НАЦІОНАЛЬНИЙ СТАНДАРТ УКРАЇНИ

ДСТУ EN ISO 19650-5:20___

(EN ISO 19650-5:2020, IDT; ISO 19650-5:2020, IDT)

ОРГАНІЗАЦІЯ ТА ОЦИФРУВАННЯ ІНФОРМАЦІЇ ЩОДО БУДІВЕЛЬ ТА СПОРУД ВКЛЮЧНО З БУДІВЕЛЬНИМ ІНФОРМАЦІЙНИМ МОДЕЛЮВАННЯМ (BIM). УПРАВЛІННЯ ІНФОРМАЦІЄЮ З ВИКОРИСТАННЯМ БУДІВЕЛЬНОГО ІНФОРМАЦІЙНОГО МОДЕЛЮВАННЯ

Частина 5. Застосування методів захисту до управління інформацією

(Проект, перша редакція)

Київ
ДП «УкрНДНЦ»
20__

ПЕРЕДМОВА

1. РОЗРОБЛЕНО: Технічний комітет стандартизації «Металобудівництво» (ТК 301), Товариство з обмеженою відповідальністю «Український інститут сталевих конструкцій імені В. М. Шимановського», за сприяння компанії Corporate Solutions Consulting Limited (Великобританія)

2. ПРИЙНЯТО ТА НАДАНО ЧИННОСТІ: наказ Державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від ___._____. 20__ р. № _____ з 20___–___–___

3. Національний стандарт відповідає EN ISO 19650-5:2020 Organization and digitization of information about buildings and civil engineering works, including building information modelling (BIM) — Information management using building information modelling — Part 5: Security-minded approach to information management (ISO 19650-5:2020) (Організація та оцифрування інформації щодо будівель та споруд включно з будівельним інформаційним моделюванням (BIM). Управління інформацією з використанням будівельного інформаційного моделювання. Частина 5. Застосування методів захисту до управління інформацією) і внесений з дозволу CEN-CENELEC, Rue de la Science 23, B-1040 Brussels, Belgium. Усі права щодо використання європейських стандартів у будь-якій формі й будь-яким способом залишаються за CEN

   Ступінь відповідності – ідентичний (IDT)
   Переклад з англійської (en)

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

5. УВЕДЕНО ВПЕРШЕ

ЗМІСТ

НАЦІОНАЛЬНИЙ ВСТУП

Цей національний стандарт ДСТУ EN ISO 19650-5:20XX (EN ISO 19650-5:2020, IDT; ISO 19650-5:2020, IDT) «Організація та оцифрування інформації щодо будівель та споруд включно з будівельним інформаційним моделюванням (BIM). Управління інформацією з використанням будівельного інформаційного моделювання. Частина 5. Застосування методів захисту до управління інформацією», прийнятий методом перекладу, – ідентичний щодо EN ISO 19650-5:2020 (версія en) «Organization and digitization of information about buildings and civil engineering works, including building information modelling (BIM) – Information management using building information modelling – Part 5: Security-minded approach to information management».

Технічний комітет стандартизації, відповідальний за цей стандарт в Україні, – ТК 301 «Металобудівництво».

У цьому національному стандарті зазначено вимоги, які відповідають законодавству України.

До стандарту внесено такі редакційні зміни:

– слова «цей міжнародний стандарт», «ця частина стандарту» і «цей документ» замінено на «цей стандарт»;

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

– у розділі «Нормативні посилання» та «Бібліографії» наведено «Національне пояснення», виділене рамкою;

– зі «Вступу» до EN ISO 19650-5:2020 у цей «Національний вступ» внесено все, що безпосередньо стосується цього стандарту;

– рисунки наведено одразу після тексту, де вперше виконано посилання на них, або на черговій сторінці;

– вилучено виноску 1 у розділі 2 як таку, що втратила актуальність на дату видання цього стандарту;

– долучено довідковий додаток НА (Перелік національних стандартів України, ідентичних міжнародним нормативним документам, посилання на які є в цьому стандарті).

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

ПЕРЕДМОВА ДО ISO 19650-5:2020

ISO (Міжнародна організація зі стандартизації) є всесвітнім об’єднанням національних органів стандартизації (органів – членів ISO). Роботу з підготування міжнародних стандартів зазвичай виконують, залучаючи технічні комітети ISO. Кожен орган – член ISO, зацікавлений у темі, за якою створено технічний комітет, має право бути представленим у цьому комітеті. У роботі беруть участь також урядові та неурядові міжнародні організації, які взаємодіють з ISO. ISO тісно співпрацює з Міжнародною електротехнічною комісією (IEC) з усіх питань електротехнічної стандартизації.

Процедури, використовувані для розроблення цього стандарту та призначені для його подальшого підтримання в актуальному стані, викладені в директивах ISO/IEC, частина 1. Зокрема, треба зазначити різні критерії схвалення, застосовні до різних типів документів ISO. Цей стандарт було розроблено відповідно до редакційних правил, викладених у директивах ISO/IEC, частина 2 (див. www.iso.org/directives).

Потрібно звернути увагу на те, що деякі елементи цього стандарту можуть бути предметом патентних прав. ISO не несе відповідальності за виявлення будь-якого чи всіх таких патентних прав. Подробиці щодо будь-яких патентних прав, виявлених під час розроблення стандарту, наведено у вступі та/або в списку отриманих патентних декларацій ISO (див. www.iso.org/patents).

Будь-яка торговельна назва, використана в цьому стандарті, є інформацією, наданою користувачам для зручності, і не означає схвалення.

Роз’яснення щодо добровільного застосування стандартів, значень специфічних термінів та формулювань ISO, пов'язаних з

оцінюванням відповідності, а також інформація про приєднання ISO до принципів Світової організації торгівлі (СОТ) щодо технічних бар'єрів у торгівлі (ТБТ) доступні на сайті www.iso.org/iso/foreword.html.

Цей стандарт було підготовлено Технічним комітетом ISO/TC 59 «Будівлі та інженерні споруди», ПК 13 «Організація та оцифрування інформації щодо будівель та споруд включно з будівельним інформаційним моделюванням (BIM)» у співпраці з Технічним комітетом Європейського комітету зі стандартизації (CEN) CEN/TC 442 «Будівельне інформаційне моделювання (BIM)», відповідно до Угоди про технічне співробітництво між ISO та CEN (Віденська угода).

Перелік усіх частин стандарту ISO 19650 доступний для перегляду на веб-сайті ISO.

Будь-які зауваження або запитання щодо цього стандарту мають бути направлені до національного органу стандартизації в країні користувача. Повний перелік цих органів наведено за адресою: www.iso.org/members.html.

ВСТУП

Антропогенне середовище переживає період бурхливої еволюції. Очікується, що впровадження будівельного інформаційного моделювання (BIM) та щодалі ширше використання цифрових технологій у проектуванні, будівництві, виробництві, експлуатації та управлінні активами чи продукцією, а також під час надання послуг у межах середовища забудови, матимуть трансформаційний вплив на сторін-учасників. Імовірно, що започаткування та реалізація проектів із розроблення нових активів чи будівельних рішень, змінення чи управління наявними об’єктами нерухомості, задля підвищення ефективності та результативності процесів ставатимуть більш колективними за своєю суттю. Така співпраця потребує більшої прозорості та відкритості у взаємодії та, за можливості, відповідного обміну й використання цифрової інформації.

Поєднання фізичного та цифрового середовища забудови потребуватиме у майбутньому досягнення цілей, пов’язаних із отриманням прибутків, фінансових та функціональних переваг, сталості та економічного зростання. Це позначиться й на процесах закупівель, постачання та виконання робіт, зокрема, як розширення співпраці між представниками різних сфер діяльності та галузей господарства. Це також призведе до поширеного використання цифрових технологій та доступності інформації. Застосування комп’ютерних технологій вже сприяє упровадженню нових методів роботи, наприклад, віддалених, а також розвитку заводського автоматизованого виробництва. Складні кіберфізичні системи, в яких використовують датчики (елементи електронних комунікаційних чи комп’ютерних мереж) для керування фізичними частинами системи, можуть працювати в реальному часі, щоб здійснювати вплив на результати діяльності в реальному світі. Очікується, що такі системи

може бути застосовано для досягнення певних переваг, як, наприклад, енергоефективності, вдосконалення управління життєвим циклом активів за допомогою збору інформації про використання та стан активів в реальному часі. Їх упровадження вже розпочато в сферах транспорту, комунальних послуг, інфраструктури, будівництва, виробництва, охорони здоров'я та оборони, і якщо вони зможуть взаємодіяти як інтегровані кіберфізичні середовища, їх може бути використано задля розвитку високорозвинених спільнот.

Внаслідок такого щодалі ширшого використання інформаційних та комунікаційних технологій та залежності від них виникає потреба у вирішенні проблем невід'ємної від цього процесу вразливості, а отже, пов'язаних з інформаційною безпекою наслідків, які виникають у середовищі забудови, управлінні активами, сфері виробництва, послуг, соціальних відносин між окремими особами чи громадами, а також у зв’язку з будь-якою супровідною інформацією.

У цьому стандарті викладено основні принципи, усвідомлення яких сприятиме кращому розумінню організаціями ключових проблем уразливості та властивостей засобів контролю, щоб управляти ризиками інформаційної безпеки, які виникають, досягаючи рівня, прийнятного для відповідних сторін. Мета стандарту – жодним чином не принизити значення співпраці чи вигоди, які можна отримати впровадженням BIM, інших методів колективної роботи та цифрових технологій.

Термін «організація» охоплює не тільки поняття «сторона призначення» і «призначена сторона», визначені в ISO 19650-1, але означає також організації користувачів, які не беруть безпосередньої участі в укладанні умов співпраці сторін.

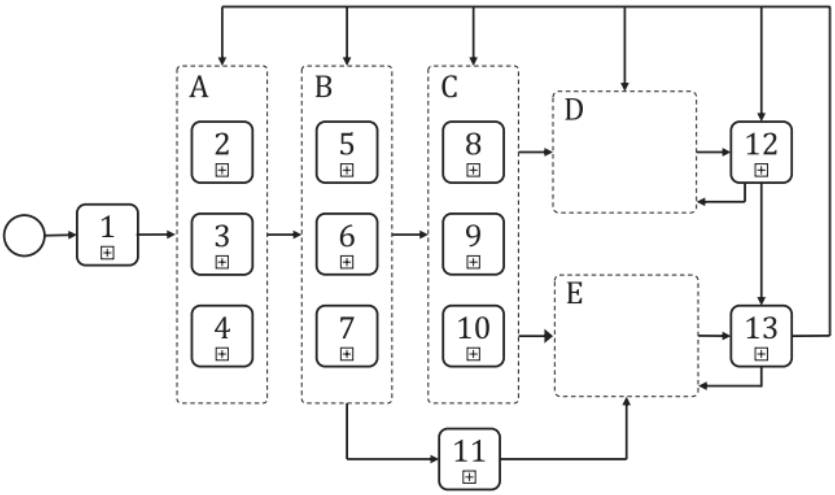
Вимоги щодо інформаційної безпеки викладено в ISO/IEC 27001 для окремої організації, організаційного підрозділу або системи, але їх

не можна застосовувати до декількох організацій. BIM і подібні методи та цифрові технології колективної роботи, зазвичай, передбачають обмін інформацією для спільного використання у широкому колі незалежних організацій певного напрямку діяльності у середовищі забудови.

Відтак, у цьому стандарті створено підстави для прийняття заснованих на оцінюванні ризиків методів захисту інформації, які може бути застосовано як в окремих організаціях, так і у відносинах між ними. Принцип відповідності та пропорційності цього підходу має також ту перевагу, що заходи безпеки не перешкоджатимуть залученню малих та середніх підприємств до складу виконавчої групи.

Методи захисту інформації може бути застосовано впродовж усього життєвого циклу ініціювання розробки, проекту, активу, виробу чи послуги, незалежно від того, чи запроектовано їх, чи вже фізично втілено, у будь-яких ситуаціях, де передбачено отримання, створення, оброблення та/або зберігання конфіденційної інформації.

На рисунку 1 показано інтегрування методів захисту з іншими організаційними стратегіями, політикою, планами та вимогами щодо інформації, пов’язаними з реалізацією проектів за допомогою цифрових технологій та обслуговуванням і експлуатацією активів за використання BIM.



Умовні познаки:

A – узгоджені та відповідні стратегії і політики;

B – узгоджені та відповідні плани;

C – узгоджені та відповідні вимоги до інформації;

D – діяльність, здійснювана на етапі експлуатації активів;

E – діяльність, здійснювана на етапі будівництва (див. також ISO 19650-2);

1 – плани та цілі організації;

2 – стратегічні плани/політика в сфері управління активами (див. ISO 55000);

3 – стратегія безпеки;

4 – інші стратегії та політика організації;

5 – план управління активом (див. ISO 55000);

6 – план управління інформаційною безпекою;

7 – інші організаційні плани;

8 – вимоги щодо інформації про актив (AIR);

9 – вимоги щодо убезпеченості інформації (у складі плану управління безпекою);

10 – вимоги щодо організаційної інформації (OIR);

11 – стратегічне економічне обґрунтування і стратегічне резюме;

12 – експлуатаційне використання активу;

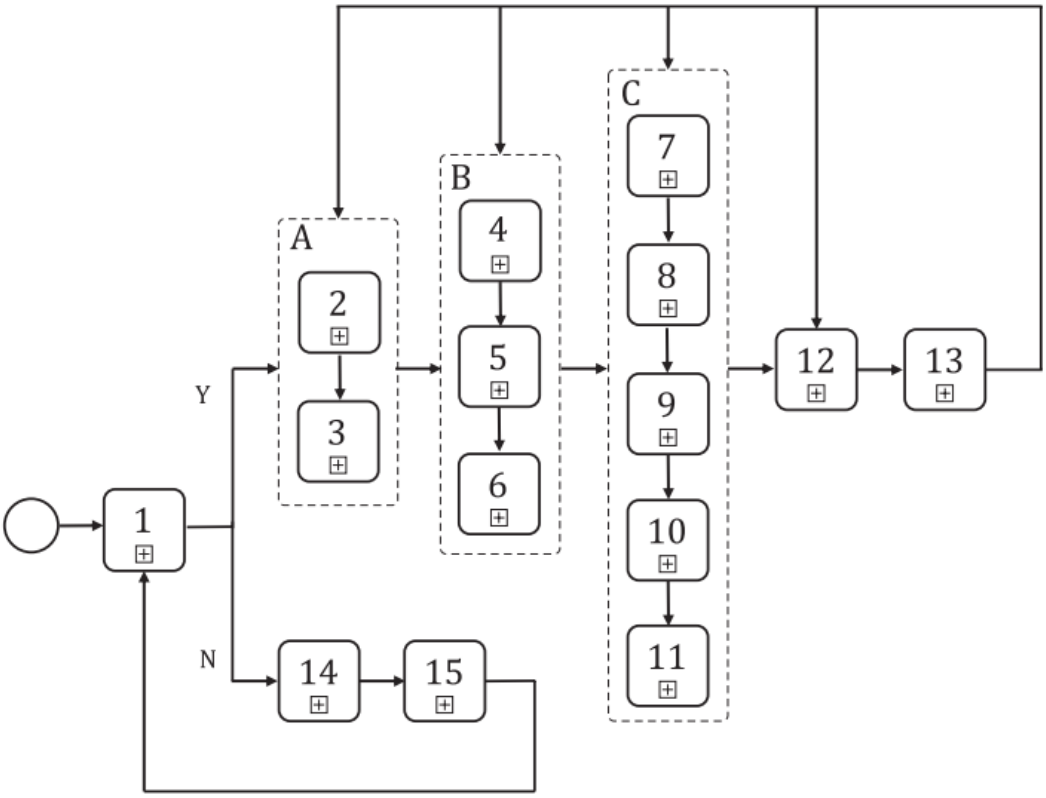
13 – вимірювання результативності та дії щодо поліпшення

Примітка. Зазначені в A, B та C номери не означають ніякої послідовності.

Рисунок 1 – Методи убезпечення інформації, інтегровані у розширений процес BIM

Примітка. Викладені в ISO 19650-1 концепції та принципи, а також пояснення стосовно OIR та AIR сприятимуть кращому усвідомленню міркувань щодо інформаційної безпеки в контексті всіх частин ISO 19650.

Процес прийняття рішення у зв’язку з потребою застосування методів захисту до управління інформацією (якщо передбачено) в узагальненому вигляді зображено на рисунку 2.



Умовні позначки:

A – ініціювання впровадження методів захисту інформації;

B – розроблення стратегії безпеки;

C – розроблення плану управління безпекою;

Y – так;

N – ні;

Рисунок 2 – Процес упровадження методів захисту інформації відповідно до цього стандарту

1 – визначення потреби в застосуванні методів захисту за допомогою процесу встановлення пріоритетів безпеки;

2 – установлення вимог щодо керування, підзвітності та відповідальності, пов’язаних із застосуванням методів захисту;

3 – розпочинання розроблення методів захисту;

4 – оцінювання ризиків безпеки;

5 – розроблення заходів з упровадження методів захисту;

6 – документування допустимих ризиків безпеки;

7 – розроблення політики і процесів для упровадження заходів безпеки;

8 – розроблення вимог щодо убезпечення інформації;

9 – розроблення вимог щодо надання інформації третім особам;

10 – розроблення вимог щодо логістичної безпеки;

11 – розроблення плану протидії порушенням безпеки/управління інцидентами;

12 – співпраця з призначеними сторонами відповідно до документованих умов призначення та без офіційного призначення, спрямована на упровадження методів захисту, зокрема, розроблення угод про спільне використання інформації, за потреби;

13 – моніторинг, аудит та аналізування;

14 – захист будь-якої конфіденційної комерційної інформації та персональних даних (за відсутності потреби впровадження інших методів захисту);

15 – перевіряння наявних змін в ініціюванні розробки, проекті, активі, виробі чи послузі, які можуть вплинути на їх вразливість

Рисунок 2 – Аркуш 2

Упровадження викладених у цьому стандарті заходів сприятиме зменшенню ризиків втрати, несанкціонованого використання або змінення конфіденційної інформації, які можуть вплинути на інформаційну безпеку, захищеність та стабільність використання активів, виробів чи послуг, надаваних у середовищі забудови за зазначених умов чи у зв’язку з ними. Це також уможливить захист від втрати, заволодіння чи розголошення комерційної інформації, особистих даних та інтелектуальної власності. Будь-які подібні інциденти можуть заподіяти суттєвої шкоди для репутації, внаслідок

впливу якої буде утрачено можливості та спрямовано ресурси для проведення розслідування, вирішення проблем та залучення засобів масової інформації, не кажучи вже про зриви та затримки у повсякденній оперативній діяльності. Крім того, якщо трапляються такі інциденти й інформація стає загальнодоступною, то стає практично неможливо відновити всю цю інформацію чи запобігти її подальшому розповсюдженню.

НАЦІОНАЛЬНИЙ СТАНДАРТ УКРАЇНИ

ОРГАНІЗАЦІЯ ТА ОЦИФРУВАННЯ ІНФОРМАЦІЇ ЩОДО БУДІВЕЛЬ ТА СПОРУД ВКЛЮЧНО З БУДІВЕЛЬНИМ ІНФОРМАЦІЙНИМ МОДЕЛЮВАННЯМ (BIM). УПРАВЛІННЯ ІНФОРМАЦІЄЮ З ВИКОРИСТАННЯМ БУДІВЕЛЬНОГО ІНФОРМАЦІЙНОГО МОДЕЛЮВАННЯ.

ЧАСТИНА 5. ЗАСТОСУВАННЯ МЕТОДІВ ЗАХИСТУ ДО УПРАВЛІННЯ ІНФОРМАЦІЄЮ

ORGANIZATION AND DIGITIZATION OF INFORMATION ABOUT BUILDINGS AND CIVIL ENGINEERING WORKS, INCLUDING BUILDING INFORMATION MODELLING (BIM) – INFORMATION MANAGEMENT USING BUILDING INFORMATION MODELLING –

PART 5: SECURITY-MINDED APPROACH TO INFORMATION MANAGEMENT

Чинний від 20XX-XX-XX

1 СФЕРА ЗАСТОСУВАННЯ

У цьому стандарті визначено вимоги та принципи застосування методів захисту до управління інформацією на етапі технологічної зрілості, який можна характеризувати як «будівельне інформаційне моделювання (BIM) відповідно до ISO 19650», згідно з ISO 19650-1, а також вимоги та принципи застосування методів захисту до управління конфіденційною інформацією, яку отримують, створюють, обробляють та зберігають як невід'ємну чи пов'язану частину будь-якого ініціювання розробки, проекту, активу, виробу чи послуги.

У стандарті розглянуто послідовність дій, спрямованих на формування та розвинення відповідного мислення та культури праці за умов інформаційної безпеки в організаціях, в яких надають доступ до конфіденційної інформації, зокрема, у разі потреби проведення моніторингу та аудиту відповідності.

Викладені принципи може бути застосовано протягом усього життєвого циклу ініціювання розробки, проекту, активу, виробу або

послуги, незалежно від того, чи їх запроектовано, чи фізично втілено, щодо яких отримують, створюють, обробляють та/або зберігають конфіденційну інформацію.

Цей стандарт призначений для використання будь-якою організацією, яку залучено до процесу управління інформацією та застосування інформаційних технологій для створення, проектування, будівництва, виробництва, експлуатації, управління, модернізації, переоснащення, знесення та/або вторинного перероблення активів/об’єктів нерухомості чи виробів, а також для надання послуг у середовищі забудови. У впровадженні цього стандарту також можуть бути зацікавлені організації, які мають намір забезпечити захист своєї комерційної інформації, персональних даних та інтелектуальної власності.

2 НОРМАТИВНІ ПОСИЛАННЯ

У наведених нижче нормативних документах зазначено положення, які через посилання в цьому тексті становлять положення цього стандарту. У разі датованих посилань застосовують тільки наведені видання. У разі недатованих посилань потрібно користуватись останнім виданням наведених нормативних документів (разом зі змінами).

ISO 19650-2 Organization and digitization of information about buildings and civil engineering works, including building information modelling (BIM) — Information management using building information modelling — Part 2: Delivery phase of the assets

ISO 19650-3, Organization and digitization of information about buildings and civil engineering works, including building information modelling (BIM) — Information management using building information modelling — Part 3: Operational phase of assets

НАЦІОНАЛЬНЕ ПОЯСНЕННЯ

ISO 19650-2 Організація та оцифрування інформації щодо будівель та споруд включно з будівельним інформаційним моделюванням (BIM). Управління інформацією з використанням будівельного інформаційного моделювання. Частина 2. Етап будівництва

ISO 19650-3 Організація та оцифрування інформації щодо будівель та споруд включно з будівельним інформаційним моделюванням (BIM). Управління інформацією з використанням будівельного інформаційного моделювання. Частина 3 Етап експлуатації

3 ТЕРМІНИ ТА ВИЗНАЧЕННЯ ПОНЯТЬ

У цьому стандарті вжито терміни та визначення понять із зазначених джерел та наведені нижче.

Термінологічні бази даних ISO та IEC, призначені для використання в стандартизації, доступні за такими адресами:

– платформа ISO для онлайн-перегляду: https://www.iso.org/obp

– IEC Electropedia: http://www.electropedia.org/

3.1 актив (*asset*)

Предмет, річ або фізичний об’єкт, який має для організації потенційну чи фактична цінність.

Примітка 1. Активом може бути основний капітал, рухомі матеріальні цінності чи майно. Активом може бути окремий об'єкт заводу, транспортний засіб, система підключеного устаткування, простір у споруді, ділянка землі, вся інфраструктура в цілому, будівля в цілому або портфоліо активів, включно з пов'язаними земельними чи водними ресурсами. Він також може бути сукупністю інформації в цифровому або друкованому вигляді.

Примітка 2. Вартість активу може змінюватися протягом його терміну служби, і наприкінці свого життєвого циклу актив може мати цінність. Цінність може бути матеріальною, нематеріальної, фінансовою чи нефінансовою.

(Джерело: ISO 55000:2014, 3.2.1, зі змінами: із тексту джерела вилучено примітки 1, 2 та 3; долучено нові примітки 1 та 2).

3.2 місце масового перебування людей (*crowded place*)

Місце чи середовище, доступне для громадян, яке у разі терористичного акту можна вважати підданим більшому ризику внаслідок щільності скупчення людей або властивостей місцевості.

Примітка 1. Місцями масового перебування людей можуть бути спортивні стадіони, арени, місця проведення музичних фестивалів; готелі та ресторани; паби, клуби, бари і казино; центральні вулиці, торгові центри та ринки; визначні пам'ятки для відвідувачів; кінотеатри та театри; школи та університети; лікарні та культові споруди; торгові центри; транспортні вузли. Ними також можуть бути місця подій та громадські місця, наприклад, парки та площі.

Примітка 2. Місце масового перебування людей не обов'язково завжди буває велелюдним: щільність натовпу може бути різною чи тимчасовою, як у разі проведення спортивних заходів або фестивалів під відкритим небом.

3.3 метадані (*metadata*)

Інформація, яка дозволяє ідентифікувати інформаційні ресурси.

3.4 потреба поінформованості (*need-to-know*)

Законна вимога потенційного одержувача інформації знати, мати доступ чи володіти конфіденційною інформацією (3.11).

3.5 схильність до ризику (*risk appetite*)

Кількість і типи ризиків, які організація має намір відстежувати або утримувати під контролем.

(Джерело: ISO 22300:2018, 3.202)

3.6 безпека (*safety*)

Стан відносної свободи від загрози (3.13) або шкоди, заподіяної внаслідок випадкових, ненавмисних дій або подій.

3.7 убезпеченість (методами захисту) (*security*)

Стан відносної свободи від загрози (3.13) або шкоди, заподіяної навмисними, небажаними, ворожими чи зловмисними діями.

3.8 порушення безпеки (*security breach*)

Порушення правил безпеки чи злом системи захисту (3.7).

(Джерело: ISO 14298:2013, 3.30)

3.9 інцидент інформаційної безпеки (*security incident*)

Підозрілий вчинок чи обставина, що загрожує убезпеченості (3.7).

3.10 убезпечений (застосуванням методів захисту) (*security-minded*)

Свідомий необхідності регулярного застосування у будь-якій діловій ситуації відповідних та пропорційних методів захисту (3.7), спрямованих на запобігання та/або припинення ворожої, зловмисної, шахрайської та злочинної поведінки чи діяльності.

3.11 конфіденційна інформація (*sensitive information*)

Інформація, втрата, неправильне використання чи змінення якої, або несанкціонований доступ до якої може:

– негативно вплинути на конфіденційність, убезпеченість (3.7) або стан безпеки (3.6) окремої особи чи осіб;

– завдати шкоди інтелектуальній власності чи комерційній таємниці організації;

– заподіяти комерційних чи економічних збитків організації чи країні; та/або

– поставити під загрозу безпеку, внутрішні та зовнішні умови існування нації.

3.12 залишковий ризик (*residual risk*)

Ризик, що залишається після впровадження заходів контролю.

(Джерело: ISO 16530‑1:2017, 3,52)

3.13 загроза (*threat*)

Потенційна причина інциденту, внаслідок якого може бути завдано шкоди.

3.14 найвище керівництво (*top management*)

Особа чи група осіб, яка спрямовує та контролює діяльність організації на найвищому рівні.

Примітка 1. Вище керівництво має право передавати повноваження та забезпечувати ресурси в межах організації.

Примітка 2. У контексті цього стандарту управління треба розглядати як функцію (керівництва), а не діяльність.

(Джерело: ISO 9000:2015, 3.1.1, зі змінами: із тексту джерела вилучено примітки 2 та 3; долучено нову примітку 2).

3.15 уразливість (*vulnerability*)

Слабкість (слабке місце), що можна використати для заподіяння шкоди.

4 УСТАНОВЛЕННЯ ПОТРЕБИ ЗАСТОСУВАННЯ МЕТОДІВ ЗАХИСТУ ЗА ПРОЦЕДУРОЮ ОЦІНЮВАННЯ ЧУТЛИВОСТІ ДО РИЗИКУ

4.1 Застосування процедури оцінювання чутливості до ризику

Процедуру оцінювання чутливості до ризику викладено в 4.2–4.4.

4.2 Визначення сфери дії ризиків безпеки

4.2.1 Найвище керівництво організації, яке бере участь у:

a) ініціюванні розробки, проектуванні нового (-их) або зміненні/ вдосконаленні наявного (-их) активу (-ів), виробу (-ів) чи послуги (послуг);

b) управлінні, експлуатації, зміненні призначеності або відчуженні активу (-ів); та/або

c) наданні послуг, заснованому на використанні активу (-ів),

має визначити сферу дії ризиків безпеки, що виникають внаслідок збільшення доступності інформації, інтегрування послуг в інформаційні системи та посилення залежності від систем, заснованих на інформаційних технологіях.

4.2.2 Інформацію про види ризиків безпеки, які потрібно враховувати, викладено у додатку А.

4.2.3 У разі залучення до співпраці двох або більше організацій між керівництвом цих організацій має бути узгоджено дотримання положень 4.2.1.

Примітка. Такі домовленості між декількома організаціями можуть бути під час співпраці в умовах міста/громади, великого багатоцільового комплексу або використання транспортної системи.

4.3 Визначення чутливості до ризику організації

4.3.1 Враховуючи сферу дії ризиків, що існують, зазначена (-і) у 4.2.1 та 4.2.3 організація (-ії) має (-ють) визначити, чи вважає (-ють) вона (-и) чутливими до ризику ініціювання розробки, проект, актив, виріб чи послугу, загалом або частково, незалежно від того, чи вони запроектовані, чи фізично втілені, а будь-яку пов'язану з ними інформацію – конфіденційною.

Примітка. У контексті цього стандарту термін «організація (-ії)» стосується організації (-ій), зазначеної (-их) у 4.2.1 та 4.2.3.

4.3.2 Побудований актив/об’єкт нерухомості вважають чутливим до ризику як повністю, так і частково, якщо він:

a) містить критично важливу для національної економіки інфраструктуру, визначену місцевими органами влади або національним урядом;

b) забезпечує виконання функцій у сфері оборони, правоохоронної системи, національної безпеки або дипломатичного представництва;

c) є місцем здійснення комерційної діяльності, пов’язаної зі створенням, переробленням, продажем або зберіганням матеріальних цінностей, валюти, фармацевтичних препаратів, хімічних речовин, нафтохімічних речовин чи газів, або із наданням чи виготовленням засобів для виробництва цих матеріалів;

d) являє собою визначну пам’ятку, об’єкт національного значення або місце масового перебування людей;

e) використовуваний або його планують використовувати для проведення заходів, пов’язаних із безпекою.

Примітка. Той факт, що побудований актив/об’єкт нерухомості не відповідає зазначеним вище критеріям, не перешкоджає застосуванню вищого рівня безпеки на розсуд організації (-ій).

4.3.3 Актив, виріб чи послугу вважають чутливими до ризику, якщо існує достатній ризик для того, що їх буде використано чи може бути використано для завдання значної втрати цілісності, порушення інформаційної безпеки, убезпеченості та/або відновлюваності активу, виробу чи послуги або їх функційної придатності.

4.3.4 Актив, виріб чи послугу також потрібно вважати чутливими до ризику, якщо ризик інформаційної безпеки, захисту та/або конфіденційності окремих осіб чи громади, або їхніх персональних даних перевищує схильність до ризику організації (організацій).

4.3.5 У разі будь-якої невизначеності стосовно того, чи є ініціювання розробки, проект, актив, виріб чи послуга чутливими до ризику, організація (-ії) має звернутися за консультацією до відповідних експертів із безпеки, які можуть продемонструвати свою компетентність у відповідній сфері діяльності.

Примітка. Роз’яснення стосовно отримання відповідних консультацій з питань безпеки наведено у додатку А.

4.4 Установлення чутливості до ризику третьої особи

4.4.1 Оцінюючи ініціювання розробки, проект, актив, виріб чи послугу, треба також враховувати, чи буде отримано або вже отримано доступ до інформації про інші організації, їх активи, вироби чи послуги, яка не є загальнодоступною.

Примітка. Прикладом інформації, яка не є загальнодоступною і може виявитися конфіденційною, може бути інформація, отримана за результатами обстеження технічного стану підземних споруд, мереж та систем інфраструктури на приватній території.

4.4.2 Організація (-ії) має (-ють), якщо це не заборонено з причин комерційної таємниці чи за місцевими умовами, проконсультуватися з організацією (-ями), убезпеченості якої (-их) це стосується, щоб установити, чи є яка-небудь інформація конфіденційною, і якщо так, то яких заходів потрібно вживати під час її отримання, оброблення, зберігання, спільного використання, вилучення та знищення.

4.5 Реєстрування результатів оцінювання чутливості до ризику

Організація (-ії) має (-ють) реєструвати та зберігати результати кожного оцінювання чутливості до ризику, включно з отриманими за умов, коли чутливості до ризику не виявлено, а також враховувати, що й сам результат оцінювання може бути конфіденційним.

4.6 Аналізування результатів оцінювання чутливості до ризику

4.6.1 Організація (-ії) має (-ють) забезпечити відповідні умови та засоби для проведення періодичного та заснованого на подіях аналізування чутливості до ризику ініціювання розробки, проекту, активу, виробу чи послуги на наявність будь-яких змін, що відбулися внаслідок впливу політичних, економічних, технологічних, правових чи екологічних чинників.

4.6.2 Аналізування також потрібно проводити в разі суттєвого змінення ініціювання розробки, проекту, активу, виробу чи послуги, що стосується, зокрема:

a) права власності, використання чи тимчасового розпоряджання побудованим активом/об’єктом нерухомості;

b) процесів або систем, які використовують для управління побудованим активом/об’єктом нерухомості або для створення активу чи виготовлення виробу;

c) інформації, яку збирають, обробляють та/або зберігають;

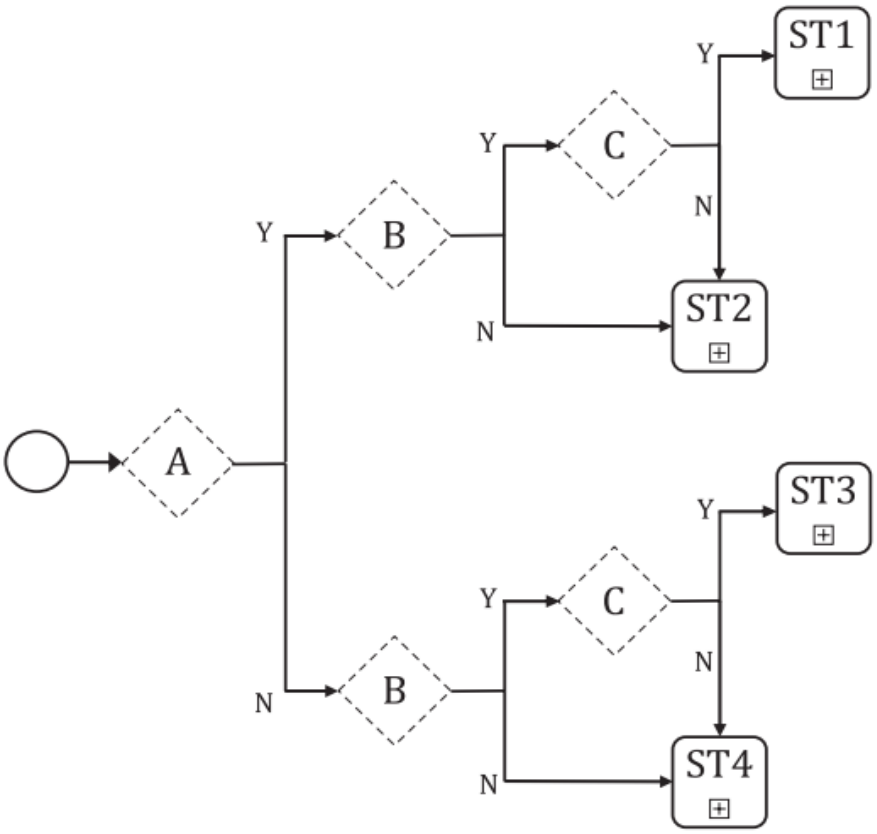
d) послуги, яку надають; або

e) контексту безпеки.

4.6.3 Додаткове засноване на подіях аналізування потрібно проводити, якщо відбулися події, за яких виявлено раніше не очікувану вразливість.

4.7 Визначення потреби застосування методів захисту

Організація (-ії) має (-ють) використовувати процес установлення пріоритетів безпеки (рисунок 3), щоб визначити потребу застосування методів захисту до ініціювання розробки, проекту, активу, виробу чи послуги.



Умовні позначки:

A – Чи вважають ініціювання розробки, проект, актив, виріб або послугу, незалежно від того, чи їх запроектовано, чи вже втілено, чутливими до ризику, а будь-яку пов'язану з ними інформацію, загалом або частково – конфіденційною? (див. 4.3)

B – Чи буде отримано або вже отримано доступ до інформації про іншу організацію, її активи, вироби або послуги, яка не є загальнодоступною? (див. 4.4.1)

C – Чи вважають конфіденційною інформація про іншу організацію, її активи, вироби або послуги? (див. 4.4.2)

Y – Так.

N – Ні.

Рисунок 3 – Процес установлення пріоритетів безпеки

ST1 – Потрібно захищати конфіденційну інформацію, пов’язану з ініціюванням розробки, проектом, активом, виробом чи послугою, а також конфіденційну інформацію третіх осіб, застосовуючи вимоги розділів від 5 до 9.

ST2 – Потрібно захищати конфіденційну інформацію, пов’язану з ініціюванням розробки, проектом, активом, виробом чи послугою, застосовуючи вимоги розділів від 5 до 9.

ST3 – Потрібно захищати конфіденційну інформацію третьої особи, застосовуючи вимоги розділів від 5 до 9. Потрібно захищати будь-яку конфіденційну комерційну інформацію та особисті дані.

ST4 – Потрібно захищати будь-яку конфіденційну комерційну інформацію та особисті дані

Примітка. Скорочений термін ST (*security triage*) означає «пріоритет безпеки».

Рисунок 3 – Аркуш 2

4.8 Реєстрування вихідних даних процесу встановлення пріоритетів безпеки

Організація (-ії) має (ть) зареєструвати вихідні дані (ST1, ST2, ST3 або ST4) процесу встановлення пріоритетів безпеки щодо кожного ініціювання розробки, проекту, активу, виробу або послуги, яких вони стосуються, включно з тими ситуаціями, коли, крім захисту конфіденційної комерційної інформації та особистих даних, потреби застосування методів захисту інформації не визначено.

4.9 Прийняття методів захисту інформації

Якщо ініціювання розробки, проект, актив, виріб або послуга:

a) визнані чутливими до ризику, загалом або частково, та/або

b) будуть містити визнану конфіденційною інформацію третьої особи,

найвище керівництво організації (-їй) має розробити та впровадити відповідні до вимог цього стандарту та пропорційні до наслідків впливу методи захисту інформації.

4.10 Відмова від методів захисту інформації

Якщо ініціювання розробки, проект, актив, виріб або послугу не вважають чутливими до ризику та пов’язаними з доступом до конфіденційної інформації третьої особи, організація (-ії) має (-ють) розглянути можливість отримання комерційної вигоди від застосування методів захисту.

Примітка 1. З боку організацій доцільно вживати відповідних заходів для мінімізації загроз, що виникають внаслідок шахрайських та інших злочинних дій, а також інцидентів кібербезпеки.

Примітка 2. Цілком імовірно, що відповідно до умов співпраці або вимог законодавства буде потрібно застосування базових методів захисту персональних даних і комерційної інформації.

Примітка 3. Якщо організація (-ії) не вбачає (-ють) потреби приймати вищий рівень убезпеченості, то застосовувати вимоги розділів від 5 до 9 щодо ініціювання розробки, проекту, активу, виробу або послуги, на момент розгляду не потрібно.

5 ІНІЦІЮВАННЯ ВПРОВАДЖЕННЯ МЕТОДІВ ЗАХИСТУ

5.1 Установлення вимог щодо управління, підзвітності та відповідальності, пов’язаних із застосуванням методів захисту

5.1.1 У разі розроблення методів захисту в організації найвище керівництво має призначити посадову особу, яка відповідатиме перед найвищим керівництвом за застосування методів захисту.

5.1.2 Якщо дві або більше організацій спільно розробляють методи захисту, найвище керівництво кожної організації має офіційно установити умови та засоби для:

a) створення потрібної структури управління, забезпечення її юридичного оформлення та документування, а також узгодження відносин цієї структури з відповідними організаціями;

b) досягнення домовленості про те, щоб одна із сторін або кілька сторін керували розробленням методів захисту, і в разі розподілу цієї функції керування між різними організаціями – забезпечення чіткого розуміння вимог щодо підзвітності та відповідальності;

c) призначення посадових осіб, які нестимуть відповідальність за застосування методів захисту;

Примітка 1. Посадових осіб призначають для реалізації законних прав та виконання зобов'язань відповідної організації.

d) перегляд та оновлення структури управління та функційних призначень, якщо застосовне;

Примітка 2. Застосування узгоджених методів захисту за умов взаємодії організацій забезпечує більшу надійність, ніж підхід, за якого ці організації працюють ізольовано.

5.1.3 Організація (-ії), яка (-і) впроваджує (-ють) методи захисту, має (-ють) призначити особу (осіб), відповідальну (-их) за:

a) забезпечення цілісного уявлення про загрози безпеки та вразливість, що виникають внаслідок використання та покладання в основу своєї діяльності інформаційних ресурсів та комунікаційних технологій, застосовних до ініціювання розробки, проекту, активу, виробу чи послуги;

b) надання рекомендацій та вказівок щодо врегулювання наслідків дії ризиків безпеки;

c) керування розробленням стратегії безпеки або, якщо організація вже має стратегію безпеки, – долучення до неї положення про додаткові ризики інформаційної безпеки та застосовні заходи щодо врегулювання їх наслідків, а також використання інформаційних

та комунікаційних технологій, застосовних до ініціювання розробки, проекту, активу, виробу чи послуги (див. розділ 6);

d) управління розробкою та технічне супроводження під час виконання плану управління інформаційною безпекою, або, якщо організація вже має план управління безпекою, – керування упровадженням відповідних додаткових положень політики і процесів (див. розділ 7);

e) сприяння внесенню відповідних вимог інформаційної безпеки до будь-яких документованих умов закупівель та призначення;

f) сприяння розвитку культури праці з урахуванням вимог інформаційної безпеки, усвідомленню персоналом своїх обов'язків щодо інформаційної безпеки та убезпеченого способу дії;

g) інформування відповідних третіх осіб щодо застосовних аспектів політики та процесів інформаційної безпеки;

h) консультування щодо потреби упровадження, а також аналізування та аудиту дотримання відповідних положень політики та процесів інформаційної безпеки;

i) консультування щодо потреби упровадження та, якщо застосовне, проведення випробувань або введення в експлуатацію відповідних засобів захисту чи заходів інформаційної безпеки;

j) за потреби і якщо доцільно, звернення до відповідних експертів з питань безпеки, які можуть продемонструвати свою компетентність у відповідних сферах діяльності, для надання додаткових рекомендацій.

5.1.4 Потрібно, щоб підзвітність особи (осіб), що виконує (-ють) зазначені в 5.1.3 дії, було чітко підпорядковано до посадової особи, яка відповідає за інформаційну безпеку в межах організації.

Примітка. Ці функції може виконувати кваліфікована і досвідчена посадова особа, яка може взяти на себе чи вже нести відповідальність за безпеку та виконує

інші обов'язки в організації, або може бути експертом у відповідній сфері діяльності, найнятим організацією.

5.1.5 Допустимо делегування конкретних щоденних завдань чи обов'язків із питань інформаційної безпеки іншим посадовим особам (наприклад, убезпеченість персоналу – фахівцю з управління кадрами, вирішення питань із кібербезпеки – IT-менеджеру, питань фізичної убезпеченості активу – менеджеру з управління активами або управителю об'єктів нерухомості). Однак посадова (-і) особа (-и), призначена (-і) відповідати за виконання зазначених у 5.1.3 дій, продовжує (-ють) нести відповідальність за ефективність роботи за кожним із установлених аспектів безпеки.

5.2 Розпочинання розроблення методів захисту інформації

5.2.1 У разі планування ініціювання розробки, проекту, активу, виробу чи послуги, методи захисту інформації має бути розроблено на етапах планування якомога раніше.

Примітка. Інформація, яка стосується розробки, що є надбанням держави, може становити інтерес для ворожої розвідки з перших етапів процесу проектування.

5.2.2 Якщо чутливі до ризику ініціювання розробки, проект, актив, виріб або послуга вже існують, методи захисту інформації потрібно розробити в найкоротші практично здійсненні терміни, враховуючи наявні обсяги інформації, що вже є у відкритому доступі.

5.2.3 Для реалізації проекту за використання BIM на етапі будівництва, додатково до виконання вимог ISO 19650-2, потрібно розробити методи захисту інформації.

5.2.4 Для виконання діяльності на етапі експлуатації активу/об’єкта нерухомості за використання BIM, додатково до виконання вимог ISO 19650-3, потрібно розробити методи захисту інформації.

6 РОЗРОБЛЕННЯ СТРАТЕГІЇ БЕЗПЕКИ

6.1 Загальні положення

6.1.1 Організація (-ії) має (-ють) розробити та забезпечувати упровадження стратегії безпеки, що охоплює:

a) записи результатів застосування процесу встановлення пріоритетів безпеки;

b) установлення засобів управління, підзвітності та відповідальності щодо застосування методів захисту інформації;

c) оцінювання конкретних ризиків безпеки, що виникають для організації (-ій) внаслідок більшої доступності інформації, інтегрування послуг в інформаційні системи та зростання залежності від систем, заснованих на інформаційних технологіях (див. 6.2);

d) визначення заходів зі зниження потенційних ризиків безпеки, їх уникнення та зменшення їх вірогідності (див. 6.3);

e) зведений реєстр допустимих ризиків безпеки та залишкових допустимих ризиків безпеки (див. 6.4);

f) установлення засобів для перегляду та оновлення стратегії безпеки (див. 6.5).

Примітка. Принципи, структуру та загальний процес управління ризиками установлено в ISO 31000.

6.1.2 У стратегії безпеки має бути враховано вимоги законодавчих та нормативних документів, які було визначено застосовними до ініціювання розробки, проекту, активу, виробу чи послуги.

6.1.3 Стратегію безпеки має бути затверджено найвищим керівництвом організації (-ій).

6.1.4 Доступ до будь-якої частини стратегії безпеки, в якій визначено чутливі до ризику аспекти ініціювання розробки, проекту, активу, виробу чи послуги або докладно описано виявлені ризики інформаційної безпеки, має бути установлено виключно для службового користування за потреби поінформованості, і в цьому разі всю таку інформацію потрібно убезпечити застосуванням методів захисту, відповідних до рівня ризику, пов’язаного з її створенням, обробленням і зберіганням.

6.2 Оцінювання ризиків безпеки

6.2.1 Організація (-ії) має (-ють) оцінювати конкретні ризики інформаційної безпеки, що виникають внаслідок більшої доступності інформації, інтегрування послуг в інформаційні систем та зростання залежності від систем, заснованих на інформаційних технологіях, враховуючи:

a) потенційні загрози;

b) потенційні вразливі місця;

c) характер шкоди, якої може бути заподіяно ініціюванню розробці, проекту, активу, виробу чи послузі, а також персоналу і громадянам та довкіллю;

d) ймовірність використання вразливості та спричинення зазначеного вище впливу.

Примітка. Для оцінювання ризиків інформаційної безпеки буває доцільно використовувати той самий метод оцінювання ризиків, який застосовують щодо інших видів діяльності організації.

6.2.2 Якщо інформацію вже опубліковано, під час оцінювання ризику інформаційної безпеки треба враховувати, що після публікування інформації в Інтернеті або надання відкритого доступу до

неї іншим способом видалити, знищити, вилучити або захистити всі її копії практично неможливо.

6.2.3 Оцінювання ризику безпеки, за можливості, потрібно виконувати з урахуванням ризиків, пов’язаних із доступом до інформації, яку надають інші організації та яка не є загальнодоступною.

6.3 Розроблення заходів зі зниження ризиків безпеки

6.3.1 Організація (-ії) має (-ють) визначити та зареєструвати можливі заходи, спрямовані на зниження кожного виявленого ризику безпеки або поєднання таких ризиків.

6.3.2 Виявляючи та реєструючи можливі заходи, спрямовані на зниження ризиків, організація (-ії) має (-ють) враховувати кадрові, фізичні та технічні засоби управління інформаційною безпекою та вимоги щодо управління інформацією.

Примітка 1. Взаємодію персоналу, фізичних та технічних засобів контролю може бути використано суб’єктами загрози, якщо зв’язки в цих сферах взаємодії не було вивчено.

Примітка 2. Розроблені заходи зі зниження ризиків може бути також спрямовано на збереження або захист комерційних, економічних та соціальних цінностей.

Примітка 3. Довідкову інформацію про типи засобів контролю та аспекти управління інформацією викладено у додатку В.

6.3.3 Для визначення доцільності кожного заходу зі зниження потенційних ризиків організації (-ям) потрібно враховувати:

a) витрати на підготування та здійснення заходу зі зниження ризику;

b) рівень зниження ризику, якого можна досягти, та рівень залишкового ризику;

c) прогнозовані наслідки витрат на упровадження заходів зі зниження ризику;

d) інші впливи, які захід зі зниження ризику може мати на актив (наприклад, на зручність його використання, ефективність та зовнішній вигляд);

e) можливість виникнення інших вразливих місць унаслідок виконання заходу зі зниження ризику;

f) чи забезпечує цей захід будь-які інші вигоди для бізнесу.

Примітка. Вигодами для бізнесу можуть бути зменшення загального ризику бізнес-діяльності та сприяння усвідомленню вартості активів, зокрема, інформації.

6.3.4 Організація (-ії) має (-ють) використовувати результати оцінювання для визначення застосовних заходів зі зниження ризику, якщо це передбачено.

Примітка. Пропорційним вважають такий захід зі зниження ризику, який є практичним, доцільним та економічно вигідним.

6.4 Документування залишкових та допустимих ризиків безпеки

6.4.1 Після розроблення заходів зі зниження ризиків безпеки організація (-ії) має (-ють) виявити та записати будь-які залишкові ризики безпеки.

6.4.2 Організація (-ії) має (-ють) продовжувати оцінювання ризиків безпеки та розробляти заходи зі зниження цих ризиків, поки не буде досягнуто рівня, який не перевищує схильності до ризику окремої організації або сукупності організацій.

6.4.3 Організація (-ії) має (-ють) задокументувати допустимі ризики безпеки.

6.5 Перегляд стратегії безпеки

6.5.1 Організація (-ії) має (-ють) установити відповідні умови і засоби для проведення періодичних та заснованих на подіях переглядів стратегії безпеки, включно з оцінюванням ефективності заходів зі зниження ризиків, щоб перевірити доцільність її положень.

6.5.2 Перегляд, заснований на подіях, проводять у разі змінення політичних, економічних, соціальних, організаційних, технологічних, правових або екологічних умов, які можуть мати суттєвий вплив на ініціювання розробки, проект, актив, товар чи послугу та пов'язану з ними інформацію, а також у разі настання подій, за яких виявлено не передбачену раніше уразливість.

6.5.3 Під час виконання перегляду потрібно враховувати потенційний вплив на чинні умови співпраці наслідків суттєвого змінення заходів зі зниження ризику, особливо якщо змінено сферу їх застосування.

6.5.4 Стратегію безпеки після перегляду має бути оновлено за урахування будь-яких змін, виявлених із боку загроз, вразливості, наслідків дії ризиків інформаційної безпеки та/або заходів зі зниження ризиків інформаційної безпеки.

6.5.5 Положення стратегії, сформульовані після перегляду в новій редакції, має бути задокументовано та збережено у складі стратегії безпеки.

6.5.6 Доступ до будь-якої частини переглянутої стратегії безпеки, в якій визначено чутливі до ризику аспекти ініціювання розробки, проекту, активу, виробу чи послуги або докладно описано виявлені ризики безпеки, має бути надано виключно для службового користування, заснованого на потребі поінформованості з усією подібною інформацією за урахування заходів безпеки, які відповідають

рівню ризику, пов’язаного зі створенням, розповсюдженням, використанням, зберіганням, вилученням та знищенням інформації.

7 РОЗРОБЛЕННЯ ПЛАНУ УПРАВЛІННЯ БЕЗПЕКОЮ

7.1 Загальні положення

7.1.1 Організація (-ії) має (-ють) розробити, підтримувати в актуальному стані та впроваджувати план управління безпекою, який забезпечує послідовне та комплексне виконання узгоджених заходів зі зниження ризиків, визначених у стратегії безпеки.

7.1.2 Потрібно, щоб план управління безпекою, якщо це доцільно, був взаємно пов’язаний з іншими положеннями політики та процесами управління безпекою та відповідними методами захисту інформації, застосовуваними в організації (-ях).

7.1.3 План управління безпекою, призначений для застосування в організації (-ях) та її (-їх) виконавчій групі, має охоплювати:

a) положення політики, в яких визначено пов'язані з безпекою правила ведення бізнесу, засновані на узгоджених заходах зменшення ризиків;

b) процеси, засновані на положеннях політики у сфері безпеки та настановах щодо їх послідовного впровадження;

c) вимоги щодо убезпеченості інформації за докладного зазначення інформації, яку вважають конфіденційною, а також положень політики та процесів, пов’язаних з її створенням, розповсюдженням, використанням, зберіганням, вилученням та знищенням;

d) вимоги щодо надання інформації третім особам (див. 7.2);

e) вимоги щодо матеріально-технічного забезпечення, якщо це можливо (див. 7.3);

f) план протидії порушенням безпеки та управління інцидентами (див. розділ 8);

g) дані щодо підзвітності та відповідальності за виконання плану за різними аспектами управління інформаційною безпекою (див. 7.4);

h) вимоги щодо проведення моніторингу та аудиту, включно з перевірянням заходів інформаційної безпеки (див. 7.5);

i) умови та засоби для перегляду та оновлення плану управління безпекою (див. 7.6).

Примітка. Будь-які прогалини або недоліки в плані управління безпекою зменшать ефективність стратегії безпеки та збільшать ризик порушення безпеки або виникнення інциденту

7.1.4 План управління безпекою призначений для інформування про вимоги безпеки, які зазначають у будь-яких документах, пов’язаних із закупівлями та умовами призначення (розділ 9).

7.2 Надання інформації третім особам

7.2.1 У плані управління безпекою має бути установлено вимоги організації щодо оцінювання чутливості до ризику нової, зміненої чи наявної інформації або інформаційної моделі перед публікацією та/або наданням її повністю або частково у спільне використання.

7.2.2 Зазначене вище оцінювання має бути засновано на принципах дотримання:

a) вимог нормативних і законодавчих документів, установлених для процесу;

b) умов надання інформації, на яку поширюються вимоги законодавства щодо забезпечення відкритого доступу до інформації чи прозорості діяльності;

с) умов надання інформаційних матеріалів, призначених для використання під час громадських і професійних заходів, для маркетингових оглядів, у технічних, наукових або інших публікаціях та на веб-сайтах.

7.2.3 Під час оцінювання потрібно враховувати, якщо це практично можливо, наявність ознак, за якими інформація чи інформаційна модель, загалом або частково:

а) містить або уможливлює отримання конфіденційної інформації, зокрема такої, що пов’язана з уразливістю ініціювання розробки, проекту, активу, виробу, послуги, особи чи групи осіб/громади;

б) уможливлює отримання конфіденційної інформації у поєднанні з наявними загальнодоступними чи опублікованими матеріалами;

в) якщо застосовне, сприяє визначенню способу використання активу(ів) та/або способу життя окремих осіб чи групи осіб/громади, стосовно яких отримати інформацію іншим способом неможливо.

Примітка. Рекомендації щодо аспектів цього виду оцінювання викладено в додатку С.

7.2.4 Якщо під час оцінювання інформації виявлено будь-яку з зазначених вище ознак конфіденційності, організація (-ії) має (-ють) застосувати відповідні та пропорційні методи захисту інформації під час її спільного використання та/або публікування.

Примітка. Рекомендації щодо впровадження заходів, які може бути застосовано для зменшення ризиків безпеки, наведено у додатку С.

7.2.5 Доступ до будь-якої частини оцінювання, в якій докладно описано конфіденційну інформацію, має бути надано виключно для службового користування, заснованого на потребі поінформованості, а до створення, розповсюдження, використання, зберігання, вилучення

та знищення наведеної в ній інформації має бути застосовано відповідні заходи захисту інформації.

7.3 Логістична безпека

7.3.1 У плані управління безпекою, якщо це можливо, має бути передбачено відповідні та пропорційні заходи захисту інформації, застосовні до специфікацій, закупівель, проектування, виготовлення, транспортування, монтажу та введення в експлуатацію будь-яких чутливих до ризику активів.

Примітка. Щодо розроблення зазначених вище заходів можна отримати консультацію у фахівців.

7.3.2 Організації (-ям) потрібно враховувати:

a) терміни монтажу будь-яких чутливих до ризику активів або їх систем, з якими пов'язано заходи інформаційної безпеки, щоб, за можливості, доступ до цих активів або територій було надано виключно тим особам, які мають для цього законні підстави;

b) упровадження відповідних та пропорційних заходів безпеки, пов’язаних із будь-якими чутливими до ризику активами та їх системами, які з логістичних міркувань має бути встановлено раніше, ніж це було очікувано;

c) упровадження відповідних та пропорційних заходів, спрямованих на запобігання чи перешкоджання фізичного доступу ворожої розвідки.

7.4 Підзвітність та відповідальність у сфері управління безпекою

Положення політики в сфері управління безпекою мають містити визначення посадової (-их) особи (осіб), яка (-і) виконує (-ють) функції управління безпекою, звітує (-ють) та відповідає (-ють) за її упровадження, управління, моніторинг та аналізування.

7.5 Моніторинг та аудит

7.5.1 У плані управління безпекою має бути установлено відповідні й пропорційні заходи з моніторингу, аудиту та контролювання, які потрібно виконувати упродовж усього життєвого циклу ініціювання розробки, проекту, активу, виробу чи послуги, які мають охоплювати оцінювання результатів застосування методів захисту інформації, засноване, щонайменше, на оцінюванні ризиків безпеки стосовно:

a) реалізації всіх аспектів плану управління безпекою;

b) дотримання плану будь-якою виконавчою групою за всіма застосовними аспектам управління безпекою.

Примітка 1. Потрібно досягти збалансованості між формальною перевіркою, що передбачає аудити призначених сторін, і системою перевіряння, заснованого на принципі довіри та добропорядності.

Примітка 2. Відповідність виконавчої групи всім застосовним аспектам плану управління безпекою, якщо доцільно, може бути виконано під час аналізування компетентності і спроможності, визначеного в ISO 19650-1.

Примітка 3. Моніторинг і аудит плану управління інформаційною безпекою можуть бути засновані на вимогах стандартів, наприклад, ISO 19011.

7.5.2 У плані управління інформаційною безпекою має бути зазначено вимогу щодо виконання зазначених вище моніторингу та аудиту лише тими посадовими особами, які мають відповідну кваліфікацію та досвід.

7.5.3 Відповідальність за перевіряння на відповідність виконавчої групи організація (-ії) може (-уть) частково делегувати керівній призначеній стороні, залишаючи за собою відповідальність за загальну ефективність контролю заходів безпеки.

7.6 Перегляд плану управління безпекою

7.6.1 Організація (-ії) маю (-ють) установити відповідні умови та засоби для проведення періодичного та заснованого на подіях перегляду плану управління безпекою, а також вимог щодо убезпеченості інформації і плану протидії порушенням безпеки/ управління інцидентами, для перевіряння їх придатності та доцільності для застосування.

7.6.2 Перегляд, заснований на подіях, виконують після перегляду стратегії безпеки у разі виявлення порушень безпеки чи інцидентів або змінення політичних, економічних, соціальних, організаційних, технологічних, правових або екологічних умов, які можуть суттєво вплинути на:

a) типи імовірних порушень інформаційної безпеки/інцидентів;

b) процес, якого потрібно дотримуватися, зокрема, необхідність збору доказів розслідування;

c) заходи із забезпечення безперервності бізнесу та відновлення функцій.

7.6.3 Під час перегляду потрібно враховувати потенційний вплив, який можуть мати будь-які зміни у політиці та процесах, на наявні умови призначення, особливо у разі змінення сфери його застосування внаслідок такого впливу.

7.6.4 Після перегляду план управління безпекою має бути оновлено за урахування будь-яких змін, а також за усунення будь-яких виявлених прогалин та недоліків, що знижують придатність плану забезпечити потрібне зниження рівня ризиків безпеки.

7.6.5 Зміни до плану управління безпекою має бути доведено до відома організації (-ій) та призначених сторін.

7.6.6 Результати кожного нового перегляду мають бути зареєстровані та збережені у складі плану управління безпекою.

8 РОЗРОБЛЕННЯ ПЛАНУ ПРОТИДІЇ ПОРУШЕННЯМ БЕЗПЕКИ ТА УПРАВЛІННЯ ІНЦИДЕНТАМИ

8.1 Загальні положення

8.1.1 Організація (-ії) має (-ють) скласти і підтримувати в актуальному стані план протидії порушенням безпеки та управління інцидентами як частину плану управління безпекою, що має охоплювати:

a) оцінювання типів імовірних порушень безпеки/інцидентів та потенційних ризиків з огляду на вплив, який вони можуть мати на організацію (-ії), її (їх) функції, активи, репутацію, персонал та третіх осіб;

b) процес, вимог якого потрібно дотримуватися у разі виявленого порушення безпеки/інцидента, в тому числі, того, що імовірно станеться (див. 8.2);

c) заходи із забезпечення безперервності бізнесу та відновлення функцій, що сприяють досягненню такого самого рівня убезпеченості, що й системи, призначені для постійного використання, включно зі збиранням доказів для розслідування, якщо застосовне (див. 8.3);

d) процес перегляду, який має бути проведено після порушення безпеки або інциденту (див. 8.4);

e) умови та засоби перегляду й оновлення плану протидії порушенням безпеки та управління інцидентами (див. 8.5).

8.1.2 Частини плану протидії порушенням безпеки та управління інцидентами може бути уведено до складу інших наявних планів організації (-ій) або прийнятих у державі правил реагування, і в цьому

разі зазначені плани або правила реагування мають бути пов’язані між собою перехресними посиланнями.

8.1.3 Частини плану протидії порушенням безпеки та управління інцидентами, в яких описано ризики для організації (-їй), мають бути доступні виключно для службового користування, заснованого на потребі поінформованості, а до створення, поширення, використання, зберігання, вилучення і знищення інформації, якої стосуються ці частини, мають бути застосовані відповідні заходи інформаційної безпеки.

8.2 Виявлення порушення безпеки або інциденту

Організація (-ії) має (-ють) визначити послідовність дій, які потрібно виконати у разі виявленого порушення безпеки або інциденту, установивши:

a) посадових осіб або ролі та контактні дані для термінового зв'язку;

b) процеси, застосовні для визначення зацікавлених сторін;

c) умови та засоби для поінформування зацікавлених сторін та інформацію, яку потрібно надати;

d) правила поводження з будь-якою третьою особою, регуляторним органом, засобами масової інформації чи інтересами громади у разі порушення безпеки або інциденту.

8.3 Стримування та відновлювання

Організація (-ії) має (-ють) установити заходи, яких потрібно вжити в разі порушення безпеки/інциденту, щоб локалізувати подію і забезпечити відновлення функцій, зокрема:

a) заходи, спрямовані на припинення подальшого пошкодження чи збитків;

b) заходи з оцінювання обсягів інформації, яку було втрачено, скомпрометовано, сфальсифіковано чи пошкоджено;

c) обставини, за яких потрібно надати докази для правоохоронних органів, і методи їх збирання;

d) заходи кримінального розслідування, спрямовані на отримання криміналістичної інформації про інцидент для використання, за потреби, правоохоронними органами та/або детального аналізу першопричин інцидентів.

Якщо потрібно зібрати докази для правоохоронних органів, всі докази (як фізичні об’єкти, так і цифрові дані), які можуть допомогти розслідуванню встановити причину події та винних осіб, має бути зібрано та збережено до того, як буде розпочато будь-які дії з відновлення функцій, крім випадків негайної потреби в таких діях, коли вони є критично важливими для життя.

Примітка. Важливо, щоб речові докази було зібрано до виконання дій з відновлення функцій, оскільки ці дії можуть призвести до знищення або псування цифрових даних, що є доказами судової справи.

8.4 Перевіряння після порушення безпеки або інциденту

8.4.1 Після впровадження первинних заходів стримування та відновлення функцій організація (-ії) має (-ють) провести оцінювання поточного ризику. Під час оцінювання має бути досліджено причини події, виявлено потенційні заходи протидії та визначено залишковий ризик, а також будь-який потенційний новий або надзвичайний ризик, що виникає внаслідок події.

8.4.2 Для зменшення або запобігання повторному виникненню ризику має бути оновлено відповідні положення політики та процеси за урахування результатів оцінювання.

8.4.3 Організація (-ії) має (-ють) установити вимоги для відповідних членів своєї виконавчої групи, якщо це доцільно, співпрацювати задля відповідного та пропорційного оцінювання події та наслідків інциденту.

9 СПІВПРАЦЯ З ПРИЗНАЧЕНИМИ СТОРОНАМИ

9.1 Робота без офіційного призначення

9.1.1 У разі виконання роботи без офіційного призначення (наприклад, за участі в торгах), якщо передбачено надання доступу до конфіденційної інформації, організація (-ії) має (-ють) укласти угоду про спільне використання інформації або еквівалентну угоду.

Примітка. Додаткові рекомендації стосовно угод про спільне використання інформації викладено в додатку D.

9.1.2 Угода про спільне використання інформації, або еквівалентний документ, має містити вимоги організації (-їй) щодо отримання, управління та знищення конфіденційної інформації.

9.1.3 Якщо виконання функційного призначення для участі в торгах потребує оприлюднення конфіденційної інформації, організація (-ії) має (-ють) упровадити відповідні та пропорційні заходи та/або окремі процеси інформаційного захисту, забезпечуючи за цих умов надання достатнього обсягу інформації.

9.1.4 У процесі обирання призначеної сторони організації (-ям) потрібно проаналізувати всю документацію, пов’язану з участю в торгах, щоб визначити способи, якими передбачено виконання вимог щодо убезпеченості інформації, викладених у плані управління безпекою.

9.1.5 Організація (-ії) має (-ють) оцінити ступінь усвідомлення вимог інформаційної безпеки, компетентність, спроможність і досвід організацій, обраних для функційного призначення, а також установити

будь-які вимоги щодо навчання, тренування та технічного супроводження з питань безпеки.

9.2 Заходи, зазначені в документованих умовах призначення

9.2.1 Організація (-ії) має (-ють) управляти ризиками інформаційної безпеки своєї виконавчої групи, долучивши до документованих умов призначення розділи, пов’язані з виконанням відповідних положень політики та процесів інформаційної безпеки, які установлено в плані управління безпекою, включно з вимогами для членів виконавчої групи, застосовних у разі завершення співпраці.

9.2.2 Організація (-ії) має (-ють) детально визначити розподіл функцій з убезпечення інформації у межах виконавчої групи, зокрема, установити вимогу щодо дотримання правил інформаційної безпеки на всіх рівнях підпорядкованості (підзвітності) у виконавчій групі, та відповідного делегування відповідальності, забезпечивши умови для результативного та ефективного управління.

9.2.3 Зазначені вище документовані умови призначення мають відповідати вимогам, що містять документовані умови співпраці з призначеними сторонами, яких було призначено безпосередньо організацією (-ями), а також документовані умови співпраці на підпорядкованих їм рівнях призначень, якщо застосовне.

9.2.4 За потреби відповідності певним стандартам безпеки (наприклад, забезпечення конкретних заходів фізичної або кібербезпеки відповідно до зазначеного стандарту), у документованих умовах призначення має бути чітко наведено посилання на ці стандарти, а також зазначено про будь-які пов’язані з цим інспектування чи перевірки з боку незалежної організації.

9.2.5 Для протидії порушенням безпеки та управління інцидентами, спричиненими професійним консультантом, підрядником або призначеною стороною, в документованих умовах призначення

має бути чітко сформульовано положення стосовно повідомлення організації (-ям) про порушення безпеки чи інцидент та надання допомоги в розслідуванні, а також про подальші дії.

9.2.6 У документованих умовах призначення мають бути положення, згідно з якими в організації (-ях) у відповідній виконавчій групі на будь-якому рівні дозволено аналізувати заходи убезпечення та дотримання відповідних положень політики і процесів.

9.2.7 Організація (-ії) має (-ють) долучити до документованих умов призначення окремий пункт, у який можна було б унести коригування у разі змінення політичних умов, законодавчих чи нормативних вимог.

9.2.8 Організація (-ії) має (-ють) установити вимогу, щоб після припинення співпраці всю відповідну інформацію, включно з тою, яку було надано призначеній стороні для спільного використання з іншими членами цієї виконавчої групи, було доставлено, надійно збережено, вилучено чи знищено відповідно до організаційних вимог та застосовних документованих умов призначення.

9.2.9 За потреби, організація (-ії) має (-ють) установити вимогу до призначеної сторони щодо перевіряння наявності визначених процедур із отримання, розпоряджання або знищення конфіденційної інформації, а також дотримання поточних заходів безпеки стосовно конфіденційної інформації, яку потрібно зберігати.

9.2.10 Організація (-ії) має (-ють) установити вимогу щодо впровадження достатньої кількості процесів, пов’язаних із виведенням з експлуатації та відокремленням ресурсів, щоб забезпечити захист інформації про активи.

9.3 Оцінювання результатів виконання умов призначення

9.3.1 Організація (її) має (-ють) контролювати та спонукати призначені сторони дотримуватися всіх пов'язаних із безпекою положень, зазначених у документованих умовах призначення, сприяючи застосуванню прийнятних методів захисту інформації під час виконання ними своїх обов'язків, пов'язаних із призначенням.

9.3.2 Організація (-ії) має (-ють) забезпечити умови для співпраці у своїй виконавчій групі, сприяючи усвідомленню вимог щодо убезпеченості та вирішенню будь-яких виявлених проблем захисту інформації.

9.4 Завершення функцій за призначенням

Організація (-ії) має (-ють) вжити відповідних та пропорційних заходів для перевіряння будь-якої виконавчої групи на дотримання вимог щодо отримання, безпечного зберігання, вилучення чи знищення конфіденційної інформації.

ДОДАТОК А

(довідковий)

ІНФОРМАЦІЯ У КОНТЕКСТІ БЕЗПЕКИ

А.1 Усвідомлення потенційних проблем безпеки

Використовуючи наявні рекомендації з інформаційної безпеки, організація (-ії) має (-ють) досягти розуміння відносно:

а) сфери дії загроз, які може бути реалізовано за використання уразливості, зокрема:

1) якщо під загрозою можуть опинитися цінність і довговічність ініціювань розробок і проектів;

2) якщо під загрозою можуть опинитися цінність, довговічність і стабільність використання активів, виробів та/або послуг організації;

3) якщо може бути заподіяно збитків, пошкоджень чи завдано страждань або поставлено під загрозу персонал організації чи інших користувачів активу або послуг;

4) якщо може бути порушено цілісність чи сфальсифіковано інформацію та/або дані інформаційних систем;

5) якщо може бути зашкоджено репутації;

6) якщо можливе заволодіння особистими даними, інтелектуальною власністю чи комерційною конфіденційною інформацією;

Примітка 1. До загроз відносять тероризм, ворожі дії країн, комерційне шпигунство, організовану злочинність, активістів-радикалів, неблагонадійних осіб, хакерів і зловмисників серед працівників організації.

b) традиційних та новітніх методів ворожої розвідки, до дії яких можуть виявитися уразливими ініціювання розробок, проекти, активи, вироби, послуги і особисті дані;

Примітка 2. Під час виконання розвідувальних дій противник шукає інформацію про:

1) застосовувані заходи захисту (наприклад, пов’язані з фізичною уразливістю чи конфігурацією системи);

2) установлені методи роботи;

3) стан системи безпеки (тобто, можливість бути виявленим/можливість досягти успіху);

4) спосіб життя окремої особи, групи осіб або спосіб використання активу.

Примітка 3. У разі планування нападу ворожої сторони досягнення успіху залежить від надійності зазначеної вище інформації та можливості її використання до того, як може бути застосовано запобіжні заходи.

c) можливості того, що компоненти чи окремі активи або вироби, які буде об’єднано у структурі більшого активу, виробу чи системи, можуть виявитися підробленими, зловмисно чи шахрайським способом, і не відповідатимуть вимогам стандартів чи будуть зіпсовані;

d) можливості настання та потенційного впливу зловмисних дій, викликаних зовнішніми та внутрішніми загрозами, зокрема, внаслідок дій зловмисного програмного забезпечення, хакерів чи невдоволеного персоналу, які можуть поставити під загрозу:

1) інтелектуальну власність та/або чутливу до ризику комерційну інформацію;

2) особисті дані;

3) цілісність метаданих;

4) цілісність основних довідкових даних.

Примітка 4. Зловмисні дії можуть призвести до втрати, розкриття або пошкодження, несанкціонованого доступу чи несанкціонованого змінення інформації.

e) можливості розкриття чи несанкціонованого доступу до конфіденційної інформації внаслідок неубезпеченості чи неналежного обслуговування інформаційних систем;

f) можливості використання інформації для аналізування способу життя, що уможливить зловмисне або злочинне використання звичок, розпорядку дня та вподобань;

g) можливість об’єднання частин інформації (агрегування), щоб:

1) установити окремих осіб або групу осіб;

2) розкрити конфіденційну інформацію, пов’язану з ініціюванням розробок, проектами, активами, виробами, послугами, окремими особами чи громадою;

3) розкрити інформацію стосовно конфігурації активів, виробів, компонентів та/або програмного забезпечення в системі.

Примітка 5. Ризики агрегування інформації можуть виникати за таких умов:

1) агрегування внаслідок накопичення, за якого через обсяги інформації, що зберігають разом, збільшується рівень імовірного впливу, якщо інформацію буде скомпрометовано;

2) агрегування за асоціацією, якщо асоціювання різних типів інформації, кожен з яких окремо у разі компрометації спричинятиме незначний вплив або взагалі не матиме ніякого впливу, але у разі їх асоціювання рівень впливу стає вищим;

3) поєднання накопичення та асоціювання.

h) репутаційні ризики, пов'язані з зазначеними вище проблемами.

A.2 Рекомендації щодо методів захисту інформації

A.2.1 Щоб забезпечити розроблення методів захисту інформації, організація (-ії) має (-ють) використовувати відповідну настанову з інформаційної безпеки для отримання рекомендацій стосовно ризиків безпеки, що виникають внаслідок збільшення доступності інформації, інтегрування послуг в інформаційні системи та підвищення залежності від систем, заснованих на інформаційних технологіях.

A.2.2 Якщо організація (-ії) вже застосовує (-ють) методи захисту, в ній (них) вже можуть бути посадові особи, які мають відповідну кваліфікацію та досвід, достатньо розуміються на управлінні системою фізичної, технологічної, особистої безпеки та безпеки персоналу, відносин і взаємозв’язків. Ці посадові особи можуть надати вичерпні роз’яснення та допомогти в досягненні розуміння контексту безпеки. В іншому разі потрібно звернутися за консультаціями до зовнішнього фахівця з питань безпеки.

ДОДАТОК В

(довідковий)

ДОВІДКОВА ІНФОРМАЦІЯ ЩОДО УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ЗА КАДРОВИМ, ФІЗИЧНИМ ТА ТЕХНОЛОГІЧНИМ АСПЕКТАМИ

В.1 Кадрові аспекти

Розробляючи положення політики та процеси, які стосуються убезпеченості персоналу, організації (-ям) потрібно враховувати:

a) функції, пов’язані з високим рівнем ризиків безпеки, в організації (-ях), а також у будь-яких інших організаціях, яких залучено для співпраці на умовах призначення або для надання послуг;

Примітка. Прикладами функцій, пов’язаних із високим рівнем ризику безпеки, можуть бути ті, для виконавців яких передбачено доступ до детального опису стратегії безпеки, інформації, що стосується чутливих до ризику активів, або функції, за яких виконують роль адміністрування ІТ-системи або ключову роль в управлінні інформацією.

b) загальні та спеціальні вимоги, пов’язані з убезпеченістю, щодо відбору та перевірки будь-якої (-их) посадової (-их) особи (осіб), що контактує (-ють) із чутливими до ризику активами, зокрема, інформацією;

c) вимоги щодо компетентності з питань управління безпекою стосовно посадових осіб – виконавців певних ролей;

d) увідний інструктаж усього нового персоналу та організацій, що надають послуги організації (-ям), для забезпечення їх належного інформування про обов'язки та прийняті норми поведінки з огляду на інформаційну безпеку, зокрема:

1) потребу забезпечення загальної обізнаності та реєстрування заходів із навчання з питань управління безпекою

в межах проекту чи поточних операцій, включно з навчанням з охорони праці, ознайомленням з вимогами проекту, умовами будівельного майданчика або іншим подібним навчанням;

2) теми навчальних лекцій, пов’язані з дотриманням обов'язкових норм і правил, і відповідні результати навчання за кожною з них;

e) загальну поінформованість із питань безпеки та вимоги щодо навчання із застосування методів захисту інформації та сприяння розвитку відповідної культури праці, включно з перепідготовкою з цих питань;

f) вимоги до навчання з питань управління безпекою виконавців ролей для сприяння впровадженню методів захисту інформації та підтриманню відповідної культури праці;

g) вимоги щодо безперервного навчання та підвищення рівня убезпеченості;

h) вимоги щодо доступу та дозволу використання інформації та інформаційних моделей;

i) розформування організацій (-ій) та скорочення чисельності персоналу.

B.2 Фізичні аспекти

Розробляючи положення політику та процеси, які стосуються фізичної безпеки, організація (-ії) має (-ють) враховувати:

a) відповідні заходи фізичної безпеки в місцях зберігання конфіденційної інформації або надання віддаленого доступу до систем у межах будь-якої частини чутливого до ризику активу;

b) відповідні заходи фізичної безпеки в місці розташування нового чи наявного побудованого активу/об’єкта нерухомості, якщо це можливо;

c) убезпеченість прилеглих побудованих об’єктів нерухомості, яких зазвичай не видно та/або вони недоступні, якщо застосовне;

Примітка. Прилеглими (суміжними) називають такі побудовані об’єкти нерухомості (так само, послуги, що їх надають), які мають спільну межу (так само, зверху чи знизу) із побудованим об'єктом нерухомості, який розглядають, або які розташовані по сусідству з цим побудованим об'єктом нерухомості, але фізично розділені з ним вулицею, незабудованим простором на громадській чи приватній території або аналогічним об'єктом.

d) відповідні заходи захисту обчислювальної техніки, електронних пристроїв та устаткування.

B.3 Технологічні аспекти

B.3.1 Розробляючи положення політику та процеси, які стосуються технологічної безпеки, організація (-ії) має (-ють) враховувати:

a) заходи, пов'язані з кібербезпекою систем, які отримують, обробляють та зберігають конфіденційну інформацію, включно з вимогою щодо регулярного оцінювання вразливості та випробовування на можливість проникнення;

b) убезпеченість взаємозв’язків та взаємодій між зазначеними вище системами;

c) убезпеченість систем, що контролюють фізичні активи;

d) допустиму сумісність систем та тривкість кожної системи щодо відмов;

e) процеси та процедури управління конфігурацією та управління змінами для систем оброблення та зберігання інформації про проект та актив, а також технічного середовища даних;

f) убезпечене вилучення та/або знищення інформації, яку зберігають в організаціях, що вже не беруть участі в співпраці,

пов’язаній з ініціюванням розробки, проектом, активом, виробом чи послугою, та/або позбавлення їх доступу до цієї інформації;

g) застосовні заходи з убезпечення інформації у разі її зберігання протягом періоду, встановленого законодавчими, нормативними або організаційним вимогам, залежно від того, який із періодів довший, а також заходи, застосовні після завершення цього періоду, спрямовані на убезпечене вилучення, знищення та/або позбавлення доступу.

B.3.2 Системи, використовувані для отримання, оброблення та/або зберігання конфіденційної інформації, має бути убезпечено за замовчуванням (тобто, у повному обсязі збережено функціональність без порушення правил безпеки, а налаштування заходів захисту за замовчуванням встановлено на найвищому рівні), або систему має бути налаштовано, якщо можливо, на максимальний захист цієї інформації.

B.3.3 Системи програмного забезпечення, використовувані для отримання, оброблення чи зберігання конфіденційної інформації, під час процесу обирання має бути оцінено на придатність функціонування за кожним із наведених нижче аспектів на рівні, відповідному та пропорційному чутливості до ризику цієї інформації:

a) конфіденційність – контролювання і запобігання несанкціонованому доступу до інформації, яка окремо чи в сукупності з іншою є конфіденційною чи такою, що призведе до компрометації;

b) доступність (з урахуванням надійності) – забезпечення того, щоб інформація, системи і пов'язані з ними процеси були постійно розпізнаваними, доступними й придатними для використання та вчасного виведення у належному вигляді, за потреби;

Примітка. Відповідно до умов співпраці доступність може бути визначено у відсотках (наприклад, 99 999 9% на рік) та зазначено максимальний період часу

для відновлення нормальної роботи сервісу (наприклад, 30 хвилин), за можливості варіювання залежно від виду активів, виробів чи послуг.

c) убезпеченість – розроблення, впровадження, експлуатування та технічне підтримання систем і пов'язаних із ними процесів так, щоб запобігти створенню їх небезпечних станів, які можуть призвести до травмування або загибелі людей, ненавмисної шкоди довкіллю чи пошкодження майна;

d) тривкість – придатність інформації, послуг та систем до своєчасного трансформування, оновлення та відновлення функцій у відповідь на несприятливі події;

e) недоступність для заволодіння – властивість систем та пов'язаних із ними процесів, заснована на способах їх проектування, упровадження, експлуатування і обслуговування, які унеможливлюють їх несанкціоноване контролювання, маніпулювання чи втручання в їх роботу, а також гарантують використання інформації виключно відповідно до встановлених вимог, прав і обов'язків, які зазначено в документованих умовах призначення;

f) достовірність – гарантування того, що вхідні та вихідні дані системи, а також стан системи та будь-які пов'язані з нею процеси є дійсними;

g) застосовність – забезпечення того, що інформація про активи та системи зберігатиме корисність протягом періоду, упродовж якого може бути потрібний доступ до цієї інформації;

h) цілісність – підтримання цілісності, точності, послідовності, узгодженості та конфігурації інформації та систем.

B.3.4 Перед впровадженням будь-якої заснованої на Інтернет-технологіях або інших технологіях системи спільного користування активами, організація (-ії) має (-ють):

a) досягти розуміння архітектури пропонованих Інтернет-технологій;

b) визначити ступінь відповідності цієї архітектури вимогам системи управління безпекою організації (-їй);

c) оцінити будь-які ризики безпеки, включно з потенційним впливом відмови технології, з огляду на схильність до ризиків організації (-їй) та очікуваної вигоди, які може бути отримано;

d) упровадити відповідні та пропорційні заходи зі зниження ризиків безпеки для управління будь-якими неприйнятними ризиками безпеки.

B.4 Методи захисту інформації

B.4.1 Під час розроблення положень політики та процесів, що стосуються інформаційної безпеки, організації (-ям) потрібно розглянути:

a) вимоги щодо проведення інспектування та оглядів (опитувань), що уможливить виявлення конфіденційної інформації, яка не є загальнодоступною;

b) управління і моніторинг убезпеченого зберігання, убезпеченого доступу та максимально убезпеченого вилучення і знищення інформації, включно з тою, яку зберігають протягом відповідного періоду, установленого законодавчими або нормативними вимогами та будь-якими спеціальними вимогами організації (-ій), залежно від того, який період є довшим;

Примітка 1. Важливо забезпечити доступ до конфіденційної інформації виключно для службового користування, заснованого на потребі поінформованості, причому персоналу та іншим організаціям має бути доступною лише актуальна конфіденційна інформація, якої вони потребують для виконання завдань.

c) максимальний обсяг інформації, пов’язаної з чутливими до ризику активами/виробами чи системами, що має бути уміщено в базах даних, доставлено під час обміну інформацією та, якщо застосовне, в інформаційних моделях;

d) упровадження будь-яких вимог, що стосуються спеціальних методів оброблення або захисту конфіденційної інформації, яку було надано організації (-ям) третьою стороною;

e) захист від втрати, розголошення, пошкодження або позбавлення доступу чи несанкціонованого змінення інформації, метаданих та основних довідкових даних;

Примітка 2. Основні довідкові дані містять набір допустимих значень, застосовних іншими полями даних у спільних інформаційних моделях.

f) моніторинг і запис змін у процесах та технологіях, використовуваних для збирання, оброблення та зберігання інформації, включно з інформаційним синтезом.

B.4.2 Політика та процеси інформаційної безпеки мають бути застосовними до усього життєвого циклу інформації, який охоплює:

a) здобування – діяльність, пов'язану зі створенням інформації та зберіганням початкових даних, включно з метаданими;

b) придбання – закупівлю чи отримання інформації від інших сторін;

c) технічне супроводження – діяльність із доставляння інформації, призначеної до синтезування чи використання у формі та способом, що забезпечують досягнення цілей і охоплюють перевіряння та затвердження, очищення, переформатування, удосконалення, переміщення, інтегрування з декількома системами та оновлення опублікованої інформації;

d) синтезування – створення похідної інформації;

e) використання – застосування інформації для виконання дій, функцій чи завдань;

f) архівування – виконання копій чи розміщення інформації в архіві, де її зберігають, але в якому не відбувається обслуговування, використання чи публікування інформації;

g) публікування – процес надання інформації в організації або за її межами;

h) видалення – вилучення всіх відомих копій конкретної частини інформації в організації.

ДОДАТОК С

(довідковий)

ЗАХОДИ З ОЦІНЮВАННЯ У ЗВ’ЯЗКУ З НАДАННЯМ ІНФОРМАЦІЇ ТРЕТІМ ОСОБАМ

С.1 Оцінювання інформації

С.1.1 Під час оцінювання має бути установлено:

a) хто матиме доступ до інформації, яку передають;

b) чи потрібні консультації з іншими сторонами та зацікавленими сторонами перед спільним використанням та/або публікуванням інформації;

c) обґрунтування спільного використання чи публікування інформації, зокрема:

1) ціль;

2) потенційні вигоди та спосіб їх отримання;

3) ризики у разі, якщо інформацію не буде надано чи опубліковано;

4) наведення свідчень того, що пропоноване спільне використання інформації є пропорційним (відповідним) щодо цілі та потенційної вигоди;

5) чи може бути досягнуто цілі чи отримано вигоди без поширення або публікування інформації;

d) право розповсюджувати чи публікувати інформацію, зокрема:

1) чи є організація, яка буде поширювати чи публікувати інформацію, контролером безпеки інформаційної мережі та/або чи має вона на це право, юридичні повноваження чи можливість;

2) чи існують які-небудь юридичні зобов'язання, пов’язані з розповсюдженням або публікуванням інформації (наприклад, закон чи постанова суду);

3) чи було надано її конфіденційно;

d) будь-які проблеми захисту інформації;

f) ризики безпеки, пов’язані із спільним використанням або публікацією інформації, і чи перевищують вони схильність до ризику організації (-їй);

g) відповідні та пропорційні заходи зі зниження ризиків безпеки для вирішення будь-яких проблем захисту інформації або запобігання неприйнятним ризикам безпеки;

h) готовність та спроможність сторони, яка отримує інформацію, управляти нею відповідним способом;

i) будь-які залишкові ризики безпеки та інші проблеми захисту інформації.

С.1.2 У разі виявлення потенційних порушень безпеки/ інцидентів, які стосуються персональних даних чи неприйнятних для організації (-ій) ризиків, спільне використання або публікування інформації має бути заборонено, доки не буде вжито відповідних та пропорційних заходів задля усунення чутливості до ризику чи зниження пов'язаних ризиків до рівня, що є прийнятним для організації (-ій).

С.2 Нормативно-законодавчі вимоги щодо процесів

С.2.1 У плані управління безпекою має бути детально зазначено методи доставляння інформації та обмінювання з третіми особами за дотримання установлених щодо процесів нормативно-законодавчих вимог.

С.2.2 План управління безпекою має містити вимоги щодо відокремлення та убезпечення відповідним способом конфіденційної інформації. Ці вимоги можуть охоплювати редагування або видалення конфіденційної інформації, пов’язаної з чутливими до ризику властивостями активів, специфічних варіантів чи сфер використання побудованого об'єкта нерухомості та застосування методів захисту. Ці вимоги також можуть стосуватися надання неструктурованої інформації, наприклад, на паперових носіях, у форматі зображення чи неінтерактивному форматі PDF, замість надання доступу, наприклад, до інтерактивних інформаційних моделей.

С.2.3 Якщо конфіденційні дані неможливо вилучити з інформації, яку представляють, організація (-ії) має (-ють) звернутися до третьої особи для узгодження відповідних застосовних заходів захисту інформації перед її наданням. Якщо третя особа підпадає під дію положень законодавства щодо забезпечення відкритості інформації чи прозорості діяльності, зазначені заходи захисту інформації мають бути достатніми для управління ризиком на рівні, прийнятному для організації (-ій).

С.3 Відкритість інформації

У плані управління безпекою має бути детально зазначено методи захисту конфіденційної інформації, які потрібно застосовувати у разі надходження до організації запиту на інформацію, на яку поширюються положення законодавства щодо відкритості чи прозорості діяльності. У цьому разі потрібно враховувати вплив потенційних проблем, які можуть виникнути внаслідок агрегування інформації.

С.4 Публічні презентації

У плані управління безпекою має бути зазначено вимоги щодо затвердження будь-яких інформаційних матеріалів, що стосуються ініціювання розробки, проекту, активу, виробу чи послуги, які буде розглянуто або продемонстровано під час публічних заходів, розміщено в доступних для інших осіб чи загальнодоступних громадських місцях, або опубліковано на веб-сайтах, у технічних чи академічних виданнях або маркетингових оглядах.

ДОДАТОК D

(довідковий)

УГОДИ ПРО СПІЛЬНЕ ВИКОРИСТАННЯ ІНФОРМАЦІЇ

D.1.1 Угоду про спільне використання інформації або еквівалентний документ має бути укладено з усіма відповідними сторонами до початку обмінювання конфіденційною інформацією та, якщо застосовне, даними для інформаційних моделей, які може бути використано для завдання шкоди ініціюванню розробки, проекту, активу, виробу, послузі, окремій особі чи групі осіб або громаді.

D.1.2 В угоді має бути докладно зазначено, щонайменше:

a) ціль (-і) спільного використання інформації;

b) потенційних одержувачів або типи одержувачів та умови, за яких вони матимуть доступ до інформації;

c) тип інформації, яку потрібно надавати для спільного використання;

d) якість інформації, призначеної для спільного використання, зокрема її достовірність, сферу застосування, точність, актуальність та зручність для використання;

e) вимоги щодо:

1) захисту інформації, якщо застосовне;

2) дозволу та заборони на право використання інформації;

3) зобов'язання відповідно до угоди про спільне використання інформації по всіх рівнях можливих призначень за системою підпорядкування;

4) обов'язків відповідно до вимог плану протидії порушенням безпеки/управління інцидентами, стосовно

повідомлення власника інформації та/або контролера безпеки інформаційної мережі у разі будь-якого потенційного чи виявленого порушення безпеки або інциденту;

f) методи адміністративного управління користувачами;

g) умови технічної підтримки інформації, включно з реагуванням на повідомлення про запити на видалення чи виправлення;

h) методи захисту інформації;

i) порядок зберігання та/або видалення інформації для спільного використання;

j) процедуру розгляду питань щодо реалізації прав суб'єктів інформації, включно із запитами на надання доступу, запитаннями та скаргами, стосовно обміну інформацією між організаціями, одержувачами за певним місцем розташування та юрисдикцією;

k) умови проведення моніторингу та аудиту дотримання положень угоди про спільне використання інформації;

l) санкції за недотримання вимог угоди про спільне використання інформації та/або протидії порушенням безпеки/управління інцидентами з боку окремого працівника колективу.

Примітка. Укладанню належної угоди про спільне використання інформації сприятиме отримання відповідної юридичної консультації.

D.1.3 У разі фактичного чи потенційного порушення безпеки/інциденту, або якщо є свідчення того, що управління та оброблення інформації виконують невідповідно до угоди про спільне використання інформації, організації (-ям) потрібно або:

a) призупинити дію угоди про спільне використання інформації та обмін інформацією, доки подію не буде розслідувано, а проблеми – розглянуто, а також узгоджено і впроваджено будь-які заходи з усунення невідповідностей; або

Примітка. За цих умов важливо проводити розслідування та впроваджувати заходи зі зниження ризику без зайвих зволікань.

b) розірвати угоду про спільне використання інформації та припинити обмін інформацією та, за потреби, вимагати видалення спільно використовуваної інформації, якщо проблему не може бути вирішено із задовільним результатом.

D.1.4 Угоди про спільне використання інформації потрібно переглядати з періодичністю, визначеною в плані управління безпекою, щоб визначити ефективність спільного використання інформації та надати підтвердження того, що:

a) обмінювання інформацією з кожним одержувачем відбувається на законних підставах, а в ситуаціях, коли такі підстави були відсутні, обмінювання було припинено;

b) якість та технічна підтримка інформації відповідають узгодженим стандартам;

c) заходи з убезпечення інформації залишаються відповідними та пропорційними, а всі порушення безпеки чи інциденти, що відбулися, було усунуто із задовільним результатом.

ДОДАТОК НА

(довідковий)

ПЕРЕЛІК НАЦІОНАЛЬНИХ СТАНДАРТІВ УКРАЇНИ, ІДЕНТИЧНИХ МІЖНАРОДНИМ НОРМАТИВНИМ ДОКУМЕНТАМ, ПОСИЛАННЯ НА ЯКІ Є В ЦЬОМУ СТАНДАРТІ

ДСТУ ISO 19650-2:2020 (ISO 19650-2:2018, IDT) Організація та оцифрування інформації щодо будівель та споруд включно з будівельним інформаційним моделюванням (BIM). Управління інформацією з використанням будівельного інформаційного моделювання. Частина 2. Етап будівництва

БІБЛІОГРАФІЯ

1 ISO 14298:2013 Graphic technology — Management of security printing processes

2 ISO 16530-1:2017 Petroleum and natural gas industries — Well integrity — Part 1: Life cycle governance

3 ISO 19011 Guidelines for auditing management systems

4 ISO 19650-1 Organization and digitization of information about buildings and civil engineering works, including building information modelling (BIM) — Information management using building information modelling — Part 1: Concepts and principles

5 ISO 22300:2018 Security and resilience — Vocabulary

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

7 ISO 31000 Risk management — Guidelines

8 ISO 55000:2014 Asset management – Overview, principles and terminology

НАЦІОНАЛЬНЕ ПОЯСНЕННЯ

1 ISO 14298:2013 Графічні технології. Управління безпекою процесів друку

2 ISO 16530-1:2017 Промисловість нафтова та газова. Цілісність свердловини. Частина 1. Управління життєвим циклом

3 ISO 19011 Настанова щодо здійснення аудитів систем управління

4 ISO 19650-1 Організація та оцифрування інформації щодо будівель та споруд включно з будівельним інформаційним моделюванням (BIM). Управління інформацією з використанням будівельного інформаційного моделювання. Частина 1. Концепції та принципи

5 ISO 22300:2018 Безпека суспільства. Словник термінів

6 ISO/IEC 27001 Інформаційні технології. Методи безпеки. Системи менеджменту інформаційною безпекою. Вимоги

7 ISO 31000 Управління ризиками. Принципи та настанови

8 ISO 55000:2014 Управління активами. Загальний огляд, принципи та термінологія

Коди згідно з НК 004 35.240.67; 91.010.01

Ключові слова: актив, інформаційна безпека, інформаційна модель, конфіденційна інформація, методи захисту інформації, пріоритет безпеки, ризик безпеки, убезпеченість, уразливість, управління ризиками, чутливість до ризику

Генеральний директор ТОВ «Укрінсталькон ім. В.М. Шимановського», заслужений діяч науки і техніки України, член-кореспондент НАНУ, д.т.н., проф.	О. В. Шимановський
Заступник генерального директора з наукової роботи, д.т.н., проф.	В. М. Гордеєв
Заступник генерального директора з науково-технічної політки, заступник голови ТК 301	В. П. Адріанов
Завідувач відділу (науковий керівник розробки)	О. І. Кордун
Завідувач групи	Я. В. Лимар
Провідний редактор-перекладач	В. П. Гаврилова