДИ ЗАХИСТУ ВІД НИХ

Вступ

У сучасному світі інформація стає одним з найважливіших ресурсів, а інформаційно-комунікаційні системи (ІКС) – невід'ємною частиною життя суспільства. Завдяки ІКС відбувається обробка, зберігання та передача інформації, що робить їх надзвичайно вразливими до різноманітних загроз.

Загрози для нормального функціонування ІКС постійно еволюціонують, стаючи все більш складними та небезпечними. Це робить актуальним дослідження та розробку нових методів та засобів захисту інформації, а також підвищення обізнаності користувачів ІКС щодо кіберзагроз.

Метою статті є дослідження сучасних загроз для нормального функціонування ІКС, а також розробка рекомендацій щодо підвищення рівня інформаційної безпеки (ІБ). Для досягнення поставленої мети необхідно виконати такі завдання:

- проаналізувати теоретичні основи інформаційної безпеки ІКС;
- вивчити та класифікувати сучасні загрози для інформації та ІКС;
- дослідити методи та засоби захисту інформації та ІКС;
- розробити рекомендації щодо підвищення рівня інформаційної безпеки ІКС.

Об'єктом дослідження є сучасні загрози для нормального функціонування ІКС. Предметом дослідження є методи та засоби захисту ІКС.

1. Класифікація і джерела загроз ІБ ІКС

Загрозу можна розглядати як атаку та можливість порушення ІБ і посягання на заволодіння інформацією, а той, хто посягає на інформацію, є зловмисником. Загрози проявляються через низький захист або знаходження вразливих місць у системі захисту ІКС [1]. Загрози інформаційної безпеки класифіковані за різними ознаками. Розглянемо це питання детальніше.

Рис. 1. Класифікація загроз для ІКС

На рис. 1 наведена класифікація загроз, що складається з п’яти основних класів, які включають в себе від двох до трьох підкласів. Першим з класів є загроза за основними принципами тріади з кібербезпеки: конфіденційності, цілісності й доступності. Очевидно, що загрози цього класу спрямовані на порушення нормального дотримання цих властивостей інформації.

Іншим, не менш цікавим класом, є визначення за джерелами загроз: внутрішніми (тими, що знаходяться всередині системи) й зовнішніми (знаходяться поза системою). Саме загрози цього класу розвиваються невпинно й постійно модернізуються.

Також виділяються загрози ІБ за розмірами нанесеної шкоди: від загальних (заподіяння шкоди об’єкту в цілому) до приватних (заподіяння шкоди деяким властивостям певного елемента об’єкта). Також ступінь впливу також підлягає таксономічним процесам: виділяють загрози пасивного й активного ступеню.

Останній з класів полягає в окресленні загрози за природою виникнення. Існують природні й штучні загрози, з природними все чітко й зрозуміло – загрози, викликані впливом на інформаційне середовище об’єктивних фізичних процесів або стихійних природних явищ, що не залежать від волі людини [1]. Щодо штучної природи виникнення – підклас розгалужується на ненавмисні й умисні загрози.

Стаття 1 Закону України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII надає чітку різницю між навмисними й ненавмисними загрозами, шляхом введення понять «кібератака» й «інцидент кібербезпеки (кіберінцидент)». Розглянемо ці визначення.

Кіберінцидент – подія або ряд несприятливих подій ненавмисного характеру та/або таких, що мають ознаки можливої кібератаки, які становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами, створюють імовірність порушення штатного режиму функціонування таких систем, ставлять під загрозу безпеку електронних інформаційних ресурсів [2].

Кібератака – спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об’єкти кіберзахисту [2].

Дійсно, визначення кіберінциденту й кібератаки повністю відповідають розгалуженням підкласу «штучні» класу загроз ІБ за природою виникнення.

2. Аналіз сучасних загроз

2.1. Внутрішні загрози

Основоположні вимоги до джерел шуму та його ентропії було запропоновано в Внутрішні загрози. Помилки та необережність персоналу, а також недосконаліть внутрішніх процесів та процедур можуть виникати через внутрішні недоліки управління, недостатню увагу до внутрішньої безпеки та недостатню освіченість персоналу щодо правил та процедур безпеки. Розглянемо внутрішні загрози ІБ у сучасному контексті детальніше.

Першим видом внутрішніх загроз є зловмисні інсайдерські загрози [3]. Основними цілями зловмисних таких загроз є шпигунство, шахрайство, крадіжка інтелектуальної власності та саботаж. Вони навмисно зловживають своїм службовим становищем, щоб викрасти інформацію або погіршити роботу системи з фінансових, особистих та/або зловмисних причин. Варто зазначити, що такі загрози можуть бути як колабораціоністського характеру, так і незалежного.

Спільники – це авторизовані користувачі, які працюють з третьою стороною, щоб навмисно завдати шкоди організації. Третьою стороною може бути конкурент, інша держава, організована злочинна мережа або фізична особа. Дії колаборациониста можуть призвести до витоку конфіденційної інформації або порушення бізнес-операцій. Під час незалежного характеру, навпаки, діють повністю самостійно і без зовнішніх маніпуляцій або впливу. Такі загрози можуть бути особливо небезпечними, оскільки зловмисники часто мають спеціальний доступ до ІКС.

Іншим видом сучасних внутрішніх загроз є загрози, що спричиняються недбалим ставленням. Вони часто є наслідком людської помилки, неправильного судження, ненавмисного сприяння та допомоги, фішингу, шкідливого програмного забезпечення (ШПЗ) і викрадених облікових даних. Співробітник несвідомо наражає корпоративні системи на зовнішню атаку. Таких співробітників також можна розділити на два види: пішаки (англ. Pawn) і дурні (англ. Goof) [3].

«Пішаки» – це авторизовані користувачі, якими маніпулюють, аби вони ненавмисно діяли зловмисно, часто за допомогою методів соціальної інженерії. Ці ненавмисні дії можуть включати завантаження ШПЗ на комп'ютер або розкриття конфіденційної інформації сторонній особі.

«Дурні» навмисно здійснюють потенційно шкідливі дії, але не мають злого наміру. Це зарозумілі, необізнані та/або некомпетентні користувачі, які не визнають необхідності дотримуватися політик і процедур безпеки. «Дурнем» може бути користувач, який зберігає конфіденційну інформацію про клієнтів на своєму персональному пристрої, навіть, якщо він знає, що це суперечить політиці організації.

Також, поза категорією знаходяться так звані «кроти». «Кроти» – це сторонні особи, які отримали інсайдерський доступ до систем організації. «Кріт» може видавати себе за постачальника, партнера, підрядника або працівника, отримуючи таким чином привілейовані повноваження, на які в іншому випадку він не мав би права претендувати. Загалом, такий вид внутрішньої загрози можна класифікувати як «неавторизований доступ». Узагальнений вигляд внутрішніх загроз у сучасному контексті наявний на рис. 2.

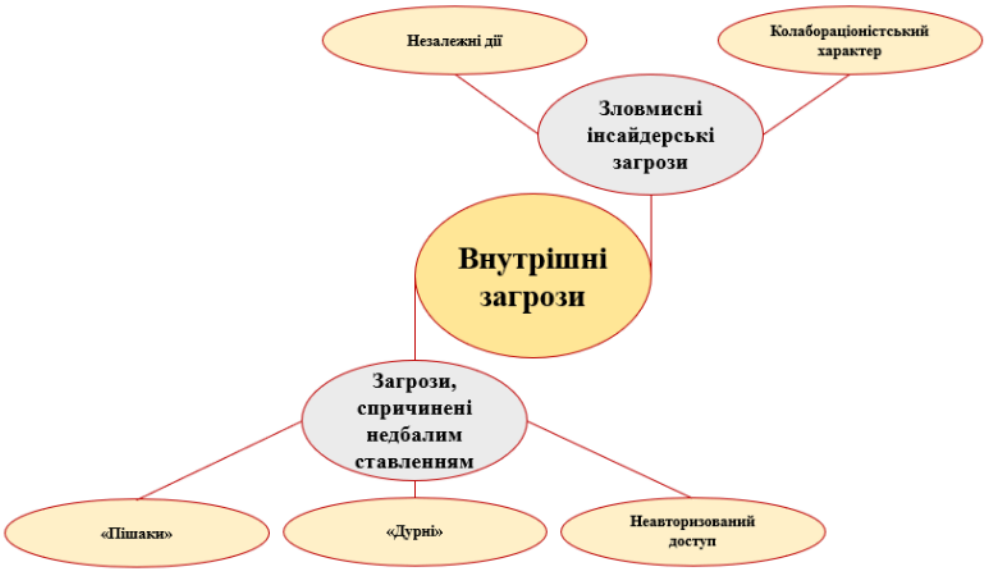

Рис. 2. Узагальнений вигляд внутрішніх загроз

2.2. Зовнішні загрози

Зовнішні загрози включають багато категорій, які виникають поза організацією та спричиняються кимось, хто не має відношення до неї. Зовнішні загрози також можуть бути спрямовані на окремих осіб. Злами або схеми викрадення паролів та онлайн-шахрайства, які спонукають нас добровільно ділитися обліковими даними, спрямовані як на особисті, так і на

корпоративні облікові записи. Зовнішні загрози включають фізичні загрози, такі як втручання в роботу пристроїв або мережі з метою порушення роботи. Зростаючий список хакерських практик, що використовуються для здійснення зовнішніх атак, включає в себе [4]:

• Фішинг.

Фішингова атака, часто у вигляді небажаного електронного листа, спрямована на те, щоб обманом змусити одержувача надати інформацію про свій обліковий запис або паролі. Деякі з них також містять посилання на небезпечні файли або веб-сайти;

• Атака методом грубої сили.

Ця поширена хакерська тактика використовує випадкові комбінації імен користувачів і паролів для спроб входу в ІКС, поки не буде знайдено збіг. Штучний інтелект (ШІ) і автоматизація дозволяють кіберзлочинцям легше здійснювати такі атаки;

• Атака «man in the middle».

Атаки типу MitM часто намагаються здійснити в місцях з незахищеним Wi-Fi з'єднанням, наприклад в аеропортах і готелях. Хоча цей тип атак зустрічається відносно рідко, кіберзлочинці можуть перехоплювати комунікації або перенаправляти користувачів на фальшиві веб-сайти, щоб викрасти їхню інформацію;

• Атаки на відмову в обслуговуванні.

Ця форма кіберзлочинності зазвичай спрямована на бізнес, використовує автоматизацію, щоб перевантажити веб-сайт трафіком, доки він врешті-решт не вийде з ладу. Розподілена атака на відмову в обслуговуванні (DDoS-атака) використовує той самий підхід, при цьому надходження трафіку в ІКС відбувається з декількох джерел, що ускладнює його блокування;

• SQL-ін'єкція.

Ін'єкція мовою структурованих запитів використовує шкідливий код, щоб обманом змусити базу даних відображати інформацію, яку не планувалося виставляти на загальний огляд. Ця складна зовнішня загроза вимагає від хакера ретельного вивчення своєї цілі та виявлення вразливих компонентів системи, з яких можна розпочати атаку;

• Атака «Drive-by».

Термін, запозичений з доцифрової епохи, така атака приховує шкідливі програми на, здавалося б, нешкідливих посиланнях або веб-сайтах. Якщо хтось несвідомо натискає на одне з таких посилань, на пристрій автоматично встановлюється ШПЗ без його відома. Можна провести зв’язок між цим підтипом зовнішньої загрози та підтипом внутрішньої загрози «пішак» з попереднього підрозділу.

Іншим великим підрозділом зовнішніх загроз інформації та нормальній роботі ІКС є ШПЗ. ШПЗ може описувати будь-який тип нав'язливого програмного забезпечення (ПЗ), яке призначене для крадіжки даних, пошкодження обладнання або іншого втручання в нормальну роботу комп'ютера. Найпоширенішими типами шкідливих програм є шпигунські програми та програми-вимагачі. Деякі шкідливі програми призначені для викрадення даних або виведення комп'ютерів і пристроїв з ладу [4]. Розглянемо деякі види атак, що спричиняють такі загрози:

• Шпигунські програми.

Ця небезпечна форма ШПЗ встановлюється на пристрій-складову ІКС і починає стежити за активністю користувача з подальшою передачею даних кіберзлочинцю. Шпигунські програми, які важко виявити, можуть використовуватися для збору конфіденційної інформації, наприклад, паролів і номерів кредитних карток;

• Програми-вимагачі.

Ця форма ШПЗ використовується для захоплення пристрою або всієї мережі в заручники, не даючи компаніям або приватним особам отримати доступ до власних файлів, поки не буде сплачено викуп, як правило, за допомогою кредитної картки або криптовалюти.

Варто зазначити, що повільна робота пристрою, незрозумілі спливаючі вікна, незвичні зміни в налаштуваннях браузера або безпеки – це тривожні ознаки атаки ШПЗ. Узагальнено зовнішні загрози наявні на рис. 3.

Рис. 3. Сучасні зовнішні загрози для інформації та ІКС

2.3. Технічні загрози

До технічних загроз можна віднести: атаки на апаратне та програмне забезпечення (розглянуті в попередньому підрозділі), мережеві атаки й атаки на криптографічні алгоритми. Розглянемо це питання детальніше.

Сучасна ІКС – це складна, тісно пов'язана екосистема обладнання, ПЗ, сервісів, комунікаційних протоколів, віртуальних ресурсів і людей. Нині такі системи є основою організацій в усьому світі, тому кібератаки, спрямовані на порушення мережевої безпеки, становлять величезну загрозу для компаній та зацікавлених сторін.

Атаки на мережеву безпеку стають все більш поширеними, дозволяючи зловмисникам пошкодити корпоративні системи та скомпрометувати конфіденційну інформацію. Після проникнення зловмисників через периметр комп'ютерної мережі відбуваються інші кіберзлочини, такі як запуск ШПЗ, атаки з вимогами викупу або атаки на кінцеві точки. Досвідчені кіберзлочинці можуть швидко розширити сферу та масштаб атаки, використовуючи всі вразливості ІКС. Мережеві атаки можуть бути [5]:

- активними: зловмисники отримують несанкціонований доступ до мережі, а потім змінюють дані (наприклад, за допомогою шифрування), щоб скомпрометувати їх і вплинути на їхню зручність та цінність;
- пасивними: кіберзлочинці атакують мережі для моніторингу або викрадення даних, не вносячи до них жодних змін.

Іншим доволі сучасним видом загроз для нормального функціонування ІКС є криптографічні атаки [6].

Криптографічна атака дозволяє зловмисникам обійти захист криптографічної системи, визначивши слабкі місця в її коді, шифрі, криптографічному протоколі або схемі управління ключами. Такий обхід також називається "криптоаналізом". Таким чином, криптографічні атаки націлені на криптографічні або шифрувальні системи, які приховують дані. Залежно від типу криптографічної системи та інформації, доступної зловмиснику, ці атаки можна умовно поділити на шість типів:

- Атаки грубої сили.

При атаці грубої сили зловмисник намагається розшифрувати зашифроване повідомлення або дані, використовуючи різні ключі. Якщо розмір ключа 8-бітний, то можливих ключів буде 256 (тобто 2^8). Для того щоб атака була успішною, зловмисник повинен знати алгоритм (як правило, у вигляді програм з відкритим вихідним кодом), щоб спробувати всі 256 можливих ключів у цій техніці атаки;

• Атака на зашифровані дані.

При цьому векторі атаки зловмисник отримує доступ до колекції зашифрованого тексту. Хоча зловмисник не може отримати доступ до відкритого тексту безпосередньо, він може успішно визначити зашифрований текст з колекції. Цей вид, як правило, менш ефективний, ніж його аналог грубого перебору;

• Атака за обраним відкритим текстом.

За допомогою атаки за обраним відкритим текстом зловмисник може вибрати дані відкритого тексту для отримання зашифрованого тексту, що, своєю чергою, спрощує його завдання з розгадування ключа шифрування;

• Атака за допомогою обраного шифрованого тексту.

У цьому методі зловмисник намагається отримати секретний ключ або дані про систему. Аналізуючи обраний шифрований текст і порівнюючи його з відкритим текстом, зловмисник намагатиметься вгадати ключ;

• Атака за відомим відкритим текстом.

Ця техніка застосовується, коли зловмисник вже знає відкритий текст деяких частин зашифрованого тексту, використовуючи методи збору інформації;

• Атака з використанням подвійного ключа та алгоритму.

Зловмисник намагається відновити ключ, який використовувався для шифрування або розшифрування даних, аналізуючи криптографічний алгоритм.

Окрім цих шести основних типів криптографічних атак, криптографічна атака може бути як пасивною, так і активною. Пасивні криптографічні атаки здійснюються з метою отримання несанкціонованого доступу до конфіденційних даних або інформації шляхом перехоплення або підслуховування загального зв'язку. У цій ситуації дані та комунікація залишаються недоторканими і не піддаються фальсифікації. Активні криптографічні атаки ґрунтуються на модифікації даних або комунікації. У цьому випадку зловмисник не тільки отримує доступ до даних, але й втручається в них. На рис. 4 узагальнена класифікація сучасних технічних загроз.

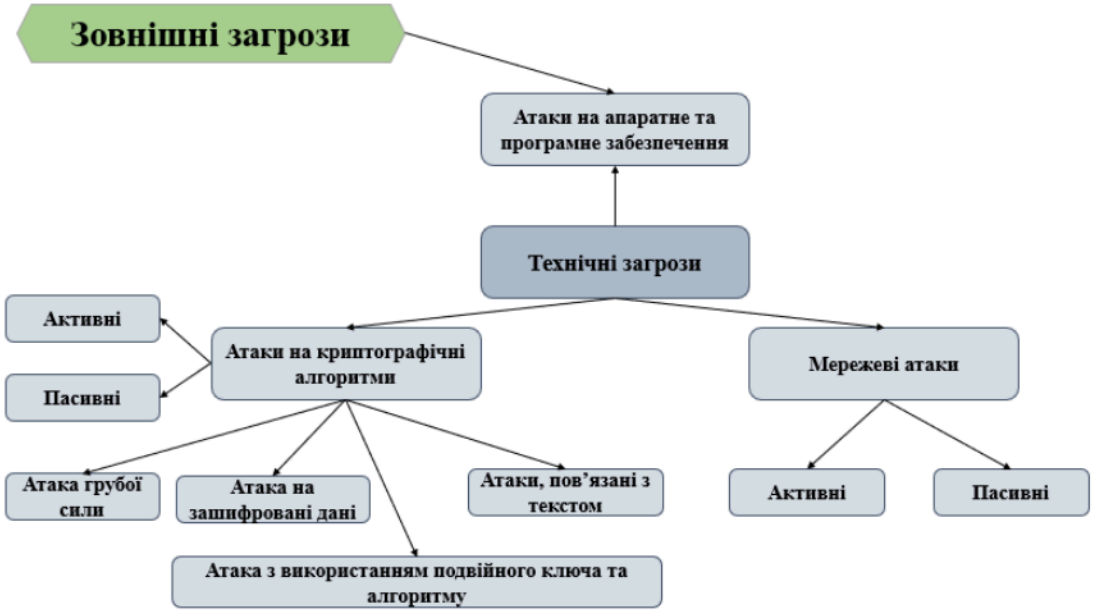

Рис. 4. Узагальнена класифікація сучасні технічних загроз

Варто зауважити, що на рис. 4 до атак на апаратне та програмне забезпечення під'єднані й зовнішні загрози з рис. 3. Ми вважаємо таке уточнення важливим, адже воно підтверджує факт пов'язаності всіх загроз тим чи іншим чином між собою.

Слід зазначити, що детально висвітлені внутрішні, зовнішні та технічні загрози. Також, у ході опису й аналізу стало зрозуміло, що всі три групи загроз тісно переплітаються між

собою: загроза несанкціонованого доступу в різних проявах наявна серед внутрішніх і технічних загроз; атака методом грубої сили входить до підгрупи «атаки на криптографічні алгоритми» технічних загроз й спільної групи «кіберзлочин» для технічних і зовнішніх загроз. Детальна мапа перетину груп, розглянутих загроз наведена на рис. 5.

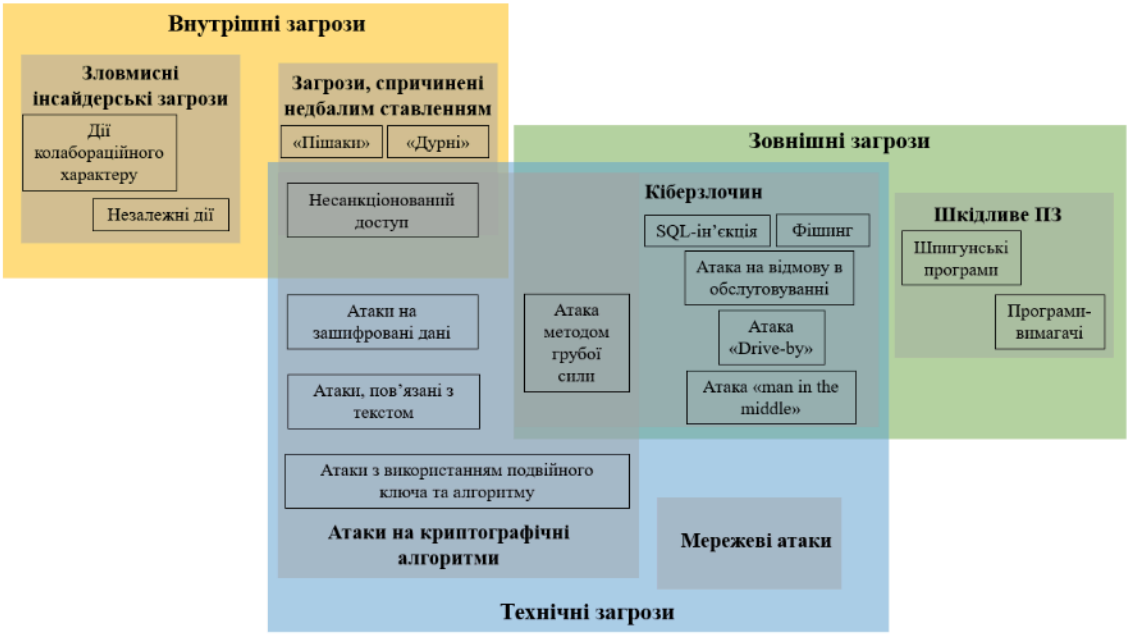

Рис. 5. Мапа перетину сучасних загроз для інформації та нормального функціонування ІКС

3. Методи та засоби захисту інформації

3.1. Класифікація методів та засобів захисту інформації

Класифікація методів та засобів захисту інформації може бути проведена за різними ознаками, такими як вплив на об'єкт захисту та рівень реалізації. Розглянемо ці дві ознаки більш детально. За ознакою впливу на об'єкт захисту, методи та засоби захисту інформації можна поділити на кілька категорій [7]:

1. Фізичні методи та засоби.

Ця категорія включає фізичні засоби захисту, такі як замки, двері, контроль доступу, відеоспостереження, бар'єри та інші заходи, спрямовані на захист фізичного доступу до інформаційних ресурсів та інфраструктури;

2. Програмні методи та засоби.

Ці методи та засоби включають в себе використання ПЗ для захисту інформації. Вони можуть включати у себе антивірусне ПЗ, файєрволи, системи виявлення та захисту від вторгнень (IDS/IPS), системи керування доступом та інші інструменти для запобігання, виявлення та виправлення кіберзагроз;

3. Криптографічні методи та засоби.

Ця категорія включає в себе використання криптографічних методів її алгоритмів для шифрування даних, захисту конфіденційності і цілісності інформації. Криптографічні методи використовуються для створення шифрів, електронних підписів та інших технік для забезпечення безпеки даних;

4. Правові методи та засоби.

Ця категорія включає в себе використання правових норм, законів та стандартів для захисту інформації. Такі методи та засоби можуть включати у себе створення та виконання політик безпеки, регулятивні вимоги до захисту даних, а також правові заходи для покарання осіб, які порушують безпеку інформації.

Кожна з цих категорій має свої особливості та призначення і може бути використана окремо або в поєднанні з іншими методами та засобами для ефективного захисту інформації

та інформаційних ресурсів. Загалом методи та засоби захисту інформації за ознакою впливу на об'єкт можна узагальнити наступним шляхом (рис. 6).

Рис. 6. Узагальнений вигляд методів та засобів захисту інформації за ознакою впливу

Кожен з цих видів методів та засобів захисту має свої особливості та призначення і може бути використаний в залежності від конкретних потреб ІКС чи організації.

3.2. Технічні та організаційні методи та засоби захисту інформації

Забезпечення безпеки інформації є важливим завданням для будь-якої організації чи підприємства в сучасному цифровому світі. Для досягнення цієї мети використовуються різні методи та засоби захисту, які можна розділити на технічні та організаційні. Розглянемо ці категорії з точки зору їх призначення, принципів дії та конкретних прикладів застосування. Почнемо з технічних методів та засобів захисту інформації, до них можна віднести наступне, в узагальненому виді інформація наведена на рис. 7:

- Системи автентифікації та авторизації.

Системи автентифікації та авторизації використовуються для контролю доступу до інформаційних ресурсів. Вони дозволяють перевірити особу користувача та надати йому доступ лише до тих ресурсів, на які він має право;

- Антивірусний захист.

Антивірусний захист використовується для захисту комп'ютерів від ШПЗ. Антивірусні програми сканують комп'ютер на наявність вірусів, троянів, шпигунських програм та інших шкідливих програм;

- Системи захисту даних.

Системи захисту даних використовуються для захисту даних від несанкціонованого доступу, модифікації, знищення або крадіжки;

- Системи виявлення та запобігання вторгнень.

Системи виявлення та запобігання вторгнень використовуються для виявлення та запобігання несанкціонованому доступу до комп'ютерних мереж;

- Мережеві екрани.

Мережеві екрани використовуються для захисту комп'ютерних мереж від несанкціонованого доступу. Мережеві екрани фільтрують трафік, який проходить через них, і дозволяють лише авторизований трафік;

- Системи криптографічного захисту.

Системи криптографічного захисту використовуються для захисту даних від несанкціонованого доступу, модифікації, знищення або крадіжки.

Використання цих методів та засобів може значно підвищити рівень безпеки ІКС. Важливо зазначити, що жоден метод або засіб не може забезпечити 100 % захисту. Тому слід використовувати комплексний підхід до захисту інформації, який включає в себе технічні, організаційні та правові методи.

Рис. 7. Узагальнений вигляд технічних методів і засобів захисту інформації

Наступним блоком є опис організаційних методів та засобів захисту інформації і ІКС. Перший і найважливіший метод – визначення політики безпеки ІКС. Політика інформаційної безпеки (ПІБ) – це набір правил, принципів і процедур, спрямованих на забезпечення дотримання всіма кінцевими користувачами та мережами в організації мінімальних вимог безпеки інформаційних технологій та захисту даних [8]. ПІБ повинна стосуватися всіх даних, програм, систем, об'єктів, інфраструктури, авторизованих користувачів і третіх осіб. ПІБ може бути дуже широкою. Вона може охоплювати ІТ-безпеку та/або фізичну безпеку, а також використання соціальних мереж, управління життєвим циклом і тренінги з ІБ.

Одним з підрозділів політики ІБ є регламентація доступу до інформації. Контроль доступу лежить в основі кібербезпеки. Для цього організації повинні завжди бути впевнені, що користувачі є тими, за кого себе видають, і, що вони мають дозвіл на використання певних мережевих ресурсів або доступ до зон з обмеженим доступом. Контроль доступу допомагає не лише захистити активи, але й, у разі порушення, відстежити дії та визначити причину.

Існує два види контролю доступу: фізичний і логічний. Фізичний контроль обмежує доступ до приміщень, робочих станцій та обладнання, в той час як логічний контроль обмежує доступ до критично важливих активів. Обидва види контролю є важливими для забезпечення кібербезпеки і виходять з того, що користувачі, пристрої та будь-які інші суб'єкти, які запитують доступ, невідомі доти, доки система не зможе їх ідентифікувати [9].

Слабкі та недостатні заходи – це, фактично, неминуча загроза виникнення надзвичайної ситуації. Найкращою міжнародною практикою є обмеження доступу до мережі до рівня, необхідного для виконання працівниками своїх службових обов'язків.

Принцип найменших привілеїв є одним з ключових заходів, рекомендованих стандартом IEC 62443-2-1 для захисту критично важливої інфраструктури та інших систем промислової автоматизації та управління від несанкціонованого доступу. Аналогічно, стандарт ISO/IEC 27001 рекомендує принцип найменших привілеїв для захисту даних: "Користувачам повинен бути наданий доступ до мережі та мережевих сервісів, на використання яких вони мають спеціальний дозвіл". Впровадження такої політики вимагає комплексного підходу до принципів управління ідентифікацією та активами. На додаток до обережного управління приві-

леями важливо також записувати всі дії користувачів, щоб мати можливість створити аудиторський слід у разі порушення.

Низка міжнародних стандартів стосується процесу автентифікації (перевірки пристрою та особи користувача) та авторизації, яка встановлює, чи може користувач отримати доступ до певного ресурсу з його або її рівнем привілеїв. До них відносяться, наприклад, серія стандартів IEC 62443 і згадана вище серія стандартів ISO/IEC 27000 [9].

IEC 60839-11-5 охоплює фізичні засоби контролю доступу, включаючи біометричні дані, такі як відбитки пальців і сканування райдужної оболонки ока, а також картки.

Також, варто зауважити, що організаційні заходи і методи забезпечення безпеки інформації та ІКС доволі чітко врегульовані й в українському законодавстві. Найголовнішим документом є Закон України «Про захист інформації в інформаційно-комунікаційних системах» [10]. Крім того, існує низка нормативних документів систем технічного захисту інформації, які допоможуть як з організаційними, так і з технічними методами забезпечення ІБ [11].

Висновки

1. Загрози інформаційної безпеки представлено як атаки, що можуть порушити ІБ та викликати заволодіння інформацією, і, зазвичай, походять з недостатньої захищеності чи вразливостей систем. Класифікація загроз включає основні категорії за принципами тріади кібербезпеки, джерелами, розмірами нанесеної шкоди та природою виникнення. У законодавстві України розрізняються кіберінциденти та кібератаки. Ця класифікація допомагає розуміти природу загроз та визначати відповідні заходи захисту.

2. У сучасному контексті внутрішні загрози ІБ можуть походити від різних джерел. Зловмисні інсайдери можуть намагатися викрасти інформацію або спричинити шкоду з метою особистої вигоди. Існують також загрози, що виникають внаслідок недбалого ставлення до безпеки, коли співробітники можуть навмисно або ненавмисно наражати системи на ризики. Категорії співробітників, які можуть бути втягнуті у ці загрози, включають «пішаків» та «дурнів», які можуть діяти ненавмисно або ненавмисно, а також «кротів», які отримують несанкціонований доступ до систем. Ідентифікація та усунення таких загроз вимагає комплексного підходу до безпеки організації.

3. Зовнішні загрози ІБ охоплюють різноманітні категорії, які походять зовні від організації і можуть бути спрямовані як на індивідуальні особи, так і на корпоративні системи. Серед них можуть бути атаки на особисті дані через викрадення паролів та онлайн-шахрайства, а також фізичні загрози, такі як втручання в роботу пристроїв або мереж з метою порушення їхньої роботи. Зараз розповсюджені різні види хакерських атак, такі як фішинг, атаки методом грубої сили, атаки "man in the middle", DDoS-атаки, SQL-ін'єкції та атаки "Drive-by". Крім цього, велика загроза існує від ШПЗ, таких як шпигунські програми та програми-вимагачі, які можуть призвести до крадіжок даних або втрати доступу до них.

4. Технічні загрози ІБ включають атаки на апаратне та програмне забезпечення, мережеві атаки та атаки на криптографічні алгоритми. Ці загрози становлять серйозну небезпеку для компаній та інших суб'єктів, оскільки можуть призвести до порушення конфіденційності, цілісності та доступності даних та інфраструктури.

5. Методи та засоби захисту інформації можна класифікувати за рівнем впливу на об'єкт захисту та рівнем реалізації. За першою ознакою вони поділяються на фізичні, програмні, криптографічні та правові. За другою ознакою – на організаційні, технічні та фізичні. Комбінація різних методів та засобів дозволяє створити ефективну систему захисту інформації, що враховує різні аспекти безпеки.

6. У сучасному цифровому середовищі захист інформації на підприємствах важливий для забезпечення безпеки даних. Для досягнення цієї мети використовуються технічні та організаційні методи і засоби. Технічні методи охоплюють системи автентифікації, антивірусний захист, системи захисту даних та інші. Організаційні заходи включають розробку полі-

тики безпеки, контроль доступу, принцип найменших привілеїв та інші. Загальний підхід до захисту інформації передбачає комплексне поєднання різних методів і засобів для максимальної ефективності.

Список літератури:

1. Основи управління інформаційною безпекою : навч. посіб. / А.М. Гребенюк, Л.В. Рибальченко. Дніпро : Дніпропетр. держ. ун-т внутр. справ, 2020. 144 с..
2. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII [Електронний ресурс] / Офіційний Вебпортал Парламенту України. Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19/ed20171005#Text.
3. What is an Insider Threat? Definition, Types, & Examples [Електронний ресурс]/ OpenText. Режим доступу: https://www.opentext.com/what-is/insider-threat.
4. Dashlane. (2024, Лютий 16) [Електронний ресурс] / A guide to External Security Threats in 2024. Режим доступу: https://www.dashlane.com/blog/guide-to-external-security-threats.
5. RiskOptics. (2022, Жовтень 31) [Електронний ресурс]/ Most Common Types of Network Security Attacks. Режим доступу: https://reciprocity.com/blog/most-common-types-of-network-security-attacks/.
6. What is a Cryptographic Attack? Your Comprehensive Guide. (2024, Січень 10) [Електронний ресурс] / Packetlabs. Режим доступу: https://www.packetlabs.net/posts/what-is-a-cryptographic-attack/.
7. Основи інформаційної безпеки : навч. посіб. / В. Б. Вишня, О. С. Гавриш, Е. В. Рижков. Дніпро : Дніпропетр. держ. ун-т внутр. справ, 2020. 128 с.
8. What is an Information Security Policy? (2023, Квітень 6) [Електронний ресурс]/ UpGuard. Режим доступу: https://www.upguard.com/blog/information-security-policy.
9. The important role of access control in cyber security. (2021, Квітень 21) [Електронний ресурс] / International Electrotechnical Commission. Режим доступу: https://www.iec.ch/blog/important-role-access-control-cyber-security.
10. Закон України «Про захист інформації в інформаційно-комунікаційних системах» від 05.07.1994 № 80/94-ВР [Електронний ресурс] / Офіційний Вебпортал Парламенту України. Режим доступу: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.
11. Нормативні документи системи ТЗІ. (2023, Березень 9). [Електронний ресурс] / Державна служба спеціального зв'язку та захисту інформації України. Режим доступу: https://cip.gov.ua/ua/news/normativni-dokumenti-sistemi-tzi.

Надійшла до редколегії 11.01.2024

Відомості про авторів:

Пелюх Олександр Іванович – Харківський національний університет імені В. Н. Каразіна, студент кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук; Україна; e-mail: oleksandrpelyukh@gmail.com; ORCID: https://orcid.org/0000–0003–0507–0262

Єсіна Марина Віталіївна – канд. техн. наук, доцент, Харківський національний університет імені В. Н. Каразіна, доцент кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук, АТ «Інститут Інформаційних Технологій», науковий співробітник-консультант; Україна; e-mail: m.v.yesina@karazin.ua; ORCID: https://orcid.org/0000-0002-1252-7606

Голубничий Дмитро Юрійович – канд. техн. наук, доцент, АТ "Інститут Інформаційних Технологій", начальник наукового відділу; Україна; e-mail: goldim1971@gmail.com; ORCID: https://orcid.org/0000-0002-6873-7004