НАЦІОНАЛЬНИЙ СТАНДАРТ УКРАЇНИ

ДСТУ ISO/IEC 27032:2016
(ISO/IEC 27032:2012, IDT)

Інформаційні технології

МЕТОДИ ЗАХИСТУ

Настанови щодо кібербезпеки

Видання офіційне

Київ
ДП «УкрНДНЦ»
2018

ПЕРЕДМОВА

1 РОЗРОБЛЕНО: Міжнародний науково-навчальний центр інформаційних технологій та систем НАН та МОН України (Міжнародний центр), Технічний комітет стандартизації «Інформаційні технології» (ТК 20)

2 ПРИЙНЯТО ТА НАДАНО ЧИННОСТІ: наказ Державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» (ДП «УкрНДНЦ») від 27 грудня 2016 р. № 448 з 2018–01–01

3 Національний стандарт відповідає ISO/IEC 27032:2012 Information technology — Security techniques — Guidelines for cybersecurity (Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки)

Ступінь відповідності — ідентичний (IDT)

Переклад з англійської (en)

4 Цей стандарт розроблено згідно з правилами, установленими в національній стандартизації України

5 НА ЗАМІНУ ДСТУ ISO/IEC 27032:2015

**Право власності на цей національний стандарт належить державі.
Заборонено повністю чи частково видавати, відтворювати
задля розповсюдження і розповсюджувати як офіційне видання
цей національний стандарт або його частини на будь-яких носіях інформації
без дозволу ДП «УкрНДНЦ» чи уповноваженої ним особи**

ДП «УкрНДНЦ», 2018

ЗМІСТ

НАЦІОНАЛЬНИЙ ВСТУП

Цей національний стандарт ДСТУ ISO/IEC 27032:2016 (ISO/IEC 27032:2012, IDT) «Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки», прийнятий методом перекладу, — ідентичний щодо ISO/IEC 27032:2012 «Information technology — Security techniques — Guidelines for cybersecurity» (версія en).

Технічний комітет стандартизації, відповідальний за цей стандарт в Україні, — ТК 20 «Інформаційні технології».

Цей стандарт прийнято на заміну ДСТУ ISO/IEC 27032:2015, прийнятого методом підтвердження.

У цьому національному стандарті зазначено вимоги, які не суперечать законодавству України.

До стандарту внесено такі редакційні зміни:

— слова «цей міжнародний стандарт» та «цей документ» замінено на «цей стандарт»;

— структурні елементи стандарту: «Титульний аркуш», «Передмова», «Національний вступ», першу сторінку, «Терміни та визначення понять» і «Бібліографічні дані» — оформлено згідно з вимогами національної стандартизації України;

— у розділі 2 наведено «Національне пояснення», виділене рамкою;

— вилучено «Передмову» до ISO/IEC 27032:2012 як таку, що безпосередньо не стосується технічного змісту цього стандарту;

— долучено довідковий додаток НА (Перелік національних стандартів, згармонізованих із міжнародними чи їхніми європейськими аналогами, на які є посилання в цьому стандарті).

Копії нормативних документів, на які є посилання в цьому стандарті, можна отримати в Національному фонді нормативних документів.

ВСТУП до ISO/IEC 27032:2012

Кіберпростір є складним середовищем взаємодії людей, програмного забезпечення та послуг у мережі Інтернет та функціонує за підтримки об'єднаних мереж і пристроїв інформаційних та комунікаційних технологій (ICT, information and communications technology). Однак є окремі питання безпеки, які не входять ні до сучасної інформаційної безпеки, ні до Інтернет-безпеки, ні до мережевої чи й ІСТ-безпеки, бо між цими видами безпеки є своєрідні прогалини, а також між організаціями та постачальниками послуг у кіберпросторі часто бракує тісних зв'язків. Це відбувається тому, що об'єднані мережі та пристрої в кіберпросторі мають багато власників, у кожного з яких свій власний бізнес та коло проблем, пов'язаних з експлуатацією та контролем. Кожна організація та постачальник послуг у кіберпросторі має свою точку зору на безпеку тих областей, у яких є незначний вхідний потік відомостей від іншої організації або постачальника, що призводить до фрагментації стану безпеки в кіберпросторі.

Отже, головну увагу цього стандарту приділено вирішенню проблем безпеки в кіберпросторі (так званої кібербезпеки), які виникають унаслідок прогалин у безпеці різних частинах кіберпростору. Цей стандарт містить технічні рекомендації для подолання ризиків кіберпростору, зокрема:

— атаки соціальної інженерії;

— злам (хакінг);

— поширення шкідливого програмного забезпечення («шкідливих програм»);

— шпигунські програми;

— інші потенційно небажані програми.

Технічні настанови стосуються контролю над цими ризиками, зокрема розглядають:

— підготовку до атак, наприклад, шкідливих програм, окремих зловмисників чи злочинних організацій в Інтернеті;

— виявлення та моніторинг атак;

— реагування на атаки.

Також у цьому стандарті увагу приділено співпраці, оскільки є потреба в ефективному обміні інформацією, координації дій та реагуванні на інциденти з боку всіх зацікавлених сторін у кіберпросторі.

Ця співпраця має відбуватися безпечно та надійно й захищати конфіденційність зацікавлених сторін. Представники цих сторін можуть перебувати в різних географічних точках, різних часових поясах та, ймовірно, можуть керуватися різними нормативними вимогами. Зацікавлені сторони охоплюють:

— споживачів, які можуть належати різним організаціям чи просто бути різними фізичними особами;

— постачальників, зокрема постачальників послуг.

Отже, цей стандарт окреслює рамки для:

— обміну інформацією;

— координації дій;

— реакції на інциденти.

Також у цьому стандарті розглянуто такі питання:

— ключові міркування щодо встановлення довірчих відносин;

— необхідні засади для співпраці й обміну інформацією та відомостями;

— технічні вимоги до системної інтеграції та взаємодії між різними зацікавленими сторонами.

Зважаючи на область застосування матеріалів цього стандарту, усі елементи контролю та керування мають бути на високому рівні. У стандарті також є посилання на інші стандарти з докладними технічним специфікаціями та вказівки щодо застосування у відповідних областях.

НАЦІОНАЛЬНИЙ СТАНДАРТ УКРАЇНИ

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

МЕТОДИ ЗАХИСТУ

Настанови щодо кібербезпеки

INFORMATION TECHNOLOGY

SECURITY TECHNIQUES

Guidelines for cybersecurity

Чинний від 2018–01–01

1 ПРИЗНАЧЕННЯ

Цей стандарт містить рекомендації щодо підвищення рівня кібербезпеки, розглядаючи різні аспекти цього питання та їхній зв'язок з іншими видами безпеки, зокрема:

— інформаційною безпекою;
— мережевою безпекою;
— Інтернет-безпекою;
— захистом інформаційної інфраструктури.

У стандарті розглянуто основні методи захисту зацікавлених сторін у кіберпросторі. Стандарт містить:

— огляд кібербезпеки;
— пояснення зв'язків між кібербезпекою та іншими видами безпеки;
— визначення зацікавлених сторін та їхньої ролі в кіберпросторі;
— настанова з вирішення основних питань кібербезпеки;
— способи взаємодії зацікавлених сторін для вирішення основних питань кібербезпеки.

2 СФЕРА ЗАСТОСУВАННЯ

2.1 Цільова аудиторія

Цей стандарт стосується постачальників послуг у кіберпросторі. Але цільова аудиторія охоплює також споживачів, які користуються цими послугами. Якщо організації надають послуги в кіберпросторі іншим організаціям або людям для домашнього використання, то таким організаціям може знадобитися підготувати настанови на основі цього стандарту, які міститимуть додаткові пояснення або приклади, необхідні для повного розуміння читачами того, як треба діяти.

2.2 Обмеження

У цьому стандарті не розглянуто таких питань, як:

— кібербезпека;
— кіберзлочин;
— захист інформаційної інфраструктури;
— захист Інтернету;
— злочинність в Інтернеті.

Потрібно зазначити, що є певний зв'язок між кібербезпекою та зазначеними вище поняттями. Однак питання зв'язків між цими поняттями та розподілу методів контролю та керування виходить за рамки цього стандарту.

Видання офіційне

Важливо зазначити, що поняття кіберзлочинності, хоча було згадано, але також не розглянуто. Цей стандарт не містить вказівок щодо різних аспектів права, пов'язаних із кіберпростором або регуляцією кіберзахисту.

У цьому стандарті розглянуто лише питання реалізації кіберпростору в Інтернеті, включаючи кінцеві точки. При цьому залишаємо поза увагою реалізацію кіберпростору в комунікаційних медіа, платформах та відповідні аспекти безпеки на фізичному рівні.

Приклад 1

Не розглянуто питання безпеки таких елементів інфраструктури, як носії зв'язку, які забезпечують функціонування кіберпростору.

Приклад 2

Не розглянуто питання безпеки мобільних телефонів, під'єднаних до кіберпростору для завантаження відомостей та/або інших операцій.

Приклад 3.

Не розглянуто відправлення текстових повідомлень та роботу в голосовому чаті на мобільних телефонах.

3 НОРМАТИВНІ ПОСИЛАННЯ

Наведені нижче документи потрібні для застосування цього стандарту. У разі датованих посилань застосовують тільки наведені видання. У разі недатованих посилань потрібно користуватись останнім виданням нормативних документів (разом зі змінами).

ISO/IEC 27000 Information technology — Security techniques — Information security management systems — Overview and vocabulary.

НАЦІОНАЛЬНЕ ПОЯСНЕННЯ

ISO/IEC 27000 Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Огляд і термінологія.

4 ТЕРМІНИ ТА ВИЗНАЧЕННЯ ПОНЯТЬ

У цьому стандарті вжито терміни та визначення понять згідно з ISO/IEC 27000, а також наведені нижче.

4.1 рекламні програми (*adware*)

Програми, які нав'язують користувачам рекламу чи збирають інформацію про онлайн-поведінку користувачів.

Примітка. Установлення таких програм може відбуватись як з відома користувача та за його згодою, так і без них, а також може бути частиною ліцензованої угоди іншого програмного продукту

4.2 програма (*application*)

ІТ-продукт, зокрема програмне забезпечення, відповідні відомості та процедури, метою яких є допомога користувачу у виконанні певних завдань чи в розв'язанні ІТ-задач за допомогою автоматизації бізнес-процесів чи функцій

[ISO/IEC 27034-1:2011]

4.3 постачальник послуг з підтримки програм (*application service provider*)

Оператор, який за допомогою програм, розміщених на хості, надає послуги з підтримки як веб-програм, так і програм у схемі клієнт-сервер.

Приклад

Оператори онлайн-ігор, постачальники офісних програм та постачальники послуг для онлайн-зберігання відомостей

4.4 послуги програм (*application services*)

Програмне забезпечення з відповідною функціональністю, що надається онлайн за вимогою абонентів і містить як веб-програми, так і програми в схемі клієнт-сервер

4.5 прикладне програмне забезпечення (*application software*)

Програмне забезпечення, створене, щоб допомагати користувачам виконувати певні завдання чи розв'язувати деякі типи задач на відміну від програмного забезпечення, яке контролює роботу комп'ютера

[ISO/IEC 18019]

4.6 актив (*asset*)

Усе, що має значення для людини, організації чи уряду.

Примітка. Узято з ISO/IEC 27000, щоб ураховувати людей та розрізняти організації та уряд (4.37)

4.7 аватар (*avatar*)

Представлення особи в кіберпросторі.

Примітка 1. Аватар можна розглядати як своєрідне альтер его людини.

Примітка 2. Аватар можна також розглядати як «об'єкт», що представляє користувача

4.8 атака (*attack*)

Спроба знищити, викрити, змінити, відключити, вкрасти чи отримати несанкціонований доступ до активу або несанкціоновано використати актив

[ISO/IEC 27000:2009]

4.9 потенціал атаки (*attack potential*)

Шанси атаки на успіх у разі її запуску; залежить від досвіду нападника, його технічних засобів та мотивації

[ISO/IEC 15408-1:2005]

4.10 вектор атаки (*attack vector*)

Спосіб чи засоби, якими зловмисник може отримати доступ до комп'ютера чи мережевого сервера з метою заподіяти певну шкоду.

4.11 гібридна атака (*blended attack*)

Атака, яка застосовує різні методи для максимізації рівня заподіяної шкоди та збільшення швидкості ланцюгових реакцій

4.12 бот, робот (*bot, robot*)

Автоматизований програмний засіб для виконання певних завдань.

Примітка 1. Цей термін часто вживають, щоб описати програми, які зазвичай запускають на стороні сервера для автоматизації таких завдань, як переадресація чи сортування електронних листів.

Примітка 2. Ботами також називають програми, які працюють як агенти щодо користувача чи інших програм або імітують людську діяльність. Найпоширенішими ботами в Інтернеті є так звані павуки (*spiders*) та сканери (*crawlers*), які збирають інформацію на сайтах для формування індексів пошукових систем

4.13 ботнет (*botnet*)

Програмне забезпечення з дистанційним керуванням, зокрема, це може бути набір шкідливих ботів, які працюють в автономному/автоматичному режимі на зламаних/уражених комп'ютерах

4.14 кукі (*cookie*) [контроль доступу]

Можливість (*capability*) або запис/тикет (*ticket*) у системі контролю доступу

4.15 кукі (*cookie*) [IPSec]

Відомості, якими обмінюються протоколи ISAKMP (*Internet Security Association and Key Management Protocol*) для запобігання DoS-атакам під час установлення SA-параметрів (*security association*)

4.16 кукі (*cookie*) [HTTP]

Обмін відомостями між HTTP-сервером і браузером для зберігання поточної інформації на стороні клієнта з подальшим використанням цих відомостей сервером.

Примітка. Веб-браузер може бути як клієнтом, так і сервером

4.17 контроль, контрзаходи (*control, countermeasure*)

Засоби керування ризиками, зокрема політики, процедури, керівні принципи, практики чи організаційні структури, які можуть бути адміністративними, технічними, управлінськими або можуть мати юридичний характер

[ISO/IEC 27000:2009]

Примітка. В інструкціях ISO 73:2009 контроль визначено просто як заходи щодо запобігання ризикам

4.18 кіберзлочин (*cybercrime*)

Кримінальна діяльність, коли послуги чи програми кіберпростору застосовують зі злочинною метою або коли кіберпростір стає джерелом, засобом, метою чи місцем злочину

4.19 кібербезпека, кіберзахищеність (*cybersafety*)

Стан захищеності від фізичного, соціального, духовного, фінансового, політичного, емоційного, професійного, психологічного, освітнього чи іншого типу наслідків несправностей, пошкоджень, помилок, нещасних випадків, збитків чи будь-яких інших подій у кіберпросторі, які можна вважати небажаними.

Примітка 1. Може йтися про захищеність від таких подій чи сторонніх впливів, які призводять до погіршення здоров'я чи економічних втрат. Це може включати захист від людей або майна.

Примітка 2. У цілому безпеку можна розуміти як стан упевненості в тому, що несприятливі наслідки не будуть зумовлені тим чи іншим чинником за тих чи інших умов

4.20 кібербезпека, безпека кіберпростору (*cybersecurity, Cyberspace security*)

Збереження конфіденційності, цілісності та доступності інформації в кіберпросторі.

Примітка 1. Це поняття також може охоплювати такі властивості, як автентичність, відповідальність, безвідмовність та надійність.

Примітка 2. Це визначення взято від визначення інформаційної безпеки з ISO/IEC 27000:2009

4.21 кіберпростір (*Cyberspace*)

Складне середовище, що є результатом взаємодії людей, програмного забезпечення та послуг у мережі Інтернет за допомогою технологічних пристроїв і підключених до них мереж; не можна сказати, що це середовище є в конкретній фізичній формі

4.22 послуги програм кіберпростору (*Cyberspace application services*)

Послуги програм (4.4), які надають у кіберпросторі

4.23 кібер-скватер, кібер-загарбник (*cyber-squatter*)

Окремі особи чи організації, які реєструють й утримують адреси (URL), що нагадують посилання або назви інших організацій у реальному світі або в кіберпросторі

4.24 шахрайське програмне забезпечення (*deceptive software*)

Програмне забезпечення, яке працює на комп'ютері користувача без його відома, без інформування користувача про свою мету та без дозволу користувача.

Приклад 1

Програма, яка змінює налаштування/конфігурації користувача.

Приклад 2

Програма, що спричинює нескінченні рекламні оголошення, що спливають, які користувачу важко відключити.

Приклад 3

Рекламні та шпигунські програми (adware and spyware)

4.25 хакінг, злам (*hacking*)

Зловмисне одержання доступу до комп'ютерної системи без дозволу користувача чи власника

4.26 хактивізм (*hactivism*)

Хакінг із політичною чи соціальною метою

4.27 інформаційний ресурс/актив (*information asset*)

Знання чи відомості, що мають цінність для людини чи організації.

Примітка. Визначення взято з ISO/IEC 27000:2009

4.28 інтернет (*an internet, internetwork*)

Сукупність взаємопов'язаних мереж.

Примітка 1. Визначення взято з ISO/IEC 27033-1:2009.

Примітка 2. Це поняття дещо відрізняється від наступного (4.29), яке, на відміну від цього (*an internet*), частіше пишуть з великої літери (*the Internet*)

4.29 Інтернет (*the Internet*)

Глобальна система взаємопов'язаних мереж відкритого доступу

[ISO/IEC 27033-1:2009]

Примітка. Це поняття дещо відрізняється від попереднього (4.28), яке, на відміну від цього (the Internet), частіше пишуть з маленької літери (an internet)

4.30 Інтернет-злочин (*Internet crime*)

Злочинна діяльність, за якої послуги або програми в Інтернеті застосовують для скоєння злочину або є об'єктом злочину, або коли Інтернет є джерелом, інструментом, метою або місцем злочину

4.31 Інтернет-безпека, Інтернет-захищеність (*Internet safety*)

Стан захищеності від фізичного, соціального, духовного, фінансового, політичного, емоційного, професійного, психологічного, освітнього чи іншого типу наслідків несправностей, пошкоджень, помилок, нещасних випадків, збитків чи будь-яких інших подій в Інтернеті, які можна вважати небажаними

4.32 Інтернет-безпека, Інтернет-захист (*Internet security*)

Збереження конфіденційності, цілісності та доступності інформації в Інтернеті

4.33 послуги Інтернет, служби Інтернет (*Internet services*)

Послуги, що надають користувачеві, щоб забезпечити доступ до Інтернету через призначення IP-адресу; зазвичай містять автентифікацію, авторизацію та доменні служби імен

4.34 постачальник послуг Інтернет, постачальник Інтернет-послуг (*Internet service provider*)

Організація, яка надає Інтернет-послуги користувачам, а також надає своїм клієнтам доступ до Інтернету.

Примітка. Постачальників Інтернет-послуг також часто називають постачальниками Інтернет-доступу

4.35 шкідливі програми, шкідливе програмне забезпечення (*malware, malicious software*)

Програмне забезпечення, розроблене зловмисниками зі злочинними намірами та має функції, які потенційно можуть завдати прямої чи непрямої шкоди користувачу та/або його комп'ютерній системі.

Приклад

Віруси, хробаки, трояни

4.36 шкідливий контент (*malicious contents*)

Програми, документи, файли, відомості або інші ресурси, що мають шкідливі функції, які можуть бути приховані в них чи замасковані

4.37 організація (*organization*)

Група людей та об'єктів з розподілом відповідальностей, повноважень і взаємовідносин

[ISO 90000:2005]

Примітка 1. У цьому стандарті фізична особа відрізняється від організації.

Примітка 2. Загалом, уряд також є організацією. У цьому стандарті уряд можна розглядати окремо від інших організацій для чіткості

4.38 фішинг (*phishing*)

Шахрайська спроба отримати особисту або конфіденційну інформацію маскуванням під надійного об'єкта в електронних комунікаціях.

Примітка. Фішинг може бути реалізовано як методами соціальної інженерії, так і технічними засобами введення в оману

4.39 фізичний актив (*physical asset*)

Актив фізичної або матеріальної природи.

Примітка. Фізичними активами, зазвичай, є готівка, обладнання, інвентар та майно, що належить фізичній особі чи організації. Програмне забезпечення вважають нематеріальним/нефізичним активом

4.40 потенційно небажане програмне забезпечення (*potentially unwanted software*)

Шахрайське програмне забезпечення, охоплюючи як шкідливе, так і нешкідливе програмне забезпечення, якщо воно має риси шахрайського програмного забезпечення

4.41 шахрайство (*scam*)

Обманні або шахрайські дії

4.42 спам (*spam*)

Зловживання в системах електронних повідомлень для відправлення великої кількості повідомлень.

Примітка. Хоча найрозповсюдженішою формою спаму є спам електронних листів, термін «спам» відносять також до аналогічних порушень щодо інших засобів масової інформації: спам у системі миттєвих повідомлень, спам у групах новин мереж Usenet, спам у пошукових системах, спам у блогах, wiki-спам, спам повідомлень у мобільних телефонах, спам на Інтернет-форумах, небажане передавання факсів

4.43 шпигунські програми (*spyware*)

Шахрайське програмне забезпечення, яке збирає особисту або конфіденційну інформацію з комп'ютерів користувачів.

Примітка. Це може бути інформація про сайти, що їх відвідують найчастіше, або така конфіденційна інформація, як паролі

4.44 стейкхолдер, зацікавлена сторона (*stakeholder*) [керування ризиками]

Фізична особа чи організація, яка може впливати, підлягати впливу відповідних рішень та дій (чи сприймати себе таким)

[Інструкції ISO 73:2009]

4.45 стейкхолдер, зацікавлена сторона (*stakeholder*) [система]
Фізична особа чи організація, яка має право, частку, вимоги або інтереси щодо системи або її властивостей, які відповідають їхнім потребам й очікуванням
[ISO/IEC 12207:2008]

4.46 загроза (*threat*)
Потенційна причина небажаного інциденту, який може завдати шкоди системі, фізичній особі чи організації.
Примітка. Визначення взято з ISO/IEC 27000:2009

4.47 троян, троянський кінь (*trojan, trojan horse*)
Шкідлива програма, яка маскується під звичайну програму

4.48 небажана пошта (*unsolicited email*)
Небажані або непрошені повідомлення електронної пошти

4.49 віртуальний актив (*virtual asset*)
Представлення активу в кіберпросторі.
Примітка. У цьому контексті валюта може бути як засобом обміну, так і чимось, що має цінність у конкретному середовищі, яким, наприклад, може бути відеогра або модель фінансових торгів

4.50 віртуальна валюта (*virtual currency*)
Грошові віртуальні активи

4.51 віртуальний світ (*virtual world*)
Змодельоване середовище з доступом до нього багатьох користувачів через онлайн-інтерфейс.
Примітка 1. Змодельовані середовища часто інтерактивні.
Примітка 2. Фізичний світ (у якому живуть люди) та його характеристики називатимемо справжнім світом, щоб відрізняти його від віртуального світу

4.52 вразливість (*vulnerability*)
Слабка сторона активу або системи контролю, яка може бути використана в разі створення загрози
[ISO/IEC 27000:2009]

4.53 зомбі, зомбований комп'ютер, дрон (*zombie, zombie computer, dron*)
Комп'ютер, який містить приховане програмне забезпечення, яке дає змогу керувати машиною віддалено, а метою такого керування найчастіше є атака на інші комп'ютери.
Примітка. Зазвичай заражений комп'ютер є одним із багатьох у ботнеті, який буде використано для здійснення шкідливої діяльності через віддалене керування.

5 ПОЗНАКИ ТА СКОРОЧЕННЯ

У цьому стандарті вжито такі скорочення:

AS	*Autonomous System* — автономна система;
AP	*Access Point* — точка доступу;
CBT	*Computer Based Training* — комп'ютерна підготовка;
CERT	*Computer Emergency Response Team* — комп'ютерна група реагування на надзвичайні ситуації;
CIRT	*Computer Incident Response Team* — комп'ютерна група реагування на інциденти;
CSIRT	*Computer Security Incident Response Team* — команда комп'ютерної безпеки з реагування на інциденти;
CIIP	*Critical Information Infrastructure Protection* — захист інфраструктури важливої інформації;
DoS	*Denial-of-Service* — відмова в обслуговуванні;
DDoS	*Distributed Denial-of-Service* — розподілена відмова в обслуговуванні;

HIDS	*Host-based Intrusion Detection System* — хост-система виявлення вторгнень;
IAP	*Independent Application Provider* — незалежний постачальник програм;
ICMP	*Internet Control Message Protocol* — протокол керуючих повідомлень в Інтернеті;
ICT	*Information and Communications Technology* — інформаційні та комунікаційні технології;
IDS	*Intrusion Detection System* — система виявлення вторгнень;
IP	*Internet Protocol* — інтернет-протокол;
IPO	*Information Providing Organization* — організація, яка збирає та надає інформацію;
IPS	*Intrusion Prevention System* — система запобігання вторгненням;
IRO	*Information Receiving Organization* — організація, яка отримує інформацію;
ISP	*Internet Service Provider* — Інтернет-постачальник;
ISV	*Independent Software Vendor* — незалежний постачальник програмного забезпечення;
IT	*Information Technology* — інформаційні технології;
MMORPG	*Massively Multiplayer Online Role-Playing Game* — масова онлайн-гра, розрахована на багатьох користувачів;
NDA	*Non-Disclosure Agreement* — договір про нерозголошення;
SDLC	*Software Development Life-cycle* — життєвий цикл розробки системи;
SSID	*Service Set Identifier* — ідентифікатор бездротової мережі;
TCP	*Transmission Control Protocol* — протокол керування передачею;
UDP	*User Datagram Protocol* — протокол датаграм користувача;
URI	*Uniform Resource Identifier* — універсальний ідентифікатор ресурсу;
URL	*Uniform Resource Locator* — уніфікований покажчик інформаційного ресурсу.

6 КОРОТКИЙ ОГЛЯД

6.1 Вступ

Безпека в Інтернеті та в кіберпросторі й надалі залишається об'єктом зростального занепокоєння. Зацікавлені сторони посилюють свою присутність у кіберпросторі за допомогою веб-сайтів і намагаються надалі впливати на віртуальний світ кіберпростору.

Приклад

Усе більше людей проводять більше часу зі своїми віртуальними аватарами у MMORPG-іграх.

У той час як деякі особи поводяться обережно зі своєю онлайн-особистістю, більшість людей завантажують свої персональні відомості в місця, де до них мають доступ усі охочі. Відомості профілів на багатьох сайтах, зокрема в соціальних мережах та чат-румах, можуть бути завантажені та збережені сторонніми особами. Це може призвести до створення цифрових досьє персональних відомостей, що можуть бути використані не за призначеністю, передані іншим особам або використані за повторного збирання відомостей. Хоча точність і цілісність цих відомостей досить сумнівні, вони все ж утворюють посилання, що ведуть до різних осіб та організацій, і ці посилання не завжди можна легко видалити. Розвиток у сферах комунікацій, розваг, транспортування, торгівлі, фінансів, страхування та охорони здоров'я створює нові ризики для зацікавлених сторін у кіберпросторі. Так, ризики можуть бути пов'язані із втратою приватності.

Конвергенція інформаційно-комунікаційних технологій, простота потрапляння в кіберпростір і звуження особистого простору між людьми привертають увагу зловмисників і злочинних організацій. Останні користуються вже наявними механізмами, такими як фішинг, спам і шпигунське програмне забезпечення, а також сучасними техніками, що розвиваються, щоб застосовувати у своїх інтересах будь-які слабкості, які вони можуть знайти в кіберпросторі. В останні роки атаки в кіберпросторі перетворилися з хакінгу для здобуття слави на організовану злочинність, або кіберзлочинність. Безліч інструментів та процесів, що раніше спостерігали в окремих випадках порушення кібербезпеки, тепер застосовують разом у змішаних атаках, часто з далекоглядними зловмисними цілями. Ці цілі змінюються від персональних атак, викрадення особистих відомостей, фінансового шахрайства чи крадіжок до політичного хактивізму. Спеціальні форуми з обговорення потенційних проблем безпеки також сприяли демонструванню методів атак та можливостей злочинців.

Багато способів бізнесових транзакцій, що проводять у кіберпросторі, стають мішенню кіберзлочинних організацій. Залежно від типу — бізнес-бізнес, бізнес-споживач або споживач-споживач — транзакції мають свої типові ризики. Ідеї на кшталт того, чим є транзакція або угода, залежать від трактування законів та від того, як кожна сторона виконує свої обов'язки. Часто проблеми використання відомостей, зібраних під час проведення транзакції або підтримки відносин, не вирішуються компетентно. Це може в результаті призвести до таких проблем безпеки, як наприклад витік інформації.

Правові й технічні проблеми, пов'язані з цими питаннями кібербезпеки, мають далекосяжні наслідки й глобальний характер. Ці проблеми можуть бути вирішені тільки коли фахівці з інформаційної безпеки, правова спільнота, нації та національні спільноти об'єднають свої зусилля в одній узгодженій стратегії. Ця стратегія має враховувати роль кожної із зацікавлених сторін та наявних ініціатив у рамках міжнародної кооперації.

Приклад

Прикладом описаної проблеми може бути той факт, що кіберпростір породжує віртуальну анонімність і непомітні атаки, які складно викрити. Це створює додаткові труднощі як для фізичних осіб, так і для організацій за встановлення довіри та ведення справ, у той самий час ускладнюючи роботу правоохоронних органів. Навіть якщо вдається визначити джерело атаки, аспекти міжнародного права часто заважають подальшому розслідуванню чи репатріації.

Просування у вирішенні цих питань ускладнене багатьма аспектами, що й сприяє подальшому розвитку кібербезпеки.

Хоча кіберзагроз і не бракує, як не бракує і нестандартизованих способів з ними боротися, увагу цього стандарту зосереджено на таких ключових питаннях:

— атаки зі сторони шкідливого та потенційно небажаного програмного забезпечення;

— атаки соціальної інженерії;

— координація дій та обмін інформацією.

Також деякі інструменти кібербезпеки будуть коротко обговорені в цьому стандарті. Ці інструменти та способи їхнього використання тісно пов'язані із запобіганням, розкриттям, розслідуванням кіберзлочинності та реагуванням на неї. Докладнішу інформацію може бути знайдено в додатку А.

6.2 Природа кіберпростору

Кіберпростір може бути описаний як віртуальне середовище, що не існує фізично, а радше є складним середовищем чи простором, що утворився в результаті виникнення Інтернету, а також включає людей, організації та різну діяльність на різних технологічних приладах та в мережах, під'єднаних до Інтернету. Безпека в кіберпросторі, тобто кібербезпека, стосується безпеки цього віртуального світу.

Більшість віртуальних світів мають віртуальну валюту, наприклад, для придбання в іграх різних предметів. Віртуальна валюта, навіть та, що застосовують в іграх, має цінність у реальному світі. Об'єкти з віртуального світу часто продаються за реальну валюту на інтернет-аукціонах, а деякі ігри мають навіть офіційний канал з опублікованими віртуальними або реальними обмінними курсами валют для монетизації віртуальних предметів. Часто такі канали для монетизації роблять ці віртуальні світи мішенню для атаки, зазвичай, за допомогою фішингу або інших методів для крадіжки відомостей акаунтів.

6.3 Природа кібербезпеки

Зацікавлені сторони в кіберпросторі мають грати певні ролі, аби, крім захисту своїх власних активів, ще максимізувати корисність кіберпростору. Програми кіберпростору виходять за рамки моделей «споживач-споживач» (*consumers-to-consumers*) та «бізнес-споживач» (*business-to-consumers*) для взаємодії та проведення транзакцій виду «усі-усім» (*many-to-many*). У зв'язку з цим зростають і вимоги

як для осіб, так і для організацій, які мають бути готові до протистояння новим ризикам та загрозам безпеці, ефективно запобігати зловживанням і протидіяти зловмисникам.

Кібербезпека охоплює дії всіх зацікавлених сторін, спрямовані на встановлення та підтримку безпеки в кіберпросторі.

Кібербезпека ґрунтується на таких фундаментальних засадах: інформаційна безпека, безпека програм, мережева безпека, а також інтернет-безпека. Кібербезпека є одним із заходів, необхідних для захисту інфраструктури важливої інформації (*CIIP*), і, разом з тим, є механізмом захисту послуг інфраструктури та сприяє задоволенню основних потреб безпеки (тобто захист, надійність і доступність критично важливих об'єктів інфраструктури) для досягнення цілей кібербезпеки.

Кібербезпека, однак, не є синонімом Інтернет-безпеки, мережевої безпеки, безпеки програм, інформаційної безпеки або CIIP. Кібербезпека вимагає, щоб зацікавлені сторони грали активну роль у підтриманні або навіть покращенні корисності та функціональності кіберпростору. Цей стандарт розрізняє кібербезпеку та інші види безпеки так:

— Інформаційна безпека пов'язана із захистом конфіденційності, цілісності й доступності інформації в цілому та спрямована на захист інформаційних інтересів споживачів.

— Безпека програм є процесом застосування методів контролю та керування програмами організацій для зменшення ризиків їхнього використання. Контроль та керування можуть бути застосовні до самих програм (їхніх процесів, складників, програм та результатів), їхніх відомостей (відомостей конфігурації, відомостей користувача, відомостей організації) та до всіх технологій, процесів та учасників циклу життя програми.

— Мережева безпека пов'язана з розробкою, реалізацією й експлуатацією мережі для досягнення цілей інформаційної безпеки на мережах всередині організацій, між організаціями, а також між організаціями та користувачами.

— Інтернет-безпека полягає в захисті Інтернет-послуг, відповідних ICT-систем та мереж і є розширенням поняття безпеки домашніх мереж та мереж організацій. Інтернет-безпека також охоплює поняття доступності й надійності Інтернет-послуг.

— Захист інфраструктур важливої інформації (*CIIP*) полягає в захисті систем, які надають або експлуатують постачальники таких глобальних інфраструктур, як енергетика, телекомунікації та водні відомства. CIIP гарантує, що ці системи та мережі захищені і є стійкими щодо ризиків інформаційної безпеки, ризиків безпеки мереж, різних загроз безпеці в Інтернеті, а також ризиків кібербезпеки.

На рисунку 1 зображено співвідношення між кіберзахистом та іншими видами захисту. Зв'язок між цими видами захисту й кіберзахистом є складним. Деякі з найважливіших об'єктів інфраструктури, наприклад, водні й транспортні, не повинні впливати на стан кіберзахисту ні безпосередньо, ні опосередковано. Проте відсутність кіберзахисту може мати негативний вплив на доступність систем інфраструктури важливої інформації, роботу яких забезпечують постачальники послуг цієї інфраструктури.

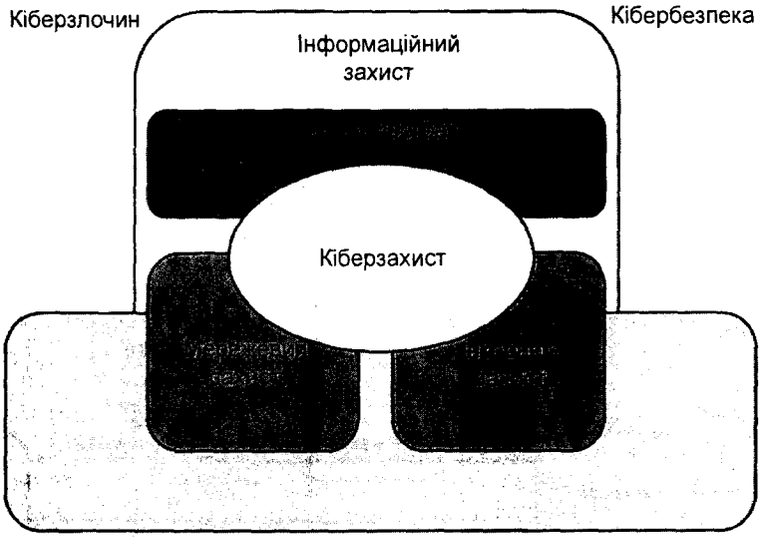

Рисунок 1 — Зв'язок між кіберзахистом та іншими видами захисту

З іншого боку, доступність і надійність кіберпростору багато в чому залежить від доступності та надійності таких послуг важливих інфраструктур, як інфраструктура мережевих телекомунікацій.

Безпека кіберпростору також тісно пов'язана з безпекою Інтернету, домашніх мереж та мереж організацій та інформаційною безпекою в цілому. Потрібно зазначити, що напрямки безпеки, описані в цьому розділі, мають свої власні цілі й сферу уваги. Розгляд питань кібербезпеки вимагає координації дій і встановлення тісних зв'язків між різними приватними й державними підприємствами різних країн й організацій. Послуги критичних інфраструктур розглядають деякі уряди як національні служби, пов'язані з безпекою, і тому не можуть бути обговорені або розголошувані відкрито. Крім того, знання слабких сторін таких інфраструктур у разі неналежного використання може створювати загрозу національній безпеці. Тому основою для обміну інформацією та координації дій є усунення недоліків і надання достатніх гарантій для зацікавлених сторін у кіберпросторі.

6.4 Загальна модель

6.4.1 *Вступ*

У цьому розділі буде подано загальну модель, яку розглядатимуть у цьому стандарті. Цей розділ передбачає наявність певних знань про безпеку і не є навчальним посібником у цій області.

У цьому стандарті йдеться про безпеку і використано відповідний набір термінів та концепцій. Розуміння цих концепцій і термінів — необхідна умова для ефективного використання цього стандарту. Проте самі поняття носять досить загальний характер і не призначені для обмеження класу задач інформаційної безпеки, до яких цей стандарт застосовний.

6.4.2 *Загальні положення безпеки*

Безпека пов'язана із захистом активів від загроз, якими є потенційні способи зловживання цими активами. Потрібно розглянути всі можливі види загроз; але в плані безпеки найбільше уваги потрібно приділити тим загрозам, які пов'язані зі шкідливою чи іншою діяльністю людей. На рисунку 2 зображено ці загальні концепції та співвідношення.

Примітка. Рисунок 2 запозичено з ISO/IEC 15408-1:2005 Інформаційні технології. Методи та засоби забезпечення безпеки. Критерії оцінювання безпеки ІТ. Частина 1. Вступ і загальна модель.

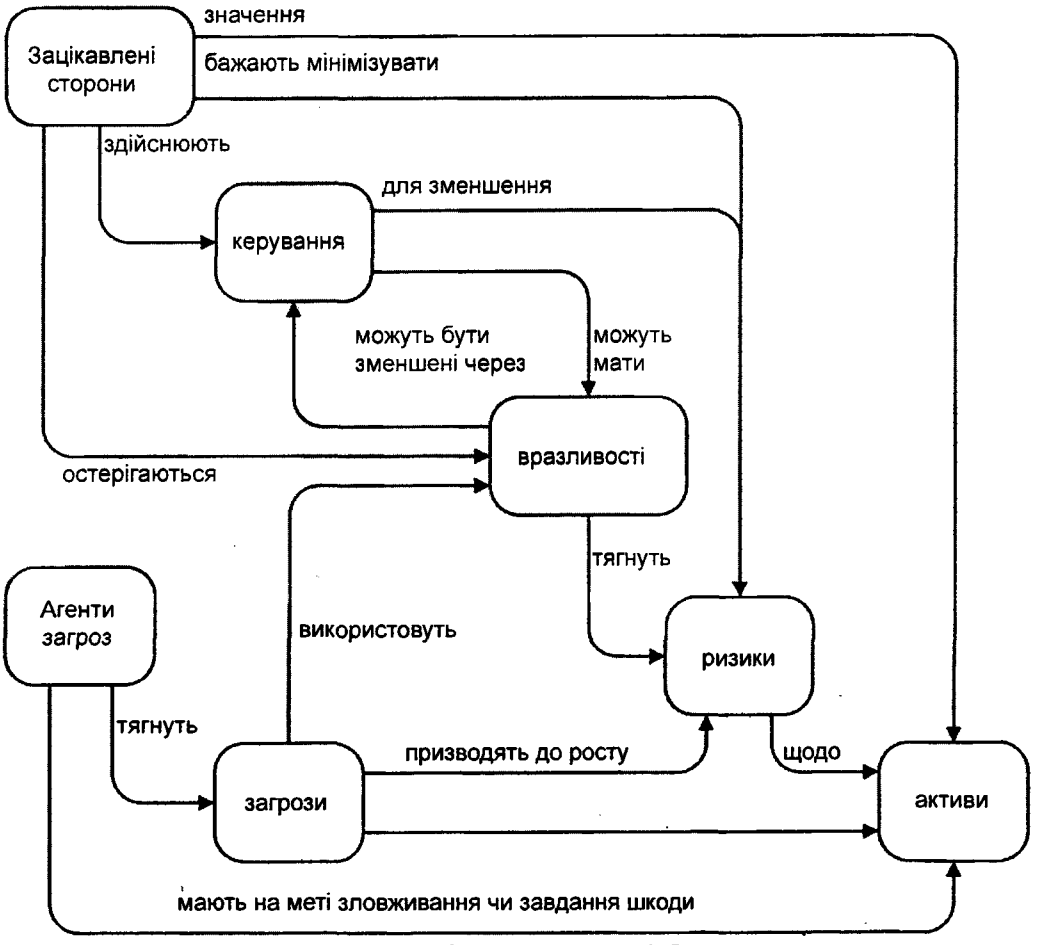

Рисунок 2 — Зв'язки та концепції безпеки

Захист відповідних активів є обов'язком тих зацікавлених сторін, для яких ці активи є важливими. Фактичні й потенційні агенти загроз можуть вбачати цінність активів та намагатись зловживати цими активами всупереч інтересам відповідних зацікавлених сторін. Зацікавлені сторони мають сприймати такі загрози як можливе погіршення активів, яке тягне зменшення їхньої цінності для зацікавлених сторін. Заходи щодо безпеки в таких випадках охоплюють, але не обмежуються, шкоду для активів через несанкціонований доступ сторонніх осіб (втрата конфіденційності), пошкодження активів несанкціонованою модифікацією (втрата цілісності) або несанкціоноване позбавлення доступу до активу (втрата доступності).

Зацікавлені сторони оцінюють ризики з урахуванням загроз для їхніх активів. Цей аналіз може допомогти у виборі методів керування боротьбою з ризиками та зменшення рівня загроз до прийнятного рівня.

Методи керування застосовують для зменшення вразливостей чи шкоди від атак, а також для задоволення вимог щодо безпеки зацікавлених сторін (безпосередньо чи опосередковано через долучення третіх сторін). Після впровадження методів керування окремі вразливості все ще можуть залишатись. Такі вразливості можуть бути використані агентами залишкового рівня небезпеки. Зацікавлені сторони будуть прагнути мінімізувати такі ризики, впроваджуючи додаткові обмеження.

Зацікавлені сторони повинні бути впевнені в тому, що заходи захисту є достатніми для протидії загрозам активів, перш ніж активи зазнають впливу цих загроз. Зацікавлені сторони можуть самі не мати можливості оцінити всі аспекти керування та через це можуть звернутися за допомогою до зовнішніх організацій.

6.5 Стратегії

Ефективний спосіб протистояння ризикам кіберпростору полягає в поєднанні багатьох стратегій, беручи до уваги інтереси різних зацікавлених сторін. Таким стратегіями є:

— використання практик передового досвіду у співпраці всіх зацікавлених сторін для виявлення ризиків і вирішення проблем кібербезпеки;

— всебічна освіта співробітників та споживачів щодо виявлення й усунення ризиків та загроз кібербезпеці як у межах організації, так і в усьому кіберпросторі;

— використання інноваційних технологічних рішень для захисту споживачів від відомих атак, щоб залишатися в курсі й бути готовим до них.

У цих інструкціях особливу увага приділено передовим практикам та освіті співробітників і споживачів, що дозволить допомогти зацікавленим сторонам у кіберпросторі брати активну участь у вирішенні проблем кібербезпеки. Розглядають такі основні напрямки:

— ролі;
— політики;
— методи;
— процеси;
— прикладні технічні засоби керування.

На рисунку 3 зображено основні положення та підходи, розглянуті в цьому стандарті. Цей стандарт не призначено для безпосереднього використання з метою забезпечення освіти широкого кола споживачів. Натомість, його призначено для використання постачальниками послуг у кіберпросторі, а також організаціями, які забезпечують відповідну освіту споживачів у кіберпросторі, і для підготовки освітніх матеріалів для широкого кола споживачів.

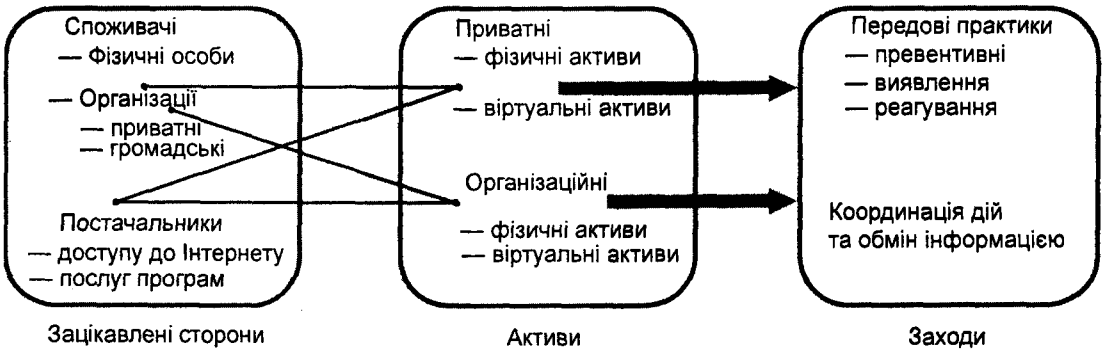

Рисунок 3 — Загальна схема

7 ЗАЦІКАВЛЕНІ СТОРОНИ В КІБЕРПРОСТОРІ

7.1 Огляд

Кіберпростір нікому конкретно не належить; кожен може завітати до нього та бути зацікавленою стороною. У цьому стандарті зацікавлені сторони в кіберпросторі поділено на такі групи:

— споживачі:
— фізичні особи;
— як приватні, так і громадські організації:
— постачальники, що є такими, але не обмежуються ними:
— постачальники послуг Інтернету,
— постачальники послуг програм.

7.2 Споживачі

Як видно з рисунка 3, до споживачів відносять як фізичних осіб, так і приватні та громадські організації. До приватних організацій належать малі та середні підприємства (МСП), а також великі підприємства. Урядові та інші громадські установи іменуються громадськими організаціями. Приватні особи та організації стають споживачами, коли отримують доступ до кіберпростору чи будь-яких послуг у кіберпросторі.

Споживач також може бути постачальником, якщо він, у свою чергу, надає іншим споживачам доступ до кіберпростору або послуги в кіберпросторі. Споживач послуги віртуального світу може стати постачальником через надання доступу до віртуальних продуктів та послуг іншим споживачам.

7.3 Постачальники послуг

До постачальників послуг належать як постачальники послуг у кіберпросторі, так й інтернет-постачальники, які надають споживачам доступ до кіберпростору і різних послуг, доступних у кіберпросторі.

Постачальниками, крім дистриб'юторів і роздрібних продавців послуг доступу до мережі, також можуть бути перевізники та оптові торгівці. Ця відмінність є суттєвою стосовно безпеки та, особливо, перспектив розвитку правоохоронної системи, бо якщо дистриб'ютор або роздрібний продавець не в змозі забезпечити належну безпеку чи законний доступ, служба підтримки за замовчуванням найчастіше буде звертатися до перевізника чи оптового продавця. Чітке розуміння природи/характеру даного постачальника послуг є корисною складовою в системі керування ризиками в кіберпросторі.

Постачальники послуг програм надають доступ до послуг споживачам через свої програмні засоби. Ці послуги можуть мати різні форми та бути поєднанням послуг з такого неповного переліку:

— редагування, зберігання та розповсюдження документів;
— віртуальні онлайн-середовища для розваг, комунікацій та взаємодії з іншими користувачами;
— цифрові медіа-сховища з послугами агрегації, індексування, пошуку, онлайн-магазинів, каталогів товарів, вибирання товарів й оплати послуг;
— функції керування такими ресурсами підприємства, як людські ресурси, фінанси, розрахунок зарплат, керування потоками поставок, взаємодія з клієнтами, виставлення рахунків-фактур.

8 АКТИВИ В КІБЕРПРОСТОРІ

8.1 Огляд

Активом може бути будь-що, що має цінність для фізичної особи чи організації. Активи охоплюють, але не обмежуються, таке:

a) інформація;
b) програмні засоби, наприклад, комп'ютерні програми;
c) фізичні активи, наприклад, комп'ютери;
d) послуги;
e) люди, їхня кваліфікація, навички та досвід;
f) нематеріальні активи, наприклад, репутація та імідж.

Примітка 1. Часто активи сприймають у спрощеному розумінні, тобто лише як інформацію та ресурси.

Примітка 2. В ISO/IEC 15408-1:2005 активи визначено як інформацію та ресурси, які треба захищати засобами контролю та керування ТОЕ (target of evaluation — об'єкт оцінки).

Примітка 3. ISO/IEC 19770-1 було розроблено, щоб організації могли довести, що вони виконують нормативи SAM (Software Asset Management — керування активами програмних засобів) на рівні, достатньому для задоволення вимог корпоративного керування та забезпечення ефективної підтримки керуванням IT-послуг. ISO/IEC 19770 призначено для докладнішого тлумачення та підтримки ISO/IEC 20000.

Примітка 4. ISO/IEC 20000-1 сприяє прийняттю комплексного підходу щодо створення, впровадження, експлуатування, моніторингу, вимірювання, аналізування та вдосконалення системи керування послугами (SMS, Service Management System) для розроблення і надання послуг, які відповідають потребам бізнесу та вимогам замовника.

У цьому стандарті активи в кіберпросторі розділено на такі класи:
— персональні;
— організаційні.
У кожному класі актив може бути:
— фізичним, якщо його форма є у фізичному світі;
— віртуальним, якщо він є лише в кіберпросторі та його неможливо побачити чи торкнутися в реальному світі.

8.2 Персональні активи

Одним із ключових віртуальних активів є онлайн-сутність (*identity*) кожного споживача та інформація про його кредитоспроможність. Онлайн-сутність є активом, оскільки вона є ключовим ідентифікатором кожного окремого споживача в кіберпросторі.

Ще одним індивідуальним віртуальним активом споживача у віртуальному світі є його відповідник. У віртуальному світі користувачі часто застосовують віртуальні аватари для свого представлення чи як свого двійника. Часто для віртуальних трансакцій користуються віртуальною валютою. Ці аватари і валюти можна вважати активами, що належать конкретному споживачеві.

Приклад

Деякі банки здійснюють операції у віртуальному світі й визнають світові віртуальні гроші як офіційну валюту.

У цьому стандарті ІТ-обладнання та програмне забезпечення, а також персональні цифрові пристрої або кінцеві точки, які дозволяють споживачам підключатися до кіберпростору та взаємодіяти у кіберпросторі, також вважають активами.

8.3 Активи організацій

Ключовим аспектом кіберпростору є його інфраструктура, завдяки якій він існує. У рамках цієї інфраструктури взаємодіють мережі, сервери та програми, які належать різним постачальникам. Проте надійність і доступність цієї інфраструктури має вирішальне значення в забезпеченні доступності послуг і програм кіберпростору. Оскільки кожна інфраструктура, яка надає споживачам доступ до кіберпростору або його послуг, є активом, який потрібно розглянути в цьому стандарті, можуть дати наявні збіги засобів безпеки, які пропонують, наприклад, для інформаційної безпеки, безпеки Інтернету та безпеки мереж. У цьому стандарті відповідні питання безпеки будуть розглянуті так, щоб приділити достатню увагу можливим загрозам активам організацій, але без надмірної уваги до тих питань, які не є першочерговими для цього стандарту.

Крім фізичних активів, віртуальні організаційні активи набувають все більшої цінності. Онлайн-бренд та інші представлення організації в Кіберпросторі окреслюють її образ і є настільки ж важливими, як і її складові в реальному фізичному світі.

Приклад 1

URL-адреса та інформація на веб-сайті організації є її активами.

Приклад 2

Країни навіть створили свої посольства у віртуальному світі, щоб представляти та захищати там свої інтереси.

Іншими організаційними активами, які можуть зазнавати впливу через уразливості в кіберпросторі, є інтелектуальна власність (формули, запатентовані процеси, патенти, результати досліджень) і бізнес-плани та стратегії (тактики маркетингу та випуску продукції, інформація про конкурентів, фінансова інформація та відомості звітності).

9 ЗАГРОЗИ БЕЗПЕЦІ КІБЕРПРОСТОРУ

9.1 Загрози

9.1.1 *Огляд*

Загрози в кіберпросторі розглядають у поєднанні з відповідними активами кіберпростору. Загрози кіберпростору можна розділити на дві категорії:
— загрози для персональних активів;
— загрози для активів організацій.

9.1.2 *Загрози для персональних активів*

Загрози для персональних активів стосуються переважно питань ідентифікації, які виникають у зв'язку з витоком або крадіжкою персональних відомостей.

Приклад 1

Інформацію про кредитоспроможність можна продати на чорному ринку, що може сприяти онлайн-крадіжкам персональних відомостей.

Якщо ідентифікаційні відомості людини вкрадені або підроблені, то така людина може бути позбавлена доступу до більшості послуг чи програм. У серйозніших випадках наслідки можуть коливатися від фінансових втрат до загроз національного рівня.

Несанкціонований доступ до фінансової інформації людини також може призвести до шахрайства та викрадення її коштів.

Ще однією загрозою є перетворення кінцевої точки на зомбі чи бота. Персональний обчислювальний пристрій може зазнати такого впливу, за якого він стане частиною великого ботнету.

Крім згаданих вище випадків, ще одним видом активів, який може зазнати впливу, є персональні активи у віртуальному світі та онлайн-іграх. Активи у віртуальному світі та світ онлайн-ігор можуть бути атаковані та використані зловмисниками.

Приклад 2

Деталі аватара та віртуальна валюта, яку можна інколи відстежити та конвертувати в реальні гроші, є першочерговими мішенями зловмисників.

Віртуальна крадіжка та віртуальне хуліганство є відносно новими термінами для атак такого типу. У такому разі безпека буде залежати від того, яка частка інформації з реального світу доступна зловмисникам у віртуальному світі, а також від самої системи безпеки віртуального світу, якою опікується адміністратор.

Хоча норми й правила щодо захисту реальних фізичних активів, пов'язаних із кіберпростором, вже частково розроблені, їхні аналоги, які стосуються віртуальних активів, практично відсутні. Через це учасникам процесу необхідна максимальна уважність та обережність для забезпечення належного захисту їхніх віртуальних активів.

9.1.3 ***Загрози для активів організацій***

Наявні в Інтернеті організації та бізнес дедалі частіше стають жертвами зловмисників, чиї наміри підступніші за звичайне хуліганство.

Приклад 1

Організовані кіберзлочинні синдикати часто погрожують організаціям зламом їхніх веб-сайтів чи лякають небезпечною діяльністю, як наприклад спотворення веб-сайтів.

Приклад 2

Якщо URL-адреса деякої організації зареєстрована чи викрадена кібер-скватером та перепродана іншим сумнівним організаціям, то онлайн-довіра до постраждалої сторони похитнеться.

У разі успішної атаки особиста інформація співробітників, клієнтів, партнерів чи постачальників може стати загальнодоступною, а це потягне санкції проти організацій, якщо буде встановлено факт незадовільного рівня керування та захисту, що й призвело до втрат.

Регламент фінансування також може бути порушено, якщо результати діяльності організації стали доступними несанкціонованим чином.

Уряди держав зберігають інформацію про національну безпеку, стратегічні та військові питання, розвідку серед багатьох інших відомостей, пов'язаних насамперед з державою та урядом, і, крім того, величезний масив інформації про окремих осіб, організації та суспільство в цілому.

Уряди повинні захищати свою інфраструктуру та інформацію від незаконного доступу та використання. Зі зростанням тенденції впровадження державних онлайн-послуг збільшується і новий канал для запуску атак й отримання доступу до наведеної вище інформації, що в разі успіху може мати серйозні наслідки для нації, уряду та суспільства.

У більших масштабах також може постраждати інфраструктура, що підтримує Інтернет й, отже, весь кіберпростір. Незважаючи на те, що це не позначиться на функціонуванні кіберпростору в цілому, це вплине на надійність та доступність інфраструктури, яка сприяє безпеці кіберпростору.

На державному чи міжнародному рівні кіберпростір — це така сіра зона, у якій процвітає тероризм. Одна з причин — легкість спілкування, яку забезпечує кіберпростір. Через природу кіберпростору, зокрема через неможливість визначити його межі та кордони, досить складно регулювати та контролювати спосіб його використання.

Терористичні групи можуть або на законних підставах купувати програми, послуги та ресурси, які полегшують їхню справу, або вдаватися до незаконних засобів постачання цих ресурсів для уникнення виявлення та відстеження. Це може бути й отриманням величезної кількості обчислювальних ресурсів через ботнети.

9.2 Агенти загроз

Агент загрози — це особа чи група осіб, яка виконує будь-яку роль у здійсненні атаки чи сприянні атаці.

Глибоке розуміння їхніх мотивів (релігійних, політичних, економічних тощо), можливостей (рівень знань, фінансування, кількість тощо) і намірів (розваги, злочини, шпигунство тощо) має вирішальне значення під час оцінювання вразливості та ризиків, у розробленні та впровадженні засобів контролю.

9.3 Вразливості

Вразливість — це слабка сторона активу чи методів контролю, яку можна використати в разі створення загрози. У контексті інформаційної системи ISO/IEC TR 19791:2006 також визначає вразливість як недолік, ваду або рису проектування чи реалізації інформаційної системи (зокрема контролю безпеки) або як її середовище, яке могло б навмисне чи ненавмисне мати негативний вплив на активи організацій та операції.

Оцінювання рівня вразливості має бути першочерговим завданням. У той час, як системи отримують патчі, оновлення чи додаються нові елементи, створюються також нові вразливості. Зацікавлені сторони вимагають глибоких знань і розуміння активу або контролю, а також загроз, агентів і ризиків для проведення комплексного оцінювання.

Примітка. ISO/IEC 27005 містить рекомендації з виявлення вразливостей.

Списку відомих вразливостей потрібно надавати обмежений доступ і бажано відокремлювати цю інформацію фізично й логічно від відповідних активів чи методів контролю. У разі виникнення порушення прав доступу та появи загрози несанкціонованого доступу до списку вразливостей цей список стане одним із найефективніших інструментів в арсеналі агента під час підготовлення та здійснення атак.

Потрібно шукати й упроваджувати рішення проблем вразливостей і, якщо вони є неможливими чи недоцільними, принаймні потрібно здійснювати відповідний контроль. Такий підхід має бути застосовано на пріоритетній основі, тобто в першу чергу розглядають саме ті вразливості, які створюють вищий ризик. Процедура виявлення вразливостей може бути визначена в рамках координації дій та обміну інформацією, як зазначено в розділі 13 цього стандарту.

Примітка. ISO/IEC 29147 містить інструкції з виявлення вразливостей.

9.4 Механізми атаки

9.4.1 *Вступ*

Багато атак у кіберпросторі здійснюють використанням такого шкідливого програмного забезпечення, як шпигунські програми, хробаки та віруси. Інформація часто збирається за допомогою фішингу. Атака може здійснюватись двома способами: як одиничний вектор атаки та як механізм гібридної атаки. Ці атаки можуть поширюватися через, наприклад, підозрілі веб-сайти, неперевірені завантаження, спам, дистанційне керування, а також заражені знімні носії інформації.

Атаки можуть відноситися до однієї з двох категорій:

— атаки зсередини приватної мережі;

— атаки ззовні приватної мережі.

Трапляються випадки, коли атаки здійснюють як усередині приватної мережі, так і поза її межами. Інші механізми проведення атак, частота використання, складність яких зростає, ґрунтуються на веб-сайтах соціальних мереж та використанні пошкоджених файлів на законних веб-сайтах.

Зазвичай, люди беззастережно довіряють повідомленням та контенту, отриманим від контактів, які були прийняті на їхніх сторінках соціальних мереж. Після того, як нападник через крадіжки особистих відомостей може прикинутись іншою особою, він може залучати інших користувачів, а це вже новий шлях запуску різних типів атак, обговорених раніше.

Законні веб-сайти можуть бути також зламаними й мати деякі файли пошкодженими, що також може бути джерелом нової атаки. Зазвичай люди довіряють відвідним сайтам, часто створюючи закладки в інтернет-браузерах на довгий час, а також застосовують рівень захисту сокетів SSL (Secure Sockets Layer). У той час, як відбувається авторизація та перевірка цілісності переданих або отриманих відомостей, SSL не розрізняє оригінального контенту від пошкодженого зловмисником, тим самим піддаючи користувачів цього веб-сайту атакам.

Незважаючи на законний вигляд сайтів у тих випадках, що зазначені вище, особам потрібно вибирати запобіжні заходи, викладені в розділі 11, щоб краще захистити себе.

9.4.2 *Атаки зсередини приватної мережі*

Ці атаки зазвичай запускають всередині приватної мережі організації, переважно, в локальній мережі. Вони можуть бути ініційовані співробітниками або кимось іншим, хто має доступ до комп'ютера або мережі всередині організації чи особистих приміщень.

Приклад 1

Один із можливих випадків — коли системні адміністратори можуть отримувати користь з привілеїв доступу до системи, яку вони утримують (наприклад, доступ до інформації про паролі користувачів) і використати це для ініціювання атаки. З іншого боку, системні адміністратори самі можуть стати об'єктом атаки як засіб для зловмисника, щоб заволодіти додатковою інформацією (імена користувачів, паролі тощо), перш ніж розпочати атаку.

Нападник може застосовувати аналізатори мережевих пакетів для одержання паролів чи інших ідентифікаційних відомостей. Як альтернатива, зловмисник може маскуватися як уповноважена особа та діяти як «людина зсередини», щоб украсти ідентифікаційні відомості.

Приклад 2

Одним із прикладів є використання шахрайських точок доступу (AP, access point) для крадіжки конфіденційних відомостей. У цьому разі нападник може сидіти в аеропорту, кафе чи будь-якому іншому публічному місці, що надає вільний доступ до Wi-Fi. Іноді він може маскуватися законним власником бездротової точки доступу приміщення, використовуючи SSID відповідного приміщення. Якщо користувач отримує доступ до цієї фальшивої точки доступу, зловмисник може діяти як «людина зсередини» й отримати цінний пароль чи ідентифікаційну інформацію від користувача (наприклад, інформацію про банківський рахунок і пароль, пароль облікового запису електронної пошти тощо).

Приклад 3

Часто буває досить перебувати поруч із незахищеною мережею Wi-Fi, наприклад, сидіти в машині поза домом, щоб мати можливість украсти інформацію в мережі.

Крім атак, запущених людиною, заражені шкідливими програмами комп'ютери також можуть бути джерелом різних атак на інші комп'ютери всередині приватної мережі.

Приклад 4

Багато шкідливих програм часто посилають пакети сканування в приватні мережі, щоб знайти комп'ютери мережі, а потім спробувати застосовувати їх.

Приклад 5

Деякі шкідливі програми застосовують змішаний режим мережевого інтерфейсу зараженого комп'ютера, щоб перехоплювати трафік, що проходить через приватну мережу.

Приклад 6

Кейлогери (key loggers) — це програмні або апаратні засоби, які фіксують усі натискання клавіш у системі. Це може відбуватися таємно, щоб стежити за діями користувача. Кейлогер часто застосовують для збору інформації про авторизацію зі стартової сторінки програми.

9.4.3 *Атаки ззовні приватної мережі (наприклад, з Інтернету)*

Є багато різних атак, які можуть бути запущені ззовні приватної мережі, зокрема Інтернет.

У той час як первісна атака завжди буде спрямована на публічно доступну систему (наприклад, роутер, сервер, брандмауер, веб-сайт тощо), нападники можуть також намагатися користуватись активами, які містяться всередині приватної мережі.

Старі методи атаки вдосконалюються, а нові безперервно розвиваються. Нападники стають все досвідченішими та зазвичай комбінують різники техніки й механізми для досягнення успіху. Це робить виявлення та попередження атак складнішими.

Сканери портів є одним з найстаріших, але все ще дуже ефективних інструментів нападників. Вони сканують усі доступні на сервері порти для перевірки, який із них є «відкритим». Зазвичай це один з перших кроків, що виконує потенційний нападник.

Ці атаки можуть проявлятися в різних DoS-атаках на сервери програм чи інше мережеве обладнання за допомогою використання переліку вразливостей чи вразливостей проектування програми.

Приклад

Величезна кількість DoS-атак може бути запущена за допомогою ботнетів, що може відключити доступ до кіберпростору цілої країни.

З поширенням програм пірингових мереж (*peer-to-peer*), які зазвичай застосовують для обміну такими файлами, як цифрова музика, відео, фото тощо, нападники все більше й більше стають досвідченими в тому, як замаскувати себе та свій шкідливий код, наприклад, троянських коней, застосовуючи обмінні файли.

Переповнення буфера є ще одним популярним методом ставити послуги під загрозу в Інтернеті. Використовуючи вразливості коду і відправлення набагато довших, ніж очікується, рядків, нападники змушують сервер працювати поза нормальним (контрольованим) середовищем/режимом, тим самим сприяючи вставці/виконанню шкідливого коду.

Іншою технікою є IP-спуфінг, що полягає в маніпуляціях нападника з IP-адресою, пов'язаною з його повідомленнями, та спробою замаскуватися під відомий, довірений ресурс, у такий спосіб отримуючи несанкціонований доступ до системи.

10 РОЛІ ЗАЦІКАВЛЕНИХ СТОРІН У КІБЕРПРОСТОРІ

10.1 Огляд

Для покращення стану справ з кібербезпекою зацікавлені сторони в кіберпросторі повинні брати активну участь у відповідному використанні й розвитку Інтернету. Інколи ролі сторін можуть збігатися з їхніми відповідними функціями як приватних осіб, так і організацій у приватних мережах та мережах організацій. Термін «мережа організації» часто охоплює комбіноване використання приватної мережі організації (наприклад, інтранету), екстранету та відкритих публічних мереж. У цьому стандарті відкриті публічні мережі є мережами, доступними з Інтернет, наприклад, це хости веб-сайтів. Через можливий збіг ролей зацікавлених сторін ці ролі можуть виявлятись незначними чи не мати прямого інтересу для окремих осіб чи організацій. Проте вони є значними для підвищення рівня кібербезпеки, коли всі зацікавлені сторони діють відповідно.

10.2 Ролі споживачів

10.2.1 *Вступ*

Споживачі не тільки мають доступ до інформації, але також можуть надавати деяку інформацію як окремим програмам кіберпростору, так й обмеженим групам осіб, що користуються відповідними програмами, або навіть усій широкій громадськості. Поведінка споживачів у таких випадках може бути активна чи пасивна та може мати безпосередній чи опосердкований вплив на стан справ з кібербезпекою.

10.2.2 *Ролі фізичних осіб*

Окремі споживачі в Кіберпросторі можуть грати різні ролі залежно від контексту та конкретної програми.

— Ролі споживачів охоплюють, хоча і не обмежуються, таке:

— Звичайний користувач програмами кіберпростору, чи просто користувач, наприклад, онлайн-геймер, користувач миттєвими повідомленнями, веб-серфер.

— Покупець/продавець, що бере участь у розміщенні товарів і послуг на інтернет-аукціонах і ринках сайтів для зацікавлених покупців, і навпаки.

— Блогер чи автор іншого контенту (такого, як наприклад статті у вікіпедії), у якому текстова чи медійна інформація (наприклад, відео-кліпи) викладається у відкритий чи обмежений доступ.

— ІАР у межах контексту програми (наприклад, онлайн-ігри) або всього кіберпростору.

— Член організації (наприклад, співробітник компанії або інша особа, що має відношення до компанії).

— Інші ролі. Інколи користувачу може бути «призначена» роль випадково чи без його згоди.

Приклад

Коли користувач відвідує сайт з обмеженим доступом і випадково отримує такий доступ, то такого користувача можна умовно назвати зловмисником.

У кожній із зазначених ролей споживачі не тільки мають доступ до інформації, але також можуть надавати деяку інформацію як окремим програмам кіберпростору, так й обмеженим групам осіб, що користуються відповідними програмами, або навіть усій широкій громадськості. Поведінка споживачів у таких випадках може бути активна чи пасивна та може мати прямий чи непрямий вплив на стан справ з кібербезпекою.

Приклад 1

Якщо IAP надає програму, яка має вразливості в системі безпеки, то ці вразливості можуть бути використані кібер-зловмисниками як канал для одержання доступу до цієї програми.

Приклад 2

Блогери та автори іншого контенту можуть отримувати запити у формі невинних питань щодо контенту. У своїй відповіді вони можуть ненавмисно розкрити деяку приватну інформацію (свою чи організації) широкій громадськості.

Приклад 3

Фізична особа, що діє як покупець або продавець, може несвідомо брати участь у злочинних оборудках з продажу крадених товарів або у відмиванні грошей.

Отже, як і в реальному світі, окремі споживачі повинні проявляти обережність у кожній ролі, яку вони відіграють у кіберпросторі.

10.2.3 ***Ролі організацій***

Організації часто користуються кіберпростором для поширення рекламної та іншої інформації, а також для просування на ринку товарів та послуг. Організації також користуються кіберпростором як частиною своєї мережі для відправлення й отримання електронних повідомлень (наприклад, повідомлення електронної пошти) та інших документів (наприклад, передавання файлів).

Для збереження високих стандартів корпоративної соціальної відповідальності організації повинні розширити свої корпоративні обов'язки в кіберпросторі та діяти так, щоб не наражати себе та інших на додаткові ризики в області безпеки в кіберпросторі. До таких заходів можуть належати:

— належне керування інформаційною безпекою за допомогою впровадження та експлуатування ефективної системи керування інформаційною безпекою.

Примітка 1. В ISO/IEC 27001 наведено вимоги щодо системи керування інформаційною безпекою;

— належний моніторинг за безпекою та вчасне реагування;

— вживання заходів щодо безпеки на всіх етапах розробки систем (*SDLC*), де рівень безпеки системи визначається критичністю/важливістю відомостей організації;

— регулярне навчання користувачів заходам щодо безпеки в організації під час постійного оновлення технологій і спостерігання за новітніми технологічними розробками;

— розуміння та використання правильних каналів у спілкуванні з продавцями та постачальниками послуг з питань безпеки, які виникають під час роботи.

Примітка 2. Майбутній стандарт ISO/IEC 29147 міститиме рекомендації щодо виявлення вразливостей.

Примітка 3. ISO/IEC 27031 містить рекомендації щодо ICT-безпеки для забезпечення безперервності бізнесу.

Примітка 4. ISO/IEC 27035 містить інструкції з керування інцидентами інформаційної безпеки.

Примітка 5. ISO/IEC 27034-1 містить інструкції з безпеки програм.

Уряд, основні правоохоронні та регулювальні органи можуть відігравати такі важливі ролі:

— надавати консультації організаціям щодо їхніх функцій у кіберпросторі;

— обмінюватися інформацією з іншими зацікавленими сторонами про сучасні тенденції та розробки в області технологій;

— обмінюватися інформацією з іншими зацікавленими сторонами про відомі поширені ризики безпеки;

— бути надійним джерелом будь-якої інформації, чи то закритої, чи відкритої, щодо загроз безпеці у кіберпросторі;

— бути основним координатором для поширення інформації та використання ресурсів як на національному, так і на корпоративному рівні в період кризи, що виникає в результаті масивних кібер-атак.

10.3 Ролі постачальників

Організації, які є постачальникам послуг, належать до однієї з двох категорій:

— постачальники доступу до кіберпростору для співробітників та партнерів,

— постачальники послуг для споживачів у кіберпросторі — як для обмежених груп (наприклад, лише для зареєстрованих користувачів), так і для широкого загалу — через спеціальні програми в кіберпросторі.

Приклад

Прикладами послуг можуть бути ринки онлайн-торгівлі, послуги платформ для дискусійних форумів, послуги платформ для блогів і послуги соціальних мереж.

Оскільки постачальники послуг є споживчими товариствами, то вони мають виконувати ті самі функції та нести таку саму відповідальність, що й споживчі товариства. Як постачальники послуг, вони мають додаткові обов'язки в збереженні або навіть підвищенні безпеки кіберпростору в такі способи:

— постачання безпечних і надійних продуктів і послуг;

— забезпечення кінцевих користувачів інструкціями з безпеки та захисту;

— здійснення свого внеску в безпеку інших постачальників послуг та споживачів аналізуванням тенденцій та через спостереження за трафіком у рамках їхніх мереж та послуг.

11 КЕРІВНІ ПРИНЦИПИ ДЛЯ ЗАЦІКАВЛЕНИХ СТОРІН

11.1 Огляд

Рекомендації, наведені в цьому розділі, сфокусовані на трьох основних сферах:

— рекомендації з безпеки для споживачів;

— внутрішнє управління ризиками інформаційної безпеки організації;

— вимоги щодо безпеки, які постачальники повинні визначити споживачам для реалізації.

Рекомендації структуровані так:

a) вступ до оцінювання та оброблення ризиків;

b) рекомендації для споживачів;

c) рекомендації для організацій, зокрема постачальників послуг:

— управління ризиками інформаційної безпеки в бізнесі;

— вимоги щодо безпеки до послуг хостингу та інших програмних послуг.

11.2 Оцінка та обробка ризиків

ISO 31000 Risk management — Principles and guidelines надає принципи та загальні рекомендації щодо управління ризиками, в той час як ISO/IEC 27005 Information technology — Security techniques — Information security risk management надає рекомендації та процеси щодо управління ризиками інформаційної безпеки в організації, зокрема підтримуючи вимоги ISMS відповідно до ISO/IEC 27001. Ці рекомендації та процеси є достатніми для управління ризиками в контексті кіберпростору.

ISO/IEC 27005:2011 не надає жодної спеціальної методології для управління ризиками інформаційної безпеки. Це завдання споживачів та постачальників визначити їхній підхід до управління ризиками. Для реалізації вимог ISMS може бути використано ряд наявних методологій у рамках архітектури, описаної в ISO/IEC 27005.

Наведені нижче аспекти мають бути враховані під час визначання підходу до управління ризиками.

— Ідентифікація критичних активів: підключення або використання кіберпростору розширює сферу визначення активів. Оскільки захист усіх активів не є рентабельним, то важливо, щоб критичні активи були ідентифіковані для того, щоб приділити особливу увагу їхньому захисту. Їхнє визначення має бути зроблено в контексті бізнесу за допомогою розглядання впливу на бізнес від втрати або деградації активу.

— Ідентифікація ризиків: зацікавлені сторони повинні належно розглядати та враховувати додаткові ризики, загрози й атаки, які стають актуальними під час взаємодії з кіберпростором.

— Відповідальність: беручи участь у кіберпросторі, зацікавлена сторона повинна прийняти додаткову відповідальність відносно інших зацікавлених сторін. Це містить:

— Визнання: визнання можливого ризику того, який вплив на кіберпростір у цілому та зокрема на інформаційні системи інших зацікавлених сторін може привнести участь зацікавленої сторони.

— Звітність: може виникнути потреба залучити зацікавлені сторони поза організацією, коли поширення звітів пов'язано з ризиками, інцидентами та загрозами.

— Обмін інформацією: як і зі звітністю, може виникнути потреба в обміні релевантною інформацією з іншими зацікавленими сторонами.

— Оцінка ризиків: необхідно визначити ступінь, за якої дії зацікавленої сторони та присутність у кіберпросторі стають ризиком для іншої зацікавленої сторони.

— Регулювання/законодавство: за приєднання до кіберпростору важко розрізнити правові та нормативні межі, і застосовують більше вимог, іноді суперечливих.

— Припинення системи або послуги: як тільки система чи послуга більше не потрібні, їх має бути припинено методом, який гарантує, що пов'язані послуги або інтерфейси не зазнаватимуть впливу. Уся інформація, що стосується безпеки, має бути анульована, щоб гарантувати, що системи, з якими вона взаємодіє або пов'язана, не поставлені під загрозу.

— Узгодженість: цей підхід до управління ризиками застосовують по всьому кіберпростору. У межах цього підходу або методології споживачі та постачальники кіберпростору мають обов'язки для певних дій, таких як планування непередбачених обставин, відновлення після аварій, розроблення та реалізація захисних програм для систем, що перебувають під їхнім контролем та/або є їхньою власністю.

Загалом, методологія управління ризиками в ISO/IEC 27005 покриває повний життєвий цикл загальної системи, що робить її застосовною як для нових систем безпеки, так і для успадкованих систем. Оскільки це стосується відновлення систем, то вона застосовна до всіх бізнес-моделей. Процеси всередині архітектури можуть обробляти мережі й послуги постачальників послуг як інтегровану систему, що складається з підсистем, які надають послуги загального користування, і приватних підсистем, які підтримують внутрішні послуги або вони можуть оброблювати кожну з індивідуальних послуг (наприклад, веб-хостинг) окремо й описувати їх забезпечення стосовно окремих систем, що взаємодіють. Для простоти може бути корисним розглядати все, що необхідно для підтримки послуг постачальника, як велику систему, яка може бути розкладена на менші системи, кожна з яких надає ліквідну послугу або утворює частину інфраструктури.

Важливими аспектами, які необхідно пам'ятати під час розгляду цілей і завдань кібербезпеки, є:

a) забезпечувати загальну безпеку кіберпростору;

b) планувати надзвичайні ситуації та кризи участю в тренуваннях та оновлювати плани реагування та плани безперервності операцій;

c) підвищувати знання зацікавлених сторін у галузі кібербезпеки та практиках управління ризиками;

d) забезпечити своєчасний, доречний і точний обмін інформацією щодо загроз між правоохоронними та розвідувальними спільнотами та особами, що приймають ключові рішення стосовно кіберпростору;

e) установити ефективні механізми між секторами та між зацікавленими сторонами для вирішення критичних взаємозалежностей, зокрема ситуаційну обізнаність з приводу інцидентів та управління інцидентами між секторами та між зацікавленими сторонами.

Цілі й завдання від a) до c) покладають безпосередньо на постачальників послуг, які є відповідальними за обладнання та послуги, що перебувають під їхнім контролем. Для цілей і завдань від d) до e) постачальників послуг залучають як активних учасників у процеси обміну інформацією та координації.

Окремі цілі постачальників послуг стосовно того, які надавати послуги, випливають з бізнес-контексту.

11.3 Керівні принципи для споживачів

Цей стандарт не спрямований безпосередньо на окремих осіб кіберпростору, але сфокусований на організаціях, які надають послуги споживачам, і організаціях, які потребують, щоб їхні співробітники або кінцеві користувачі практикували захищене використання кіберпростору для того, щоб ефективно управляти ризиками кібербезпеки. Рекомендації щодо ролей і безпеки користувачів у кіберпросторі та того, як вони можуть позитивно впливати на стан кібербезпеки, мають слугувати як настанова для проектування та розроблення документів цими організаціями в контексті забезпечення послуг і здійснення навчальних та тренувальних програм для їхніх кінцевих користувачів.

Як описано в 10.2, споживачі можуть бачити чи збирати інформацію так само, як надавати певну інформацію всередині програмного простору кіберпростору, або відкривати для обмежених членів чи груп всередині програмного простору, або для широкого загалу. Дії, вчинені споживачами в цих ролях, можуть бути активними чи пасивними та можуть впливати безпосередньо чи опосередковано на стан кібербезпеки.

Наприклад, як незалежні постачальники програм, якщо надана програма містить уразливості безпеки, вони можуть призвести до експлуатації кіберзлочинцями, застосовуючи їх як канал для досягнення непричетних користувачів програми. Як блогери або у вигляді інших форм поширення інформації, вони можуть отримати запит у формі невинних запитань щодо їхньої інформації, у якій вони можуть ненавмисно розкрити більше, ніж бажано, персональної чи корпоративної інформації широкому загалу. Як покупець або продавець, споживач може несвідомо брати участь у кримінальних транзакціях щодо продажу викрадених речей або діяльності, пов'язаної з відмиванням грошей. Отже, як і у фізичному світі, споживачі повинні проявляти обережність у всіх і кожній ролі, яку вони відіграють у кіберпросторі.

Загалом, споживачі повинні взяти до відома такі рекомендації:

a) Вивчити і розуміти політику безпеки і конфіденційності сайту і програми, опубліковану постачальником сайту.

b) Вивчити і розуміти пов'язані ризики безпеки і конфіденційності та визначити відповідні доречні заходи. Брати участь у відповідних Інтернет-форумах або запитувати когось, хто знає сайт або програму, перед тим як надати персональну або корпоративну інформацію або брати участь і передавати інформацію у дискусіях.

c) Установити й застосовувати особисту політику конфіденційності для захисту особистості за допомогою визначення категорій доступної персональної інформації та принципів поширення, пов'язаних з цією інформацією.

d) Управляти онлайн-особистістю. Застосовувати різні ідентифікатори для різних веб-програм і мінімізувати поширення персональної інформації кожному веб-сайту чи програмі, які запитують таку інформацію. Зареєструвати онлайн-акаунт на популярних сайтах соціальних мереж, навіть якщо акаунт не буде проявляти активність.

Приклад

Єдиний вхід (*single sign on*) є формою управління онлайн-особистістю.

e) Повідомляти про підозрілі події або звертатися до відповідних органів (див. додаток B для прикладу публічно доступного списку контактів).

f) Як покупець або продавець, читати й розуміти політику безпеки та конфіденційності сайту онлайн-ринку та виконувати кроки для перевірки достовірності задіяних сторін. Не розповсюджувати персональну інформацію, зокрема банківську інформацію, якщо не встановлено справжнього інтересу до покупки чи продажу. Користуватись механізмом оплати, який заслуговує на довіру.

g) Як незалежний постачальник програм, застосовувати безпечну розробку програмного забезпечення і надавати в онлайн геш-значення коду так, щоб замовники могли перевірити значення, якщо необхідно гарантувати цілісність коду. Надавати документацію щодо політик безпеки та конфіденційності коду, практик та поважати конфіденційність користувачів коду.

h) Як блогер або інший розповсюджувач інформації (зокрема ті, хто супроводжує веб-сайти), гарантувати, щоб відповідна приватна та конфіденційна інформація зацікавлених сторін не була розповсюджена через блоги чи онлайн-публікації. Перевіряти коментарі та записи, отримані на сайті, та переконуватися, що вони не містять жодного шкідливого вмісту, такого, як посилання на фішингові веб-сайти або шкідливі завантаження.

i) Як член організації, індивідуальний споживач повинен вивчити й розуміти корпоративну політику інформаційної безпеки організації та переконатися, що класифікована та/або конфіденційна інформація не буде розповсюджена умисно або випадково на жодному веб-сайті в кіберпросторі, крім випадку, коли попередньо формально був наданий дозвіл на таке опублікування.

j) Інші ролі. Коли споживач відвідує сайт, який потребує авторизації, і ненавмисно отримує доступ, користувач може бути позначений як порушник. Необхідно негайно вийти з сайту і повідомити відповідний орган, оскільки факт можливості отримання доступу може бути індикатором компрометації.

11.4 Рекомендації для організацій і постачальників послуг

11.4.1 *Огляд*

Заходи щодо управління ризиками кібербезпеки значно залежать від зрілості процесів управління безпекою всередині організацій (охоплюючи постачальників послуг). У той час, як рекомендації, запропоновані тут, є в основному дискреційними для організацій, рекомендовано, щоб постачальники послуг застосовували ці рекомендації як базисні, необхідні заходи.

Рекомендації в цьому розділі можуть бути підсумовані як:

— Управляти ризиками інформаційної безпеки в бізнесі.

— Висувати вимоги щодо безпеки до послуг веб-хостінгу та інших кібер-програм.

— Надавати рекомендації з безпеки споживачам.

11.4.2 *Управління ризиками інформаційної безпеки в бізнесі*

11.4.2.1 *Система управління інформаційною безпекою*

На промисловому рівні організації, з'єднані з кіберпростором, повинні впровадити систему управління інформаційною безпекою (ISMS) для визначення й управління відповідними ризиками інформаційної

безпеки для бізнесу. Серії стандартів ISO/IEC 27000 для систем управління інформаційною безпекою надають необхідні рекомендації та кращі практики для впровадження таких систем.

Ключовим чинником у реалізації ISMS є гарантування того, що організація має систему для неперервної ідентифікації, оцінки, обробки й управління ризиками інформаційної безпеки, що стосуються бізнесу, охоплюючи забезпечення послуг в Інтернет, безпосередньо кінцевим користувачам чи абонентам.

Примітка 1. ISO/IEC 27005 Information technology — Security techniques — Information security risk management надає рекомендації для управління ризиками інформаційної безпеки в організації, зокрема підтримуючи вимоги ISMS згідно з ISO/IEC 27001.

Примітка 2. ISO 31000 Risk management — Principles and guidelines надає принципи і загальні рекомендації щодо управління ризиками.

Організації можуть також розглянути формальну сертифікацію їхньої відповідності вимогам ISMS, таким як ISO/IEC 27001.

Як частина реалізації ISMS, організація повинна також забезпечити можливості для моніторингу та реагування на інциденти безпеки та координувати їхню діяльність щодо реагування на інциденти із зовнішніми організаціями CIRT, CERT або CSIRT у країні. Забезпечення реагування на інциденти й аварійні ситуації має містити моніторинг і оцінку стану безпеки використання послуг організації кінцевими користувачами та клієнтами та надавати рекомендації для допомоги постраждалим сторонам в ефективному реагуванні на інциденти безпеки.

Примітка. ISO/IEC 27035 Information technology — Security techniques — Information security incident management надає рекомендації щодо управління інцидентами інформаційної безпеки.

11.4.2.2 *Надання безпечних продуктів*

Деякі організації розробляють[1)] і розповсюджують їхні власні панелі інструментів для веб-браузерів, номеронабирачі або код для надання послуг з доданою вартістю кінцевим користувачам, або для забезпечення простоти доступу до послуг чи програм організації. У таких випадках повинна бути правильна угода з кінцевим користувачем на відповідній мові, зокрема документи щодо політики кодування організації, політики конфіденційності, і засоби, за допомогою яких користувачі можуть змінити їхню згоду пізніше або поставити питання, які вони можуть мати щодо політики та практик. Якщо застосовують таку угоду, її має бути поставлено під контроль версій, і організація повинна забезпечити, щоб кінцеві користувачі послідовно підписували її.

Там, де є високий ступінь залежності від безпеки програмних продуктів, їх має бути незалежно перевірено за схемою «Common Criteria», як описано в ISO/IEC 15408.

Організації повинні документувати поведінку коду та здійснювати оцінювання того, в яких випадках його поведінка може попадати до сфер, що можуть бути розглянуті як шпигунське або шахрайське програмне забезпечення. В останньому випадку необхідно залучити відповідно підготовленого експерта для оцінювання того, чи відповідає код цільовим критеріям постачальників антишпигунського програмного забезпечення, які притримуються кращих практик, так, що програмні інструменти для кінцевих користувачів, надані організацією, не будуть відмічені як шпигунські або рекламні програми постачальниками антишпигунського програмного забезпечення. Багато постачальників антишпигунського програмного забезпечення публікують критерії, за якими вони оцінюють прикладні програми.

Організації повинні впровадити цифрове підписування для своїх бінарних файлів, щоб постачальники антишкідливого та антишпигунського програмного забезпечення могли легко визначити власника файла та незалежних постачальників програмного забезпечення, які постійно створюють програмне забезпечення, що слідує кращим практикам. Таке підписане програмне забезпечення ймовірно буде категоризовано як безпечне, навіть до проведення аналізу.

Якщо організація винайшла корисні програмні методи, які можуть допомогти зменшити проблеми від шпигунського або шкідливого програмного забезпечення, організація повинна розглянути партнерство та співпрацю з постачальником, щоб зробити такі методи доступними для широкого загалу.

Для виконання цих вимог дуже важливим є навчання в галузі безпеки для розробників. Життєвий цикл безпечної розробки програмного забезпечення потрібно застосовувати там, де можуть бути зменшені програмні вразливості, і як наслідок надавати більш захищений програмний продукт.

Примітка. ISO/IEC 27034 Information technology — Security techniques — Application security надає рекомендації для визначення, розроблення, реалізації, управління, підтримання та припинення прикладних програм.

11.4.2.3 *Моніторинг мережі та реагування*

Моніторинг мережі зазвичай застосовують організації для забезпечення надійності та якості їхніх мережевих послуг. Наразі цей засіб може бути використаний для пошуку надзвичайних умов у мережевому трафіку і виявлення шкідливої активності, що виникає в мережі. Загалом, організації повинні здійснити таке:

[1)] Або внутрішньо, або через стороннього постачальника.

— Розуміти трафік у мережі — що є нормальним, що не є нормальним.— Користуватись інструментом управління мережею для розпізнання сплесків у трафіку, «незвичайного» трафіка/портів і забезпечення наявності інструментів для виявлення та реагування на причину такої поведінки.

— Випробувати засоби реагування перед тим, як вони знадобляться для реальної події. Удосконалювати методи реагування, процеси й інструменти на основі результатів регулярних тренувань.

— Розуміти складові на індивідуальній основі — якщо хтось, хто зазвичай є неактивним користувачем, раптово починає застосовувати 100 % доступної смуги пропускання, то може бути необхідним ізолювати такого користувача, доки причину не буде знайдено. Мережева ізоляція може запобігати розповсюдженню шкідливого програмного забезпечення, хоча певні реалізації можуть вимагати згоди користувача чи оновлення умов обслуговування.

— Розглядати моніторинг активності з розвідувальних точок, таких як DNS і фільтри повідомлень, які можуть слугувати для позначення пристроїв, що були скомпрометовані шкідливим програмним забезпеченням, але з різних причин не були виявлені за допомогою антивірусних або IDS-служб.

Приклад

З огляду на обсяг інформації в мережі такі інструменти, як IDS та IPS, можуть бути застосовні для моніторингу виключних ситуацій.

11.4.2.4 *Підтримка і ескалація*

Бізнеси, зокрема постачальники послуг і державні організації, зазвичай мають службу підтримки для відповіді на запити клієнтів, надання технічної допомоги та підтримки у вирішенні проблем кінцевих користувачів. Зі зростом шкідливого програмного забезпечення в Інтернет організація, що надає послуги, може отримувати повідомлення щодо заражень шкідливим і шпигунським програмним забезпеченням та щодо інших питань кібербезпеки. Така інформація є важливою та корисною для відповідних постачальників, щоб оцінити ризики та ситуацію зі шкідливим програмним забезпеченням та оновити необхідні інструменти для забезпечення того, що будь-яке нове виявлене шкідливе або шпигунське програмне забезпечення може бути ефективно видалене або вимкнене. У зв'язку з цим організація повинна встановити контакт з постачальниками засобів безпеки й надавати відповідні повідомлення та зразки шкідливого програмного забезпечення постачальникам для подальшої обробки, особливо якщо спостерігається сплеск поширеності. Більшість постачальників підтримують список розсилки для отримання таких повідомлень або зразків для аналізу та подальшої обробки. Наприклад, див. таблицю В.1 у додатку В.

11.4.2.5 *Підтримка актуальності з останніми розробками*

Як частина впровадження системи управління інформаційною безпекою для управління ризиками інформаційної безпеки підприємства та забезпечення того, що організації слідують кращим практикам галузі й обізнані щодо останніх вразливостей та ситуацій експлуатації/атак, організації повинні брати участь у відповідних спільнотах або галузевих форумах для обміну своїми кращими практиками та для навчання від інших схожих постачальників.

11.4.3 ***Вимоги щодо безпеки до хостингу веб- та інших заснованих на кіберпрограмах послуг***

Більшість постачальників послуг надають послуги хостингу в їхніх мережах та датацентрах як частину їхніх бізнес-послуг. Ці послуги, що охоплюють веб-сайти та інші онлайн-програми, часто перепаковуються і перепродаються абонентами хостингу іншим клієнтам, таким як невеликі підприємства та кінцеві користувачі. Якщо абоненти хостингу встановлять незахищений сервер або розмістять шкідливий вміст у їхніх сайтах або програмах, безпека споживачів буде під загрозою. Важливо, щоб послуги щонайменше відповідали стандартам кращих практик за допомогою дотримання політик або умов обслуговування.

Там, де застосовано кілька постачальників, взаємодія між постачальниками повинна бути проаналізована та відповідні угоди про надання послуг повинні регламентувати будь-які критичні взаємодії. Наприклад, оновлення чи патчі для систем одного постачальника мають бути скоординовані з іншими постачальниками, якщо оновлення може призвести до негативної взаємодії.

Умови угод мають охоплювати щонайменше таке:

а) Чіткі сповіщення, що описують безпеку онлайн-сайту чи програми та практики конфіденційності, практики збору відомостей, поведінку будь-якого коду (наприклад, допоміжного об'єкта для браузера), які онлайн-сайт чи програма можуть поширювати й виконувати на комп'ютерах кінцевих користувачів або в середовищі веб-браузерів.

b) Згода користувача, що забезпечує прийняття або неприйняття користувачем умов обслуговування, описаних у сповіщеннях. Це дасть користувачу здійснити свободу вибору та визначити, чи може він прийняти відповідні умови обслуговування.

c) Елементи керування користувача, що забезпечують користувачів можливістю змінювати їхні налаштування або іншим способом припиняти їхню згоду в будь-який час у майбутньому після початкової згоди.

Умови є важливими для забезпечення того, що кінцеві користувачі мають чітке уявлення про поведінку та практики онлайн-сайту чи програми у зв'язку з конфіденційністю та безпекою кінцевих користувачів. Умови має бути розроблено за допомогою професійного юриста для того, щоб забезпечити, що вони також будуть захищати постачальника послуг від потенційних юридичних дій кінцевих користувачів як результату певних втрат або шкоди, понесених унаслідок шкідливого вмісту або нечітких політик і практик на веб-сайті.

Додатково до захисту відомостей та положень особистої конфіденційності на онлайн-сайтах або в програмах постачальники послуг повинні вимагати від сайтів або програм, що містяться в їхніх мережах, реалізації набору кращих практик управління безпекою на програмному рівні перед тим, як вони почнуть функціонування. Це має містити, але не обмежуватися, прикладами, наведеними у 12.2.

Як частина хостинг-інфраструктури постачальника послуг, сервери має бути захищено від неавторизованого доступу та можливості розміщувати шкідливий вміст. Див. 12.3 для прикладів таких засобів.

Щоб дозволити правозастосування цих засобів забезпечення безпеки, зокрема пов'язаних із безпекою онлайн-сайтів і програм, постачальники послуг повинні розглянути приєднання цих положень до умов угод про обслуговування.

11.4.4 ***Рекомендації з безпеки для споживачів***

Постачальники послуг повинні надавати рекомендації споживачам щодо того, як забезпечувати безпеку онлайн. Постачальники послуг можуть або безпосередньо створити рекомендації, або спрямувати користувачів на доступні сайти з рекомендаціями, які можуть надати таку інформацію. Вкрай важливо інформувати кінцевих користувачів щодо того, як вони можуть сприяти безпечному Інтернету у зв'язку з кількома ролями, які вони можуть відігравати в кіберпросторі, як описано в розділі 7. Додатково кінцевим користувачам потрібно рекомендувати застосовувати необхідні технічні засоби управління безпекою, в яких постачальники послуг можуть також відігравати активну роль, як описано в 11.3.

Прикладами рекомендованої діяльності можуть бути:

a) Періодичні (наприклад, щомісячні) інформаційні бюлетені з безпеки, що можуть рекомендувати спеціальні методи захисту (наприклад, як вибрати надійний пароль); новини про тенденції в безпеці; повідомлення про веб-трансляції з безпеки або інші відео на вимогу, аудіо-трансляції та інформація з безпеки, яка доступна на веб-порталі організації або інших постачальників інформації з безпеки.

b) Прямі трансляції навчальних відео з безпеки або веб-трансляції, що охоплюють різні теми у сфері безпеки, для покращення практик захисту й обізнаності кінцевих користувачів.

c) Ведення колонки з безпеки у друкованому періодичному виданні постачальника послуг, що надсилається кінцевим користувачам додому або до офісу для висвітлення ключових подій або інформації у сфері безпеки.

d) Щорічні або інші періодичні семінари з безпеки для кінцевих користувачів, можливо, у партнерстві з іншими гравцями галузі, постачальниками та державними організаціями.

Постачальники послуг, що користуються електронною поштою як основним засобом комунікації з кінцевими користувачами, повинні робити це способом, що допомагає кінцевим користувачам протистояти атакам соціальної інженерії. Зокрема, кінцевим користувачам необхідно постійно нагадувати, що неочікувані електронні листи від постачальника послуг ніколи не вимагають:

— персональну інформацію;

— імен користувачів;

— паролів;

— ніколи не містять посилань, пов'язаних з безпекою, за якими повинен перейти читач.

Коли постачальник послуг бажає, щоб користувач перейшов до їхнього сайту за інформацією, він повинен повідомити користувачу, як безпечно під'єднатися до необхідного URL. Наприклад, він може попросити користувача надрукувати URL у лапках у браузері та переконатися, що URL у лапках не містить посилання, на яке можна натиснути.

Як частину підвищення обізнаності користувачів у галузі безпеки та рекомендацій проти шпигунського та такого, що вводить в оману, програмного забезпечення, організації та постачальники послуг повинні рекомендувати своїм кінцевим користувачам застосовувати відповідні технічні засоби управління безпекою для захисту своїх систем від відомих експлоїтів та атак. Як загальна порада, потрібно заохочувати користувачів до реалізації засобів управління безпекою, наведених у 12.4.

У додатку В надано приклад списку посилань та онлайн-ресурсів, які можна застосовувати для підтримки впровадження наведених вище рекомендацій.

12 ЗАСОБИ УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ

12.1 Огляд

Як тільки ризики кібербезпеки ідентифіковані та складені відповідні рекомендації, можуть бути вибрані та реалізовані засоби управління кібербезпекою, що задовольняють вимоги щодо безпеки. Цей розділ надає огляд ключових засобів управління кібербезпекою, які можуть бути впроваджені для підтримки рекомендацій, що наведені в цьому стандарті.

12.2 Засоби управління програмного рівня

Засоби управління програмного рівня містять таке:

a) Відображення коротких повідомлень, що надають зрозумілі, невеликі резюме на одну сторінку (застосовуючи просту мову) суттєвих онлайн-політик компанії. За допомогою цього користувачі можуть приймати усвідомленіші рішення щодо обміну їхньою інформацією онлайн. Короткі повідомлення мають відповідати всім нормативним вимогам та надавати посилання на повні юридичні документи та іншу доречну інформацію, щоб клієнти, які хочуть знайти більше деталей, могли легко перейти за посиланням і прочитати повну версію. За допомогою одного повідомлення клієнти можуть отримати більш послідовний досвід щодо всіх властивостей компанії з тими самими стандартами конфіденційності та очікуваннями, поширеними на багато сайтів.

b) Захищена обробка сесій для веб-програм; це може задіювати онлайн-механізми, такі як кукі.

c) Захищена перевірка вводу та обробка відомостей для запобігання загальним атакам, таким як SQL-Injection. Виходячи з того факту, що веб-сайти, які зазвичай розглядають як такі, що заслуговують на довіру, все більше застосовують для поширення шкідливого коду, перевірку вхідних та вихідних відомостей потрібно виконувати як активним умістом, так і за допомогою динамічного вмісту.

d) Застосування захищених сценаріїв веб-сторінок для запобігання загальним атакам, таким як Cross-site Scripting.

e) Перевірка та тестування коду на предмет захищеності за допомогою відповідно підготовлених осіб.

f) Послуги організації, незалежно від того, чи надає їх організація або третя сторона, що представляє організацію, має бути надано так, щоб користувачі могли перевірити справжність послуг. Це може бути використання постачальником субдомену від брендованого доменного імені організації і, можливо, використання HTTPS-сертифікатів, зареєстрованих на організацію. Послуги повинні уникати використання методів, що вводять в оману, коли клієнт може мати труднощі із визначенням того, з ким він має справу.

12.3 Захист серверів

Ці засоби управління можна застосовувати для захисту серверів від неавторизованого доступу та розміщення шкідливого вмісту на серверах:

a) Налаштування серверів, а також операційних систем згідно з вимогами настанови з безпечного налаштування базового рівня. Це має містити належне відокремлення користувачів серверів від адміністраторів, застосування засобів контролю доступу до програм, системних директорій та файлів і ввімкнення журналів аудиту, зокрема, для системних подій, пов'язаних із безпекою та іншими збоями. Більше того, рекомендовано встановлювати на сервери мінімальну версію системи для того, щоб зменшити вектор атаки.

b) Реалізація системи тестування та розгортання оновлень безпеки та забезпечення, що операційна система й прикладні програми швидко приводяться до актуального стану, коли з'являються нові оновлення безпеки.

c) Спостерігання ефективності захисту серверів за допомогою регулярних перевірок журналів аудиту.

d) Перевірка конфігурації захисту.

e) Запуск програмних засобів захисту (таких як антивірусні та антишпигунські) від шкідливого програмного забезпечення на серверах.

f) Регулярне сканування всієї розміщеної та завантаженої інформації, застосовуючи актуальні програмні засоби захисту від шкідливого програмного забезпечення. Усвідомлення того, що файл може залишатися, наприклад, шпигунським або шкідливим, навіть якщо його не виявлено поточними засобами захисту внаслідок недостатньої інформації.

g) Регулярне проведення оцінки вразливостей та перевірки безпеки онлайн-сайтів та прикладних програм для забезпечення того, що їх безпека належно підтримується.

h) Регулярне сканування на предмет компрометації.

12.4 Засоби управління кінцевого користувача

Наступний список є неповним списком засобів управління, що їх кінцеві користувачі можуть застосовувати для захисту своїх систем від відомих експлоїтів та атак:

a) Використання підтримуваних операційних систем зі встановленими найсвіжішими оновленнями безпеки. Корпоративні споживачі зобов'язані знати та притримуватися корпоративної політики щодо підтримуваних операційних систем. Індивідуальним споживачам потрібно знати й розглянути використання операційних систем, рекомендованих постачальником. У всіх випадках операційну систему потрібно підтримувати в актуальному стані стосовно оновлень безпеки.

b) Використання останнього підтримуваного прикладного програмного забезпечення зі встановленими найсвіжішими оновленнями. Корпоративні споживачі зобов'язані знати та притримуватися корпоративної політики щодо підтримуваних прикладних програм. Індивідуальним споживачам потрібно знати й розглянути використання прикладного програмного забезпечення, рекомендованого постачальником. У всіх випадках прикладне програмне забезпечення потрібно підтримувати в актуальному стані стосовно оновлень безпеки.

c) Використання антивірусних та антишпигунських інструментів. Якщо можливо, постачальнику послуг, такому як ISP, потрібно розглянути партнерство з довіреними постачальниками засобів захисту для пропонування кінцевим користувачам цих інструментів як частини пакета підписки на послуги, так, щоб зробити засоби управління безпекою доступними за допомогою оформлення підписки або її поновлення. Корпоративні споживачі зобов'язані знати та притримуватися корпоративної політики щодо використання програмних засобів захисту. Індивідуальні споживачі повинні застосовувати програмні засоби захисту. Вони повинні звертатися до постачальника за будь-яким рекомендованим, наданим або непідтримуваним захисним програмним забезпеченням. У всіх випадках захисне програмне забезпечення потрібно підтримувати в актуальному стані щодо оновлень безпеки та баз відомостей сигнатур.

d) Реалізація відповідного антивірусного та антишпигунського захисту. Поширені веб-браузери та розширення для браузерів мають наразі можливості блокування спливаючих повідомлень, що запобігають шкідливим веб-сайтам відображати вікна, що містять шпигунське або таке, що вводить в оману, програмне забезпечення, яке може експлуатувати систему або слабкі місця браузерів чи застосовувати соціальну інженерію, щоб обманним способом змусити користувачів завантажити та встановити його в системі. Організації повинні встановити політику для того, щоб забезпечити використання таких інструментів. Організації, що надають послуги, повинні формувати список рекомендованих інструментів та заохочувати кінцевих користувачів до їхнього використання з рекомендаціями щодо вмикання та надання дозволу тим веб-сайтам, які необхідні користувачам.

e) Ввімкнення блокувальників скриптів. Ввімкнення блокувальників скриптів або жорсткіших налаштувань веб-захисту для забезпечення того, що на локальному комп'ютері можна виконувати скрипти тільки з довірених джерел.

f) Використання фішингових фільтрів. Поширені веб-браузери та розширення для браузерів часто містять цю можливість, яка може визначити, чи відвідуваний користувачем сайт міститься в базі відомостей відомих фішингових веб-сайтів або містить скриптові шаблони, що схожі з тими, які знайдені на типових фішингових сайтах. Браузер буде видавати застороги, зазвичай у формі кольорових підказок, щоб попередити користувачів про потенційний ризик. Організації повинні встановити політику для того, щоб забезпечити використання такого інструменту.

g) Використання інших доступних засобів захисту веб-браузерів. Час від часу, з появою нових ризиків кібербезпеки постачальники веб-браузерів та розширень для браузерів додають нові

засоби захисту, щоб захистити користувачів від ризиків. Кінцеві користувачі повинні бути в курсі цих розробок за допомогою вивчення таких оновлень, які зазвичай надають постачальники програмного забезпечення. Організації та постачальники послуг повинні аналогічно перевіряти ці нові засоби та оновлювати пов'язані політики та послуги, щоб краще задовольняти потреби своїх організацій та клієнтів й обробляти пов'язані ризики кібербезпеки.

h) Увімкнення персонального брандмауера та HIDS. Персональні брандмауери та HIDS є важливими інструментами для контролю мережевих служб, що мають доступ до систем користувачів. Ряд нових операційних систем мають вбудовані персональні брандмауери та HIDS. Коли вони увімкнені за замовчуванням, користувачі або прикладні програми можуть вимкнути їх, що призведе до небажаної мережевої незахищеності. Організації повинні прийняти політику використання персонального брандмауера та HIDS і оцінити доречні інструменти або продукти для їхньої реалізації так, щоб вони були увімкнені за замовчуванням для всіх співробітників. Постачальники послуг повинні заохочувати використання персонального брандмауера та функцій HIDS та/або рекомендувати інші сторонні персональні брандмауери та HIDS-продукти, які були оцінені та визнані довіреними, і навчати та допомагати користувачам у вмиканні базового мережевого захисту на рівні систем кінцевих користувачів.

i) Увімкнення автоматичних оновлень. У той час, як наведені вище засоби управління безпекою здатні справлятися з більшістю шкідливого програмного забезпечення на своїх відповідних рівнях роботи, вони не дуже ефективні проти експлуатації вразливостей, що є в операційних системах та прикладному програмному забезпеченні. Для запобігання таким експлоїтам функція оновлення, доступна в операційних системах, так само, як функція, надана користувачам довіреними прикладними програмами (наприклад, довірене та оцінене стороннє антишпигунське та антивірусне програмне забезпечення), має бути увімкнено для здійснення автоматичних оновлень. Це забезпечить, що системи підтримуються в актуальному стані щодо останніх оновлень безпеки, як тільки вони стають доступними, що зменшує часовий проміжок для використання експлоїтів.

12.5 Засоби управління захистом від атак соціальної інженерії

12.5.1 *Огляд*

Кіберзлочинці все частіше вдаються до психологічних або соціально-інженерних тактик для того, щоб домогтися успіху.

Приклад 1

Використання електронних листів, що містять URI, який веде довірливих користувачів на фішингові веб-сайти.

Приклад 2

Шахрайські листи, що просять користувачів надати персональну ідентифікаційну інформацію або інформацію, що стосуються до корпоративної інтелектуальної власності.

Поширення соціальних мереж та сайтів спільнот надає нові засоби, що в подальшому забезпечує проведення правдоподібніших видів шахрайства. Зростальними темпами такі атаки також виходять за межі технологій, за межі комп'ютерних систем і традиційних мережевих комунікацій, застосовуючи мобільні телефони, бездротові мережі (зокрема Bluetooth) та голосові Інтернет-послуги (*VoIP*).

У цьому розділі надано архітектуру засобів управління, що є застосовними для управління та мінімізації ризиків кібербезпеки стосовно атак соціальної інженерії. Рекомендації, наведені в цьому розділі, ґрунтуються на ідеї, що єдиним ефективним способом зменшення загроз соціальної інженерії є поєднання:

— технологій захисту;

— політик безпеки, що встановлюють основоположні правила для особистої поведінки як приватної особи, так і працівника;

— відповідної просвіти й тренування.

Зазначена архітектура охоплює:

— політики;

— методи та процеси;

— людей та організації;

— придатні технічні засоби управління.

12.5.2 *Політики*

Відповідно до загальних практик управління ризиками інформаційної безпеки базові політики, що регулюють створення, збирання, зберігання, передачу, обмін, обробку та загальне використання корпоративної та персональної інформації та інтелектуальної власності в Інтернеті та в кіберпросторі, мають бути визначені та задокументовані. Зокрема, це має відношення до прикладних програм, таких як обмін миттєвими повідомленнями, ведення блогів, P2P-обмін файлами та соціальні мережі, які зазвичай містяться поза сферою корпоративної мережі та інформаційної безпеки.

Як частина корпоративних політик, заяви та штрафні санкції, що мають відношення до неправильного використання прикладних програм у кіберпросторі, повинні також міститися для запобігання неправильному використанню співробітниками та третіми сторонами в корпоративній мережі або системах, що мають доступ до кіберпростору.

Повинні бути розроблені та оприлюднені адміністративні політики, що підвищують обізнаність та розуміння ризиків кібербезпеки та заохочують (якщо не змушують) вивчення та зростання навичок протидії кібератакам, зокрема, атакам соціальної інженерії. Вони мають містити вимоги регулярного відвідування таких інструктажів та тренувань.

За допомогою поширення відповідних політик та підвищення обізнаності щодо ризиків соціальної інженерії співробітники більше не зможуть посилатися на незнання таких ризиків і вимог та наразі будуть підвищувати розуміння кращих практик і політик, очікуваних від зовнішніх прикладних програм, соціальних мереж та інших програм у кіберпросторі, наприклад, в угодах про політику безпеки постачальника послуг.

12.5.3 *Методи та процеси*

12.5.3.1 *Категоризація та класифікація інформації*

Процеси категоризації та класифікації інформації мають бути реалізовані для підтримки політик, що підвищують обізнаність та захист корпоративної класифікованої та персональної конфіденційної інформації, охоплюючи інтелектуальну власність.

Для кожної категорії та класифікації задіяної інформації має бути розроблено та задокументовано спеціальні засоби управління безпекою для захисту від випадкового розголошення та навмисного неавторизованого доступу.

Користувачі в організації тоді зможуть розрізняти між різними категоріями та класифікаціями інформацію, яку вони створюють, збирають та обробляють. Користувачі зможуть виконувати необхідні превентивні та захисні перевірки під час використання кіберпростору.

Процедури щодо того, як обробляти корпоративну інтелектуальну власність, персональні відомості та іншу конфіденційну інформацію, має також бути розроблено та оприлюднено.

12.5.3.2 *Обізнаність та навчання*

Обізнаність та навчання в галузі безпеки, охоплюючи регулярне оновлення відповідних знань, є важливим елементом протидії атакам соціальної інженерії.

Як частина програми кібербезпеки організації, співробітники та сторонні підрядники повинні бути зобов'язані проводити мінімальну кількість годин навчань для того, щоб забезпечити, що вони проінформовані про свої ролі та обов'язки в кіберпросторі й технічні засоби управління, які вони повинні впровадити як приватні особи, використовуючи кіберпростір. Додатково як частина програми протидії атакам соціальної інженерії, такі навчання мають містити таке:

a) Останні загрози та форми атак соціальної інженерії, наприклад, як фішинг еволюціонував від одних підроблених веб-сайтів до комбінації спаму, Cross-Site Scripting-атак та SQL-Injection-атак.

b) Як персональна та корпоративна інформація може бути викрадена та використана за допомогою атак соціальної інженерії, що надає розуміння того, як зловмисники можуть скористатися людською природою, такою як тенденція виконувати запити, які йдуть від авторитета (навіть якщо це може бути нереальним), доброзичлива манера поведінки, видання себе жертвою та взаємність за допомогою надання чогось цінного або допомоги.

c) Яку інформацію необхідно захищати та як її захищати відповідно до політики інформаційної безпеки.

d) Коли повідомляти або виконувати ескалацію підозрілих подій або шкідливого програмного забезпечення відповідним органам чи агентствам реагування, та інформація про їхні доступні контакти. Наприклад, див. додаток B.

Організації, що надають прикладні онлайн-програми та послуги в кіберпросторі, повинні надавати інформаційні матеріали абонентам або споживачам, охоплюючи наведене вище в контексті їхніх прикладних програм або послуг.

12.5.3.3 *Тестування*

Співробітники повинні підписати підтвердження, що вони приймають та розуміють зміст політики безпеки організації. Як частина процесу покращення обізнаності та приділення належної уваги такому ризику, організація повинна розглянути проведення періодичних тестів для визначення рівня обізнаності та дотримання відповідних політик і практик. Працівники можуть зробити письмовий тест або виконати CBT для визначення того, чи розуміють вони зміст політики безпеки організації. Такі тести можуть містити, але не обмежуватися, створенням цільових, але контрольованих, фішингових сайтів, спаму та шахрайськими електронними повідомленнями, використовуючи соціальну інженерію та правдоподібний зміст. Під час проведення таких тестів важливо переконатися в тому, що:

a) усі тестові сервери та їхній вміст перебувають під контролем та управлінням команди тестування;

b) по можливості залучають професіоналів, які мають попередній досвід проведення таких тестів;

c) користувачів підготовлено до таких тестів за допомогою програм підвищення обізнаності та навчання;

d) усі результати тесту представлено в агрегованому вигляді з метою захисту конфіденційності приватних осіб, оскільки вміст, поданий у таких тестах, може занепокоювати приватних осіб та спричиняти проблеми конфіденційності, якщо його виконують неналежно.

Примітка. Етика та законодавство кожної країни має бути взято до уваги.

12.5.4 ***Люди та організація***

У той час як приватні особи є головними цілями атак соціальної інженерії, організація також може бути навмисною жертвою. Проте люди залишаються головною точкою входу для атак соціальної інженерії. Тому людей повинно бути поінформовано щодо пов'язаних ризиків у кіберпросторі, та організації повинні встановити відповідні політики та здійснити застережні кроки для фінансової підтримки таких програм, які спрямовані на забезпечення обізнаності та компетентності людей.

Як загальна рекомендація, усі організації (зокрема підприємства, постачальників послуг та державні органи) повинні заохочувати споживачів вивчати та розуміти ризики соціальної інженерії в кіберпросторі й кроки, які вони мають здійснити для їхнього захисту від потенційних атак.

12.5.5 ***Технічні засоби***

Додатково до встановлення політик та практик протидії атакам соціальної інженерії повинні бути розглянуті та, де можливо, застосовані технічні засоби управління для мінімізації незахищеності й потенційної експлуатації зловмисниками.

На особистому рівні користувачі кіберпростору повинні прийняти рекомендації, наведені в 11.3.

Організації та постачальники послуг повинні виконати необхідні кроки, описані в 11.4.4, для сприяння користувачам у прийнятті та використанні технічних засобів захисту.

Організації та постачальники послуг повинні також прийняти рекомендації, наведені в 11.4, які є важливими як базові засоби управління проти атак соціальної інженерії в кіберпросторі.

Додатково повинні бути розглянуті такі технічні засоби управління, які є корисними проти певних атак соціальної інженерії:

a) Там, де в онлайн-програмах залучена персональна чи корпоративна інформація, розглянути забезпечення стійких засобів автентифікації або як частину автентифікації при вході та/або там, де виконуються критичні транзакції. Під стійкою автентифікацією розуміють використання двох або більше додаткових чинників перевірки особистості, крім ідентифікатора користувача та пароля. Другий та додаткові чинники можуть бути надані, застосовуючи смарт-карти, біометрію та інші переносні токени безпеки.

b) Для веб-послуг організації повинні розглянути використання «сертифіката високої гарантії» для надання онлайн-користувачам додаткової гарантії. Більшість комерційних центрів сертифікації та Інтернет-браузерів здатні підтримувати використання таких сертифікатів, які зменшують загрозу фішингових атак.

c) Для убезпечення комп'ютерів користувачів, під'єднаних до сайту організації або постачальника послуг, або програми в кіберпросторі повинні бути розглянуті додаткові засоби, які гарантували б мінімальний рівень безпеки, такі як останні оновлення безпеки. Використання таких засобів має бути опубліковане в договорі про надання послуг для кінцевих користувачів та/або політиках безпеки та конфіденційності, коли це доречно.

12.6 Готовність кібербезпеки

У додатку А описано додаткові технічні засоби, придатні для покращення готовності кібербезпеки організації в галузі виявлення подій за допомогою моніторингу Darknet, розслідувань, відстежування та реагування за допомогою операції Sinkhole.

12.7 Інші засоби

Інші засоби можуть містити засоби, пов'язані з підняттям тривоги та розміщенням у карантині пристроїв, залучені в підозрілій активності через спостереження кореляції подій від постачальника послуг та/або елементів підприємства, таких як сервери DNS, мережеві потоки маршрутизаторів, фільтри вихідних повідомлень та P2P-комунікації.

13 АРХІТЕКТУРА ОБМІНУ ІНФОРМАЦІЄЮ ТА КООРДИНУВАННЯ

13.1 Загальний огляд

Інциденти кібербезпеки часто перетинають національні географічні та організаційні кордони, і швидкість потоку інформації та змін від розгортання інциденту часто дає обмежену кількість часу приватним особам та організаціям на дії. Має бути встановлено систему для обміну інформацією та координування з метою, щоб допомогти приготуватися та прореагувати на події та інциденти кібербезпеки. Це важливий крок, який організації повинні здійснити як частину своїх засобів управління кібербезпекою. Така система для обміну інформацією та координування повинна бути захищеною, ефективною та надійною.

Система повинна бути захищеною для того, щоб гарантувати, що інформація, якою обмінюються, включаючи деталі щодо координування дій, є захищеною від неавторизованого доступу, зокрема від порушника, що спричинив інцидент. Безпека інформації, що стосується подій кібербезпеки, також необхідна для запобігання неправильному тлумаченню та невиправданій паніці або тривогам громадськості. Наразі цілісність та автентичність інформації є критичною для забезпечення її точності та надійності, незалежно від того, чи така інформація поширена всередині закритої групи, чи серед широкого загалу. Система має бути ефективною, щоб виконувати свої функції з мінімальним використанням ресурсів та протягом необхідного часу та місця.

Цей розділ надає базову архітектуру для реалізації системи для обміну інформацією та координування. Архітектура містить чотири галузі для розгляду, а саме: політики, методи й процеси, люди й технічні елементи.

Примітка. ITU-T's Study Group 17 проводить інтенсивну роботу щодо обміну інформацією про кібербезпеку. Див. таблицю С.17 «Обмін інформацією про кібербезпеку» для додаткової інформації.

13.2 Політики

13.2.1 *Організації, що надають інформацію, та організації, що отримують інформацію*

Для цілей цієї архітектури визначають два типи обміну інформацією:

— організації, що надають інформацію (IPO);

— організації, що отримують інформацію (IRO).

Для IPO базові політики щодо класифікації та категоризації інформації, серйозність подій та інцидентів і форма можливого обміну повинні бути визначені заздалегідь до появи будь-яких інцидентів кібербезпеки або до будь-якого обміну (у разі перетворення IPO до IRO для обміну отриманою інформацією з іншими уповноваженими органами в інформаційному ланцюгу).

На приймальній стороні IRO має погодитися забезпечити безпеку та відповідні процедури під час отримання інформації від IPO відповідно до раніше досягненої домовленості та основи класифікації та категоризації залученої інформації.

13.2.2 *Класифікація та категоризація інформації*

IPO мають визначити різні категорії інформації, які вони збирають, зберігають, безпечно зберігають та поширюють. Приклади категорій інформації можуть містити такі категорії: події безпеки, загрози безпеки, вразливості безпеки, профілі підозрілих/підтверджених порушників, організовані групи, інформацію жертв та профілі інформаційно-комунікаційних систем.

Кожну категорію далі має бути розділено на дві чи більше класифікації залежно від змісту залученої інформації. Мінімальною класифікацією може бути: конфіденційна інформація та інформація

з необмеженим доступом. Якщо інформація містить персональні відомості, можуть бути застосовні класифікації конфіденційності.

13.2.3 *Мінімізація інформації*

Для кожної категорії та класифікації IPO має ставитися обережно, щоб мінімізувати інформацію, яка буде поширюватися. Мінімізація необхідна для запобігання інформаційному перенавантаженню на приймальній стороні для забезпечення ефективного використання системи обміну без загрози зниження ефективності. Іншою метою мінімізації є вилучення конфіденційної інформації для охорони конфіденційності людей в IPO та IRO. У зв'язку з цим IPO та IRO мають визначити бажаний рівень деталізації, коли це можливо, для кожної категорії та класифікації інформації, яку може бути ідентифіковано заздалегідь до фактичного обміну.

13.2.4 *Обмежена аудиторія*

Відповідно до принципу мінімізації політика для обмеження аудиторії, яку може бути звужено до конкретної контактної особи, групи чи організації, є необхідною під час поширення інформації, що містить персональні або конфіденційні відомості. Для менш конфіденційної інформації таку політику має бути розглянуто для запобігання інформаційному перенавантаженню, якщо вигоди від максимального поширення (наприклад, поширення критичних оповіщень безпеки) переважують вплив на інформаційне перенавантаження для IRO.

13.2.5 *Протокол координування*

Має бути встановлена високорівнева політика для координування запитів та поширення (залежно від того, чи ініціатором була IPO чи IRO). Така політика формалізує застосовуваний протокол, що надає засоби IPO та IRO для ефективної взаємодії. Процедури взаємної автентифікації та перевірки зможуть тоді бути побудовані на основі такого протоколу для забезпечення справжності джерела та доказу доставки там, де це необхідно, зокрема для персональної та/або конфіденційної інформації.

13.3 Методи та процеси

13.3.1 *Огляд*

Для здійснення політик обміну інформацією та забезпечення узгодженості практик, ефективності та стабільності виконання повинні бути розроблені та реалізовані відповідні методи та процеси. Такі методи та процеси мають ґрунтуватися на доступних стандартах. В іншому випадку, під час оперативної перевірки вони можуть бути формалізовані для стандартизації. Наступні розділи надають рекомендації щодо методів та процесів, які зазвичай застосовують організації для досягнення відповідних цілей та політик обміну інформацією та координування в контексті кібербезпеки.

13.3.2 *Класифікація та категоризація інформації*

Інформація, яку необхідно поширити, буде надходити з відкритих та закритих джерел. Інформацію з відкритих джерел часто можна знайти в Інтернеті або з інших публічних джерел, таких як газети. Інформація з відкритих джерел зазвичай є найнижчою класифікацією, тому що авторів інформації може бути кілька або вони невідомі, вік інформації може бути невизначений і точність інформації піддається сумніву. Інформація із закритих джерел недоступна для широкого загалу, часто пов'язана з джерелом та відомим віком. Прикладами інформації із закритих джерел є приватні дослідження та аналітика чи емпірично зібрані розвідувальні відомості.

Примітка. Рекомендації для цього розділу можуть ґрунтуватися на результатах періоду дослідження з цієї теми, посилаючись на цей стандарт, якщо період дослідження переходить до етапу розробки, або приймаючи резюме тексту з періоду дослідження, якщо він припиняється без подальшої розробки.

13.3.3 *Угода про нерозголошення*

Угоду про нерозголошення (*NDA*) можна застосовувати щонайменше для двох цілей у контексті обміну інформацією та координування для покращення кібербезпеки. Типовим використанням NDA є забезпечення належної обробки та захисту персональної та/або конфіденційної інформації, поширеної серед IPO та IRO, і попереднє встановлення умов обміну та подальшого поширення та використання такої інформації.

У контексті реагування на події кібербезпеки попереднє встановлення NDA дає змогу ефективно виконувати швидкий обмін та поширення серед уповноважених органів, навіть якщо класифікацію інформації не було чітко визначено.

13.3.4 *Процесуальний кодекс*

Одним із загальнозастосовуваних методів забезпечення належного обміну та обробки секретної інформації є створення процесуального кодексу, що охоплює детальні процедури, відповідальність та зобов'язання зацікавлених організацій (наприклад, IPO та IRO) щодо реагування та дій, які має бути виконано відповідними органами, залученими для кожної категорії та класифікації інформації.

Приклад

Див. майбутній стандарт ISO/IEC 29147 Information technology — Security techniques — Vulnerability disclosure.

13.3.5 *Тестування та навчання*

Для забезпечення ефективності та надійності й досягнення бажаного рівня продуктивності має бути розроблено методи та процеси для проведення регулярних тестувань і виконання навчань за сценарієм.

Як довідкову інформацію для тестування безпеки потрібно застосовувати стандартну методологію, щоб забезпечити виконання її вимог та відповідати цілям і потребам організації.

Тести безпеки можуть бути виконані на активах із високим ризиком. Це може бути зроблено використанням власної номенклатури організації для класифікації відомостей.

Оцінювання безпеки потрібно проводити на регулярній основі для:

— прикладних програм;

— операційних систем;

— систем управління базами відомостей.

13.3.6 *Вибір часу та планування обміну інформацією*

Вимога поширювати інформацію або заздалегідь, або під час реагування на інцидент буде варіюватися від суб'єкта до суб'єкта. Деякі організації матимуть вимогу до інформації в реальному часі: у момент, коли відбувається попередження або аварійний сигнал, вони бажають мати відомості для подальшого аналізу. Інші суб'єкти не матимуть ресурсів для управління обміном інформацією у реальному часі. Насправді, багато організацій можуть не мати можливості управляти обміном інформацією за графіком у будь-який період.

Вибір часу обміну інформацією та графіки повинні бути чітко визначені з конкретними цілями рівня обслуговування, визначеними для добровільних відносин, і з угодами про рівень обслуговування для комерційних відносин.

13.4 Люди та організації

13.4.1 *Огляд*

Люди та організації є ключовими чинниками, що визначають успіх кібербезпеки. Люди — особи, залучені до здійснення методів і процесів для обміну інформацією та координування, щоб здійснити позитивний вплив на результати подій кібербезпеки. Організації — групи людей всередині компанії, аж до всієї компанії, залучені до такої діяльності. Для ефективності та продуктивності повинна бути розглянута необхідність у людях та організаціях одночасно.

13.4.2 *Контакти*

Список контактів повинен бути зібраний IPO та IRO і взаємно поширений для того, щоб кожний суб'єкт міг ідентифікувати особу, яка запитала або надіслала інформацію всередині спільноти для обміну.

Також більш гранульовані списки контактів можуть бути розроблені й поширені серед обмеженої аудиторії (див. 13.2.4) та відповідно до політик класифікації та категоризації інформації (див. 13.2.2).

Список контактів не повинен містити секретної персональної інформації відповідно до політики мінімізації інформації (див. 13.2.3). Для цілей конфіденційності замість повних імен може бути розглянуто використання псевдонімів. Мінімальна інформація для списку контактів має містити ім'я (псевдонім), контактні номери (мобільний телефон, якщо можливо) та електронну адресу. Також може бути встановлений альтернативний контакт для кожної ключової особи в списку контактів.

Додатково до контактного списку для обміну інформацією та координування також може бути зібрано окремий контактний список для ескалації інцидентів з метою забезпечення швидкої ескалації. Такий список зазвичай містить зовнішні контакти, яких немає в мережі обміну. Приклади див. у додатку В.

Щонайменше контактний список має бути захищено від недозволених модифікацій з метою запобігання пошкодженням та підтримки цілісності. Технічні засоби управління (див. 13.5) потрібно застосовувати залежно від обставин.

13.4.3 *Союзи*

Для забезпечення обміну інформацією та встановлення загальних і послідовних практик, що регулюються узгодженим процесуальним кодексом та/або NDA, організації та групи осіб можуть формувати союзи на основі їхніх спільних областей інтересу, якими можуть бути промисловість, технології або інші спеціальні області інтересу. Див. додаток В для прикладу списку наявних союзів та неприбуткових організацій, які слугують цій меті.

13.4.4 *Обізнаність та навчання*

Людей в організаціях має бути поінформовано, щодо ризиків, що з'являються, та нових ризиків кібербезпеки та відповідно навчені, щоб сформувати необхідні вміння й досвід для ефективного та продуктивного реагування, коли вони стикаються з певним ризиком чи отримують інформацію, що потребує їхніх дій для пом'якшення або покращення цієї ситуації. Для досягнення цих цілей:

— Потрібно проводити регулярні інструктажі щодо статусу ризиків кібербезпеки та одержаних відомостей, які стосуються організації та індустрії.

— Для нових учасників групи та організації повинні бути спроектовані, організовані та проведені з регулярним оновленням цілеспрямовані навчання з моделюванням сценаріїв кібератак та майстер-класи зі спеціальних необхідних галузей діяльності.

— Регулярне тестування з покроковим виконанням необхідних сценаріїв для забезпечення повного розуміння та здатності застосовувати процедури та спеціальні інструменти.

Ці навчання, тренування й тестування можуть проводити внутрішні експерти, зовнішні консультанти або інші експерти з числа учасників пов'язаних союзів, залучених до обміну інформацією та координування зусиль.

Використання сценаріїв, як частина процесів навчання та тестування, настійно рекомендовано, оскільки такий підхід дає змогу особам отримати близький до життя досвід відповідних ситуацій та вивчити і практикувати необхідні дії під час реагування. Додатково минулі інциденти можуть бути використані як частина сценаріїв для максимального поширення досвіду та розуміння, отриманих із таких ситуацій.

13.5 Технічні засоби

13.5.1 *Огляд*

Технічні засоби та стандартизація можуть бути застосовні для покращення ефективності, зменшення людських помилок та поліпшення безпеки в процесах обміну інформацією та координування. Можуть бути спроектовані, розроблені та реалізовані ряд технічних систем і рішень. Цей стандарт надає деякі із загальнозастосовуваних підходів та методів, які були прийняті деякими організаціями та в подальшому можуть бути адаптовані для потреб і процесів поліпшення обміну інформацією та координування, щоб мати справу зі змінним середовищем ризиків кібербезпеки.

13.5.2 *Стандартизація відомостей для автоматизованих систем*

Як частина мережі обміну, автоматизовані системи можуть бути розроблені та розгорнуті серед координувальних організацій для збирання відомостей щодо еволюції подій кібербезпеки для онлайн- та офлайн-аналізу й оцінки з метою визначення найновішого статусу безпеки в кіберпросторі в межах залучених організацій. Такі відомості можуть містити мережеві відомості трафіку, оновлення безпеки для програмних систем та апаратних пристроїв, відомості про вразливості безпеки, шкідливе програмне забезпечення, спам, шпигунські відомості, зокрема їхнє корисне навантаження та перехоплену інформацію. Автоматизовані системи, що підтримують початкове реагування та ескалацію інцидентів, як описано в 13.4.2, будуть також містити відомості, що стосуються організацій та людей. Беручи до уваги секретність та обсяг відомостей, що залучаються в таких системах, організації (зокрема союзи організацій) повинні оцінити схеми відомостей та їхній зміст для визначення відповідних засобів управління, необхідних для покращення ефективності, продуктивності та безпеки. Це може містити, але не обмежуватися, таким:

a) стандартизація схеми відомостей для кожної категорії та класифікації зібраних відомостей, дотримуючись політики мінімізації інформації та конфіденційності, та надання технічних гарантій усім задіяним суб'єктам і власникам відомостей такої практики;

b) стандартизація формату відомостей для полегшення обміну та покращення сховища, передачі, обробки й сумісності між системами. Наприклад, див. ITU-T X.1205;

c) стандартизація функціонала базової обробки відомостей та застосовуваних алгоритмів, наприклад, геш-функції та процедур для анонімізації IP-адреси та інших вимог до попередньої обробки.

13.5.3 *Візуалізація відомостей*

Рекомендовано розглянути методи візуалізації відомостей для подання інформації про події, що допомагає покращити видимість змін та появу інциденту безпеки без потреби операторам читати деталі кожної події в разі її появи. Наприклад, див. додаток А, який надає візуальне подання активності у Darknet, що сприяє ефективнішому реагуванню на зміни.

13.5.4 *Обмін криптографічними ключами та програмне/апаратне резервне копіювання*

Для забезпечення обміну конфіденційною інформацією повинні бути розглянуті для реалізації криптографічні системи, зокрема систему для обміну ключів, які можуть бути швидко введені в експлуатацію. Система має містити належне резервне копіювання для програмного та апаратного забезпечення, так само, як криптографічні ключі, що застосовують на етапі підготовки для цілей обміну та потреб аварійного відновлення.

13.5.5 *Захищений обмін файлами, миттєвими повідомленнями, веб-портал та онлайн-форум*

Для забезпечення онлайн-взаємодії та швидкого й захищеного обміну інформацією, що може містити обмін цифровим контентом, таким як текст та мультимедіа-файли, і онлайн- та офлайн-дискусій організації обміну (IPO та IRO) повинні розглянути прийняття придатних інструментів обміну файлами, обміну миттєвими повідомленнями та онлайн-дискусій на форумах, які можуть відповідати потребам безпеки, ефективності, продуктивності та надійності.

Канали веб-порталу щодо подій та статусу кібербезпеки повинні бути реалізовані у формі комунікацій для публічних та приватних спільнот, які відповідно зацікавлені або залучені. Там, де застосовують такий веб-портал, повинно бути чітко закріплене адміністративне право власності та відповідальності для забезпечення безпеки та доступності веб-порталу. Приватні ділянки веб-порталу повинні бути надані для обмеженої аудиторії, коли це необхідно.

13.5.6 *Тестові системи*

У той час, як кожна технічна система та пов'язані методи й процеси мають бути строго протестовані для гарантування їхньої надійності та цілісності, потрібно розглянути використання однієї чи більше технічних систем, виділених для покращення ефективності й продуктивності тестування, зокрема сценаріїв тестування. Така система може бути у формі моделювальної системи для моделювання робочих середовищ, передбачених кожною організацією кіберпростору, та еволюції ситуації кібербезпеки, надаючи можливості для впровадження ряду подій безпеки для забезпечення проведення необхідного тесту.

13.6 Рекомендації щодо впровадження

Упровадження такої архітектури потребує співпрацю організацій та окремих осіб у формі зібрання разом (віртуально або фізично), щоб визначити відповідну політику, засоби управління та кроки, необхідні для досягнення її цілей безпечного, ефективного, надійного та продуктивного обміну інформацією та координування під час реагування на інциденти кібербезпеки, що з'являються. Наступні високорівневі кроки рекомендовано як настанову для впровадження:

a) Визначити та зібрати відповідні організації та окремих осіб до форми мережевої спільноти для обміну інформацією та координування або неформально, або формально.

b) Визначити ролі кожної залученої організації/особи або як IPO, IRO, або обидві (див. 13.2.1).

c) Установити вид необхідної інформації та координування, який буде корисним для спільноти.

d) Здійснити категоризацію та класифікацію інформації, щоб визначити, чи залучена будь-яка секретна та/або конфіденційна інформація (див. 13.2.2).

e) Установити політики та принципи, що регулюють спільноту та залучену інформацію (див. 13.2).

f) Визначити методи та процеси, необхідні для кожної категорії та класифікації залученої інформації (розділ 13.3).

g) Визначити вимоги продуктивності та критерії і створити процесуальний кодекс та підписати NDA залежно від обставин (див. 13.3.3 та 13.3.4).

h) Визначити необхідні та придатні стандарти і технічні системи для підтримки впровадження та роботи спільноти (див. 13.5).

i) Підготувати до роботи; звірити список контактів; та провести навчання і тренувальні майстер-класи для підготовки зацікавлених сторін.

j) Проводити регулярне тестування, зокрема покрокове виконання сценаріїв та моделювання залежно від обставин (див. 13.3.5 та 13.5.6).

k) Проводити періодичні перевірки після тестів та після інцидентів для покращення систем обміну і координування, зокрема залучених людей, процеси та технології; збільшити або зменшити розмір спільноти залежно від обставин.

Примітка. ISO/IEC 27001 Information technology — Security techniques — Information security management systems requirements та ISO/IEC 27003 Information technology — Security techniques — Information security management system implementation guidance надають вимоги та рекомендації щодо впровадження.

ДОДАТОК А
(довідковий)

ГОТОВНІСТЬ КІБЕРБЕЗПЕКИ

А.1 Огляд

Засоби управління кібербезпекою, описані в розділі 12, мінімізують незахищеність та ризик організацій та кінцевих користувачів для більшості відомих кібератак. Після появи інцидентів кібербезпеки архітектура для обміну інформацією та координування, описана в розділі 11, надає для реалізації систему обміну інформацією та координування під час підготовки до реагування на події та інциденти кібербезпеки. Таку інформацію належно захищено між IPO та IRO.

У той час, як ці засоби управління зменшують ризик та покращують обробку й управління інцидентами, кіберзлочинці або інші порушники продовжуватимуть розробляти нові або еволюціонувальні атаки для подолання наявних систем захисту. Тому для організацій також важливо впровадити системи та інфраструктуру, які забезпечують динамічніший та строгий підхід до виявлення, розслідування та реагування на атаки.

ISO/IEC 27031 надає рекомендації щодо систем управління та пов'язаних процесів для підготовки інформаційно-комунікаційних систем організації до виявлення та реагування на події безпеки, що виникають, зокрема події кібербезпеки. Ця настанова висвітлює додаткові технічні підходи, які застосовні для підвищення готовності кібербезпеки організації у сфері виявлення подій за допомогою моніторингу Darknet, розслідувань, відстежування та реагування за допомогою операції Sinkhole.

Організації, зокрема CIIP, повинні розглянути використання цих підходів для покращення готовності кібербезпеки та, відповідно, її статусу.

А.2 Моніторинг Darknet

А.2.1 *Вступ*

Darknet — це набір IP-адрес, які не застосовують в організаціях. IP-адреси у Darknet не закріплені за жодними робочими серверами/комп'ютерними системами. Методом використання контрольованих пакетів у IP-доменах Darknet організації можуть спостерігати мережеві атаки, що з'являються, охоплюючи мережеве сканування, ініційоване шкідливим програмним забезпеченням; поведінку шкідливих програм під час інфікування та розповсюджувачами DDoS. Оскільки IP-адреси Darknet опубліковані, але не закріплені за легітимними системами, весь вхідний трафік, що належить IP-доменам Darknet, можна розглядати як результат або шкідливої активності, або неправильної конфігурації.

Загалом є три методи, що зазвичай застосовують у Darknet, для спостерігання трафіку, пов'язаного зі шкідливою активністю в Інтернеті, а саме: моніторинг Black Hole, моніторинг низької та високої взаємодії.

А.2.2 *Моніторинг Black Hole*

Під моніторингом Black Hole розуміють моніторинг систем, які не відповідають ні на що, крім вхідних пакетів усередині IP-доменів Darknet. Цей тип систем моніторингу часто застосовують для непримітного спостерігання за скануванням мережевих портів шкідливим програмним забезпеченням, за поведінкою шкідливих програм під час інфікування (UDP з корисним навантаженням, зокрема shell-код) та розповсюджувачами DDoS. Мережеве сканування портів часто є початковим кроком, що виконують зловмисники для пошуку вразливих систем, які можуть бути проексплуатовані. Шкідлива поведінка під час інфікування є зазвичай наступним кроком, що здійснюють зловмисники після ідентифікації вразливих комп'ютерних систем. Такі дії з інфікування часто спостерігають за допомогою моніторингу Black Hole як такі, що застосовують UDP з корисним навантаженням. Більше того, розповсюджувачів DDoS також спостерігають засобами моніторингу Black Hole в разі підміни IP-адреси джерел (зловмисників). Ціль DDoS може бути розпізнано за цим трафіком розповсюджувачів. На рисунку А.1 зображено знімок екрана візуалізації шкідливої активності, виявленої системою моніторингу Black Hole. Приклад відео може бути знайдено тут:

https://www. youtube.com/watch?v=asemvKgkib4&feature=related

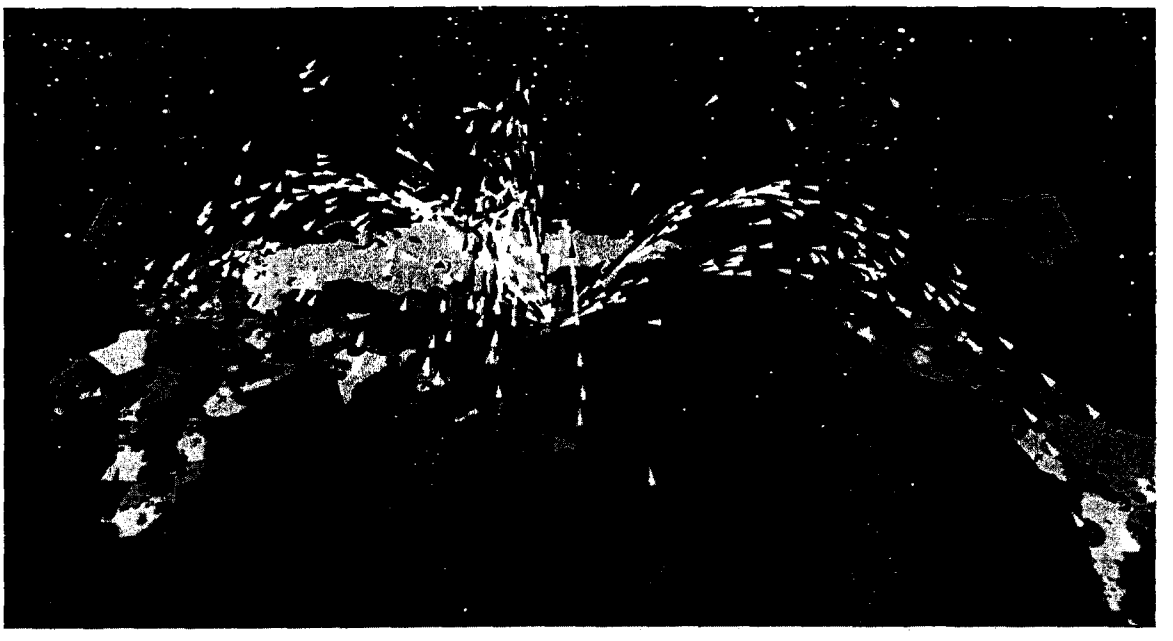

Рисунок А.1 — Приклад візуалізації шкідливої активності з використанням системи моніторингу Black Hole

Стрілки над картою світу (рисунок А.1) позначають напрямок руху IP-пакетів від джерел до цілей. Різні відтінки (кольори на відео) позначають тип пакета (наприклад, TCP SYN, TCP SYN-ACK, інші типи TCP, UDP та ICMP). Висоту кожної стрілки наведено в пропорції до її номера порту.

А.2.3 *Моніторинг низької взаємодії*

Моніторинг низької взаємодії — це система моніторингу Darknet, що відповідає на виявлені IP-пакети Darknet спробою зворотного підключення до підозрілих комп'ютерних систем. Метою спроби підключення є отримання більшої інформації про комп'ютерні системи зловмисника, використані мережеві шляхи та іншу інформацію, що стосується атаки, якщо це можливо. Систему моніторингу часто налаштовано так, щоб маскуватися під систему з незакритими вразливостями для привертання атак. Систему моніторингу низької взаємодії також застосовують для спостерігання наслідків шкідливої поведінки та активності, такої як виконання shell-скриптів після початкового сканування мережевих портів.

А.2.4 *Моніторинг високої взаємодії*

Система моніторингу високої взаємодії (також відома як приманка високої взаємодії) також є системою моніторингу Darknet, що відповідає на виявлені IP-пакети Darknet спробою зворотного підключення до підозрілих комп'ютерних систем та якомога більшою взаємодією з цими системами. Метою взаємодії є отримання якомога глибшої інформації, зокрема стратегію експлуатації вразливостей, шкідливі програми, введені після експлуатації, та система моніторингу високої взаємодії може бути реалізована на реальних або віртуальних операційних системах з незакритими вразливостями так, що вони привернуть увагу зловмисників, будуть проексплуатовані та, зрештою, захоплять зразки введених шкідливих програм.

А.3 Операція Sinkhole

Операцію Sinkhole визначено як метод для перенаправлення певного IP-трафіку до «зливного» пристрою (наприклад, «зливний» маршрутизатор) з метою аналізу трафіку, відхилення атак та виявлення аномальної поведінки в мережі. Наприклад, якщо робота бізнесу цільової системи паралізована засобами DDoS-атаки, одним з ефективних рішень є ініціювання операції Sinkhole введенням альтернативного маршруту для цілі та перенаправлення DDoS-трафіка за цим маршрутом замість дозволу його проходження до оригінальної цілі. «Зливний» пристрій здатний поглинати, аналізувати та/або відкидати DDoS-трафік. Маршрут перенаправлення цілі, який рухається до «зливного» маршрутизатора, зазвичай опубліковує граничний BGP-маршрутизатор. Операцію Sinkhole за допомогою BGP-конфігурації описано в RFC 3882. Недоліком цього методу є те, що IP-адресу, яка зазнає

атаки, не можна застосовувати для комунікації з іншими мережевими користувачами, доки маршрут не буде видалено.

Операції Sinkhole часто застосовують для захисту від DDoS-атак, як було описано вище. Її також застосовують для захисту від атак ботів перенаправленням командного центру (C&C) ботнету до «зливного» пристрою. Оскільки кожен бот має встановити з'єднання із C&C-сервером, щоб отримати інструкції для атаки від командного центру ботнету, вони надсилають DNS-запити для визначення IP-адреси C&C-сервера за URL. Тоді DNS-сервери надсилають ботам IP-адресу «зливного» пристрою замість оригінальної IP-адреси C&C-сервера. Отже, командний центр ботнету позбавляється з'єднання з ботами і не може надсилати їм інструкцій щодо атак.

A.4 Відстежування

Для автоматизації або прискорення ручного відстеження шкідливих атак, таких як DDoS, де система-джерело фальсифікована, були вивчені багато методів автоматичного відстежування. Методи відстежування розглядають як методи, що відбудовують шлях атаки та локалізують вузли зловмисника способом перевірки трафіку атаки, інформації щодо маршрутизації, помічених пакетів або аудиту журналів трафіку атаки.

Ще не було створено або використано на практиці в реальному робочому мережевому середовищі жодного методу відстежування, який міг би відновити шлях атаки через кілька мережевих доменів. Труднощі реалізації міждоменних (через кілька мережевих доменів) методів відстежування випливають із таких проблем:

a) Для цілей міждоменного відстежування обмін секретною інформацією, такою як детальна магістральна топологія, може спричинити серйозні проблеми для операторів мереж.

b) Оскільки операцію відстежування може бути тісно пов'язано з мережевою безпекою магістралі постачальника Інтернет-послуг, довільні спроби відстежування неавторизованими особами не будуть прийнятними для більшості постачальників Інтернет-послуг. Тому є страх неправильного використання іншими особами методу відстежування на кожному мережевому домені.

c) Якщо єдиний та спеціальний міждоменний метод відстежування застосовують серед кількох мережевих доменів, єдиний унікальний метод також має бути реалізовано відповідними автономними системами (AS), які беруть у ньому участь. Крім того, зловмисники рано чи пізно розроблять методи атаки. По суті, багато постачальників Інтернет-послуг застосовують кілька інструментів виявлення та відстежування в їхніх мережах.

Наведені вище робочі проблеми стають актуальними, коли спроби відстежування виходять за межі конкретної мережі. Методи відстежування мають враховувати межі мережевої роботи та відмінність оперативних політик між різними мережевими доменами. Вважають, що механізми міждоменного відстежування та пом'якшення атак повинні бути розміщені повсюдно в Інтернеті.

У процесі розробки методів та систем міждоменного відстежування на практиці потрібно враховувати таку архітектуру відстежування:

a) Для зберігання границь мереж архітектура відстежування повинна залишити кожній AS вибір того, чи приймати запит відстежування за допомогою оперативної політики кожної AS.

b) Архітектура відстежування також повинна залишити кожній AS вибір того, чи проводити глибше розслідування всередині власного мережевого домену.

c) Архітектура також повинна дозволяти кожному піддомену AS вирішувати, чи здійснювати перевірку кожної мережі піддомену за допомогою його оперативної політики. Операція відстежування споживатиме багато ресурсів на пов'язаних AS; тому архітектура відстежування не повинна генерувати або масово надсилати безцільні запити, якщо це можливо; тому архітектура відстежування не повинна перенаправляти повідомлення запитів до інших AS, які не стосуються атаки.

d) Для зменшення збитків від зловживань повідомлення не повинно містити такої інформації, яка може призвести до витоку секретної або конфіденційної інформації AS; тому архітектура відстежування не повинна розкривати секретної інформації AS іншим системам.

e) Навіть якщо відбулося зловживання або компрометація, простежуваність повідомлення дозволить визначити порушника, отже, повідомлення всередині архітектури повинні мати свою власну відстежуваність для доказування або підтвердження порушників.

f) Якщо архітектура залежить від одного специфічного методу, зловмисники розроблять відповідні методи атаки та приховають розташування вузлів, з яких виконується атака. Для подолання таких атак архітектура відстежування має бути незалежною від конкретних технік відстежування.

g) Багато операційних систем переходять до підтримки подвійного стеку IPv4/IPv6, і кілька атак застосовують 6to4 IPv6-тунелювання. Якщо архітектура відстежування не може відстежувати атаки на IPv6-мережах або атаки через певні транслятори, більшість атак перейдуть до таких складних атак. Тому архітектура відстежування повинна відстежувати атаки в середовищі з подвійним стеком, навіть якщо атака застосовує певні методи трансляції адрес.

h) Для автоматизації процесу пом'якшення атаки архітектура відстежування повинна мати можливість експортувати результат спроби відстежування як тригер пом'якшення атаки. Тому архітектура відстежування має дозволяти кожній AS виконувати іншу дію разом з результатом відстежування, таку як фільтрацію або інше відстежування.

i) Архітектура повинна мати можливість взаємодіяти з системами виявлення або системами захисту (*IDS/IPS*).

j) Зловмисник може змінити шаблон трафіку атаки для уникнення ефекту від таких дій, спрямованих на пом'якшення атаки. Ведучи боротьбу зі змінами складної атаки, час, витрачений на відстежування шляху атаки, повинен бути якомога коротшим. Тому архітектура повинна вилучити людський чинник максимально, наскільки це можливо.

ДОДАТОК В
(довідковий)

ДОДАТКОВІ РЕСУРСИ

В.1 Посилання на онлайн-ресурси з безпеки та антишпигунського програмного забезпечення

Є ряд веб-сайтів, на які можна посилатися за додатковою інформацією щодо Інтернет-безпеки та кібербезпеки. Нижче наведений невичерпний перелік прикладів таких веб-сайтів:

— **Anti-spyware Coalition** (http://www.antispywarecoalition.org/) — група, що займається узгодженням щодо визначень та кращих практик у дискусії щодо шпигунського програмного забезпечення та інших потенційно небажаних технологій. Утворена антишпигунськими компаніями, вченими та групами споживачів, ASC прагне об'єднати широке коло точок зору навколо проблеми контролю шпигунських та інших потенційно небажаних технологій.

— **APWG** (http://www.antiphishing.org) — інформаційно-освітній сайт з фішингу, що постачає документи, які оновлюються щоквартально, щодо тенденцій, поширення, впливу та новин у галузі атак.

— **Be Web Aware** (http://www.bewebaware.ca) — національна, двомовна публічна освітня програма з Інтернет-безпеки, покликана забезпечити, щоб молоді канадці отримували вигоду з Інтернету, будучи одночасно безпечними та відповідальними у своїх онлайн-діях.

— **Centre for Safe and Responsible Internet Use** (http://csriu.org) — організація, що надає послуги з вирішення питань безпеки та відповідального використання Інтернету.

— **Childnet International** (http://www.childnet-int.org) — неприбуткова організація, що співпрацює з іншими організаціями по всьому світу, щоб допомогти зробити Інтернет гарним та безпечним місцем для дітей.

— **ECPAT** (http://www.ecpat.net) — мережа організацій та приватних осіб, що співпрацюють разом над ліквідуванням комерційної сексуальної експлуатації дітей.

— **GetNetWise** (http://www.getnetwise.org) — публічна послуга, що надає коаліція корпорацій у галузі Інтернет та зацікавлені громадські організації, яка прагне надавати у зручній формі ресурси користувачам, яких вони потребують для прийняття усвідомлених рішень щодо використання Інтернету для них та їхньої родини.

— **Global Infrastructure Alliance for Internet Safety (GIAIS)** (http://www.microsoft.com/security/msra/default.mspx) — об'єднання деяких постачальників послуг, які були організовані для покращення безпеки в Інтернеті, постійного управління загрозами широкого спектра, ідентифікації та зменшення існуючих вразливостей.

— **INHOPE** (http://inhope.org) — міжнародна асоціація, яка підтримує телефони довіри Інтернету для реагування на повідомлення про незаконний уміст ресурсів, щоб зробити Інтернет безпечнішим.

— **Internet Safety Group** (www.netsafe.org.nz) — веб-сайт NetSafe є домашньою сторінкою групи Internet Safety Group з Нової Зеландії (ISG) та Hector the Protector.

— **Interpol** (http://www.interpol.int) — міжнародна поліцейська організація, що забезпечує транскордонну співпрацю поліції та підтримує і допомагає всім організаціям, органам та службам, місією яких є запобігання та боротьба з міжнародною злочинністю.

— **iSafe** (http://www.isafe.org) — Інтернет-лідер з освіти в галузі Інтернет-безпеки; містить навчальні програми з динамічною спільнотою для розширення можливостей студентів, викладачів, батьків, правоохоронних органів та зацікавлених дорослих, щоб зробити Інтернет безпечнішим місцем.

— **ISECOM** (http://www.isecom.org) — безкоштовні, відкриті методології з професійного тестування безпеки (оцінка вразливостей, тести на проникнення, етичний хакінг), технічної оцінки ризиків (RAV та інші). ISECOM підтримує OSSTMM (відкрита настанова з методології тестування безпеки), де-факто світовий стандарт для проведення тестувань безпеки IT/ICT (http://www.osstmm.org).

— **COP** (http://www.itu.int/cop/) — Children Online Protection (COP) є спеціальним проектом, що виконує ITU (International Telecommunication Union) та інші спеціалізовані агентства/фірми, що постачають рекомендації з безпеки для дітей, батьків, опікунів та вихователів, підприємців та політиків. Children, Parents, Guardians and Educators, Industry and Policy Makers.

— **Microsoft Security At Home** (http://www.microsoft.com/protect) — інформація та ресурси, покликані допомогти громадськості захистити свої комп'ютери, їх самих та свої сім'ї.

— **National Institute of Telecommunications Technologies, INTECO** (http://www.inteco.es, http://cert.inteco.es, http://www.osi.es, http://observatorio.inteco.es) — безкоштовна публічна послуга, що надає іспанська державна адміністрація для сприяння зміцненню довіри та безпеки в Інтернеті для громадян, SME, технічних спеціалістів, дітей тощо за допомогою таких організацій, як Computer Emergence Response Team (INTECO-CERT), Security Helpdesk For Citizens (OSI) та Information Security Observatory.

— **Net Family News** (http://netfamilynews.org) — неприбуткова публічна служба, що надає форум та технічні дитячі новини для батьків та вихователів у більше ніж 50 країнах.

— **NetAlert Limited** (http://www.netalert.net.au) — неприбуткова громадська організація, створена урядом Австралії для надання незалежних рекомендацій та навчань щодо управління доступом до онлайн-інформації.

— **NetSmartzKids** (http://www.netsmartzkids.org) — NetSmartz є інтерактивним освітнім ресурсом з безпеки від організацій National Centre for Missing and Exploited Children (*NCMEC*) та Boys and Girls Clubs of America (*BGCA*) для дітей віком від 5 до 17 років, батьків, опікунів, вихователів та правоохоронних органів, що застосовують відповідні до віку 3D-технології для навчання дітей тому, як залишатися безпечнішими в Інтернеті.

— **Saferinternet.be** (www.saferinternet.be) — цей веб-сайт пропонує корисну інформацію щодо головних ризиків та шкідливого вмісту, з яким можуть зіткнутися неповнолітні онлайн, та у галузі інформаційно-комунікаційних технологій загалом (тобто також за допомогою мобільних телефонних мереж тощо), наприклад, з дитячою порнографією, расизмом та дискримінацією, сектами, незаконними комерційними практиками та аферами і, зрештою, технічними ризиками. Веб-сайт, який також надає стратегії правильного поводження з цими ризиками, складається з кількох секцій, які сфокусовані на різноманітних цільових групах. Крім того, цей веб-сайт надає педагогічні та освітні файли для вихователів (батьків та вчителів), ігри для дітей (віком від 6 до 12 років) та повністю окремий сайт (web4me.be) для підлітків.

— **SafeKids.com** (http://www.safekids.com) — ресурс, що допомагає сім'ям зробити Інтернет та технології веселими, безпечними та продуктивними.

— **StaySafe.org** (http://www.staysafe.org) — освітній веб-сайт, спрямований на допомогу споживачам у розумінні як позитивних аспектів Інтернет, так і тому, як управляти різними питаннями безпеки, які існують онлайн.

— **UNICEF** (http://www.unicef.org) — глобальний захисник прав дітей, присвячений довготривалому наданню гуманітарної та пов'язаної з розвитком допомоги для дітей та батьків у країнах, що розвиваються.

— **WebSafe Crackerz** (http://www.websafecrackerz.com) — інтерактивні ігри та загадки, створені, щоб допомогти підліткам та запропонувати стратегії поведінки в різних онлайн-ситуаціях, охоплюючи спам, фішинг та шахрайства.

B.2 Приклад списку контактів для ескалації інцидентів безпеки

У наведеній нижче таблиці B.1 надано невичерпний перелік прикладів контактів для ескалації інцидентів безпеки в Інтернеті.

Таблиця B.1 — Приклад списку контактної інформації для ескалації інцидентів безпеки

Організації	Контакти
Cisco Systems Inc.	mailto:safetyandsecurity@cisco.com http://www.cisco.com/security
Microsoft Corporation	mailto:avsubmit@submit.microsoft.com mailto:secure@microsoft.com
Forum of Incident Response and Security Teams (FIRST)	http://www.first.org/about/organization/teams/
Відповідні національні команди CERT (наприклад)	
National Institute of Telecommunications Technologies, INTECO, Spain	http://cert.inteco.es (English: http://cert.inteco.es/cert/INTECOCERT_1/?postAction=getCertHome)
Telecom-ISAC Japan	https://www.telecom-isac.jp/contact/index.html
KrCERT/CC (Korea Internet Security Center	http://www.krcert.or.kr/index.jsp

ДОДАТОК С
(довідковий)

ПРИКЛАДИ ПОВ'ЯЗАНИХ ДОКУМЕНТІВ

C.1 Вступ

У цьому додатку надано невичерпний перелік прикладів документів, що можуть бути корисними під час розгляду кібербезпеки. Він не має на меті бути повним списком стандартів і технічних звітів з кібербезпеки.

C.2 ISO та IEC

Таблиця C.1 — Системи управління інформаційною безпекою

Посилання	Назва
ISO/IEC 27000	Information technology — Security techniques — Information security *management systems — Overview and vocabulary*
ISO/IEC 27001	Information technology — Security techniques — Information security management systems — Requirements
ISO/IEC 27002	Information technology — Security techniques — Code of practice for information security management
ISO/IEC 27003	Information technology — Security techniques — Information security *management system implementation guidance*
ISO/IEC 27010	Information technology — Security techniques — Information security management for inter-sector communications

Таблиця C.2 — Управління ризиками

Посилання	Назва
ISO/IEC 27005	Information technology — Security techniques — Information security risk management
ISO/IEC 16085	Systems and software engineering — Life cycle processes — Risk management

Таблиця C.3 — Оцінка IT-безпеки

Посилання	Назва
ISO/IEC 15408	Information technology — Security techniques — Evaluation criteria for IT security
ISO/IEC 18045	Information technology — Security techniques — Methodology for IT security evaluation
ISO/IEC TR 19791	Information technology — Security techniques — Security assessment of operational systems

Таблиця С.4 — Забезпечення безпеки

Посилання	Назва
ISO/IEC TR 15443	Information technology — Security techniques — A framework for IT Security assurance
ISO/IEC 15026	Systems and software engineering — Systems and software assurance

Таблиця С.5 — Проектування та реалізація

Посилання	Назва
ISO/IEC 12207	Systems and software engineering — Software life cycle processes
ISO/IEC 14764	Software Engineering — Software Life Cycle Processes — Maintenance
ISO/IEC 15288	Systems and software engineering — System life cycle processes
ISO/IEC 23026	Software Engineering — Recommended Practice for the Internet — Web Site Engineering, Web Site Management, and Web Site Life Cycle
ISO/IEC 42010	Systems and software engineering — Architecture description

Таблиця С.6 — Аутсорсинг та сторонні послуги

Посилання	Назва
ISO/IEC TR 14516	Information technology — Security techniques — Guidelines for the use and management of Trusted Third Party services
ISO/IEC 15945	Information technology — Security techniques — Specification of TTP services to support the application of digital signatures

Таблиця С.7 — Мережева та програмна безпека

Посилання	Назва
ISO/IEC 18028	Information technology — Security techniques — IT network security
ISO/IEC 18043	Information technology — Security techniques — Selection, deployment and operations of intrusion detection systems
ISO/IEC 27033	Information technology — Security techniques — Network security
ISO/IEC 27034	Information technology — Security techniques — Guidelines for application security

Таблиця С.8 — Безперервність та управління інцидентами

Посилання	Назва
ISO/IEC TR 18044	Information technology — Security techniques — Information security incident management
ISO/IEC 24762	Information technology — Security techniques — Guidelines for information and communications technology disaster recovery services
ISO/IEC 27031	Information technology — Security techniques — Guidelines for ICT readiness for business continuity
ISO/IEC 27035	Information technology — Security techniques — Information security incident management

Таблиця С.9 — Управління особистістю

Посилання	Назва
ISO/IEC 24760	Information technology — Security techniques — A framework for identity management

Таблиця С.10 — Конфіденційність

Посилання	Назва
ISO/IEC 29100	Information technology — Security techniques — Privacy framework

Таблиця С.11 — Управління активами

Посилання	Назва
ISO/IEC 19770	Information technology — Software asset management

Таблиця С.12 — Управління послугами

Посилання	Назва
ISO/IEC 20000	Information technology — Service management

С.3 ITU-T

Таблиця С.13 — Кібербезпека

Посилання	Назва
ITU-T X.1200 — X.1299 Series	Series X: Data Networks, Open System Communications and Security, Telecommunication Security — Cyberspace security
ITU-T X.1205	Series X: Data Networks, Open System Communications and Security, Telecommunication Security — Overview of Cybersecurity

Таблиця С.14 — Безперервність та управління інцидентами

Посилання	Назва
ITU-T X.1206	Series X: Data Networks, Open System Communications and Security, Telecommunication Security — A vendor-neutral framework for automatic notification of security related information and dissemination of updates

Таблиця С.15 — Небажане програмне забезпечення

Посилання	Назва
ITU-T X.1207	Series X: Data Networks, Open System Communications and Security, Telecommunication Security — Guidelines for Telecommunication Service Providers for Addressing the Risk of Spyware and Potentially Unwanted Software

Таблиця С.16 — Спам

Посилання	Назва
ITU-T X.1231	Series X: Data Networks, Open System Communications and Security, Telecommunication Security — Technical strategies for countering spam
ITU-T X.1240	Series X: Data Networks, Open System Communications and Security, Telecommunication Security — Technologies involved in countering e-mail spam
ITU-T X.1241	Series X: Data Networks, Open System Communications and Security, Telecommunication Security — Technical framework for countering email spam
ITU-T X.1244	Series X: Data Networks, Open System Communications and Security, Telecommunication Security — Overall aspects of countering spam in IP-based multimedia applications

Таблиця С.17 — Обмін інформацією з кібербезпеки

Посилання	Назва
ITU-T X.1500 — X.1598 Series (CYBEX)	Series X: Data networks, Open System Communications and Security — Cybersecurity Information Exchange

Примітка. Станом на вересень 2011, оскільки робота CYBEX триває в ITU-T тільки X.1500, X.1520, X.1521 та X.1570 доступні як рекомендації або проекти. Кілька інших з'являться в майбутньому, тому рекомендовано, щоб користувачі перевіряли веб-сайт ITU-T для останньої доступної інформації.

БІБЛІОГРАФІЯ

1 An Autonomous Architecture for Inter-Domain Trace back across the Borders of Network Operation (iscc06)

2 IETF RFC 3882 Configuring BGP to Block Denial-of-Service Attacks

3 ISO Guide 73:2009 Risk management — Vocabulary

4 ISO/IEC 12207:2008 Systems and software engineering — Software life cycle processes

5 ISO/IEC 15408-1 Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model

6 ISO/IEC 19770-1 Information technology — Software asset management — Part 1: Processes and tiered assessment of conformance

7 ISO/IEC TR 19791 Information technology — Security techniques — Security assessment of operational systems

8 ISO/IEC 20000-1 Information technology — Service management — Part 1: Service management system requirements

9 ISO/IEC 27001 Information technology — Security techniques — Information security management systems — Requirements

10 ISO/IEC 27002 Information technology — Security techniques — Code of practice for information security management

11 ISO/IEC 27005 Information technology — Security techniques — Information security risk management

12 ISO/IEC 27010 Information technology — Security techniques — Information security management for inter-sector and inter-organizational communications

13 ISO/IEC 27031 Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity

14 ISO/IEC 27033 (all parts) Information technology — Security techniques — Network security

15 ISO/IEC 27034 (all parts) Information technology — Security techniques — Application security

16 ISO/IEC 27035, Information technology — Security techniques — Information security incident management

17 ISO/IEC 29147 Information technology — Security techniques — Vulnerability disclosure2)

18 ISO 31000 Risk management — Principles and guidelines

19 ITU-T X.1200 — X.1299, Series X: Data Networks, Open System Communications and Security, Telecommunication Security — Cyberspace security

20 ITU-T X.1500 — X.1598, Series X: Data Networks, Open System Communications and Security — Cybersecurity Information Exchange.

ДОДАТОК НА
(довідковий)

ПЕРЕЛІК НАЦІОНАЛЬНИХ СТАНДАРТІВ, ЗГАРМОНІЗОВАНИХ ІЗ МІЖНАРОДНИМИ ЧИ ЇХНІМИ ЄВРОПЕЙСЬКИМИ АНАЛОГАМИ, НА ЯКІ Є ПОСИЛАННЯ В ЦЬОМУ СТАНДАРТІ

ДСТУ ISO/IEC 27000:2015 (ISO/IEC 27000:2014) Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Огляд і словник

ДСТУ ISO/IEC 12207:2014 Інженерія систем і програмного забезпечення. Процеси життєвого циклу програмного забезпечення (ISO/IEC 12207:2008, IDT)

ДСТУ ISO/IEC 20000-1:2015 (ISO/IEC 20000-1:2011, IDT) Інформаційні технології. Менеджмент послуг. Частина 1. Вимоги до системи управління послугами

ДСТУ ISO/IEC 27005:2015 Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2011, IDT)

ДСТУ ISO/IEC 27001-2015 Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT)

ДСТУ ISO/IEC 27031:2015 Інформаційні технології. Методи захисту. Настанови щодо готовності інформаційно-комунікаційних технологій для неперервності роботи бізнесу (ISO/IEC 27031:2011, IDT)

ДСТУ ISO/IEC 27002:2015 (ISO/IEC 27002:2013; Cor 1:2014, IDT) Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки

ДСТУ ISO/IEC 16085:2015 Розробка систем і програмного забезпечення. Процеси життєвого циклу. Управління ризиками (ISO/IEC 16085:2006, IDT)

ДСТУ ISO/IEC 18045:2015 (ISO/IEC 18045:2008, IDT) Інформаційні технології. Методи захисту. Методологія оцінювання безпеки IT

ДСТУ ISO/IEC TR 19791:2015 (ISO/IEC TR 19791:2010, IDT) Інформаційні технології. Методи захисту. Оцінювання безпеки операційних систем

ДСТУ ISO/IEC 12207:2014 Інженерія систем і програмного забезпечення. Процеси життєвого циклу програмного забезпечення (ISO/IEC 12207:2008, IDT)

ДСТУ ISO/IEC 14764:2014 Інженерія програмного забезпечення. Процеси життєвого циклу програмного забезпечення. Технічне обслуговування (ISO/IEC 14764:2006, IDT)

ДСТУ ISO/IEC 15288:2014 Інженерія систем і програмного забезпечення. Процеси життєвого циклу систем (ISO/IEC 15288:2008, IDT)

ДСТУ ISO/IEC/IEEE 23026:2015 Розробка програмного забезпечення. Рекомендована практика для Інтернету. Розробка веб-сайтів, адміністрування веб-сайтів і життєвий цикл веб-сайтів (ISO/IEC/IEEE 23026:2015, IDT)

ДСТУ ISO/IEC TR 14516:2008 Інформаційні технології. Методи захисту. Настанова для керування послугами третьої довіреної сторони та користування ними (ISO/IEC TR 14516:2002, IDT)

ДСТУ ISO/IEC 15945:2012 Інформаційні технології. Методи захисту. Специфікація послуг TTP для підтримки застосування цифрових підписів (ISO/IEC 15945:2002, IDT)

ДСТУ ISO/IEC 24760:2015 Інформаційні технології. Методи захисту (ISO/IEC 24760).

Код УКНД 35.040

Ключові слова: кібербезпека, кіберпростір, кіберзагрози, ризики безпеки, зацікавлені сторони, методи захисту, політики безпеки, інформаційна безпека.

Редактор **М. Клименко**

Верстальник **М. Кравченко**

Підписано до друку 13.04.2018. Формат 60 × 84 1/8.
Ум. друк. арк. 5,58. Зам. 554. Ціна договірна.

Виконавець
Державне підприємство «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» (ДП «УкрНДНЦ»)
вул. Святошинська, 2, м. Київ, 03115

Свідоцтво про внесення видавця видавничої продукції до Державного реєстру видавців, виготівників і розповсюджувачів видавничої продукції від 14.01.2006 серія ДК № 1647