УДК 004.056.53

АНАЛІЗ ВПЛИВУ НА ЕКОЛОГІЮ СТАНУ КІБЕРБЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Гончар С.Ф.
Інститут проблем моделювання в енергетиці
імені Г.Є. Пухова
Національної академії наук України
вул. Генерала Наумова, 15, 03164, м. Київ
sfgonchar@ipme.kiev.ua

Виконано аналіз впливу на екологію стану кібербезпеки об'єктів критичної інфраструктури. Розглянуто методику оцінки ступеня можливого збитку від реалізації загроз безпеці інформації. *Ключові слова:* кібербезпека, кіберзахист, критична інфраструктура, аналіз, фактори.

Анализ влияния на экологию состояния кибербезопасности объектов критической инфраструктуры. Гончар С.Ф. Выполнен анализ влияния на экологию состояния кибербезопасности объектов критической инфраструктуры. Рассмотрена методика оценки степени возможного ущерба от реализации угроз безопасности информации. *Ключевые слова:* кибербезопасность, киберзащита, критическая инфраструктура, анализ, факторы.

Analysis of the impact on the environment of the state of cybersecurity of objects of the critical infrastructure. Honchar S.F. Analysis of the impact on the environment of the state of cybersecurity of objects of the critical infrastructure is performed. The methodology for assessing the degree of possible damage from the implementation of the threats for information security is considered. *Key words:* cybersecurity, cyber protection, critical infrastructure, analysis, factors.

Постановка проблеми. Сучасний етап розвитку суспільства характеризується впровадженням новітніх технологій, що є ознакою рівня економічного розвитку країни. Зростаюча роль інформаційної сфери для економіки держави пов'язана зі стрімким її входженням у комунікаційну, транспортну, енергетичну, фінансову, оборонну та інші сфери.

Стратегічно важливими для функціонування економіки і безпеки держави, суспільства та населення є об'єкти критичної інфраструктури − підприємства та установи (незалежно від форми власності) таких галузей, як енергетика, хімічна промисловість, транспорт, інформаційні технології та телекомунікації (електронні комунікації), продовольство, охорона здоров'я, комунальне господарство. Тому, враховуючи, що у сучасному суспільстві кібератаки стають частішими та мають тенденцію чинити дедалі значніший і триваліший вплив через підприємства на економіку країни, незаперечним є той факт, що надійний захист від кібератак активно впливає на стан економічної, політичної, соціальної, оборонної та інших складових частин національної безпеки держави.

Очевидним є той факт, що порушення функціонування об'єктів критичної інфраструктури держави може призвести до розвитку надзвичайних ситуацій, пов'язаних із загибеллю людей, екологічними катастрофами, заподіянням великого матеріального, фінансового, економічного збитку або великомасштабними порушеннями життєдіяльності міст та населених пунктів тощо. У цих умовах надзвичайно важливу роль відіграє забезпечення безпеки, у тому числі кібербезпеки об'єктів критичної інфраструктури держави.

Актуальність дослідження. Враховуючи зазначене вище, необхідний аналіз впливу на екологію і, як наслідок, розроблення ефективних та адекватних пропозицій і заходів кіберзахисту інформаційних систем об'єктів критичної інфраструктури.

Аналіз останніх досліджень. При всій важливості питання щодо забезпечення кібербезпеки об'єктів критичної, нині питання дослідження впливу на екологію залишається мало вивченим та дослідженим і потребує розвитку.

Виклад основного матеріалу. Кібератаки спрямовані на те, щоб заподіяти шкоду активам. Активом є деяка сутність, цінна для особистості, організації або держави. Тому програми безпеки спрямовані на захист активів від збитків.

Активи об'єктів критичної інфраструктури (ОКІ) можуть бути класифіковані за видами [1]: фізичні, логічні, людські.

Розглянемо більш детально кожен різновид активів.

Фізичні активи включають у себе будь-які фізичні компоненти або групи компонентів, які належать організації. В 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 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 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 бере участь у виконанні виробничих процесів. Ці процеси надзвичайно залежать від повторного або безперервного виконання чітко визначених подій. І тому завдання шкоди цим активам, наприклад видалення або несанкціонована модифікація, може призвести до втрати цілісності або доступності безпосередньо до самого процесу.

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

Оцінка збитків активам може бути виражена або кількісно, або якісно [1].

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 порівняних значеннях. Багато активів можуть бути проаналізовані тільки з позиції якісних збитків.

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

Прямі збитки є витратами, які пов'язані із 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 щодо їх корисності, оскільки носій, який використовується для зберігання активу, як правило, має низьку вартість. Незначні пошкодження людських активів із коротким часом відновлення можуть мати низькі прямі збитки для організації, навіть у разі довгострокових наслідків для травмованої людини.

Непрямі збитки є збитками, завданими внаслідок втрати активів. Вони можуть включати в себе збитки, пов'язані із 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 у 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 наведених вище даних за видами активів і способом вираження їх оцінки можна співвіднести види збитків для кожного типу активів.

Для оцінки ступеня можливого збитку від реалізації загроз безпеці інформації визначаються можливий результат реалізації загрози безпеці інформації в автоматизованій системі ОКІ, вид збитку, до якого може призвести реалізація загрози безпеці інформації, ступінь наслідків від реалізації загрози безпеці інформації для кожного виду збитку.

У результаті реалізації загрози безпеці інформації можливі прямий або непрямий впливи на конфіденційність, цілісність, доступність інформації, що циркулює в автоматизованій системі управління ОКІ [2].

Прямий вплив на конфіденційність, цілісність, доступність інформації можливий у результаті реалізації прямої загрози безпеці інформації. У цьому разі об'єктами впливу загрози є безпосередньо інформація та/або інші об'єкти захисту, які забезпечують отримання, обробку, зберігання, передачу, знищення інформації в автоматизованих системах ОКІ, в результаті доступу до яких або впливу на які можливий вплив на конфіденційність, цілісність або доступність інформації.

Непрямий вплив на конфіденційність, цілісність, доступність інформації розглядається в результаті реалізації непрямих загроз безпеці інформації. Реалізація непрямих загроз безпеці інформації не приводить безпосередньо до впливу на конфіденційність, цілісність, доступність інформації, але створює умови для реалізації одної або кількох прямих загроз безпеці інформації, що дають змогу реалізувати такий вплив. У цьому разі як результат реалізації непрямої загрози необхідно розглядати результати реалізації всіх прямих загроз безпеці інформації, які можна реалізувати в разі реалізації цієї непрямої загрози.

При визначенні ступеня можливого збитку необхідно зважати на те, що залежно від цілей і завдань, що вирішуються автоматизованою системою ОКІ, видів оброблюваної інформації, вплив на конфіденційність, цілісність або доступність кожного виду інформації, що міститься в системі, може призвести до різних видів збитку. При цьому для різних

власників інформації будуть характерні різні види збитку.

Основними категоріями впливу в автоматизованих системах управління ОКІ є:

– *фізичний вплив* – включає в себе безліч прямих наслідків аварій автоматизованих систем управління технологічними процесами. 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 автоматизованих систем управління технологічними процесами. Фізичний вплив може призвести до наслідків для системи, що, своєю чергою, може завдати більший економічний збиток підприємству чи організації. У великих масштабах ці наслідки можуть негативно позначитися на місцевому, регіональному, національному рівнях, а можливо, глобальній економіці;

– *соціальні впливи* − наслідки другого порядку, які є похідними від втрати державної або громадської довіри в організації.

Враховуючи приведені вище категорії впливу в автоматизованих системах управління ОКІ, можна навести перелік наслідків цих впливів [1]:

– порушення національної безпеки;
– сприяння вчиненню акту тероризму;
– втрата або скорочення виробництва;
– травми або смерть 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.

Зазначені наслідки можуть доповнюватися іншими видами залежно від цілей і завдань, що вирішуються автоматизованою системою ОКІ, а також виду інформації, яка в ній обробляється.

Ступінь можливих наслідків від реалізації загроз безпеці інформації визначається ступенем негативних наслідків від порушення конфіденційності, цілісності або доступності кожного виду інформації, що циркулює в автоматизованій системі ОКІ.

Таким чином, ступінь негативних наслідків від порушення конфіденційності, цілісності або доступності інформації визначається для кожного виду збитку, залежить від цілей і завдань, які виконуються автоматизованою системою ОКІ, може мати різні значення для різних власників інформації й операторів і визначається експертним методом.

У разі, якщо в автоматизованій системі ОКІ обробляються два і більше видів інформації, ступінь можливого збитку необхідно визначати окремо для кожного виду інформації, яка циркулює у системі. Підсумкова ступінь можливого збитку буде визначатися найвищим значенням ступеня можливого збитку, визначеним для конфіденційності, цілісності, доступності кожного виду інформації.

Проведений аналіз наявних систем захисту інформації [3] дає змогу визначити основні складові частини системи кіберзахисту інформаційних систем об'єктів критичної інфраструктури:

– нормативно-правова;
– організаційна;
– технічна;
– підготовка, перепідготовка та підвищення кваліфікації відповідних фахівців.

Кожна із приведених вище складових частин так чи інакше впливає на стан кібербезпеки інформаційних систем об'єктів критичної інфраструктури.

Так, одними з актуальних питань є наявність нормативно-правової бази з питань забезпечення кібербезпеки інформаційних систем об'єктів критичної інфраструктури, узгодження національної нормативно-правової бази з питань забезпечення кібербезпеки об'єктів критичної інфраструктури з положеннями міжнародних документів, виконання узгодженості понятійного апарату, що використовується в чинних національних законодавчих та нормативно-правових документах, доопрацювання (за необхідності − розробка) нормативних документів, вимог, методологій до оцінки загроз об'єктам, що є критичними для життєдіяльності держави, загальної методології оцінки ризиків для критично важливих об'єктів та критичної інфраструктури загалом.

Крім того, варто зазначити, що керівники та/або власники об'єктів критичної інфраструктури мають усвідомлювати можливість і ймовірність здійснення кібератак та наслідки, у разі їх реалізації. Запровадження заходів із питань забезпечення кібербезпеки потребує залучення додаткових ресурсів, на що керівники цих об'єктів не завжди згодні, а механізм, який би вимагав від цих керівників запровадження необхідних заходів, відсутній. Тому без запровадження згаданого механізму усі стандарти інструкції тощо з питань забезпечення кібербезпеки інформаційних систем об'єктів критичної інфраструктури матимуть рекомендаційний характер, оскільки та інформація, яка циркулює, наприклад, в автоматизованих системах управління технологічними процесами, не належить до жодного виду інформації, що підлягає захисту згідно із чинним законодавством.

Кібератакам зовнішнього порушника протистоїть система захисту інформації інформаційної системи об'єктів критичної інфраструктури, до функцій якої обов'язково мають входити:

– захист периметра мережі;
– забезпечення безпеки міжмережевих взаємодій;
– моніторинг і аудит безпеки;
– виявлення і запобігання діям атак;

– резервне копіювання і відновлення даних;

– аналіз захищеності і керування політикою безпеки;

– контроль цілісності даних;

– захист від шкідливого програмного забезпечення;

– фільтрація контенту і запобігання витоку конфіденційної інформації;

– установка оновлень програмного забезпечення;

– адміністрування безпеки.

За результатами проведеного аналізу загроз та уразливостей [1], можна зазначити, що захист таких систем має розглядатися за такими напрямами:

– захист інформаційних і фізичних компонентів інформаційної системи об'єктів критичної інфраструктури;

– технічний захист інформації інформаційних систем об'єктів критичної інфраструктури;

– захист процесів, процедур і програм обробки інформації інформаційних систем об'єктів критичної інфраструктури;

– захист каналів зв'язку інформаційних систем об'єктів критичної інфраструктури;

– придушення побічних електромагнітних випромінювань;

– керування та контроль системою захисту.

Таким чином, з урахуванням викладеного можна зазначити, що на стан забезпечення кібербезпеки інформаційної системи об'єкта критичної інфраструктури впливають такі фактори:

– наявність необхідної та достатньої нормативно-правової бази з питань забезпечення кібербезпеки інформаційних систем об'єктів критичної інфраструктури;

– наявність джерел кіберзагроз, їхні можливості, тип, вид, мета, мотиви, зацікавленість у здійсненні кібератак;

– наявність уразливостей у системах кіберзахисту, які можуть використовуватися у разі здійснення кібератак;

– наявність чи відсутність сприятливих умов для реалізації кіберзагроз;

– привабливість активів, на які, власне, і спрямовуються кібератаки;

– наслідки від можливої реалізації кіберзагроз;

– рівень фахової підготовки співробітників, відповідальних за кібербезпеку на всіх рівнях: організація, підприємство, галузь, відомство тощо.

Висновки і перспективи подальших досліджень у цьому напрямку. Виконано аналіз впливу на екологію стану кібербезпеки об'єктів критичної інфраструктури та факторів, що впливають на стан кібербезпеки інформаційної системи об'єкта критичної інфраструктури. Розглянуто методику оцінки ступеня можливого збитку від реалізації загроз безпеці інформації.

Результати проведеного аналізу можна використати під час розробки пропозицій та заходів, спрямованих на уникнення наслідків кібератак на об'єкти критичної інфраструктури.

Перспективою подальших наукових досліджень є розроблення методики визначення співвідношення між конкретними кібератаками та можливими кількісними збитками.

Література

1. Industrial communication networks – Network and system security: IEC 62443-1-1. Part 1-1: Terminology, concepts and models.
2. Гончар С., Леоненко Г., Юдін О. Підходи до оцінки небезпеки атак в інформаційних системах об'єктів критичної інфраструктури. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. 2015. № 2(30). С. 47−52 с.
3. Домарев В. Безопасность информационных технологий. Методология создания систем защиты. Киев, Украина: ООО «ТИД «ДС», 2002.