2 Забезпечення комп'ютерної безпеки в інформаційних системах

Сергій Гончар, Геннадій Леоненко, Олексій Юдін
ДержНДІ Спецзв'язку
УДК 004.056.5

ПІДХОДИ ДО ОЦІНКИ НЕБЕЗПЕКИ АТАК В ІНФОРМАЦІЙНИХ СИСТЕМАХ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Анотація: **Запропонований підхід до оцінки небезпеки атак в інформаційних системах об'єктів критичної інфраструктури через коефіцієнт небезпеки який враховує перелік загроз, перелік можливих атак, взаємозв'язок між атаками і загрозами, взаємозв'язок між атаками і наслідками.**
Summary: **The approach to assessing the risk of attacks on information systems of critical information objects by means of hazard ratio, which takes into account the list of threats, a list of possible attacks, the relationship between the attacks and threats, the relationship between the attacks and the consequences.**
Ключові слова: **ІС ОКІ, критична інфраструктура, захист інформації, загрози інформації.**

I Вступ

На сьогоднішній день в галузях, які життєво важливі для критичної інфраструктури держави, широко використовуються автоматизовані системи управління технологічними процесами (інформаційні системи) [1], які включають системи диспетчерського управління і збору даних, системи розподіленого управління та інші конфігурації систем управління.

Розвиток та поширення інформаційних технологій, глобалізація інформаційно-телекомунікаційних мереж, інтеграція з корпоративними системами та іншими бізнес-програмами через різні системи зв'язку, включаючи Інтернет, надає можливість забезпечити управління виробничою діяльністю в режимі реального часу, здійснювати дистанційний моніторинг систем управління технологічним процесом, підвищити безпеку підприємства і персоналу, зменшити витрати на експлуатацію. Однак ціною цих переваг являється зростання уразливості до загроз та здійснення атак на зазначені системи.

Враховуючи зазначене та зважаючи на особливості автоматизованих систем управління технологічними процесами [2], для вирішення задач щодо забезпечення захисту інформації виникає необхідність визначення множини можливих атак, а також оцінки коефіцієнта їх небезпеки.

II Основна частина

Загрози інформації в інформаційних системах та можливі наслідки їх реалізації

Загрози інформації в інформаційних системах об'єктів критичної інфраструктури (ІС ОКІ) можна класифікувати за результатом їх впливу на інформацію. В результаті реалізації загроз інформації є порушення інформаційної безпеки, тобто – порушення конфіденційності, цілісності, доступності інформації і неспростовності.

Розрізняють чотири типи загроз безпеки інформації:

- несанкціонований доступ до інформації;
- несанкціоновані зміни або викрадення інформації;
- відмова в обслуговуванні або профілактика авторизованого доступу;
- відмова у визнанні участі, авторства або відмова від одержання.

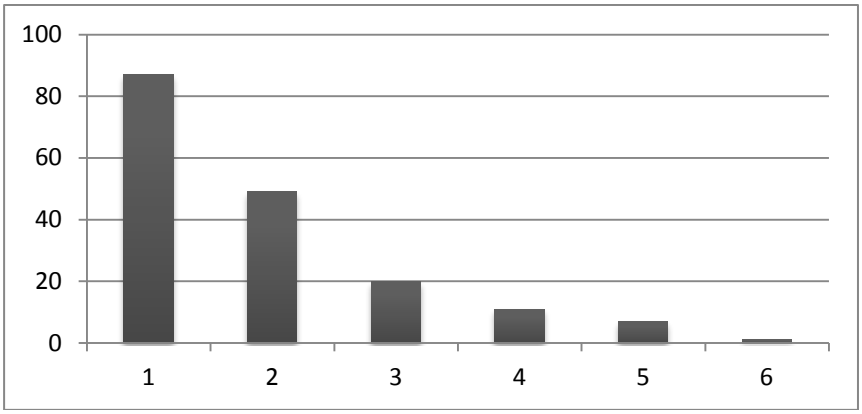
Таким чином, конфіденційність буде забезпечена, якщо дотримуються встановлені правила доступу до системи, цілісність – якщо дотримуються встановлені правила модифікації інформації або її видалення, доступність – якщо зберігається можливість доступу до системи або модифікації інформації відповідно до встановлених правил упродовж будь-якого певного (малого) проміжку часу. Неспростовність буде забезпечена якщо факт участі в події, що трапилась, причетність до утворення або передачі якого-небудь документа чи повідомлення, причетність до одержання якого-небудь документа або повідомлення буде зафіксована.

Загрози, реалізація яких призводить до втрати інформацією якої-небудь з названих властивостей, відповідно є загрозами конфіденційності, цілісності, доступності інформації або неспростовності.

Загрози для ІС ОКІ можуть виходити з різних джерел: навмисних (терористичні групи, промислові шпигуни, невдоволені працівники, зловмисники), ненавмисних (складність системи, людські помилки, аварії, відмови обладнання), природних (стихійні лиха, кліматичні умови тощо).

Спробою реалізації загрози є атака - спроба знищення, розкриття, внесення змін, пошкодження, викрадання або отримання несанкціонованого доступу до активу [3]. Прикладом несанкціонованого внесення змін є маніпулювання технологічною інформацією, що циркулює в ІС ОКІ. Тобто зміна даних, які передаються від датчика до програмованого логічного контролера (ПЛК) або зміна керуючого впливу від програмованого логічного контролера до виконавчого пристрою. Також можливі атаки типу "відмова в обслуговуванні", дія яких спрямована на компоненти ІС ОКІ або лінії зв'язку, і які можуть бути навмисними або спричиненими відмовами обладнання. Атаки такого типу можуть призвести до неможливості подальшого керування технологічним процесом і до його вимушеної зупинки. У тому випадку, коли цикл виробництва підприємства повинен бути безперервним, це призведе до збитків, які будуть викликані простоєм виробництва і повторним запуском технологічного процесу.

Аналіз статистичних даних показує [4], що за період з 2005 року по жовтень 2010 року найбільшу кількість уразливостей для атак виявлено в системах SCADA і людино-машинних інтерфейсах (ЛМІ), рис. 1.



1–SCADA; 2–ЛМІ; 3–ПЛК; 4–обладнання; 5–ПЗ; 6-інтерфейс/протокол

Рисунок 1 – Кількість уразливостей в компонентах АСУ ТП

Крім того, порушення інформаційної безпеки на об'єктах деяких критичних інфраструктур можуть мати значні фізичні впливи.

Основними категоріями впливу є:

- фізичний вплив – включає в себе безліч прямих наслідків аварій ІС ОКІ; найважливішими потенційними наслідками є такі, які можуть призвести до травм і загибелі людей; інші наслідки включають втрату майна (включаючи дані) і потенційні збитки навколишньому середовищу;
- економічні впливи – наслідки другого порядку від фізичних впливів, що є похідними від аварій ІС ОКІ; фізичний вплив може призвести до наслідків для системи, що, у свою чергу може нанести більший економічний збиток підприємству чи організації; у великих масштабах ці наслідки можуть негативно позначитися на місцевому, регіональному, національному рівнях, а можливо і для глобальної економіки;
- соціальні впливи – наслідки другого порядку, які є похідними від втрати державної або громадської довіри в організації.

Враховуючи приведені вище категорії впливу порушення інформаційної безпеки ІС ОКІ можливо навести перелік наслідків цих впливів [4]:

- порушення національної безпеки;
- сприяння вчиненню акту тероризму;
- втрата або скорочення виробництва;
- каліцтва або загибель людей;
- пошкодження обладнання;
- викид (витікання, випаровування) або крадіжка небезпечних матеріалів;
- екологічні збитки;
- кримінальні або цивільно-правові зобов'язання;
- втрата приватної або конфіденційної інформації;
- втрата іміджу бренду або довіри клієнтів.

Слід зазначити, що елементи приведеного переліку не є незалежними. Очевидно, що один з наслідків може призвести до іншого.

Активи ІС ОКІ

Атаки спрямовані на те, щоб заподіяти шкоду активам. Актив - деяка сутність, цінна для особистості, організації або держави [3]. Тому програми безпеки спрямовані на захист активів від збитків.

Активи ІС ОКІ можуть бути класифіковані за видами наступним чином [6]: фізичні, логічні, людські.

Розглянемо більш детально кожний з видів активів.

Фізичні активи включають в себе будь-які фізичні компоненти або групи компонентів, які належать організації. В ІС ОКІ вони включають: системи управління, фізичні компоненти мережі передачі інформації або будь-які інші фізичні об'єкти, які певним чином залучені до процесів управління та аналізу виробничих процесів.

Логічні активи можуть включати в себе інтелектуальну власність, алгоритми, спеціальні знання, або інші інформаційні елементи, які містять в собі здатність функціонування організації або інноваційної діяльності. Крім того, ці види активів можуть містити суспільну репутацію, довіру покупця, або інші заходи, які, у разі їх пошкодження, безпосередньо впливають на виробничий процес. Логічні активи можуть бути представлені у формі особистої пам'яті, документів, інформації, що міститься на фізичному або електронному носіях інформації та включати в себе результати тестів, нормативних даних, або будь-яку іншу інформацію, яка розглядається як конфіденційна або приватна. Втрата логічних активів часто викликає значну шкоду організації і на тривалий час.

Активи ІС ОКІ є особливою формою логічних активів. Вони містять логіку автоматизації, яка приймає участь у виконанні виробничих процесів. Ці процеси надзвичайно залежать від повторного або безперервного виконання чітко визначених подій. І тому нанесення шкоди цим активам, наприклад, видалення або несанкціонована модифікація, може призвести до втрати цілісності або доступності безпосередньо до самого процесу.

Людські активи мають на увазі людей, знання, а також теоретичні і практичні навички, якими вони володіють, і які пов'язані з їх виробничою діяльністю. Вони можуть включати в себе необхідні сертифікати або важливі навички, необхідні для дій під час надзвичайних ситуацій.

Оцінка збитків активам може бути виражена або кількісно, або якісно [6].

Кількісна оцінка активу дає точну відповідь щодо фінансових витрат, які пов'язані з цим активом. Це може бути вартість заміни, вартість втраченого продажу або інші заходи грошово-кредитної політики.

Якісна оцінка активів, як правило, виражається більше на абстрактному рівні, як, наприклад, показники у відсотках або у відносних значеннях. Багато активів можуть бути проаналізовані тільки з точки зору якісних збитків.

Збитки в ІС ОКІ

Збитки в ІС ОКІ можуть бути класифіковані як прямі і непрямі.

Прямі збитки є витратами, які пов'язані з заміною активів. Збитки можуть мати місце за причиною фізичного пошкодження активу, в результаті втрати цілісності або доступності, переривання точної послідовності або зміни характеру процесу. Логічні ж активи мають порівняно низькі прямі збитки по відношенню до їх корисності, оскільки носій, який використовується для зберігання активу, як правило, має низьку вартість. Незначні пошкодження людських активів з коротким часом відновлення можуть мати низькі прямі збитки для організації навіть у випадку довгострокових наслідків для травмованої людини.

Непрямі збитки є збитками, завданими внаслідок втрати активів. Вони можуть включати в себе збитки, пов'язані з процесом простою, переробки або інші виробничі витрати через втрату активів.

Для фізичних активів непрямі збитки, як правило, включають наслідки, які виникають через втрату компонентів. Непрямі збитки від пошкодження обладнання можуть призвести до ремонту, реінжинірингу або інших зусиль для відновлення контролю над промисловим процесом. Для логічних активів непрямі збитки часто є дуже великими. Вони включають в себе втрату довіри громадськості, втрату ліцензії на діяльність, втрату конкурентних переваг від випуску інтелектуальної власності, як, наприклад, конфіденційний процес, нові технології тощо.

Шляхом здійснення упорядкування приведених вище даних за видами активів і способом вираження їх оцінки можна співвіднести види збитків для кожного типу активів. Результати приведені в табл. 1.

Таблиця 1

Вид активу	Прямі збитки	Непрямі збитки	Оцінка збитків, кількісна/якісна
Фізичні	Можуть бути досить високими через заміну вартості активу	Наслідки в результаті втрати або пошкодження активу (залежно від вартості активу)	Якісна або кількісна (спочатку якісна при високому рівні ризиків, а далі кількісна для більшої точності)
Логічні	Зазвичай досить низькі, часто порівняно дешеві і можуть бути досить легко відновлені	Досить часто великі	В основному якісна, але в деяких випадках може бути кількісною
Людські	Як правило, низькі і середні (залежно від ступеня пошкодження)	Як правило низькі або великі (залежно від ступеня травми)	Безпосередній якісний вплив на виробництво, а потім кількісний вплив для відновлення

Взаємозв'язок між загрозами і атаками

Загрози можуть бути реалізовані різними типами атак. Тому контрзаходи, які впроваджуються для захисту інформації, повинні враховувати різні типи загроз і можливих атак. Взаємозв'язок між загрозами і можливими атаками приведений на рис. 2 [7].

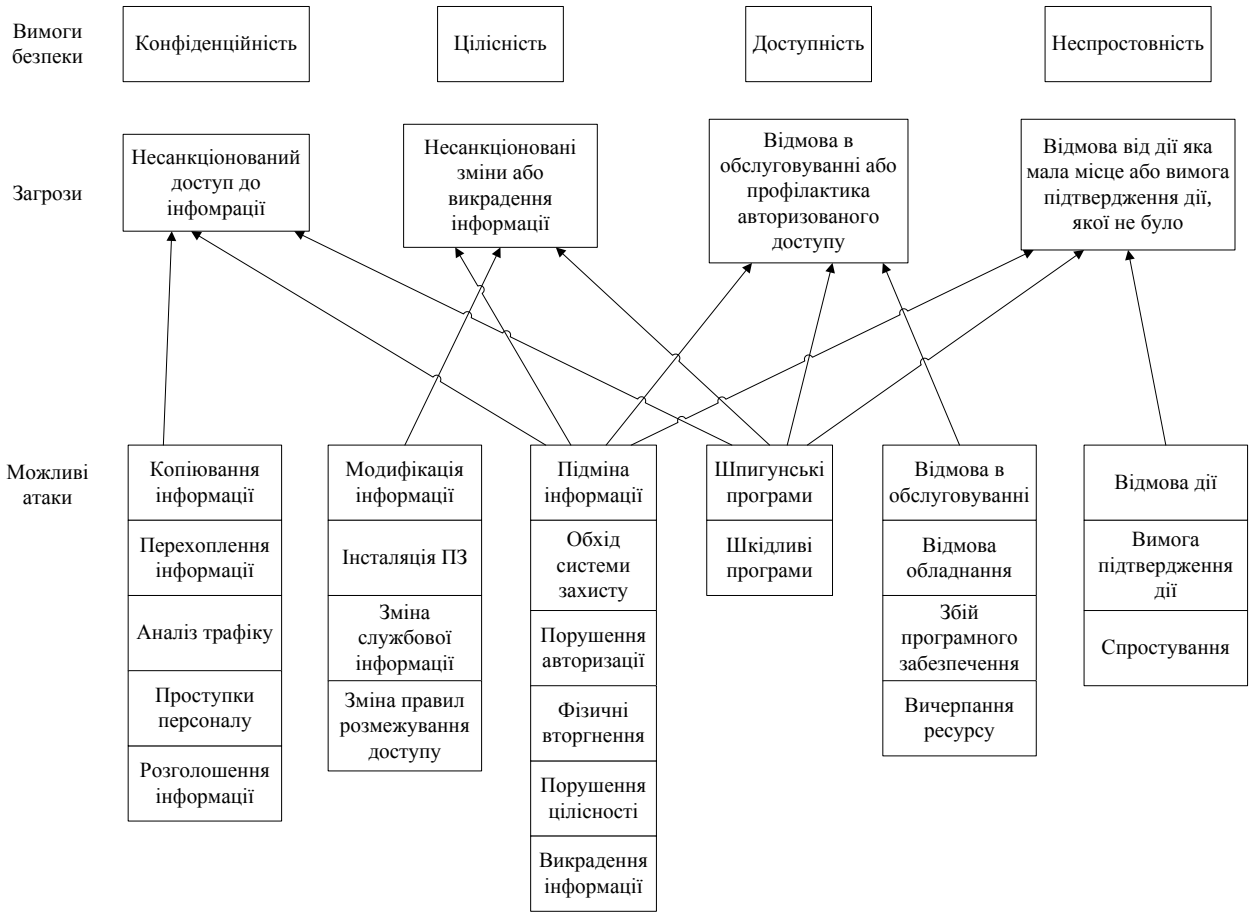


Рисунок 2 - Взаємозв'язок між загрозами і можливими атаками

Взаємозв'язок між атаками і загрозами, які виникають в результаті реалізації цих атак, можливо представити у вигляді матриці:

$$G = [g_{dn}], \tag{1}$$

де $d = \overline{1, D}$ - множина можливих атак;

$n = \overline{1, N}$ - множина загроз.

Елементи g_{dn} матриці (1) набувають значення 1, якщо в результаті *d–ї* атаки реалізується *n–та* загроза, і набувають значення 0 – в протилежному випадку.

На відміну від традиційних систем ІТ, в АСУ ТП існує досить тісний взаємозв'язок автоматизованих систем з фізичними процесами і виконавчими пристроями [3]. Тому порушення інформаційної безпеки в АСУ ТП може призвести до наслідків у промисловому секторі.

Враховуючи зазначене, небезпека атаки в АСУ ТП буде визначатися оцінкою можливих наслідків від її реалізації з позиції впливу на функціонування автоматизованих систем управління технологічними процесами, а рівень тяжкості таких наслідків – коефіцієнтом небезпеки даної атаки.

Нехай h_{dn} – коефіцієнт небезпеки *d–ї* атаки, яка призводить до реалізації *n-ї* загрози, де $d = \overline{1, D}$ – множина можливих атак, $n = \overline{1, N}$ – множина загроз.

Тоді, враховуючи, що атака може призводити до реалізації декількох загроз, коефіцієнт небезпеки *d–ї* атаки буде визначатися наступним чином:

$$H_d = \sum_{n=1}^{N} h_{dn} \cdot g_{dn}, \tag{2}$$

де h_{dn} – коефіцієнт небезпеки *d–ї* атаки, яка призводить до реалізації *n-ї* загрози і визначається за рівнем тяжкості наслідків даної реалізації.

Таким чином, з урахуванням виразів (1) і (2) коефіцієнт небезпеки можливих атак буде визначатися наступним чином:

$$H = \sum_{d=1}^{D} \sum_{n=1}^{N} h_{dn} \cdot g_{dn}. \tag{3}$$

Як випливає з виразів (2) і (3) для оцінки коефіцієнта небезпеки атак необхідні наступні вихідні дані:

- перелік загроз безпеки інформації;
- перелік можливих атак;
- взаємозв’язок між можливими атаками і загрозами;
- взаємозв’язок між можливими атаками і наслідками від їх реалізації.

ІІІ Висновки

Враховуючи викладене можна сформулювати наступні висновки.

1. За результатами дослідження загрози класифіковані за наступними категоріями:
- несанкціонований доступ до інформації;
- несанкціоновані зміни або викрадення інформації;
- відмова в обслуговуванні або профілактика авторизованого доступу;
- відмова у визнанні участі, авторства або відмова від одержання.

2. Активи ІС ОКІ класифіковані за видами як фізичні, логічні та людські, а збитки представлені як прямі і непрямі.

3. В ході аналізу взаємозв’язку між загрозами і можливими атаками визначено підходи до оцінки коефіцієнта небезпеки атак в ІС ОКІ. Вихідними даними, необхідними для оцінки коефіцієнта небезпеки, є:
- перелік загроз безпеки інформації;
- перелік можливих атак;
- взаємозв’язок між можливими атаками і загрозами;
- взаємозв’язок між можливими атаками і наслідками від їх реалізації.

Список використаної літератури: ***1.*** *Методологічні засади розробки та впровадження систем захисту інформації на об’єктах критичної інфраструктури / Гончар С. Ф., Леоненко Г. П., Юдін О. Ю. // Спеціальні телекомунікаційні системи та захист інформації. – 2014. Випуск 1 (25).* ***2.*** *Особенности обеспечения*

кибербезопасности индустриальных систем управления / Гончар С. Ф. // Тези доповідей міжнародної науково-практичної конференції "Проблеми та перспективи розвитку енергетики, електротехнологій та автоматики в АПК", Київ, – 2013. – С. 36-37. ***3.*** *Мохор В. В. Наставления по кибербезопасности (ISO/IEC 27032:2012) / В. В. Мохор, А. М Богданов, А. С. Килевой – К.: ООО «ТриК», 2013. – 129 с.* ***4.*** *Грицай Г., Тиморин А., Гольцев Ю., Ильин Р. Безопасность промышленных систем в цифрах. – М.: Positive Technologies, 2012.* ***5.*** *Теоретико-методологічний аспект забезпечення інформаційної безпеки об'єктів критичної інфраструктури / Гончар С. Ф., Леоненко Г. П., Юдін О. Ю. // Вісник Національного університету "Львівська політехніка": "Комп'ютерні системи та мережі". №806. – 2014. – 34 с.* ***6.*** *Industrial communication networks – Network and system security: IEC 62443-1-1. – Part 1-1: Terminology, concepts and models.* ***7.*** *Power systems management and associated information exchange – Data and communications security: IEC 62351-1. – Part 1: Communication network and system security – Introduction to security issues.*

Анна Ільєнко
Національний авіаційний університет

УДК 004.056.53(045)

СУЧАСНІ МЕТОДИ ГОМОМОРФНОГО ШИФРУВАННЯ ІНФОРМАЦІЙНИХ РЕСУРСІВ

Анотація: **Проведено порівняльний аналіз гомоморфних методів шифрування інформаційних ресурсів на основі забезпечення цілісності. В результаті складена порівняльна таблиця оцінки ефективності використання даних алгоритмів.**
Summary:. **Conduct comparative analysis homomorphic encryption methods of information sources based on integrity As a result, compiled a comparative table of assessing the efficiency of these algorithms.**
Ключові слова: **Інформаційна безпека, гомоморфне шифрування, криптографічна система, цілісність, електронно-цифровий підпис**

I Вступ

Наразі з метою захисту інформаційних ресурсів, що передаються, обробляються та зберігаються в сучасних інформаційно-комунікаційних системах та мережах (далі – ІКСМ), зазвичай використовують різноманітні криптографічні методи шифрування. Методи шифрування дозволяють досить надійно та ефективно захищати інформацію від несанкціонованого доступу та ознайомлення з нею. Застосування криптографічного захисту, тобто використання процедури шифрування тексту за допомогою складних математичних алгоритмів завойовує все більшу популярність. Одним з таких методів є алгоритм гомоморфного шифрування інформації.

Вперше поняття «гомоморфне шифрування» було використане в 1978 році після розробки відомого асиметричного алгоритму RSA його авторами Рональдом Рівестом, Леонардо Адлеманом та Майклом Дертузосом, але їх перші спроби обґрунтувати необхідність та можливість практичного застосування гомоморфного шифрування були невдалими. В 2009 році співробітником IBM Крейгом Джентрі була запропонована модель повністю гомоморфної криптографічної системи, за допомогою якої стало можливим реалізувати операції додавання та множення над зашифрованими даними без їх попереднього розшифрування [1 – 3].

II Постановка задачі

Наразі криптографічні гомоморфні алгоритми шифрування інформації широко використовуються в автоматизованих системах, хмарних обчисленнях і реалізуються у вигляді апаратних, програмних та/або програмно-апаратних методів. Використовуючи новітні методи шифрування повідомлень в поєднанні з правильною установкою комунікаційних засобів, належними процедурами ідентифікації користувача, можна досягнути високого рівня захищеності інформаційного обміну.

Метою даної статті є аналіз та порівняльна характеристика сучасних алгоритмів гомоморфного шифрування, визначення їх переваг та недоліків, принципів та специфіки використання, перспективи застосування в сучасних інформаційно-комунікаційних системах та мережах на основі забезпечення цілісності та конфіденційності.

III Основна частина

Характеристика сучасних гомоморфних алгоритмів шифрування та їх порівняльний аналіз