InterConf
Scientific Publishing Center

THE ISSUE CONTAINS:

Proceedings of the 6th International Scientific and Practical Conference

SCIENTIFIC PARADIGM IN THE CONTEXT OF TECHNOLOGIES AND SOCIETY DEVELOPMENT

Geneva, Switzerland
26-28.11.2023

Scientific Collection
InterConf

№ 180
November, 2023

OPEN ACCESS

LIGHT INDUSTRY AND FOOD INDUSTRY

RADIO ENGINEERING, ELECTRONICS AND ELECTRICAL ENGINEERING

INFORMATION AND WEB TECHNOLOGIES

Proceedings of the 6th International
Scientific and Practical Conference
«Scientific Paradigm in the Context of
Technologies and Society Development»
(November 26-28, 2023).
Geneva, Switzerland

No
180

INFORMATION AND WEB TECHNOLOGIES

Визначення рівнів критичності при реагуванні на кіберінциденти

Голубничий Дмитро Юрійович[1], **Коломійцев Олексій Володимирович**[2], **Третяк Вячеслав Федорович**[3], **Бречко Вероніка Олександрівна**[4], **Колмиков Максим Миколайович**[5], **Шумило Ліна Сергіївна**[6], **Любченко Олексій Вікторович**[6]

[1] кандидат технічних наук, доцент, доцент кафедри Інформаційних систем;
Харківський національний економічний університет імені Семена Кузнеця; Україна

[2] Заслужений винахідник України, доктор технічних наук,
професор кафедри комп'ютерної інженерії та програмування;
Національний технічний університет «Харківський політехнічний інститут»; Україна

[3] кандидат технічних наук, доцент, старший науковий співробітник,
науковий співробітник наукового центру Повітряних Сил;
Харківський національний університет Повітряних Сил імені Івана Кожедуба; Україна

[4] кандидат технічних наук, доцент кафедри комп'ютерної інженерії та програмування;
Національний технічний університет «Харківський політехнічний інститут»; Україна

[5] кандидат технічних наук, старший науковий співробітник,
провідний науковий співробітник науково-дослідної лабораторії;
Харківський національний університет Повітряних Сил імені Івана Кожедуба; Україна

[6] магістрант;
Харківський національний економічний університет імені Семена Кузнеця; Україна

[7] аспірант кафедри комп'ютерної інженерії та програмування;
Національний технічний університет «Харківський політехнічний інститут»; Україна

У сучасному світі важко уявити наше існування без інформаційних технологій, а кіберпростір став не лише невід'ємною складовою, а й невичерпним резервуаром можливостей. Даний прогрес супроводжується зростанням як кількісної, так і якісної складності кіберінцидентів, що можуть становити серйозну загрозу для окремих користувачів, підприємств, організацій, державних структур тощо. З такої причини виявлення та ефективне реагування на кіберзагрози стає надзвичайно актуальною проблемою у інформаційному суспільстві. Вирішення висвітлених завдань відіграє ключову роль у підвищенні рівня безпеки та надійного захисту інформаційних ресурсів, систем і мереж, забезпечуючи

INFORMATION AND WEB TECHNOLOGIES

безперебійну функціональність інфраструктури.

На даний час проблема полягає у тому, що кіберзагрози стають усе більш складними та різнобічними. Зловмисники активно впроваджують та вдосконалюють нові технології, методи та інструменти для проведення кібератак на різні об'єкти, ускладнюючи виявлення таких кіберінцидентів та їх захист. Наприклад, хакери можуть застосовувати фішинг, DDoS-атаки, використання вразливостей у програмному забезпеченні та інші методи для отримання несанкціонованого доступу та завдання шкоди. Тому, важливо розробляти та впроваджувати ефективні заходи щодо забезпечення інформаційної безпеки. Реагування на кіберінциденти повинно бути адаптоване до їх критичності, що визначає ступінь загрози, з метою ефективного протидії та мінімізації наслідків для системи або організації, які потрапили під вплив.

Реагування на кіберінциденти/кібератаки здійснюється суб'єктами забезпечення кібербезпеки шляхом вжиття заходів до кіберзахисту, спрямованих на швидке виявлення та захист від кіберінцидентів/кібератак, належне інформування про них, запобігання негативним наслідкам, їх мінімізації та усунення, виправлення вразливостей, а також відновлення сталості і надійності функціонування інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, технологічних систем та інших об'єктів кіберзахисту [5].

Реагування на кіберінциденти/кібератаки здійснюється суб'єктами забезпечення кібербезпеки послідовно такими етапами, як підготовка, виявлення та аналіз, стримування, усунення, відновлення, аналіз ефективності заходів з реагування на кіберінциденти/кібератаки [6].

Вирішення даної проблеми вимагає постійного вдосконалення та розгортання стратегій реагування і захисту від кіберінцидентів у сучасному високотехнологічному світі, де залежність від інформаційних систем лише збільшується, надаючи їй велику актуальність.

У останні роки світ став свідком значного зростання кількості і якості кібератак, які мають серйозні наслідки: витік конфіденційних даних, фінансові збитки, порушення приватності, призупинення роботи критичних систем та інші негативні випадки. Усе це ставить під загрозу безпеку та стабільність суспільства у цілому.

Окремі заходи є повторюваними і можуть виконуватися та змінюватися безперервно, доки підозріла поведінка не буде усунена, наслідки кіберінциденту (кібератаки) не будуть ліквідовані, електронні докази, необхідні для проведення

INFORMATION AND WEB TECHNOLOGIES

розслідування та аналізу процесу реагування на кіберінциденти (кібератаки), – не будуть зібрані.

Кіберінцидент – це подія, яка може завдати шкоди інформаційній системі, мережі або даним. Більш розвинуте визначення надається у Законі України "Про основні засади забезпечення кібербезпеки України" [7].

Кіберінцидент – подія або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактора) та/або таких, що мають ознаки можливої (потенційної) кібератаки, які становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами, створюють ймовірність порушення штатного режиму функціонування таких систем (у тому числі зриву та/або блокування роботи системи, та/або несанкціонованого управління її ресурсами), ставлять під загрозу безпеку (захищеність) електронних інформаційних ресурсів [7].

Кіберінциденти поділяються на різні типи залежно від характеру атак та їхньої мети. До загальної класифікації кіберінцидентів можливо віднести наступні:

1. Шкідливе програмне забезпечення (ПЗ) (Malware – скорочення від malicious – зловмисний і software – ПЗ):

– віруси (Viruses): програми, які прикріплюються до інших програм та поширюються під час їх використання;

– черв'яки (Worms): самостійні програми, які поширюються через мережу та використовують автоматичні засоби для розповсюдження;

– троянські коні (Trojans): зловмисні програми, які приховуються під корисними, але виконують шкідливі функції.

2. Атаки на мережевий рівень:

– відмова в обслуговуванні (Denial of Service): спроби зробити ресурс або мережу недоступними для легітимних користувачів;

– віддалена відмова в обслуговуванні з використанням великої кількості серверів (Distributed Denial of Service, DDoS): використання багатьох комп'ютерів для організації атаки DoS.

3. Фішинг: спроби обдурити користувачів, щоб отримати їхні конфіденційні дані.

4. Соціальна інженерія: використання маніпуляційних технік для отримання конфіденційної інформації від людей.

5. Витік інформації (Data Breach): несанкціоноване отримання, витік або втрата конфіденційної інформації.

INFORMATION AND WEB TECHNOLOGIES

6. Шпигунство (Espionage): атаки, спрямовані на отримання конфіденційної інформації для користування конкурентами, країнами або злочинцями.

7. Крадіжка ідентичності (Identity Theft): використання чужого ідентифікаційного матеріалу для здійснення шахрайських дій.

8. Атаки на ПЗ: використання вразливостей у ПЗ для здійснення атак.

9. Фармінг (Pharming): ведення користувачів на підроблені веб-сайти для збору їхніх конфіденційних даних.

10. Зловживання привілеїв: використання несанкціонованих привілеїв для отримання доступу до системи або даних.

Перелічена класифікація відображає різноманітність та складність кіберінцидентів, які можуть виникати вусучасному інтернет-просторі.

Зміцнення кібербезпеки в організації вимагає комплексного підходу та прийняття різноманітних заходів. Отже, до рекомендацій можливо віднести наступні:

– оцінка ризиків: проведення регулярних аналізів ризиків для виявлення потенційних загроз і слабких місць в інформаційній системі;

– політика безпеки: розробка та впровадження чіткої політики безпеки, яка охоплює усі аспекти інформаційної безпеки;

– співробітництво з персоналом: навчання персоналу щодо основ безпеки, включаючи правила безпечного користування паролями, впізнавання фішингових атак тощо;

– антивірусні заходи: використання актуального антивірусного ПЗ та регулярне оновлення вірусних баз даних;

– оновлення ПЗ: регулярне оновлення усього ПЗ для усунення вразливостей, які можуть бути використані зловмисниками;

– захист мережі: використання файерволів та інших технічних засобів для захисту мережі від несанкціонованого доступу;

– захист даних: шифрування чутливої інформації та встановлення обмежень доступу до неї;

– аудит безпеки: проведення регулярних аудитів безпеки для виявлення вразливостей та слабких місць;

– резервне копіювання: регулярне резервне копіювання важливої інформації та перевірка можливості відновлення даних;

– моніторинг інцидентів: встановлення систем моніторингу для виявлення незвичайної активності та реагування на

потенційні інциденти безпеки;

– управління доступом: впровадження систем контролю доступу і привілеїв для обмеження доступу до інформації на необхідному рівні;

– безпека мобільних пристроїв: забезпечення безпеки мобільних пристроїв, включаючи використання паролів, шифрування та віддалену блокування/видалення даних у разі втрати;

– захист фізичного доступу: обмеження фізичного доступу до серверних приміщень та інших важливих об'єктів;

– страхування від кіберзагроз: розгляд можливості отримання страхового покриття від кіберзагроз.

Перелічені заходи допоможуть створити більш безпечне інформаційне середовище для організації (підприємства тощо).

Слід зазначити, що стан справ у галузі кібербезпеки постійно змінюється, оскільки зловмисники розвивають нові методи атак та/або вдосконалюють існуючі. Тенденції розвитку засобів захисту від кіберзагроз включають наступні:

– машинне навчання та штучний інтелект: використання машинного навчання для аналізу великої кількості даних для виявлення нестандартної активності та автоматичного реагування на загрози;

– аналіз великих даних (Big Data): збільшення обсягів даних, які обробляються для виявлення аномальних патернів та ідентифікації потенційних загроз;

– захист у реальному часі: перехід від реактивного підходу до проактивного, здатного реагувати у реальному часі на потенційні загрози;

– кібергігієна: зростання уваги до людей, як слабкої ланки у інформаційній безпеці та акцент на навчанні і освіті для зменшення ризиків, пов'язаних з соціальним інженерінгом;

– кіберзахист на рівні архітектури: врахування аспектів кіберзахисту при розробці та впровадженні архітектури інформаційних систем;

– розширений захист від мобільних загроз: розвиток рішень для захисту мобільних пристроїв та додатків, оскільки вони стають більшою мішенню для кіберзлочинців;

– блокчейн для кіберзахисту: використання технології блокчейн для забезпечення конфіденційності, цілісності та доступу до даних у інформаційних системах;

– захист від атак на рівні додатків: зростання уваги до безпеки додатків, включаючи розробку безпечних кодів та виявлення вразливостей під час тестування;

– безпека інтернет речей (IoT): розвиток рішень для

INFORMATION AND WEB TECHNOLOGIES

захисту підключених до Інтернету пристроїв та мереж, щоб запобігти можливим атакам через IoT;

– захист від розподілених атак: розвиток засобів захисту, які можуть виявляти та запобігати розподіленим атакам, таким як DDoS (розподілене блокування послуг).

Застосування даних тенденцій може допомогти організаціям (підприємствам тощо) підтримувати високий рівень кібербезпеки в умовах постійно змінюючогося кіберсередовища.

Визначення рівнів критичності при реагуванні на кіберінциденти є важливим етапом в управлінні кібербезпекою. Процес визначення рівнів критичності допомагає оцінити серйозність ймовірних наслідків для організації та призначити відповідні рівні придатності для кожного кіберінциденту. Такий процес може бути реалізований через створення матриці критичності, де враховуються різні аспекти інциденту.

На приклад, декілька ключових кроків та критеріїв, які можуть використовуватися для визначення рівнів критичності:

– визначення важливості систем та даних: оцінка того, наскільки критичні для діяльності організації є системи та дані, які можуть бути залучені до кіберінциденту;

– оцінка потенційного впливу: аналіз можливих наслідків для бізнес-процесів, фінансів, репутації та інших аспектів діяльності організації у разі кіберінциденту;

– врахування рівня конфіденційності: визначення того, або інцидент може призвести до витоку чутливої інформації та його можливих наслідків для конфіденційності;

– оцінка доступності: врахування можливих перерв у роботі систем та послуг, що може призвести до зупинки виробництва або інших негативних впливів на доступність і послуги;

– аналіз ймовірності виникнення: врахування ймовірності виникнення конкретного інциденту на основі внутрішніх та зовнішніх факторів;

– структурування матриці критичності: створення матриці, де різні аспекти критичності оцінюються на числових або категорійних шкалах;

– призначення рівнів критичності: призначення кожному інциденту конкретного рівня критичності відповідно до його місця у матриці;

– розробка плану реагування: засновано на призначеному рівні критичності, розробка конкретних кроків та заходів для реагування на інцидент.

Категорія (рівень) критичності кіберінциденту (кібератаки) визначається відповідно до трьох критеріїв критичності кіберінциденту (кібератаки) [6]:

INFORMATION AND WEB TECHNOLOGIES

А. Загроза порушення сталого, надійного та штатного режиму функціонування систем (системи):

А1. Загрози немає.

А2. Безпосередня загроза для сталого, надійного та штатного режиму функціонування систем (конкретної системи суб'єкта забезпечення кібербезпеки).

А3. Безпосередня загроза для сталого, надійного та штатного режиму функціонування декількох систем окремого суб'єкта забезпечення кібербезпеки.

А4. Безпосередня загроза для сталого, надійного та штатного режиму функціонування значної кількості систем декількох суб'єктів забезпечення кібербезпеки.

А5. Транскордонний вплив загрози порушення сталого, надійного та штатного режиму функціонування систем.

Б. Загроза порушення захищеності (конфіденційності, цілісності і доступності) інформації та даних, які обробляються у системах (системі):

Б1. Загрози немає.

Б2. Створені передумови для порушення захищеності (конфіденційності, цілісності та доступності) інформації та даних, які обробляються у системах (системі).

Б3. Порушення захищеності (конфіденційності, цілісності та доступності) інформації та даних, що обробляються у системах (системі).

В. Загрози для національної безпеки і оборони, стану навколишнього природнього середовища, соціальної сфери, національної економіки та її окремих галузей, припинення виконання функцій та/або надання послуг об'єктами критичної інфраструктури:

В1. Загрози немає.

В2. Передумови для припинення виконання функцій та/або надання послуг об'єктами критичної інфраструктури.

В3. Потенційні загрози для національної безпеки і оборони, стану навколишнього природнього середовища, соціальної сфери, національної економіки та її окремих галузей, припинення виконання функцій та/або надання послуг об'єктами критичної інфраструктури.

В4. Реальні загрози для національної безпеки і оборони, стану навколишнього природнього середовища, соціальної сфери, національної економіки та її окремих галузей, припинення виконання функцій та/або надання послуг об'єктами критичної інфраструктури.

В5. Невідворотна загроза для повноцінного функціонування держави або загроза життю громадян України.

INFORMATION AND WEB TECHNOLOGIES

Суб'єкт забезпечення кібербезпеки, вибравши необхідні варіанти в трьох критеріях критичності кіберінциденту (кібератаки), визначає категорію (рівень) критичності кіберінциденту (кібератаки) відповідно до таблиці 1.

Таблиця 1

Визначення категорії (рівня) критичності кіберінциденту (кібератаки)

Критерії визначення категорії (рівня) критичності												Категорія (рівень) критичності, що визначається
А					Б			В				
А1	А2	А3	А4	А5	Б1	Б2	Б3	В1	В2	В3	В4	В5	
●					●			●					0, некритичний (білий)
	●				●			●					1, низький (зелений)
	●				●								1, низький (зелений)
		●			●			●					1, низький (зелений)
		●				●		●					1, низький (зелений)
	●					●		●					2, середній (жовтий)
	●					●			●				2, середній (жовтий)
		●				●		●					2, середній (жовтий)
	●						●	●					3, високий(помаранчевий)
	●						●		●				3, високий(помаранчевий)
	●						●			●			3, високий(помаранчевий)
	●						●				●		4, критичний (червоний)
		●					●				●		4, критичний (червоний)
		●					●					●	5, надзвичайний (чорний)
			●				●					●	5, надзвичайний (чорний)
				●			●				●		5, надзвичайний (чорний)
				●			●					●	5, надзвичайний (чорний)

Зіставлення критеріїв критичності кіберінциденту (кібератаки) необхідно здійснювати послідовно від А до В.

Варіанти категорій (рівнів) критичності кіберінциденту (кібератаки) враховуються відповідно до однакової важливості усіх критеріїв визначення категорії (рівня) критичності кіберінциденту (кібератаки) та узгоджені між собою.

За умови, якщо для кіберінциденту (кібератаки) можливі два варіанти категорії (рівня) критичності кіберінциденту (кібератаки) (наприклад, середній (жовтий) та високий (помаранчевий)), то рекомендовано обирати вищу категорію (рівень) критичності кіберінциденту (кібератаки) (в зазначеному прикладі – високий (помаранчевий)).

Про кіберінциденту (кібератаки) інформують відповідальних суб'єктів за реагування на конкретний кіберінциденту (кібератаки) (CERT-UA, за необхідності можуть бути проінформовані інші суб'єкти). Для інформування використовують картку інформування про кіберінцидент (кібератаку). Також, інформується керівництво суб'єкта

забезпечення кібербезпеки та керівник відповідного підрозділу у сфері IT, інформаційної безпеки або кібербезпеки/кіберзахисту, а також відповідальний адміністратор системи (мережевий адміністратор, адміністратор безпеки тощо) про необхідність проведення розслідування та реагування.

У випадках, коли мають місце декілька кіберінцидентів (кібератак), необхідно визначити черговість реагування на кожен кіберінцидент (кібератака) з метою ефективного розподілу ресурсів на реагування (часових, людських, матеріальних тощо) та зменшення негативного впливу (подальшої ескалації) кіберінциденту (кібератаки) на системи/мережі суб'єкта забезпечення кібербезпеки. Для цього необхідно визначити пріоритети реагування відповідно до:

– категорії кіберінциденту (кібератаки);

– особливостей впливу кіберінциденту (кібератаки) системи/мережі суб'єкта забезпечення кібербезпеки (особливості підозрілої поведінки, виявленої у рамках реагування на кіберінциденту (кібератаки), шляхи проникнення в системи/мережі, способи поширення у внутрішньому периметрі системи/мережі, негативний вплив на інфраструктуру системи/мережі (мережеві пристрої, хости, сховища даних, а також на ПЗ зазначеної інфраструктури);

– функціональних наслідків кіберінциденту (кібератаки) (впливу на поточну функціональність уражених систем/мереж, впливу на бізнес-процеси та надання послуг користувачам таких систем/мереж, майбутніх функціональних наслідків кіберінциденту (кібератаки), якщо його не буде негайно стримано (локалізовано));

– інформаційних наслідків кіберінциденту (кібератаки) (впливу на конфіденційність, цілісність і доступність (інші властивості) інформації, що обробляється в уражених системах/мережах суб'єкта забезпечення кібербезпеки), інформаційного впливу на інші суб'єкти забезпечення кібербезпеки (партнерів, наприклад, у випадках доступу та модифікації конфіденційної інформації);

– можливості відновлення після кіберінциденту (кібератаки) (кількість ресурсів (часових, людських, матеріальних тощо), які необхідно витратити на відновлення після цього кіберінциденту (кібератаки), зусилля, необхідні для фактичного відновлення після кіберінциденту (кібератаки), визначення, наскільки ці зусилля будуть варті мети, задля якої вони застосовуються, та як зусилля з відновлення співвідносяться з будь-якими іншими вимогами з реагування на

INFORMATION AND WEB TECHNOLOGIES

кіберінциденту (кібератаки)).

Враховуючи дані аспекти, організації (підприємства тощо) можуть ефективно призначати критичність кіберінцидентів та вчасно реагувати для зменшення можливих наслідків.

Проведені експериментальні дослідження показали, що методика визначення рівнів критичності при реагуванні на кіберінциденти є ефективним інструментом для забезпечення ефективного реагування на перелічені інциденти. Методика дозволяє оцінити масштаб і ризики, які пов'язані з інцидентом та, на основі цього, прийняти рішення про необхідність і обсяги реагування.

References:

[1] Шумило Л. С. Порядок реагування на кіберінциденти відповідно до рівнів критичності / Л. С. Шумило // Матеріали Міжнародної науково-практичної конференції – Сучасні інформаційні системи та технології в цифровому суспільстві : тези доповідей, 13-14 квітня 2022 р. – Харків : ХНЕУ імені Семена Кузнеця, 2022. – С. 28.

[2] Остапов С. Е. Технології захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Харків : Вид. ХНЕУ, 2013. – 476 с.

[3] Голубничий Д. Ю. Аналіз сучасних загроз в інформаційних системах за складовими загроз: кібербезпеки, інформаційної безпеки та безпеки інформації / Д.Ю. Голубничий, О.В. Сєвєрінов, О.В. Коломійцев та ін. // Scientific Collection «InterConf»: with the Proceedings of the 3th International Scientific and Practical Conference «Scientific Community: Interdisciplinary Research» (March 16-18, 2021). — Hamburg, Germany: Busse Verlag GmbH, 2021. – № 45. — Pp. 541 – 550.

[4] Голубничий Д. Ю. Функціональна модель управління системою інформаційної безпеки / Д. Ю. Голубничий, В. Ф. Третяк, Д. М. Запара та ін. // Theoretical and practical aspects of development of legal knowledge, national security and physical education of citizens: Collective Scientific Monograph (1st edition). Tomkins R. (ed.). – Dallas, USA: Primedia eLaunch LLC, 2022. – С. 68-79.

[5] Про План реалізації Стратегії кібербезпеки України / Рішення Ради національної безпеки і оборони України від 30.12.2021. Введено в дію Указом Президента України від 1 лютого 2022 року № 37/2022. – Київ : РНБО, 2022. – 15 с.

[6] Про затвердження Методичних рекомендацій щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі / Наказ Адміністрації Держспецзв'язку від 03.07.2023 р. № 570.

[7] Закон України "Про основні засади забезпечення кібербезпеки України" № 2163-VIII / Відомості Верховної Ради (ВВР), 2017, № 45, ст. 403. [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-viii.

SCIENTIFIC EDITION

SCIENTIFIC COLLECTION «INTERCONF»

№ 180 | November, 2023

The issue contains:

Proceedings of the 6th International
Scientific and Practical Conference

SCIENTIFIC PARADIGM IN THE CONTEXT OF TECHNOLOGIES AND SOCIETY DEVELOPMENT

Geneva, Switzerland
26-28.11.2023

All materials are reviewed.
The editorial office did not always agree with the position of authors.

Sighed for online publication: November 28, 2023.

Printed: December 26, 2023. Circulation: 200 copies. Format 60×84/8.
Batang & Courier New typefaces. Offset paper 100gsm. Digital color printing.

Contacts of the editorial office:

LLC Scientific Publishing Center «InterConf»
info@interconf.center
https://www.interconf.center

Certificate on the entry of publishing business subject in the State Register of Publishers, Manufacturers and Distributors of Publishing Products of Ukraine: ДК № 7882 of 10.07.2023.