НАЦІОНАЛЬНИЙ СТАНДАРТ УКРАЇНИ

Інформаційні технології

МЕТОДИ ЗАХИСТУ

Звід практик щодо заходів інформаційної безпеки (ISO/IEC 27002:2013; Cor 1:2014, IDT)

ДСТУ ISO/IEC 27002:2015

Видання офіційне

Київ
ДП «УкрНДНЦ»
2016

ПЕРЕДМОВА

1 ВНЕСЕНО: Технічний комітет стандартизації «Інформаційні технології» (ТК 20) за участю Технічного комітету стандартизації «Банківські та фінансові системи і технології» (ТК 105), Міжнародний науково-навчальний центр інформаційних технологій та систем НАН України та Міносвіти і науки України

ПЕРЕКЛАД І НАУКОВО-ТЕХНІЧНЕ РЕДАГУВАННЯ: **І. Івченко,** канд. фіз.-мат. наук; **М. Карнаух; Т. Тищенко**

2 НАДАНО ЧИННОСТІ: наказ ДП «УкрНДНЦ» від 18 грудня 2015 р. № 193 з 2017–01–01

3 Національний стандарт відповідає ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls (Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки) зі зміною Cor.1:2014

Ступінь відповідності — ідентичний (IDT)

Переклад з англійської (en)

4 УВЕДЕНО ВПЕРШЕ

ЗМІСТ

НАЦІОНАЛЬНИЙ ВСТУП

Цей стандарт ідентичний ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls (Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки) зі зміною Cor 1:2014.

Технічний комітет стандартизації, відповідальний за цей стандарт в Україні, — ТК 105 «Банківські та фінансові системи і технології».

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

До цього стандарту внесено такі редакційні зміни:

— слова «цей міжнародний стандарт», «ISO/IEC 27002», «цей документ» замінено на «цей стандарт»;

— вилучено «Передмову» до ISO/IEC 27002:2014 як таку, що безпосередньо не стосується тематики цього стандарту;

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

— у розділах «Нормативні посилання» та «Бібліографії» наведено «Національні пояснення», виділені рамкою;

— у 6.1.1, 7.2.1 і 8.1.2 наведено «Національні примітки», виділені рамкою;

— долучено довідковий національний додаток НА (Перелік національних стандартів України, ідентичних з міжнародними стандартами, посилання на які є в цьому стандарті).

У цьому стандарті є посилання на міжнародний стандарт ISO/IEC 27000, який прийнято як ДСТУ ISO/IEC 27000:2015 Системи управління інформаційною безпекою. Огляд і словник (ISO/ IEC 27000:2015, IDT).

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

0 ВСТУП до ISO/IEC 27002:2013

0.1 Загальні положення

Цей міжнародний стандарт розроблено для організацій для використання як довідкової інформації щодо вибору заходів безпеки під час впровадження системи управління інформаційною безпекою (СУІБ) на базі ISO/IEC 27001 [10] або як настанову для організацій, які впроваджують загальноприйняті заходи інформаційної безпеки. Цей стандарт також призначено для використання в розробленні настановчих документів з управління інформаційною безпекою, специфічних для промисловості та організацій, з урахуванням специфічних ризиків інформаційної безпеки їх середовища.

Організації всіх типів та розмірів (охоплюючи публічний та приватний сектор, комерційні та неприбуткові) збирають, обробляють, зберігають та передають інформацію в багатьох формах, включаючи електронну, фізичну та усну (наприклад, бесіди та презентації).

Цінність інформації виходить за межі записаних слів, чисел та зображень: знання, концепції, ідеї та бренди є прикладами нематеріальних форм інформації. У взаємопов'язаному світі інформація та пов'язані процеси, системи, мережі й персонал, який бере участь в їх функціонуванні, обробленні та захисті, є ресурсами СУІБ, які нарівні з іншими важливими бізнес-активами є цінними для бізнесу організації і тому заслуговують чи потребують захисту від різних небезпек.

Ресурси СУІБ є суб'єктами як навмисних, так і випадкових загроз, а пов'язані процеси, системи, мережі та персонал мають притаманні вразливості. Зміни в бізнес-процесах і системах або зовнішні зміни (такі як нові закони та регуляторні вимоги) можуть створювати нові ризики інформаційної безпеки. Отже, маючи величезну кількість шляхів, за якими загрози можуть використовувати вразливості для завдання шкоди організації, ризики інформаційної безпеки завжди наявні. Ефективна інформаційна безпека зменшує ці ризики за допомогою захисту організації від загроз та вразливостей і таким чином зменшує впливи на її активи.

Інформаційної безпеки досягають впровадженням відповідного набору заходів безпеки, який охоплює політику, процеси, процедури, організаційні структури й програмні та апаратні функції. Ці заходи безпеки необхідно розробити, впровадити, здійснювати моніторинг, переглядати та, за потреби, вдосконалювати для гарантування досягнення певного рівня безпеки та бізнес-цілей організації. СУІБ, як це визначено в ISO/IEC 27001 [10], надає цілісний, узгоджений розгляд ризиків інформаційної безпеки організації для того, щоб впровадити всебічний набір заходів інформаційної безпеки в межах загальних принципів зрозумілої системи управління.

Багато інформаційних систем не проектували як безпечні з точки зору ISO/IEC 27001 [10] і цього стандарту. Безпека, якої може бути досягнуто технічними засобами, є обмеженою і має підтримуватися відповідним управлінням та процедурами. Визначення, які заходи безпеки треба застосовувати на місці,

потребує ретельного планування й уваги до дрібниць. Успішна СУІБ потребує щонайменше участі всього персоналу організації. Вона може також потребувати співучасті від акціонерів, постачальників або інших зовнішніх сторін. Рекомендації фахівців зі сторонніх організацій також можуть стати в нагоді.

Загалом ефективна інформаційна безпека також гарантує керівництву та іншим акціонерам, що ресурси організації достатньо безпечні та захищені від втрат, таким чином сприяючи розвитку бізнесу.

0.2 Вимоги щодо інформаційної безпеки

Організація повинна ідентифікувати свої вимоги щодо безпеки. Існують три основні джерела формування вимог щодо безпеки:

a) результат оцінки ризиків для організації, який враховує загальну бізнес-стратегію та цілі. Під час оцінювання ризиків ідентифікують загрози ресурсам СУІБ, вразливості та ймовірність подій і оцінюють величину потенційного впливу;

b) законодавство, нормативні та контрактні вимоги, яким організація, її партнери, підрядники та постачальники послуг повинні відповідати, а також їх соціально-культурне середовище.

c) набір принципів, цілей та бізнес-вимог щодо управління, оброблення, зберігання, передавання та архівування інформації, який організація розробила для підтримки свого функціонування.

Ресурси, задіяні у впроваджуваних заходах безпеки, мають бути збалансовані із втратами бізнесу, які можуть бути результатом порушення безпеки за відсутності цих заходів безпеки. Результати оцінювання ризиків допоможуть керувати й визначити відповідну керівну діяльність та пріоритети щодо управління ризиками інформаційної безпеки і зробити вибір заходів безпеки, щоб захиститися від цих ризиків.

ISO/IEC 27005 [11] описує настанови стосовно управління ризиками інформаційної безпеки, зокрема й консультації щодо оцінювання, оброблення, приймання, перенесення, моніторингу та перегляду ризиків.

0.3 Вибір заходів безпеки

Заходи безпеки можна вибирати з цього стандарту або інших наборів заходів безпеки, або, за потреби, можна спроектувати нові заходи безпеки для задоволення специфічних потреб.

Вибір заходів безпеки залежить від управлінських рішень, основаних на критеріях прийняття ризику, варіантах оброблення ризику та загальному підході до управління ризиком, застосовному в організації, а також він має відповідати всьому чинному національному й міжнародному законодавству та нормативним документам. Вибір заходів безпеки має також залежати від способу взаємодії цих заходів безпеки для забезпечення глибшого захисту.

Деякі із заходів безпеки в цьому стандарті можна розглядати як настановчі принципи щодо управління інформаційною безпекою і їх може бути застосовано для більшості організацій. Заходи безпеки пояснено більш детально нижче разом з настановою щодо впровадження. Більше інформації щодо вибору заходів безпеки та інших варіантів оброблення ризику можна знайти в ISO/IEC 27005 [11].

0.4 Розроблення власних настанов

Цей стандарт можна вважати відправною точкою для розроблення певних настанов організації. Не всі заходи безпеки та настанови цього зводу правил може бути застосовно. Крім того, можуть бути потрібні додаткові заходи безпеки та настанови, які не містить цей стандарт. Під час розроблення документів, які містять додаткові настанови чи заходи безпеки, може бути корисним наводити в тих місцях, за потреби, перехресні посилання на розділи цього стандарту для полегшення перевірки відповідності аудиторами та бізнес-партнерами.

0.5 Розгляд життєвого циклу

Інформація має життєвий цикл від створення й початку через зберігання, оброблення, використання й передавання до її кінцевого знищення чи руйнування. Цінність і ризики ресурсів СУІБ можуть змінюватися протягом їх життєвого циклу (наприклад, неавторизоване розкриття чи викрадення фінансових рахунків компанії після того, як їх було формально опубліковано, стають менш значимими), але інформаційна безпека залишається важливою до певного ступеня на всіх стадіях.

Інформаційні системи мають життєвий цикл, протягом якого їх планують, визначають, конструюють, розробляють, тестують, впроваджують, експлуатують, підтримують і остаточно виводять з експлуатації та знищують. Інформаційну безпеку треба брати до уваги на кожній стадії. Розроблення нових систем та внесення змін до наявних систем надає можливість організації оновити й покращити заходи безпеки з урахуванням актуальних інцидентів і наявних та вже захищених ризиків інформаційної безпеки.

0.6 Пов'язані стандарти

У той час, як цей стандарт надає настанови стосовно широкого діапазону заходів інформаційної безпеки, які зазвичай використовує велика кількість різних організацій, інші стандарти серії ISO/IEC 27000 містять детальні консультації або вимоги до інших аспектів загального процесу управління інформаційною безпекою.

Треба звернутися до ISO/IEC 27000 для загального роз'яснення як СУІБ, так і цієї серії стандартів. ISO/IEC 27000 надає словник, який формально визначає більшість із термінів, які використовують всюди в серії стандартів ISO/IEC 27000, та описує межі та цілі кожного стандарту цієї серії.

НАЦІОНАЛЬНИЙ СТАНДАРТ УКРАЇНИ

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

МЕТОДИ ЗАХИСТУ

Звід практик щодо заходів інформаційної безпеки

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

МЕТОДЫ ЗАЩИТЫ

Свод практик для средств информационной безопасности

INFORMATION TECHNOLOGY

SECURITY TECHNIQUES

Code practice for information security controls

Чинний від 2017–01–01

1 СФЕРА ЗАСТОСУВАННЯ

Цей стандарт встановлює настанови стосовно організаційних стандартів щодо інформаційної безпеки та загальні практики управління інформаційною безпекою, охоплюючи вибір, впровадження та управління заходами безпеки з урахуванням розгляду середовища ризиків інформаційної безпеки організації.

Цей стандарт розроблено для використання організаціями, які намагаються:

a) визначити заходи безпеки в межах процесу впровадження системи управління інформаційною безпекою на основі ISO/IEC 27001 [10];

b) впровадити загальноприйняті заходи інформаційної безпеки;

c) розробити власні настанови щодо управління інформаційною безпекою.

2 НОРМАТИВНІ ПОСИЛАННЯ

Наведені нижче нормативні документи повністю або частково необхідні для застосування цього стандарту. У разі датованих посилань застосовують лише наведені видання. У разі недатованих посилань потрібно користуватись останнім виданням нормативних документів (разом зі змінами).

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

НАЦІОНАЛЬНЕ ПОЯСНЕННЯ

ISO/IEC 27000 Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Огляд і словник.

3 ТЕРМІНИ ТА ВИЗНАЧЕННЯ ПОНЯТЬ

У цьому стандарті використовують терміни та визначення, які наведено в ISO/IEC 27000.

Видання офіційне

4 СТРУКТУРА ЦЬОГО СТАНДАРТУ

Цей стандарт містить 14 розділів заходів безпеки, які загалом охоплюють 35 основних категорій безпеки та 114 заходів безпеки.

4.1 Розділи

Кожний розділ, який визначає заходи безпеки, містить одну чи більшу кількість основних категорій безпеки.

Порядок розділів у цьому стандарті не означає їх важливості. Залежно від обставин заходи безпеки будь-якого чи всіх розділів можуть бути важливими, тому кожна організація, яка застосовує цей стандарт, повинна ідентифікувати заходи безпеки, які використовують, для розуміння їх важливості та необхідності їх застосування до конкретного бізнес-процесу. Крім того, усі переліки в цьому стандарті не впорядковано в пріоритетному порядку.

4.2 Категорії безпеки

Кожна основна категорія безпеки містить:

a) ціль заходу безпеки, яка визначає, чого треба досягти; та

b) один або більше заходів безпеки, які може бути застосовано для досягнення цілі заходу безпеки.

Описи заходів безпеки структуровано, як наведено нижче.

Заходи безпеки

Визначає певне положення щодо заходу безпеки для досягнення цілі цього заходу.

Настанова щодо впровадження

Надає детальнішу інформацію для підтримки впровадження заходу безпеки й досягнення цілі цього заходу. Деякі з цих настанов можуть бути не цілком придатними чи ефективними в усіх випадках і, отже, можуть не задовольняти особливі вимоги заходів контролю організації.

Додаткова інформація

Надає подальшу інформацію, яка може потребувати розгляду, наприклад, правові підстави й посилання та інші стандарти. Якщо не передбачено додаткової інформації, цей пункт не наведено.

5 ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

5.1 Принципи управління інформаційною безпекою

Ціль: Забезпечити принципи управління та підтримку інформаційної безпеки згідно з вимогами бізнесу та відповідними законами й нормативами.

5.1.1 *Політики інформаційної безпеки*

Заходи безпеки

Набір політик щодо інформаційної безпеки повинен бути визначений, затверджений керівництвом, виданий і доведений до відома всього найманого персоналу та потрібних зовнішніх сторін.

Настанова щодо впровадження

На найвищому рівні організація повинна визначити «політику інформаційної безпеки», яка затверджена керівництвом і встановлює принципи організації щодо управління власними цілями інформаційної безпеки.

Політики інформаційної безпеки мають відповідати вимогам, створеним:

a) бізнес-стратегією;

b) законодавством, нормативними й контрактними вимогами;

c) поточним і можливим у майбутньому середовищем загроз інформаційної безпеки.

Політика інформаційної безпеки має містити положення стосовно:

a) визначення інформаційної безпеки, цілей та принципів для забезпечення спрямованості всіх дій, пов'язаних з інформаційною безпекою;

b) визначення загальних та спеціальних обов'язків з управління інформаційною безпекою для певних ролей;

c) процесів оброблення відхилень та винятків.

На нижчому рівні політика інформаційної безпеки повинна бути підтримана політиками за окремими розділами, які детально описують запровадження заходів інформаційної безпеки й зазвичай структуровані для потреб певних кінцевих груп всередині організації або стосуються певних тем.

Приклади таких політик за окремими розділами містять:

a) контроль доступу (див. розділ 9);

b) класифікацію інформації (та оброблення) (див. 8.2);

c) фізичну безпеку та безпеку інфраструктури (див. розділ 11);

d) політики, орієнтовані на кінцевого користувача, такі як політика:

1) допустимого використання ресурсів (див. 8.1.3.);

2) чистого стола та чистого екрана (див. 11.2.9);

3) передавання інформації (див. 13.2.1);

4) мобільного обладнання та віддаленої роботи (див. 6.2.);

5) обмеження на інсталяцію та використання програмного забезпечення (див. 12.6.2);

e) резервне копіювання (див. 12.3);

f) передавання інформації (див. 13.2);

g) захист від зловмисного коду (див. 12.2);

h) управління технічними вразливостями (див. 12.6.1);

i) криптографічні засоби безпеки (див. розділ 10);

j) безпеку комунікацій (див. розділ 13);

k) захист персональних ідентифікаційних даних (див. 18.1.4);

l) взаємовідносини з постачальниками (див. розділ 15).

Ці політики повинні бути доведені до відома користувачів і відповідних третіх сторін у належній, доступній та зрозумілій для читача, якому її призначено, формі, наприклад, у контексті «програми ознайомлення, навчання й тренінгу інформаційної безпеки» (див. 7.2.2).

Додаткова інформація

Потреба у внутрішніх політиках для інформаційної безпеки змінюється залежно від організації. Внутрішні політики дуже корисні для великих та більш комплексних організацій, де визначені та затверджені очікувані рівні заходів безпеки відокремлено від упроваджених заходів безпеки або в ситуаціях, коли політику запроваджують до великої кількості різного персоналу чи функцій в організації. Політики для інформаційної безпеки можна розглядати як єдиний документ «політика інформаційної безпеки» чи як набір окремих, але пов'язаних документів.

Якщо будь-яка з політик інформаційної безпеки поширюється за межі організації, треба подбати про нерозголошення конфіденційної інформації.

Деякі організації використовують інші терміни для цих документів політик, такі як «Стандарт», «Директива» чи «Правила».

5.1.2 *Перегляд політики інформаційної безпеки*

Заходи безпеки

Політики інформаційної безпеки потрібно переглядати в заплановані інтервали часу або за появи істотних змін для забезпечення їх постійної придатності, адекватності й ефективності.

Настанова щодо впровадження

Кожна політика інформаційної безпеки повинна мати власника, який несе затверджену керівництвом відповідальність за розвиток, перегляд і оцінювання політики безпеки. Перегляд має охоплювати оцінку можливостей вдосконалення політик інформаційної безпеки організації і підхід до управління інформаційною безпекою в разі змін інфраструктури організації, бізнес-обставин, правових умов або технічної інфраструктури.

Перегляд політики інформаційної безпеки має враховувати результати переглядів з боку керівництва.

Переглянута політика повинна бути затверджена керівництвом.

6 ОРГАНІЗАЦІЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

6.1 Внутрішня організація

Ціль: Визначити структуру управління для започаткування та контролю впровадження та функціонування інформаційної безпеки в організації.

6.1.1 *Ролі та обов'язки щодо інформаційної безпеки*

Заходи безпеки

Усі обов'язки щодо інформаційної безпеки необхідно чітко визначити та розподілити.

Настанова щодо впровадження

Розподіл обов'язків щодо інформаційної безпеки має здійснюватися відповідно до політики інформаційної безпеки (див. 5.1.1). Обов'язки щодо захисту окремих ресурсів СУІБ та виконання певних процедур безпеки має бути чітко ідентифіковано. Обов'язки щодо діяльності стосовно управління ризиками інформаційної безпеки і зокрема для прийняття залишкових ризиків має бути визначено. Такі обов'язки має бути доповнено, за потреби, більш докладною настановою щодо окремих місць розміщення та засобів обробки інформації. Треба чітко визначити конкретні обов'язки щодо захисту ресурсів СУІБ на місцях та виконання певних процедур безпеки.

Особи з визначеними обов'язками щодо інформаційної безпеки можуть делегувати задачі безпеки іншим. Незважаючи на це, вони залишаються відповідальними і повинні визначити, чи всі делеговані задачі виконуються правильно.

Треба чітко встановити сфери відповідальності окремих осіб; зокрема, повинно мати місце наведене нижче:

a) треба ідентифікувати й чітко визначити ресурси СУІБ та процедури безпеки;

b) треба призначити особу, відповідальну за кожний ресурс СУІБ чи процедуру безпеки і ці обов'язки треба докладно задокументувати (див. 8.1.2);

c) треба чітко визначити й задокументувати рівні санкціонування;

НАЦІОНАЛЬНЕ ПОЯСНЕННЯ

Рівні санкціонування доступу до інформаційних ресурсів СУІБ можуть бути, наприклад, «лише читати», «читати й записувати», «лише записувати» тощо.

d) призначені особи мають бути компетентними у сфері інформаційної безпеки й мати можливість отримувати інформацію щодо сучасних розробок для того, щоб виконувати обов'язки з інформаційної безпеки;

e) треба ідентифікувати й задокументувати координацію та нагляд за всіма аспектами інформаційної безпеки взаємодії з постачальниками.

Додаткова інформація

У багатьох організаціях керівник з інформаційної безпеки призначається повністю відповідальним за розвиток і впровадження безпеки та за підтримку ідентифікації заходів безпеки.

Проте відповідальність за добір ресурсів та впровадження заходів безпеки часто залишається за окремими менеджерами. Звичайною практикою є призначення для кожного ресурсу СУІБ власника, який внаслідок цього стає відповідальним за щоденний захист ресурсу СУІБ.

6.1.2 *Розподіл обов'язків*

Заходи безпеки

Несумісні обов'язки та сфери відповідальності мають бути розподілені для зменшення можливостей неавторизованої чи ненавмисної модифікації, або неправильного використання ресурсів СУІБ організації.

Настанова щодо впровадження

Треба бути уважними, щоб жодна окрема особа не мала можливості модифікувати чи використати ресурси СУІБ без авторизації чи виявлення. Ініціалізацію дії має бути відокремлено від її авторизації. Можливість колізії має бути проаналізовано під час визначення (обрання) заходів безпеки.

Невеликі організації мають враховувати, що досягти розподілення обов'язків дуже важко, але цей принцип потрібно запроваджувати наскільки це можливо і припустимо на практиці. Якщо дуже важко розподілити обов'язки, потрібно застосовувати інші заходи безпеки, такі як моніторинг дій, журнали аудиту і нагляд керівництва.

Додаткова інформація

Розподіл обов'язків — це засіб зменшення ризиків випадкового чи ненавмисного неправильного використання ресурсів СУІБ організації.

6.1.3 *Контакти з повноважними органами*

Заходи безпеки

Необхідно підтримувати належні контакти з відповідними повноважними органами.

Настанова щодо впровадження

В організації мають бути наявні процедури, які визначають, коли і з якими повноважними органами (наприклад, органами забезпечення правопорядку, пожежної охорони, наглядовими органами)

треба контактувати і як своєчасно звітувати про ідентифіковані інциденти інформаційної безпеки (наприклад, якщо очікують, що цим може бути порушено закони).

Додаткова інформація

Організації, на яку здійснений напад з Інтернету, можуть знадобитись уповноважені органи для виконання дій проти джерела нападу.

Підтримування таких контактів може бути вимогою щодо підтримки управління інцидентом інформаційної безпеки (див. розділ 16) або безперервності бізнесу та процесу планування дій у надзвичайних ситуаціях (див. розділ 17). Контакти з регуляторними органами також є корисними для передбачення та підготовки до наступних змін до законів і нормативів, яких повинна дотримуватися організація. Контакти з іншими повноважними органами охоплюють підприємства комунального обслуговування, аварійного обслуговування, постачальників електроживлення. а також здоров'я та безпеки, наприклад, відділів пожежної охорони (для забезпечення безперервності бізнесу), провайдерів телекомунікаційних послуг (для забезпечення маршрутизації та доступності ліній), постачальників води (для роботи охолоджувальних засобів обслуговування обладнання).

6.1.4 *Контакти з групами фахівців з певної проблематики*

Заходи безпеки

Необхідно підтримувати належні контакти з групами фахівців з певної проблематики або іншими форумами фахівців з безпеки чи професійними об'єднаннями.

Настанова щодо впровадження

Членство в групах фахівців з певної проблематики чи форумах потрібно розглядати як засіб для:

a) вдосконалення знань щодо найкращих практик та поінформованості щодо важливої та найсучаснішої інформації стосовно безпеки;

b) забезпечення того, що розуміння інформаційної безпеки є сучасним та повним;

c) отримання ранніх попереджень із застереженнями, повідомленнями щодо небезпеки, і кодів оперативного виправлення (patches), які стосуються атак і вразливостей;

d) одержання доступу до рекомендацій фахівців з інформаційної безпеки;

e) спільного користування та обміну інформацією щодо нових технологій, продуктів, загроз або вразливостей;

f) забезпечення можливості обговорення під час роботи з інцидентами інформаційної безпеки (див. розділ 16).

Додаткова інформація

Для вдосконалення співпраці та координації у питаннях безпеки можна укладати угоди щодо спільного використання інформації. Такі угоди мають ідентифікувати вимоги щодо захисту конфіденційної інформації.

6.1.5 *Інформаційна безпека в управлінні проектами*

Заходи безпеки

Інформаційну безпеку потрібно брати до уваги під час управління проектами незалежно від типу проекту.

Настанова щодо впровадження

Інформаційна безпека має бути інтегрована до методу(-ів) управління проектами організації для гарантії того, що ризики інформаційної безпеки ідентифіковані і їх беруть до уваги як частину проекту. Такий підхід зазвичай застосовують для будь-яких проектів незалежно від їх характеру, наприклад проекту для основного бізнес-процесу, ІТ, управління обладнанням та інших процесів підтримки. Методи управління проектами, які використовують, мають потребувати, щоб:

a) цілі інформаційної безпеки було долучено до цілей проекту;

b) оцінювання ризиків інформаційної безпеки виконували на ранніх стадіях проекту для ідентифікації потрібних заходів безпеки;

c) інформаційна безпека була частиною на всіх фазах методології, яку застосовують у проекті.

Питання інформаційної безпеки потрібно брати до уваги й регулярно переглядати в усіх проектах. Відповідальності за інформаційну безпеку мають бути визначені та затверджені для певних ролей в методах управління проектами.

6.2 Мобільне обладнання та віддалена робота

Ціль: Гарантувати безпеку віддаленої роботи та використання мобільного обладнання.

6.2.1 ***Політика щодо мобільного обладнання***

Заходи безпеки

Політика та заходи підтримання безпеки мають бути пристосовані до управління ризиками, які виникають за рахунок використання мобільного обладнання.

Настанова щодо впровадження

У разі використання мобільного обладнання має бути прийнято спеціальні міри для гарантування того, що бізнес-інформація не буде скомпрометована. Політика щодо мобільного обладнання має брати до уваги ризики роботи з мобільним обладнанням у незахищеному середовищі.

Політика щодо мобільного обладнання має розглядати:

a) обмеження використання мобільного обладнання;

b) вимоги стосовно фізичного захисту;

c) обмеження стосовно інсталяції програмного забезпечення;

d) вимоги щодо версій програмного забезпечення та патчей (patches), які використовують;

e) обмеження стосовно приєднання до інформаційних сервісів;

f) контроль доступу;

g) криптографічні методи;

h) захист від зловмисного коду;

i) віддалені виведення з ладу, знищення інформації або заборона доступу;

j) резервне копіювання;

k) використання веб-сервісів та веб-додатків.

Треба бути обережними під час використання мобільного обладнання в публічних місцях, кімнатах для нарад та інших незахищених місцях. Захист власноруч придбаного мобільного обладнання всередині треба здійснювати для запобігання неавторизованому доступу чи розкриттю інформації, яка зберігається та обробляється цим мобільним обладнанням, наприклад з використанням криптографічних методів (див. розділ 10) та примушенням до використання секретної інформації автентифікації (див. 9.2.4).

Мобільне обладнання має також бути фізично захищеним від крадіжок, зокрема коли залишається, наприклад, в автомобілях або інших типах транспорту, кімнатах готелів, конференційних центрах та місцях зустрічі. Має бути встановлено певні процедури, які враховують вимоги законодавства, страхування та інші вимоги щодо безпеки для випадків крадіжки чи втрати мобільного обладнання. Обладнання, яке містить важливу, чутливу чи критичну бізнес-інформацію не потрібно залишати без уваги, воно має бути фізично замкнуте, якщо це можливо, чи потрібно використовувати спеціальні замки для безпеки цього обладнання.

Потрібно проводити тренінги для персоналу, який використовує мобільне обладнання, для того, щоб підвищити їхні знання стосовно додаткових ризиків, які з'являються внаслідок такого способу роботи, і заходів безпеки, які має бути запроваджено.

Якщо політика щодо мобільного обладнання дозволяє використовувати власноруч придбане мобільне обладнання, ця політика та пов'язані заходи безпеки мають також розглядати такі питання як:

a) розділення приватного та бізнес-використання цього обладнання, включаючи програмне забезпечення, використане задля підтримки такого розділення й захисту даних бізнесу на приватному обладнанні;

b) надання доступу до бізнес-інформації лише після того, як користувачі підпишуть угоду кінцевого користувача, яка визначає їхні обов'язки (фізичний захист, оновлення програмного забезпечення тощо), відмову від власності на бізнес-дані, дозвіл на віддалене видалення даних організації в разі крадіжки чи втрати обладнання, або коли далі не передбачена авторизація на використання сервісу. Ця політика потребує врахування законодавства щодо конфіденційності.

Додаткова інформація

Безпровідне з'єднання мобільного обладнання подібне іншим типам мережевого з'єднання, але має важливі відмінності, які необхідно розглядати під час ідентифікації заходів безпеки. Типовими відмінностями є такі:

a) деякі безпровідні захищені протоколи є незрілими та мають відомі вразливості;

b) інформація, яку зберігають на мобільному обладнанні, не може бути зарезервована через обмежену полосу пропускання мережі або через те, що мобільне обладнання не може бути на зв'язку в той час, коли здійснюють резервне копіювання за процедурою.

Мобільне обладнання загалом має звичайні функції, наприклад робота в мережі, доступ до Інтернету, електронна пошта та оброблення файлів для обладнання з фіксованим використанням. Заходи інформаційної безпеки для мобільного обладнання загалом з тих, що їх прийнято для обладнання з фіксованим використанням, і тих, що спрямовані проти загроз, які виникають під час їхнього використання за межами приміщень організації.

6.2.2 ***Віддалена робота***

Заходи безпеки

Політика та заходи підтримання безпеки мають бути запроваджені для захисту інформації, яка доступна, обробляється чи зберігається в місцях віддаленої роботи.

Настанова щодо впровадження

Організації, які дозволяють віддалену роботу, повинні мати політику, де визначено умови та обмеження для віддаленої роботи. Там, де можливо та дозволено законодавством, треба розглянути такі питання як:

a) наявна фізична безпека місця віддаленої роботи, зокрема фізична безпека будівлі та локальної інфраструктури;

b) пропонована фізична інфраструктура для віддаленої роботи;

c) вимоги щодо безпеки комунікацій, беручи до уваги потребу віддаленого доступу до внутрішніх систем організації, конфіденційність інформації, до якої потрібний доступ та яка передається каналами зв'язку, і конфіденційність внутрішньої системи;

d) забезпечення доступу віртуального комп'ютера, що запобігає обробленню та зберіганню інформації на власноруч придбаному обладнанні;

e) загроза несанкціонованому доступу до інформації або ресурсів інших осіб згідно з домовленістю, наприклад родини та друзів;

f) використання домашніх мереж та вимоги чи обмеження стосовно конфігурації послуг бездротових мереж;

g) політики та процедури для запобігання спорів стосовно прав на інтелектуальну власність, розроблену на обладнанні, що перебуває в приватній власності;

h) доступ до обладнання, що перебуває в приватній власності (для перевіряння безпеки комп'ютера або під час розслідування), якому може перешкоджати законодавство;

i) ліцензійні угоди на програмне забезпечення мають бути такими, щоб організація могла бути відповідальною за ліцензування клієнтського програмного забезпечення на робочих станціях, які власноруч придбані персоналом чи користувачами зовнішньої сторони;

j) вимоги стосовно захисту від зловмисного коду та міжмережевого екранування.

Настанови та структура документа мають містити:

a) забезпечення відповідним обладнанням та пристроями для зберігання для місць віддаленої роботи, де не дозволено використання обладнання, що перебуває в приватній власності, яке не перебуває під контролем організації;

b) визначення дозволених видів робіт, годин роботи, класифікації інформації, яку можна обробляти, та внутрішніх систем і сервісів, до яких дозволений доступ особам, що працюють віддалено;

c) забезпечення придатним комунікаційним обладнанням, включаючи методи для безпечного віддаленого доступу;

d) фізичну безпеку;

e) ролі та настанови для доступу родини й відвідувачів до обладнання та інформації;

f) забезпечення підтримки й технічного обслуговування обладнання та програмного забезпечення;

g) забезпечення до страхування;

h) процедури резервного копіювання та безперервності бізнесу;

i) аудит та моніторинг безпеки;

j) скасування повноважень і прав доступу, а також повернення обладнання після припинення віддаленої роботи.

Додаткова інформація

Віддалена робота охоплює всі форми роботи за межами офісу, включаючи нетрадиційне робоче середовище, таке як «віддалений зв'язок», «гнучке робоче місце», «дистанційна робота» та «віртуальна робота».

7 БЕЗПЕКА ЛЮДСЬКИХ РЕСУРСІВ

7.1 Перед наймом

Ціль: Гарантувати, що найманий персонал та підрядники розуміють свої обов'язки, придатні до ролей, на які претендують.

7.1.1 *Ретельна перевірка*

Заходи безпеки

Підтверджувальні перевірки біографічних даних усіх кандидатів на найм мають виконуватись згідно з усіма відповідними законами, нормативами та морально-етичними нормами, а також співвідносно до бізнес-вимог, класифікації інформації, до якої потрібен доступ, і усвідомлюваних ризиків.

Настанова щодо впровадження

Підтверджувальні перевірки мають враховувати все відповідне законодавство щодо конфіденційності, захисту персональних ідентифікаційних даних та найму і там, де це дозволено, містити таке:

a) наявність задовільних характеристик, наприклад одної бізнесової і одної особової;

b) перевірку (на повноту й точність) резюме претендентів;

c) підтвердження заявленої освітньої та професійної кваліфікації;

d) незалежну ідентифікаційну перевірку особи (паспорт або аналогічний документ);

e) детальніші перевірки, такі як кредитні або перевірки за кримінальним обліком.

Якщо особу наймають для виконання певної ролі щодо інформаційної безпеки, організація повинна впевнитися, що кандидат:

a) має необхідну компетенцію для виконання ролі щодо безпеки;

b) йому можна довіряти виконувати цю роль, особливо якщо ця роль є критичною для організації.

Там, де на посаду чи в разі початкового призначення, чи в разі підвищення по службі залучають осіб, які матимуть доступ до засобів оброблення інформації, і особливо, якщо вони оброблятимуть інформацію з обмеженим доступом, наприклад фінансову чи конфіденційну інформацію, організація повинна передбачити також і подальші детальніші перевірки.

Процедури мають визначати критерії та обмеження для підтверджувальних перевірок, наприклад, хто має право ретельно перевіряти людей і як, коли й чому підтверджувальні перевірки проводять.

Процес ретельної перевірки потрібно також проводити для підрядників. Тоді угода між організацією та підрядником має чітко визначати обов'язки щодо проведення ретельної перевірки й процедури сповіщення, яких вона повинна дотримуватися, якщо ретельну перевірку не було завершено або якщо результати викликають сумнів або занепокоєння.

Інформація щодо всіх кандидатів, яких розглядають на посади в організації, потрібно збирати й обробляти згідно з відповідним законодавством, чинним у відповідній юрисдикції. Залежно від чинного законодавства кандидати повинні бути наперед поінформовані щодо діяльності з ретельної перевірки.

7.1.2 *Терміни та умови найму*

Заходи безпеки

Контрактна угода з найманим персоналом та підрядниками повинна встановити взаємні відповідальності щодо інформаційної безпеки.

Настанова щодо впровадження

У контрактних обов'язках для найманого персоналу та підрядників має бути відображено політику безпеки організації, а також роз'яснено та встановлено:

a) що весь найманий персонал та підрядники, яким надано доступ до інформації з обмеженим доступом, повинні підписати угоду щодо конфіденційності або нерозголошення до надання доступу до засобів оброблення інформації;

b) правову відповідальність і права найманого персоналу та підрядників, наприклад, стосовно законів про авторське право чи законодавства про захист даних (див. також 18.1.2 і 18.1.4);

c) відповідальності за класифікацію інформації та управління інформацією організації, іншими ресурсами СУІБ організації, пов'язаними з інформацією, засобами оброблення інформації та інформаційними послугами, з якими має справу найманий персонал та підрядники (див. також розділ 8);

d) відповідальності найманого персоналу чи підрядників за оброблення інформації, отриманої від інших компаній або зовнішніх сторін;

e) дії, яких треба вжити, якщо найманий персонал чи підрядник нехтує вимогами щодо безпеки організації (див. також 7.2.3).

Ролі та обов'язки стосовно інформаційної безпеки має бути доведено кандидатам на найм протягом процесу до найму.

Організація повинна впевнитися, що найманий персонал та підрядники згодні з термінами та умовами щодо інформаційної безпеки, які відповідають виду та ступеню доступу, який вони матимуть до ресурсів СУІБ організації, пов'язаних з інформаційними системами та послугами.

Там, де це потрібно, відповідальність, яка є в термінах та умовах найму, потрібно розповсюджувати на визначений період після закінчення найму (див. також 7.3).

Додаткова інформація

Можна застосувати кодекс поведінки, щоб охопити відповідальності найманого персоналу та підрядників стосовно конфіденційності, захисту даних, етики, належного використання обладнання та засобів організації, а також гідні поваги правила поведінки, очікувані організацією. Від зовнішньої сторони, з якою підрядники можуть бути пов'язані, можна вимагати вступ у контрактні угоди від імені контрактної особи.

7.2 Протягом найму

Ціль: Впевнитися, що весь найманий персонал та підрядники усвідомлюють і виконують свої обов'язки з інформаційної безпеки.

7.2.1 *Відповідальність керівництва*

Заходи безпеки

Керівництво повинно вимагати від найманого персоналу та підрядників застосування заходів безпеки згідно з установленими в організації політиками та процедурами.

Настанова щодо впровадження

Керівництво повинно нести відповідальність за забезпечення того, щоб найманий персонал та підрядники:

a) належним чином були ознайомлені зі своїми ролями щодо інформаційної безпеки та обов'язками перед наданням доступу до інформації з обмеженим доступом або інформаційних систем;

b) були забезпечені настановами для встановлення в організації очікуваної безпеки для їхніх ролей;

c) були мотивовані на виконання політики безпеки організації;

Національна примітка

Мотивація на виконання політики безпеки охоплює: усвідомлення важливості дотримання процедур, інструкцій, настанов тощо, розуміння своїх обов'язків та відповідальностей і наслідків невідповідних дій чи зловживань інформацією або засобами оброблення інформації організації, до яких надано доступ, а також знання дисциплінарного процесу і впевненість, що своєчасні попередження про інциденти інформаційної безпеки чи власні ненавмисні порушення безпеки й виконання передбачених для цих випадків дій призведе до менших втрат для організації та наслідків для особи, що їх спричинила.

d) досягли рівня поінформованості щодо безпеки, який відповідає їх ролям та обов'язкам в організації;

e) задовольняють терміни та умови найму, що охоплюють політику інформаційної безпеки організації та відповідні методи роботи;

f) підтримують належні навички та кваліфікацію на відповідному рівні;

g) забезпечені анонімним каналом інформування для доповіді про порушення політики чи процедур інформаційної безпеки («сигнал щодо незаконної діяльності»).

Керівництво повинно демонструвати підтримку політик, процедур і заходів інформаційної безпеки й діяти відповідно до ролевої моделі.

Додаткова інформація

Якщо найманий персонал та підрядники не ознайомлені щодо їхніх обов'язків щодо інформаційної безпеки, вони можуть спричинити значну шкоду організації. Мотивований персонал імовірніше буде більш надійним і спричинятиме меншу кількість інцидентів інформаційної безпеки.

Незадовільне управління може викликати у персоналу недооцінення, що призводить до негативних впливів на інформаційну безпеку організації. Наприклад, незадовільне управління може призвести до нехтування інформаційною безпекою чи потенційного зловживання ресурсами СУІБ організації.

7.2.2 *Поінформованість, освіта й навчання щодо інформаційної безпеки*

Заходи безпеки

Увесь найманий персонал організації, а там, де це суттєво, і підрядники повинні одержати належне навчання й тренінги для поінформованості та регулярно отримувати оновлені дані щодо політик і процедур організації, суттєвих для їх посадових функцій.

Настанова щодо впровадження

Програма навчання з питань інформаційної безпеки має бути спрямована на поінформованість найманого персоналу, а там, де це суттєво, підрядників, їх відповідальностям з питань інформаційної безпеки і заходів, за допомогою яких ці відповідальності відміняють.

Програму поінформованості з питань інформаційної безпеки потрібно розробляти відповідно до політик і відповідних процедур інформаційної безпеки організації, беручи до уваги інформацію організації, яка потребує захисту, і заходи безпеки, які потрібно використовувати для захисту інформації. Програма поінформованості має включати ряд дій, які підвищують поінформованість, як наприклад кампаній (наприклад, «день інформаційної безпеки») і друкованих буклетів або інформаційних листів.

Програму поінформованості потрібно планувати з розглядом ролей найманого персоналу в організації, а там, де це суттєво, очікуваннями організації стосовно поінформованості підрядників. Діяльність у програмі поінформованості має бути спроектовано в часі, бажано регулярно, щоб діяльність повторювалась і охоплювала новий найманий персонал та підрядників. Програму поінформованості також потрібно регулярно поновлювати, щоб вона постійно відповідала політикам і процедурам організації, і була побудована на уроках, отриманих від інцидентів інформаційної безпеки.

Тренінги з поінформованості потрібно проводити відповідно до вимог програми поінформованості з питань інформаційної безпеки організації. Тренінги поінформованості можуть використовувати різні середовища інформування, зокрема й навчання в класах, дистанційне навчання, веб-навчання, самонавчання тощо.

Навчання й тренінги з питань інформаційної безпеки повинні охоплювати загальні аспекти, такі як:

a) визначення обов'язків керівництва до інформаційної безпеки в організації;

b) необхідність ознайомлення та відповідності ролям і обов'язкам з інформаційної безпеки, як це визначено в політиках, стандартах, законах, регуляторних актах, контрактах і угодах;

c) персональна відповідальність за власні дії чи бездіяльність особи, та загальні обов'язки стосовно безпеки чи захисту інформації, яка належить організації та зовнішнім сторонам;

d) базові процедури інформаційної безпеки (такі, як звітування про інцидент інформаційної безпеки) і базові заходи безпеки (такі, як безпека паролів, антивірусні заходи й політика чистого стола);

e) точки контактів і ресурси для отримання додаткової інформації та консультацій стосовно інформаційної безпеки, включаючи подальші матеріали навчання й тренінгів з питань інформаційної безпеки.

Навчання й тренінги з питань інформаційної безпеки потрібно проводити періодично. Початкові навчання й тренінги застосовують для тих, кого переводять на нову посаду чи роль із суттєво іншими вимогами щодо інформаційної безпеки, і їх потрібно проводити перед тим, як ця роль стає активною.

Організація повинна розробляти програми навчання й тренінгу так, щоб проводити навчання й тренінги ефективно. Програма має відповідати чинним політикам і відповідним процедурам інформаційної безпеки організації, беручи до уваги інформацію організації, яка потребує захисту, і заходи безпеки, які потрібно використовувати для захисту інформації.

Додаткова інформація

Під час розроблення програми поінформованості важливо звертати увагу не лише на «що» і «як», а також «чому». Важливо, щоб найманий персонал розумів ціль інформаційної безпеки і потенційний вплив, позитивний і негативний, їх власної поведінки на організацію.

Поінформованість, навчання й тренінги можуть бути частиною інших тренінгів або їх проводять разом з ними, наприклад загальний тренінг щодо інформаційних техологій чи безпеки. Поінформованість щодо безпеки, освіта та навчання мають відповідати займаній ролі, відповідальності й навичкам особи.

Наприкінці курсу поінформування, навчання й тренінгу потрібно проводити оцінювання розуміння питань щодо інформаційної безпеки для тестування отриманих знань.

7.2.3 *Дисциплінарний процес*

Заходи безпеки

Має існувати формальний та офіційно оформлений дисциплінарний процес щодо найманого персоналу, який порушив інформаційну безпеку.

Настанова щодо впровадження

Дисциплінарний процес не потрібно розпочинати без попереднього підтвердження того, що порушення безпеки сталося (див. 16.1.7).

Офіційно оформлений дисциплінарний процес має забезпечувати коректний та справедливий розгляд справи найманого персоналу, якого підозрюють у вчиненні порушень безпеки. Офіційно оформлений дисциплінарний процес має забезпечувати диференційоване реагування, де враховано такі чинники: сутність і тяжкість порушення та його вплив на бізнес, чи це є перше чи повторне правопорушення, чи проходив порушник належне навчання, відповідне законодавство, бізнес-контракти, а також інші необхідні чинники.

Дисциплінарний процес треба також використовувати як запобіжний захід для утримання найманого персоналу від порушень політик і процедур інформаційної безпеки організації та будь-яких інших порушень інформаційної безпеки. Навмисне порушення може потребувати невідкладних дій.

Додаткова інформація

Дисциплінарний процес має також стати мотивацією або спонуканням, якщо визначено позитивні заохочення для зразкової поведінки відносно інформаційної безпеки.

7.3 Припинення чи зміна умов найму

Ціль: Захистити інтереси організації як частини процесу зміни умов чи припинення найму.

7.3.1 *Припинення чи зміна відповідальностей*

Заходи безпеки

Має бути чітко визначено, доведено до найманого персоналу чи підрядників і встановлено відповідальності за інформаційну безпеку та обов'язки, які залишаються дійсними після припинення чи зміни умов найму.

Настанова щодо впровадження

У разі припинення відповідальностей потрібно доводити до відома вимоги щодо безпеки та правову відповідальність, що продовжують діяти, і за потреби, відповідальності, які є в будь-якій угоді щодо конфіденційності (див. 13.2.4), терміни й умови найму (див. 7.1.2), продовжені на визначений період після звільнення найманого персоналу чи підрядника.

Відповідальності та обов'язки, чинні після припинення найму, мають бути в контрактах найманого персоналу чи підрядника (див. 7.1.2).

Змінами відповідальності чи умов найму треба управляти припиненням передбаченої відповідальності чи найму разом з ініціацією нових відповідальностей або умов найму.

Додаткова інформація

Зазвичай відділ кадрів є відповідальним за весь процес припинення найму і для управління аспектами інформаційної безпеки відповідних процедур співпрацює з безпосереднім керівником особи, що звільняється. Якщо це підрядник, найманий через зовнішню сторону, цей процес припинення відповідальності може виконувати зовнішня сторона відповідно до контракту між організацією і зовнішньою стороною.

Може виникнути необхідність повідомляти найманий персонал, клієнтів або підрядників про зміни персоналу та операційного середовища.

8 УПРАВЛІННЯ РЕСУРСАМИ СУІБ

8.1 Відповідальність за ресурси СУІБ

Ціль: Ідентифікувати ресурси СУІБ організації і визначити відповідні обов'язки щодо їх захисту.

8.1.1 *Інвентаризація ресурсів СУІБ*

Заходи безпеки

Інформація, ресурси СУІБ, пов'язані з інформацією та обладнанням для обробки інформації, мають бути ідентифіковані та має підтримуватися їх актуальний інвентарний опис.

Настанова щодо впровадження

Організація повинна ідентифікувати ресурси СУІБ відповідно до життєвого циклу інформації та задокументувати їх важливість. Життєвий цикл інформації має охоплювати створення, оброблення, передавання, вилучення та знищення. Документацію потрібно підтримувати належним чином у вигляді написів або наявних інвентарних описів.

Інвентарний опис ресурсів СУІБ має бути акуратним, відповідати часу, бути сумісним і узгодженим з іншими інвентарними описами.

Для кожного ідентифікованого ресурсу СУІБ повинні бути погоджені та задокументовані власник ресурсу СУІБ (див. 8.1.2) та класифікація інформації (див. 8.2).

Додаткова інформація

Інвентарні описи ресурсів СУІБ допомагають забезпечити наявність ефективного захисту ресурсів СУІБ і також можуть бути потрібними для інших бізнес-цілей, таких як здоров'я та безпека, страхові або фінансові (управління ресурсами СУІБ) причини.

ISO/IEC 27005 [11] надає приклади ресурсів СУІБ, які необхідно враховувати організації під час ідентифікації ресурсів СУІБ. Процес складання інвентарного опису ресурсів СУІБ є важливою передумовою управління ризиками (див. також ISO/IEC 27000 та ISO/IEC 27005 [11]).

8.1.2 *Володіння ресурсами СУІБ*

Заходи безпеки

Ресурси СУІБ, наявні в інвентарному описі, мають «бути у власності».

Національна примітка

Термін «власник» ідентифікує особу чи організацію, для якої встановлено затверджену керівництвом відповідальність щодо контролювання виробництва, розвитку, підтримування, використання та безпеки ресурсів СУІБ. Термін «власник» не означає, що особа дійсно має право власності на ресурс СУІБ.

Настанова щодо впровадження

Особу або іншу штатну одиницю, призначену керівництвом відповідальною за придатність ресурсу СУІБ протягом життєвого циклу, розглядають як власника ресурсу СУІБ.

Зазвичай використовують процес своєчасного призначення власників ресурсу СУІБ. Власник повинен бути призначений, коли ресурси СУІБ створюють або коли ресурси передають в організацію. Власник ресурсу СУІБ повинен бути відповідальним за відповідне управління ресурсом протягом всього його життєвого циклу.

Власник ресурсів СУІБ повинен:

a) гарантувати, що ресурси СУІБ інвентаризовані;

b) гарантувати, що ресурси СУІБ відповідним чином класифіковані та захищені;

c) визначити й періодично переглядати обмеження доступу та класифікацію для важливих ресурсів СУІБ, беручи до уваги політики контролю доступу, які використовують;

d) гарантувати належне оброблення в разі вилучення або знищення ресурсів СУІБ.

Додаткова інформація

Ідентифікованим власником може бути особа чи штатна одиниця (підрозділ), на яку керівництвом покладено відповідальність контролю ресурсу СУІБ протягом всього його життєвого циклу. Ідентифікований власник не обов'язково може мати право власності на цей ресурс СУІБ.

Повсякденні завдання можуть бути делеговані, наприклад, куратору, який щоденно наглядає за ресурсом СУІБ, проте відповідальність залишається за власником.

У разі складних інформаційних систем може бути корисним призначити групи ресурсів СУІБ, які діють разом для надання окремої функції, такої як «послуги». У цьому разі власник послуги є відповідальним за постачання послуги, зокрема за функціонування ресурсів СУІБ, які її надають.

8.1.3 *Припустиме використання ресурсів СУІБ*

Заходи безпеки

Правила щодо припустимого використання інформації та ресурсів СУІБ, пов'язаних із засобами оброблення інформації, мають бути ідентифіковані, задокументовані та впроваджені.

Настанова щодо впровадження

Весь найманий персонал та користувачі зовнішньої сторони, які використовують чи мають доступ до ресурсів СУІБ організації, повинні бути поінформовані стосовно вимог щодо інформаційної безпеки до інформації, ресурсів СУІБ організації, пов'язаних з інформацією, ресурсами та обладнанням оброблення інформації. Вони повинні бути відповідальними за використання ними будь-яких ресурсів оброблення інформації і будь-яке таке використання здійснюють під їх відповідальністю.

8.1.4 *Повернення ресурсів СУІБ*

Заходи безпеки

Увесь найманий персонал та користувачі зовнішньої сторони повинні повернути всі ресурси СУІБ організації, що перебувають у їх володінні, після припинення їх найму, контракту чи угоди.

Настанова щодо впровадження

Офіційно оформлений процес припинення найму повинен охоплювати повернення всіх раніше виданих фізичних та електронних ресурсів СУІБ, власниками яких вони були чи які використовували в організації.

Якщо найманий персонал чи користувачі зовнішньої сторони купують обладнання, що належить організації, або використовують своє власне персональне обладнання, треба слідувати процедурам, які гарантують, що всю важливу інформацію передають організації і надійно видаляють з обладнання (див. також 11.2.7).

Коли найманий персонал або користувачі зовнішньої сторони мають відомості, важливі для подальшого функціонування організації, цю інформацію (наприклад, інтелектуальну власність) має бути задокументовано й передано організації.

8.2 Класифікація інформації

Ціль: Забезпечити належний рівень захисту інформації відповідно до її важливості для організації.

8.2.1 *Класифікація інформації*

Заходи безпеки

Інформація має бути класифікована в термінах правових вимог, її цінності, критичності й чутливості для неавторизованого розкриття чи модифікації.

Настанова щодо впровадження

Класифікація та пов'язані з нею заходи безпеки щодо інформації мають брати до уваги бізнес-потреби, які стосуються спільного використання чи обмеження інформації, а також вимоги законодавства. Ресурси СУІБ, крім інформації, можуть бути також класифікованими відповідно до класифікації інформації, яку зберігають, обробляють або іншим чином управляють нею, чи захищають за допомогою цього ресурсу СУІБ.

Власники інформаційних ресурсів СУІБ повинні бути відповідальними за їх класифікацію.

Схема класифікації має містити домовленості щодо первинної класифікації та критерії для перегляду класифікації через певний час. Рівень захисту на схемі має бути визначеним за допомогою аналізу конфіденційності, цілісності й доступності та будь-яких інших вимог для інформації, яку розглядають. Схему треба погоджувати з політикою контролю доступу (див. 9.1.1).

Кожен рівень має отримати ім'я, яке має сенс у контексті використання схеми класифікації.

Схема має бути сумісною всередині всієї організації так, щоб будь-хто, хто буде класифікувати інформацію і відповідні ресурси СУІБ подібним чином, мав загальне розуміння вимог щодо захисту і використовував відповідний захист.

Класифікація має бути долученою до процесів організації і бути сумісною та однаковою всередині організації. Результати класифікації мають показати цінність ресурсів СУІБ відповідно до їх чутливості й критичності в організації, наприклад в термінах конфіденційності, цілісності й доступності. Результати класифікації потрібно оновлювати відповідно до змін їхніх цінності, чутливості й критичності протягом їхнього життєвого циклу.

Додаткова інформація

Класифікація показує людям, які працюють з інформацією з певною позначкою, як обробляти й захищати її. Створення груп інформації з подібними потребами захисту та визначення процедур інформаційної безпеки, які відносять до всієї інформації в кожній групі, полегшує це завдання. Такий підхід зменшує потреби виконання оцінювання ризиків і розроблення заходів безпеки для користувачів кожного разу.

Інформація може переставати бути конфіденційною або критичною після певного періоду часу, наприклад після того, як інформація стає загальнодоступною. Ці аспекти треба брати до уваги, оскільки надмірна класифікація може призвести до впровадження непотрібних заходів безпеки, наслідком яких будуть додаткові витрати чи навпаки надмірна класифікація може наражати на небезпеку досягнення цілей бізнесу.

Приклад схеми класифікації конфіденційності інформації може базуватися на чотирьох рівнях, як показано далі:

a) розкриття не нанесе шкоди;

b) розкриття призведе до мінімальної шкоди або мінімальних операційних незручностей;

c) розкриття має значний короткочасний вплив на операцію або тактичні цілі;

d) розкриття має великий вплив на довгострокові стратегічні цілі або призводить до виживання організації з ризиком.

8.2.2 *Маркування інформації*

Заходи безпеки

Має бути розроблено та впроваджено належну множину процедур для маркування й оброблення інформації згідно зі схемою класифікації, прийнятою організацією.

Настанова щодо впровадження

Необхідно, щоб процедури маркування інформації поширювалися на інформацію та пов'язані з нею ресурси СУІБ в матеріальному та електронному вигляді. Маркування має відображати схему класифікації, визначену у 8.2.1. Позначки маркування мають легко розпізнаватися. Процедури повинні надавати настанови про те, де і яким чином позначки має бути встановлено, беручи до уваги, яким чином здійснюють доступ до інформації чи обробляють ресурсами СУІБ залежно від типів середовища. У процедурах має бути визначено випадки, коли позначки маркування не застосовують, наприклад маркування не конфіденційної інформації для зменшення робочих загрузок. Найманий персонал та підрядники повинні бути поінформованими стосовно процедур маркування.

Вихідні дані систем, що містять інформацію, яку класифіковано як чутливу або критичну, мають підтримувати відповідні позначки класифікації.

Додаткова інформація

Маркування класифікованої інформації є ключовою вимогою угод щодо спільного використання інформації. Фізичні позначки та метадані є загальноприйнятою формою маркування.

Маркування інформації і пов'язаних з нею ресурсів СУІБ іноді може мати негативні наслідки. Класифіковані ресурси СУІБ простіше ідентифікувати і відповідно атакувати інсайдерами або зовнішніми хакерами.

8.2.3 *Поводження з ресурсами СУІБ*

Заходи безпеки

Має бути розроблено та впроваджено процедури поводження з ресурсами СУІБ відповідно до схеми класифікації інформації, яку офіційно прийнято в організації.

Настанова щодо впровадження

Має бути розроблено процедури поводження, оброблення, збереження та доведення до відома інформації відповідно до її класифікації (див. 8.2.1).

Треба розглянути наведені нижче елементи:

a) обмеження доступу, яке підтримує вимоги щодо захисту інформації для кожного рівня класифікації;

b) підтримування офіційно оформленого реєстру санкціонованих одержувачів ресурсів СУІБ;

c) захист тимчасових чи постійних копій інформації на рівні, який відповідає захисту первинної інформації;

d) зберігання ІТ-ресурсів СУІБ відповідно до специфікацій виробника;

e) чітке маркування всіх копій носіїв до уваги санкціонованого одержувача.

Схема класифікації, яку використовують всередині організації, може не суміщатися зі схемою, яку використовують в інших організаціях, навіть якщо імена рівнів подібні; крім того, інформація, що переміщується між організаціями, може змінюватися в класифікації залежно від її контексту в кожній організації, навіть якщо їх схеми класифікації однакові.

Угоди з іншими організаціями, які містять спільне використання інформації, мають описувати процедури для ідентифікації класифікації такої інформації і для інтерпретації рівнів класифікації від іншої організації.

8.3 Поводження з носіями

Ціль: Запобігти несанкціонованому розголошенню, модифікації, вилученню або знищенню інформації, яка зберігається на носіях.

8.3.1 *Управління змінними носіями*

Заходи безпеки

Має бути впроваджено процедури управління змінними носіями відповідно до схеми класифікації, запровадженої в організації.

Настанова щодо впровадження

Треба розглянути наведені нижче настанови щодо управління змінними носіями:

a) інформація, якщо вона більше не потрібна, що міститься на будь-яких носіях багаторазового використання, які має бути видалено з організації, має бути зроблена невідновлюваною;

b) там, де необхідно й доцільно, потрібна авторизація для носіїв, які вилучають з організації, і записи про такі вилучення треба зберігати для підтримки журналу аудиту;

c) усі носії потрібно зберігати в надійному, безпечному середовищі згідно зі специфікаціями виробника;

d) якщо конфіденційність і цілісність даних є важливими, потрібно використовувати криптографічні методи для захисту даних на змінних носіях;

e) щоб уникнути ризику псування носія, коли збережені дані залишаються потрібними, ці дані має бути перенесено на свіжий носій до того, як їх не можна буде прочитати;

f) численні копії цінних даних потрібно зберігати на окремих носіях для подальшого зменшення ризику ушкодження чи втрати відповідних даних за рахунок співпадіння носія їх зберігання;

g) треба розглянути реєстрацію змінних носіїв для обмеження можливості втрати даних;

h) треба використовувати дисководи змінних носіїв лише тоді, коли для цього є бізнес-причина;

i) якщо необхідно використовувати змінні носії, перенос інформації на такі носії має підлягати моніторингу.

Усі процедури та рівні санкціонованого доступу має бути чітко задокументовано.

8.3.2 *Вилучення носіїв*

Заходи безпеки

Коли носії більше не потрібні, їх треба безпечно вилучати із застосуванням офіційно оформлених процедур.

Настанова щодо впровадження

Офіційно оформлені процедури безпечного вилучення носіїв має бути визначено для того, щоб мінімізувати ризик витоку конфіденційної інформації до осіб, які не мають санкцій. Процедури безпечного вилучення носіїв, які містять інформацію з обмеженим доступом, мають бути сумірними з конфіденційністю інформації. Треба розглянути наведені нижче елементи:

a) носії, що містять інформацію з обмеженим доступом, потрібно зберігати й вилучати безпечно, наприклад спаленням або розрізанням, або стиранням даних перед використанням для іншої прикладної програми в організації;

b) мають бути наявні процедури ідентифікації елементів, які можуть потребувати безпечного вилучення;

c) може бути легше вжити заходів щодо безпечного накопичення та вилучення всіх елементів носіїв, ніж намагатися виділити чутливі елементи;

d) багато організацій пропонує послуги з накопичення та вилучення паперів, обладнання та носіїв; треба подбати про вибір придатного підрядника з відповідними заходами безпеки й досвідом;

e) вилучення чутливих елементів має бути зареєстровано для підтримання журналу аудиту.

У разі накопичування носіїв для вилучення треба розглянути ефект об'єднання, внаслідок якого велика кількість нечутливої інформації може стати чутливою.

Додаткова інформація

Ушкоджене обладнання, яке містить чутливі дані, може потребувати оцінювання ризиків для визначення, чи мають бути ці елементи фізично знищені, чи може бути їх передано для ремонту або вилучення (див. 11.2.7).

8.3.3 *Фізичні носії під час передавання*

Заходи безпеки

Носії, що містять інформацію, має бути захищено від несанкціонованого доступу, зловживання чи руйнування під час транспортування.

Настанова щодо впровадження

Для захисту носіїв інформації, які транспортують, треба розглянути наведені нижче настанови:

a) треба використовувати надійний засіб транспортування чи кур'єрів;

b) перелік санкціонованих кур'єрів повинен бути погоджений керівництвом;

c) треба розробити процедури перевірки ідентифікації кур'єрів;

d) упаковка має бути достатньою для захисту вмісту від будь-якого фізичного пошкодження, яке може трапитися протягом транзиту, і відповідати всім специфікаціям виробника, наприклад захисту від будь-яких чинників довкілля, які можуть знизити ефективність поновлення носія, таких як вплив підвищеної температури, вологості або електромагнітних полів;

e) треба зберігати журнали аудиту, які ідентифікують зміст носія, застосований захист разом із записами часу переносу на транзитне збереження та часу отримання отримувачем.

Додаткова інформація

Інформація може бути вразливою до несанкціонованого доступу, зловживання чи руйнування під час фізичного транспортування, наприклад під час відсилання носіїв поштою чи кур'єром. У цьому заході безпеки під носіями розуміють також паперові документи.

Якщо інформацію з обмеженим доступом на носії не зашифровано, треба розглянути додаткові засоби фізичного захисту носія.

9 КОНТРОЛЬ ДОСТУПУ

9.1 Бізнес-вимоги до контролю доступу

Ціль: Обмежити доступ до інформації та засобів оброблення інформації.

9.1.1 *Політика контролю доступу*

Заходи безпеки

Політика контролю доступу має бути розроблена, задокументована та переглядатися на основі вимог бізнесу та інформаційної безпеки.

Настанова щодо впровадження

Власники ресурсів СУІБ повинні визначити відповідні ролі щодо контролю доступу, права доступу та обмеження ролей певних користувачів до їх ресурсів СУІБ разом з детальними і суворими контролями, що відображають пов'язані ризики інформаційної безпеки.

Контролі доступу можуть бути як логічними, так і фізичними (див. розділ 11) і їх треба розглядати разом. Користувачам і постачальникам послуг треба надати чітке положення щодо бізнес-вимог, які мають задовольняти контролі доступу.

Політика повинна брати до уваги наведене нижче:

a) вимоги щодо безпеки до окремих прикладних програм бізнесу;

b) політики щодо поширення інформації та санкціонування, наприклад, потребу знати принципи та рівні інформаційної безпеки і класифікацію інформації (див. 8.2);

c) несуперечливість прав доступу та політик класифікації інформації різних систем та мереж;

d) відповідне законодавство й будь-які контрактні зобов'язання стосовно обмеження доступу до даних чи послуг (див. 18.1);

e) управління правами доступу в розподіленій і об'єднаній в мережу інфраструктурі, яка розпізнає всі типи доступних підключень;

f) відокремлення правил контролю доступу, наприклад запит доступу, санкціонування доступу, адміністрування доступу;

g) вимоги щодо офіційного оформлення санкцій на запити доступу (див. 9.2.1 та 9.2.2);

h) вимоги щодо періодичного перегляду прав доступу (див. 9.2.5);

i) видалення прав доступу (див. 9.2.6);

j) архівація записів усіх значущих подій, пов'язаних з використанням та управлінням ідентифікацією користувачів і таємною інформацією автентифікації;

k) ролі з привілейованими правами доступу (див. 9.2.3).

Додаткова інформація

Під час визначання правил контролю доступу треба приділити увагу:

a) встановленню правил, основаних на передумові «Усе взагалі заборонено, доки явно не дозволено», а не на слабкішому правилі «Усе взагалі дозволено, доки явно не заборонено»;

b) зміні інформаційних позначок (див. 8.2.2), створених автоматично засобами оброблення інформації, і тих, які створюються на розсуд користувача;

c) зміні дозволів для користувачів, створених автоматично інформаційною системою, і тих, що створюються адміністратором;

d) ролі, які потребують спеціального затвердження до введення в дію, і тих, що його не потребують.

Правила контролю доступу потрібно підтримувати офіційно оформленими процедурами (див. 9.2, 9.3, 9.4) і чітко визначеними відповідальностями (див. 6.1.1, 9.3).

Контроль доступу, заснований на ролях, є підходом, який успішно використовує велика кількість організацій для визначення зв'язку між правами доступу та бізнес-ролями.

Два принципи, на яких часто основана політика контролю доступу, такі.

a) Треба знати: надано доступ лише до інформації, необхідної для виконання завдань (різні завдання/ролі означають різну інформацію, що треба знати, тобто різні профілі доступу);

b) Треба використовувати: надано доступ лише до засобів оброблення інформації (IT-обладнання, прикладних програм, процедур, кімнат), потрібних для виконання завдання/роботи/ролі.

9.1.2 *Доступ до мереж та послуг мережі*

Заходи безпеки

Користувачі повинні отримувати доступ до мережі та послуг мережі лише тоді, коли вони були спеціально авторизовані для використання.

Настанова щодо впровадження

Має бути сформульовано політику стосовно використання мереж і послуг мережі. Ця політика має охоплювати:

a) мережі та послуги мережі, до яких дозволено доступ;

b) процедури санкціонування для визначення, кому дозволено доступ і до яких мереж та мережевих послуг;

c) заходи безпеки та процедури управління для захисту доступу до мережевих підключень та послуг мережі;

d) засоби, які використовують для доступу до мереж та послуг мережі (наприклад, використання VPN або бездротових мереж);

e) вимоги стосовно автентифікації користувача для доступу до різних послуг мережі;

f) моніторинг використання послуг мережі.

Політика користування послугами мережі не повинна суперечити політиці контролю доступу (див. 9.1.1).

Додаткова інформація

Несанкціоновані та незахищені підключення до послуг мережі можуть зашкодити всій організації. Такі заходи безпеки є особливо важливими для мережевих підключень до чутливих або критичних прикладних програм бізнесу або до користувачів, розташованих у місцях високого ризику, наприклад загальнодоступних чи зовнішніх зонах, що перебувають поза межами управління та заходів безпеки організації.

9.2 Управління доступом користувача

Ціль: Забезпечити санкціонований доступ користувача і запобігти несанкціонованому доступу до систем та послуг.

9.2.1 *Реєстрація та зняття з реєстрації користувача*

Заходи безпеки

Має бути впроваджено процес реєстрації та зняття з реєстрації для того, щоб була можливість управляти правами доступу.

Настанова щодо впровадження

Процес управління ідентифікаторами (IDs) користувача має включати:

a) використання унікальних ідентифікаторів (IDs), які дають змогу користувачам підключатися і нести відповідальність за свої дії; використання групових ідентифікаторів (IDs) має бути затверджено та задокументовано і бути дозволено лише там, де це необхідно, з причин, обумовлених бізнесом або функціонуванням;

b) негайне блокування чи видалення прав доступу користувачів, які залишили організацію (див. 9.2.6);

c) періодичну перевірку та видалення чи блокування зайвих ідентифікаторів (IDs) користувачів;

d) гарантування, що зайві ідентифікатори (IDs) користувачів не надають іншим користувачам.

Додаткова інформація

Надання або вилучення доступу до інформації чи засобів оброблення інформації звичайно є двоступеневою процедурою:

a) визначення й надання або вилучення ID користувача;

b) надання чи вилучення прав доступу для цього ID користувача (див. 9.2.2).

9.2.2 *Забезпечення доступу користувачів*

Заходи безпеки

Має бути впроваджено формально затверджений процес забезпечення доступу користувачу для надання або вилучення прав доступу для всіх типів користувачів до всіх систем та послуг.

Настанова щодо впровадження

Процес забезпечення доступу користувачу для надання або вилучення прав доступу для визначених IDs користувачів має містити:

a) отримання дозволу від власника інформаційної системи чи послуги для використання інформаційної системи чи послуги (див. заходи безпеки 8.1.2);

b) перевірку, що рівень доступу наданий відповідно до політик доступу (див. 9.1) та погоджений з іншими вимогами, такими як розділення обов'язків (див. 6.1.2);

c) гарантування, що права доступу не активовані (наприклад, сервіс-провайдером) до того, як процедури авторизації буде завершено;

d) підтримка головного журналу прав доступу, наданих ID користувача для доступу до інформаційних систем чи послуг;

e) зміна прав доступу користувачам, які змінили ролі чи роботу та негайне вилучення чи блокування прав доступу користувачам, які звільнилися з організації;

f) періодичний перегляд прав доступу разом із власниками інформаційних систем або послуг (див. 9.2.5).

Додаткова інформація

Треба виконати аналіз для визначення ролей доступу користувачів, основаних на бізнес-вимогах, щоб узагальнити ряд прав доступу в типові профілі доступу користувача. Заявами на доступ та перегляд прав доступу (див. 9.2.4) легше управляти на рівні таких ролей, ніж на рівні окремих прав доступу.

Треба виконати аналіз для долучення пунктів у персональні контракти й контракти про надання послуг, у яких визначено санкції на випадок, якщо будуть спроби несанкціонованого доступу з боку персоналу чи підрядників (див. 7.1.2, 7.2.3, 13.2.4, 15.1.2).

9.2.3 *Управління привілейованими правами доступу*

Заходи безпеки

Призначення та використання привілейованих прав доступу має бути обмежено та контрольовано.

Настанова щодо впровадження

Призначення привілейованих прав доступу потрібно контролювати за допомогою формального процесу санкціонування відповідно до визначеної політики контролю доступу (див. 9.1.1). Має бути розглянуто такі питання:

a) має бути ідентифіковано привілейовані права доступу, пов'язані з кожною системою чи послугою, наприклад операційною системою, системою керування базами даних і кожною прикладною програмою та користувачами, до яких вони потребують призначення доступу;

b) привілейовані права доступу має бути призначено користувачам на основі необхідності використання і основі від-події-до-події згідно з політикою контролю доступу (див. 9.1.1), тобто повноваження призначають на рівні мінімальних вимог їх функціональних ролей;

c) потрібно підтримувати процеси санкціонування та реєстрацію всіх призначених привілейованих ролей. Привілейовані права доступу не потрібно надавати до завершення процесу санкціонування;

d) має бути визначено вимоги для уникнення необхідності надання привілейованих прав доступу;

e) привілейовані права доступу потрібно призначати ідентифікаторам (IDs) користувача, які відрізняються від тих, що використовуються для регулярної бізнес-діяльності. Регулярна бізнес-діяльність не повинна здійснюватися від імені привілейованих ID;

f) компетенцію користувачів з привілейованими правами доступу треба регулярно переглядати для впевненості в тому, що вони відповідають своїм обов'язкам;

g) має бути розроблено та впроваджено спеціальні процедури для уникнення несанкціонованого використання загальних адміністративних IDs користувача згідно з можливостями конфігурації систем;

h) для загальних адміністративних IDs користувача потрібно підтримувати конфіденційність таємної інформації автентифікації під час загального використання (наприклад, часта зміна паролів і одразу, коли привілейований користувач звільняється чи змінює роботу, розповсюджуючи їх між привілейованими користувачами за допомогою відповідних механізмів).

Додаткова інформація

Невідповідне використання повноважень адміністрування системи (будь-яка властивість або засіб інформаційної системи, які дозволяють користувачеві скасувати системні чи прикладні заходи безпеки) може бути головним чинником відмов або порушень систем.

9.2.4 *Управління таємною інформацією автентифікації користувачів*

Заходи безпеки

Облік таємної інформації автентифікації користувачів повинен контролюватися за допомогою офіційно оформленого процесу управління.

Настанова щодо впровадження

Цей процес має містити такі вимоги:

a) від користувачів треба вимагати підписання положення щодо конфіденційного зберігання персональної таємної інформації автентифікації і зберігання групової (загальної) інформації автентифікації винятково серед членів групи; це підписане положення можна розмістити в термінах та умовах найму (див. 7.1.2);

b) якщо від користувачів вимагають підтримки їх власної таємної інформації автентифікації, їм треба спочатку надати безпечну тимчасову таємну інформацію автентифікації, яку їх примушують замінити під час першого використання;

c) має бути визначено процедури верифікації перевірки ідентичності користувача перед наданням нової, заміненої або тимчасової таємної інформації автентифікації;

d) тимчасову таємну інформацію автентифікації потрібно надавати користувачам у безпечний спосіб; треба уникати залучення зовнішніх сторін або використання незахищених (відкритий текст) повідомлень електронної пошти;

e) тимчасова таємна інформація автентифікації має бути унікальною для особи і не повинна бути такою, про яку можна здогадатися;

f) користувачі повинні підтвердити отримання таємної інформації автентифікації;

g) використовувану за замовчуванням таємну інформацію автентифікації постачальника має бути змінено після інсталяції систем або програмного забезпечення.

Додаткова інформація

Паролі є типом таємної інформації автентифікації, який зазвичай використовують, і є загальними засобами верифікації особи користувача. Іншими типами таємної інформації автентифікації користувача є криптографічні ключі та інші дані, які зберігаються на апаратних токенах (наприклад, смарт-картках), які виробляють коди автентифікації.

9.2.5 *Перегляд прав доступу користувача*

Заходи безпеки

Власники ресурсів СУІБ повинні переглядати права доступу користувача через регулярні встановлені інтервали.

Настанова щодо впровадження

Під час перегляду прав доступу потрібно брати до уваги наведені нижче настанови:

a) права доступу користувача потрібно переглядати через суворо дотримувані інтервали часу і після будь-яких змін, таких як підвищення або зниження по службі, або припинення найму (див. розділ 7);

b) права доступу користувача потрібно переглядати та перепризначати у разі переходу з однієї посади на іншу в межах тієї самої організації;

c) санкцію на певні привілейовані права доступу потрібно переглядати через частіші інтервали;

d) призначення привілейованих прав доступу потрібно перевіряти через суворо дотримувані інтервали часу для забезпечення того, щоб не було отримано несанкціонованих привілеїв;

e) зміни до привілейованих облікових записів потрібно реєструвати для періодичного перегляду.

Додаткова інформація

Цей захід безпеки компенсує можливі слабкі місця у разі використання заходів безпеки 9.2.1, 9.2.2 та 9.2.6.

9.2.6 *Вилучення або корекція прав доступу*

Заходи безпеки

Права доступу всього найманого персоналу та користувачів зовнішніх сторін до інформації та засобів оброблення інформації мають вилучатися після припинення найму, контракту чи угоди, або корегуватися після змін.

Настанова щодо впровадження

Після припинення найму права доступу особи до інформації та ресурсів СУІБ, пов'язаних із засобами оброблення інформації та послугами, має бути вилучено чи заблоковано. Потрібно визначити, чи треба видалити права доступу. Зміни умов найму має бути відображено у видаленні всіх

прав доступу, які не затверджено для нових умов найму. Права доступу, які має бути видалено або скориговано, стосуються фізичного та логічного доступу. Вилучення або корекцію може бути зроблено за допомогою вилучення, повторного признання або заміни ключів, ідентифікаційних карток, засобів оброблення інформації або підписки. Будь-яка наявна документація, яка ідентифікує права доступу найманого персоналу та підрядників, має відображати вилучення або корекцію прав доступу. Якщо найманий персонал або користувач зовнішньої сторони, які звільняються, знають паролі облікових записів, які залишаються активними, їх має бути змінено після припинення чи зміни умов найму, договору чи угоди.

Права доступу до інформації та інформаційних ресурсів СУІБ, пов'язаних із засобами оброблення інформації, має бути скорочено або видалено до припинення чи зміни умов найму залежно від зіставляння таких чинників ризику:

a) чи було припинення або зміна умов найму ініційовано найманим персоналом, користувачем зовнішньої сторони чи керівництвом і причини припинення найму;

b) поточні обов'язки найманого персоналу, користувача зовнішньої сторони чи будь-якого іншого користувача;

c) цінність ресурсів СУІБ, які залишаються доступними.

Додаткова інформація

За деяких обставин права доступу можуть розподілятися так, щоб бути доступними більшій кількості людей, ніж найманий персонал, що звільняється, або користувач зовнішньої сторони, наприклад групові ідентифікатори. За таких обставин особи, що звільнилися, повинні бути видалені з усіх списків групового доступу, і має бути вжито заходів, щоб рекомендувати іншому найманому персоналу або користувачам зовнішньої сторони, яких це стосується, далі не використовувати інформацію спільно з особою, що звільнилася.

У разі припинення найму, ініційованого керівництвом, ображений найманий персонал або користувач зовнішньої сторони можуть навмисно зіпсувати інформацію або пошкодити засоби оброблення інформації. У разі відставки людей вони можуть зробити спробу зібрати інформацію для майбутнього використання.

9.3 Відповідальності користувача

Ціль: Зробити користувачів відповідальними за збереження їх інформації автентифікації.

9.3.1 *Використання таємної інформації автентифікації*

Заходи безпеки

Треба вимагати від користувачів додержання визначених в організації практик у використанні таємної інформації автентифікації.

Настанова щодо впровадження

Усіх користувачів треба попередити щодо:

a) збереження конфіденційності таємної інформації автентифікації з гарантією того, що її не розповсюджують до будь-яких інших сторін, зокрема і владних осіб;

b) уникнення зберігання записів (наприклад, на папері, у файлі програмного забезпечення чи в портативному пристрої) таємної інформації автентифікації, доки їх не будуть зберігати безпечно і спосіб збереження не буде затверджено (наприклад, пристрої для паролів);

c) зміни таємної інформації автентифікації кожного разу, коли є якась ознака можливої компрометації системи або пароля;

d) якщо як таємну інформацію автентифікації використовують паролі, вибирати якісні паролі з обґрунтовано мінімальною довжиною, які:

1) легкі для запам'ятовування;
2) не базуються на чомусь, про що будь-хто інший може легко здогадатися чи отримати, використовуючи особисту інформацію, наприклад імена, телефонні номери, дати народження тощо;
3) не уразливі до словникових атак (тобто не складаються зі слів, що є в словниках);
4) не мають послідовності однакових лише цифрових або лише абеткових символів;
5) якщо ці паролі є тимчасовими, їх змінюють під час першого входу до системи;

e) спільно не використовувати індивідуальну таємну інформацію автентифікації користувача;

f) гарантувати відповідний захист паролів, коли паролі використовують як таємну інформацію автентифікації в автоматизованих процедурах реєстрації та зберігають;

g) не використовувати ту саму таємну інформацію автентифікації як пароль для бізнес- і не бізнес-цілей.

Додаткова інформація

Використання Single Sign On (SSO) або інших інструментів управління таємною інформацією автентифікації зменшує кількість таємної інформації автентифікації, яку користувачам треба захистити, і таким чином підвищує ефективність цього заходу безпеки. Однак ці інструменти можуть збільшити вплив розкриття таємної інформації автентифікації.

9.4 Контроль доступу до систем та прикладних програм

Ціль: Запобігти несанкціонованому доступу до систем та прикладних програм.

9.4.1 *Обмеження доступу до інформації*

Заходи безпеки

Доступ до інформації та функцій прикладних систем має бути обмежений відповідно до визначеної політики контролю доступу.

Настанова щодо впровадження

Обмеження доступу мають базуватися на вимогах конкретної прикладної програми бізнесу та відповідати визначеній політиці контролю доступу.

Для підтримки вимог щодо обмеження доступу має бути розглянуто таке:

a) надання меню для контролю доступу до функцій прикладних систем;

b) контроль того, які дані можуть бути доступними для конкретного користувача;

c) контроль прав доступу користувачів, наприклад на зчитування, записування, видалення та виконання;

d) контроль прав доступу інших прикладних програм;

e) обмеження інформації, що міститься у вихідних даних;

f) забезпечення контролю фізичного та логічного доступу для ізоляції чутливих прикладних програм, прикладних даних або систем.

9.4.2 *Процедури безпечного підключення (log-on)*

Заходи безпеки

Доступ до систем та прикладних програм повинен контролюватися процедурою безпечного підключення, коли це визначено політикою контролю доступу.

Настанова щодо впровадження

Має бути вибрано відповідну методику автентифікації для забезпечення потрібної ідентифікації користувача.

Якщо потрібна сувора автентифікація та верифікація ідентичності, потрібно використовувати методики автентифікації, альтернативні паролям, такі як криптографічні засоби, смарт-картки, токени чи біометричні засоби.

Процедуру підключення до системи чи прикладної програми має бути спроектовано так, щоб звести до мінімуму можливість несанкціонованого доступу. Тому процедура підключення має розкривати мінімум інформації щодо системи чи прикладної програми, щоб уникнути надання несанкціонованому користувачу будь-якої непотрібної допомоги. Надійна процедура підключення має:

a) не виводити на екран ідентифікатори системи чи прикладної програми до успішного завершення процесу підключення;

b) виводити на екран загальне попередження, що комп'ютер буде доступним лише користувачу, який має санкцію;

c) не надавати протягом процедури підключення допоміжних повідомлень, які б надавали допомогу несанкціонованому користувачу;

d) підтверджувати інформацію підключення лише після завершення вводу всіх даних. У разі виникнення помилки система не повинна показувати, яка частина даних є коректною чи некоректною;

e) захищати проти спроб несанкціонованого підключення;

f) реєструвати невдалі та успішні спроби;

g) визначати подію безпеки, якщо виявлено потенційні спроби чи вдале порушення заходів безпеки підключення;

h) після завершення успішного підключення виводити на екран наведену нижче інформацію:

1) дату та час попереднього успішного підключення;

2) подробиці всіх невдалих спроб підключення після останнього успішного підключення;

i) не виводити на екран пароль, який вводять;

j) не передавати паролі відкритим текстом через мережу;

k) завершати неактивні сеанси після визначеного періоду неактивності, зокрема в місцях великого ризику, таких як публічні або зовнішні місця за межами управління безпекою організації чи на мобільному обладнанні;

l) обмежувати час підключення для забезпечення додаткової безпеки для прикладних програм з великими ризиками та зменшувати можливість для несанкціонованого доступу.

Додаткова інформація

Паролі є звичайним способом забезпечення ідентифікації та автентифікації, який базується на секреті, відомому лише користувачеві. Того самого може бути досягнуто за допомогою криптографічних засобів і протоколів автентифікації. Суть автентифікації користувача має відповідати класифікації інформації, до якої треба надавати доступ.

Якщо паролі протягом сеансу підключення передають відкритим текстом через мережу, їх може бути перехоплено мережевою програмою спостереження за даними в мережі (Sniffer).

9.4.3 *Система управління паролем*

Заходи безпеки

Системи для управління паролями мають бути інтерактивними і забезпечувати якісні паролі.

Настанова щодо впровадження

Система управління паролем має:

a) змушувати до використання індивідуальних ідентифікаторів користувача (IDs) та паролів для підтримки спостережності;

b) дозволяти користувачам вибирати та змінювати свої власні паролі, а також містити процедуру підтвердження на введення поправок помилкового вводу;

c) змушувати вибирати якісні паролі;

d) примушувати користувачів змінювати їх паролі під час першого підключення;

e) змушувати до регулярної зміни паролів та за потреби;

f) підтримувати запис попередніх паролів користувача і перешкоджати повторному їх використанню;

g) не виводити паролі на екран під час їх введення;

h) зберігати файли паролів окремо від системних даних прикладних програм;

i) зберігати й передавати паролі в захищеній формі.

Додаткова інформація

Деякі прикладні програми потребують, щоб паролі користувача призначала незалежна повноважна структура; у таких випадках пункти b), d) та e) наведеної вище настанови не застосовують. Здебільшого паролі вибирають і підтримують користувачі.

9.4.4 *Використання привілейованих системних утиліт*

Заходи безпеки

Використання програм утиліт, що можуть бути спроможні скасовувати заходи безпеки системи та прикладних програм, має бути обмежено та суворо контрольовано.

Настанова щодо впровадження

Має бути розглянуто наведені нижче настанови щодо використання системних утиліт, що можуть бути спроможні скасовувати заходи безпеки системи та прикладних програм:

a) для системних утиліт використовувати процедури ідентифікації, автентифікації, санкціонування;

b) сегментувати системні утиліти з програмного забезпечення прикладних програм;

c) обмежувати використання системних утиліт найменш можливою кількістю довірених користувачів, які мають на це санкцію (див. 9.2.3);

d) санкціонувати спеціальне використання системних утиліт;

e) обмежувати доступність системних утиліт, наприклад на період санкціонованої зміни;

f) реєструвати всі використання системних утиліт;

g) визначати й документувати рівні санкціонування для системних утиліт;

h) видаляти чи блокувати всі утиліти й системне програмне забезпечення, основані на непотрібному програмному забезпеченні;

і) не робити системні утиліти доступними для користувачів, які мають доступ до прикладних програм у системах, де вимагається розподіл обов'язків.

Додаткова інформація

Більшість комп'ютерних інсталяцій мають одну чи більше системних утиліт, які здатні скасовувати заходи безпеки системи та прикладних програм.

9.4.5 *Контроль доступу до початкових кодів програм*

Заходи безпеки

Доступ до початкових кодів програм має бути обмежено.

Настанова щодо впровадження

Доступ до початкових кодів програм та пов'язаних елементів (таких як проект, специфікації, плани верифікації та плани підтвердження) має бути ретельно контрольованим для запобігання внесенню несанкціонованої функціональності та уникнення ненавмисних змін, а також для підтримання конфіденційності цінної інтелектуальної власності. Для початкових кодів програм цього можна досягти за допомогою контрольованого централізованого зберігання такого коду, краще в бібліотеках початкових програм. У такому разі треба розглянути наведені нижче настанови для контролю доступу до таких бібліотек початкових програм, щоб зменшити можливість руйнування комп'ютерних програм:

а) за можливості, бібліотеки початкових програм не потрібно зберігати в системах, які перебувають в експлуатації;

b) управління початковим кодом програми та бібліотекою початкових програм потрібно здійснювати відповідно до розроблених процедур;

c) допоміжний персонал не повинен мати необмежений доступ до бібліотек початкових програм;

d) оновлення бібліотек початкових програм та пов'язаних елементів і надання джерел програм програмістам потрібно здійснювати лише після отримання відповідної санкції;

e) лістинги програм потрібно зберігати в безпечному середовищі;

f) треба підтримувати журнал аудиту всіх доступів до бібліотек початкових програм;

g) підтримування та копіювання бібліотек початкових програм має бути об'єктом процедур жорсткого контролю змін (див. 14.2.2).

Якщо початковий код програми призначений для опублікування, потрібно розглядати додаткові заходи безпеки для гарантування його цілісності (наприклад, електронний цифровий підпис).

10 КРИПТОГРАФІЯ

10.1 Криптографічні засоби захисту

Ціль: Гарантувати відповідне та ефективне використання криптографії для захисту конфіденційності, автентичності та/або цілісності інформації.

10.1.1 *Політика використання криптографічних засобів*

Заходи безпеки

Має бути розроблено та впроваджено політику використання криптографічних засобів для захисту інформації.

Настанова щодо впровадження

Під час розроблення криптографічної політики треба розглянути викладене нижче:

а) підхід керівництва до використання криптографічних засобів у всій організації, включаючи загальні принципи, згідно з якими бізнес-інформацію потрібно захищати;

b) виходячи з оцінки ризику, має бути ідентифіковано потрібний рівень захисту з урахуванням типу, стійкості та якості необхідного алгоритму шифрування;

c) використання шифрування для захисту інформації, яку транспортують на мобільних або змінних носіях, пристроях або через комунікаційні канали;

d) підхід до управління ключами, зокрема й методи, що стосуються захисту криптографічних ключів та відновлення зашифрованої інформації в разі втрачених, скомпрометованих або ушкоджених ключів;

e) ролі та відповідальності, наприклад, хто є відповідальним за:

1) впровадження політики;

2) управління ключами, включаючи генерацію ключа (див. також 10.1.2);

f) стандарти, які має бути прийнято для ефективного впровадження в усій організації (яке саме рішення використовують для якого саме бізнес-процесу);

g) вплив застосування зашифрованої інформації на заходи безпеки, які залежать від перегляду вмісту (наприклад, виявлення вірусу).

У разі запровадження криптографічної політики організації треба розглянути нормативи та національні обмеження, які можуть застосовуватися до використання криптографічних методів у різних частинах світу, і проблеми транскордонних потоків зашифрованої інформації (див. також 18.1.5).

Криптографічні заходи безпеки можна використовувати для досягнення різних цілей безпеки, наприклад:

a) конфіденційності: використання шифрування інформації для захисту чутливої або критичної інформації, як збереженої, так і тієї, що передається;

b) цілісності/автентичності: використання цифрових підписів або кодів автентифікації повідомлення для захисту автентичності та цілісності збереженої або тієї, що передають, конфіденційної або критичної інформації;

c) неспростовності: використання криптографічних методів для отримання доказів виникнення або не виникнення події або дії;

d) автентифікації: використання криптографічних методів для автентифікації користувачів та інших підключень до системи, які потребують доступу або взаємодії з користувачами системи, входами та ресурсами.

Додаткова інформація

Прийняття рішення щодо того, чи криптографічне рішення є належним, потрібно розглядати як частину більш широкого процесу оцінки ризиків та вибору заходів безпеки. Цю оцінку може потім бути використано для визначення, чи криптографічні засоби є належними, заходи безпеки якого саме типу треба застосувати й для яких цілей і бізнес-процесів.

Політика використання криптографічних засобів є необхідною для максимізації переваг та мінімізації ризиків використання криптографічних методів, а також для уникнення неналежного або некоректного використання.

Треба отримати рекомендації фахівця для ідентифікації відповідних криптографічних засобів для досягнення цілей політики інформаційної безпеки.

10.1.2 *Управління ключами*

Заходи безпеки

Має бути розроблено та впроваджено політику використання, захисту й часу життя криптографічних ключів для всього їх життєвого циклу.

Настанова щодо впровадження

Політика повинна містити вимоги для управління криптографічними ключами протягом усього їх життєвого циклу, охоплюючи генерацію, зберігання, архівування, відновлення, розподіл, виведення з дії та знищення ключів.

Криптографічні алгоритми, довжина ключів та практики використання потрібно вибирати згідно з кращими практиками. Відповідне управління ключами потребує безпечних процесів для генерації, зберігання, архівування, відновлення, розподілу, виведення з дії та знищення криптографічних ключів.

Усі криптографічні ключі має бути захищено від модифікації, втрати та знищення. Крім того, таємні та особисті ключі потребують захисту від несанкціонованого розповсюдження. Обладнання, яке застосовують для генерації, зберігання та архівування ключів, має бути фізично захищено.

Система управління ключами має базуватися на погодженому наборі стандартів, процедур та методів безпеки щодо:

a) генерації ключів для різних криптографічних систем та різних прикладних програм;

b) генерації та отримання сертифікатів відкритих ключів;

c) розподілу ключів серед призначених користувачів, включаючи те, як ключі повинні бути активовані після отримання;

d) зберігання ключів, зокрема й, як користувачі, які мають санкцію, отримують доступ до ключів;

e) заміни чи оновлення ключів, включаючи правила стосовно того, коли ключі потрібно замінювати і як це треба робити;

f) поводження зі скомпрометованими ключами;

g) відкликання ключів, зокрема й те, як ключі має бути скасовано або деактивовано, наприклад, коли ключі скомпрометовано чи коли користувач залишає організацію (у якому випадку ключі мають також бути архівовані);

h) відновлення ключів, які втрачено чи зруйновано;

i) резервного копіювання чи архівування ключів;

j) знищення ключів;

k) реєстрації та аудиту діяльності, пов'язаної з управлінням ключами.

Для зниження ймовірності компрометації, активацію й деактивацію даних для ключів має бути визначено так, щоб ключі можна було застосовувати лише обмежений період часу, визначений відповідно до політики управління ключами.

Додатково до безпечного управління таємним та особистим ключами також має бути розглянуто автентичність відкритих ключів. Такий процес автентифікації можна виконувати з використанням сертифікатів відкритих ключів, які зазвичай випускає повноважна організація із сертифікації, яка має бути визнаною організацією з наявними заходами безпеки та процедурами, придатними для забезпечення необхідного ступеня довіри.

Зміст угод або контрактів щодо рівня послуг зовнішніх постачальників криптографічних послуг, наприклад повноважної організації із сертифікації, має охоплювати питання обов'язків, надійності послуг та часу реагування щодо надання послуг (див. 15.2).

Додаткова інформація

Управління криптографічними ключами є важливим для ефективного використання криптографічних методів. ISO/IEC 11770 [2], [3], [4] надає додаткову інформацію щодо управління ключами.

Криптографічні методи можна також використовувати для захисту криптографічних ключів. Може бути потрібний розгляд процедур для обробки правових запитів на доступ до криптографічних ключів, наприклад, може вимагатися, щоб зашифрована інформація була доступною в незашифрованій формі як доказ у судовій справі.

11 ФІЗИЧНА БЕЗПЕКА ТА БЕЗПЕКА ІНФРАСТРУКТУРИ

11.1 Зони безпеки

Ціль: Запобігти несанкціонованому фізичному доступу, пошкодженню та втручанню в її інформацію та засоби оброблення інформації.

11.1.1 *Периметр фізичної безпеки*

Заходи безпеки

Для захисту зон, що містять конфіденційну або критичну інформацію, чи засоби оброблення інформації, треба визначити та використовувати периметри безпеки.

Настанова щодо впровадження

Щодо периметрів фізичної безпеки треба розглянути та впровадити там, де належно, такі настанови:

a) периметри безпеки має бути чітко визначено, а розміщення та міцність кожного з периметрів має залежати від вимог щодо безпеки ресурсів СУІБ у межах цього периметра та результатів оцінки ризику;

b) периметри будівлі або приміщень, які містять засоби оброблення інформації, мають бути фізично надійними (тобто там не повинно бути проміжків у периметрі чи зон, де легко може статися зламування); зовнішні стіни приміщень мають бути міцної конструкції і всі зовнішні двері має бути відповідним чином захищено від несанкціонованого доступу контрольними механізмами (наприклад, засувами, тривожною сигналізацією, замками тощо); двері та вікна має бути замкнено, коли залишаються без нагляду, також треба передбачити зовнішній захист для вікон, особливо на рівні землі;

c) мають бути наявними зона чергування або інші засоби контролю фізичного доступу до приміщень чи будівлі; доступ до приміщень чи будівель потрібно дозволяти лише персоналу, який отримав санкцію;

d) щоб запобігти несанкціонованому фізичному доступу та псуванню інфраструктури там, де це потрібно, має бути побудовано фізичні бар'єри;

e) усі пожежні двері в периметрі безпеки має бути обладнано тривожною сигналізацією, треба здійснювати їх моніторинг і тестувати разом зі стінами, щоб встановити потрібний рівень опору згідно

з відповідними регіональними, національними та міжнародними стандартами; вони мають безвідмовно функціонувати згідно з місцевими правилами пожежної безпеки;

f) згідно з національними, регіональними або міжнародними стандартами має бути встановлено придатні системи виявлення порушників, їх треба регулярно тестувати щодо охоплення цими системами всіх зовнішніх дверей і доступних вікон; незайняті зони мають постійно бути під охороною тривожної сигналізації; також треба забезпечувати належний захист для інших зон, наприклад кімнат з комп'ютерами та засобами комунікацій;

g) засоби оброблення інформації, якими управляє організація, має бути фізично відокремлено від засобів, якими управляють зовнішні сторони.

Додаткова інформація

Фізичної захищеності можна досягти створенням одного чи більше фізичних бар'єрів навколо службових приміщень і засобів оброблення інформації організації. Використання численних бар'єрів надає додатковий захист, за якого відмова одного бар'єра не означає негайної компрометації безпеки.

Зоною безпеки може бути офіс, що замикається, або кілька кімнат, оточених суцільним внутрішнім бар'єром фізичної безпеки. Для контролю фізичного доступу між зонами з різними вимогами щодо безпеки всередині периметра безпеки можуть бути потрібні додаткові бар'єри та периметри. Особливої уваги щодо безпеки фізичного доступу потребують будівлі, де розташовано різні організації.

Використання фізичних заходів безпеки, особливо для зон безпеки, має бути адаптовано до технічних та економічних можливостей організації, як окрема позиція в оцінюванні ризиків.

11.1.2 *Заходи безпеки фізичного прибуття*

Заходи безпеки

Зони безпеки має бути захищено належними заходами безпеки прибуття, щоб забезпечити, що доступ дозволений лише персоналу, який отримав санкцію.

Настанова щодо впровадження

Треба розглянути наведені нижче настанови:

a) треба записувати дату й час прибуття та відбуття відвідувачів і наглядати за всіма відвідувачами, якщо лише надання їм доступу не було попередньо затверджено; треба надавати доступ лише з урахуванням певних санкціонованих цілей і проводити інструктаж стосовно вимог щодо безпеки зони та процедур на випадок надзвичайних обставин. Ідентифікацію відвідувачів потрібно автентифікувати відповідними засобами;

b) доступ до зон, де зберігають чи обробляють конфіденційну інформацію, має бути обмежено лише авторизованим персоналом за допомогою впровадження відповідних контролів доступу, наприклад впровадження механізму двофакторної автентифікації, таких як картка доступу плюс таємний ПІН (персональний ідентифікаційний номер);

c) треба підтримувати та моніторити безпеку фізичних паперових журналів чи електронних журналів аудиту всіх доступів;

d) треба вимагати, щоб весь найманий персонал, підрядники та користувачі зовнішньої сторони носили певну видиму ідентифікацію і негайно сповіщали персонал служби безпеки, якщо вони зустрічають відвідувачів без супроводу та будь-кого без видимої ідентифікації;

e) персоналу служби підтримки зовнішньої сторони, лише за потреби, має бути надано обмежений доступ до зон безпеки чи засобів оброблення конфіденційної інформації; треба здійснювати санкціонування та моніторинг цього доступу;

f) права доступу до зон безпеки треба регулярно переглядати й актуалізувати, а в разі потреби — відміняти (див. 9.2.5 і 9.2.6).

11.1.3 *Убезпечення офісів, кімнат та обладнання*

Заходи безпеки

Має бути розроблено й застосовано фізичну безпеку офісів, кімнат та обладнання.

Настанова щодо впровадження

Треба розглянути наведені нижче настанови щодо безпеки офісів, кімнат та обладнання:

a) основні засоби має бути розташовано так, щоб уникнути публічного доступу;

b) за можливості, будівлі не повинні привертати уваги і мають мінімально позначати своє призначення, без видимих ознак всередині чи ззовні будівлі, що ідентифікують наявність діяльності щодо оброблення інформації;

c) обладнання має бути розміщено так, щоб конфіденційна інформація або діяльність не були видимими та чутними ззовні. Електромагнітне екранування також потрібно розглядати як доречне;

d) довідники та внутрішні телефонні книжки, які ідентифікують розміщення засобів оброблення конфіденційної інформації, не повинні бути легко доступними для широкого загалу.

11.1.4 ***Захист від зовнішніх та інфраструктурних загроз***

Заходи безпеки

Має бути розроблено та застосовано фізичний захист від пошкодження внаслідок природних катаклізмів, акцій громадської непокори та аварій.

Настанова щодо впровадження

Треба отримати консультацію спеціалістів про те, як уникнути пошкоджень від пожежі, повені, землетрусу, вибуху, акцій громадської непокори та інших форм стихійного чи спричиненого людьми лиха.

11.1.5 ***Робота в зонах безпеки***

Заходи безпеки

Має бути розроблено та застосовано процедури роботи в зонах безпеки.

Настанова щодо впровадження

Треба розглянути наведені нижче настанови:

a) про існування зон безпеки або діяльність у них персонал має бути поінформовано лише в межах необхідних для нього знань;

b) треба уникати роботи в зонах безпеки без нагляду як з причин безпеки, так і для запобігання можливій зловмисній діяльності;

c) незайняті зони безпеки мають бути фізично замкнені і періодично перевірятися;

d) використання фото-, відео-, аудіо- та іншого обладнання для запису, як наприклад, камер у мобільних телефонах, не потрібно дозволяти, доки це не санкціоновано.

Заходи щодо роботи в зонах безпеки включають як заходи безпеки щодо найманого персоналу і користувачів зовнішньої сторони, які працюють у зонах безпеки, так і щодо всієї іншої діяльності, яку здійснюють у зонах безпеки.

11.1.6 ***Зони доставки та відвантаження***

Заходи безпеки

Щоб уникнути несанкціонованого доступу, має бути контрольовано й, за можливості, ізольовано від засобів оброблення інформації точки доступу, такі як зони доставки та відвантаження, а також інші точки, через які особи, доступ яких не санкціоновано, можуть увійти до службових приміщень.

Настанова щодо впровадження

Треба розглянути наведені нижче рекомендації:

a) доступ до зон доставки та відвантаження іззовні будинку має бути обмежено для персоналу, який ідентифікований і повинен мати санкцію на такий доступ;

b) зони доставки та відвантаження має бути спроектовано так, щоб поставки могли бути завантажені й розвантажені без отримання персоналом, який здійснює доставку, доступу до інших частин будівлі;

c) зовнішні двері зони доставки та відвантаження має бути замкнено, коли відчинено внутрішні двері;

d) матеріали, що надходять, повинні обстежувати й перевіряти на наявність вибухівки, хімікатів та інших небезпечних матеріалів до того, як їх буде переміщено із зони доставки та відвантаження;

e) матеріали, що надходять, потрібно реєструвати згідно з процедурою управління ресурсами (див. розділ 8) на вході до приміщення;

f) партії товару, що надходять і відсилаються, має бути, за можливості, фізично розподілено;

g) матеріали, що надходять, потрібно інспектувати на наявність пошкодження під час транспортування. Якщо пошкодження було виявлено, про це треба негайно повідомити персонал служби безпеки.

11.2 Обладнання

Ціль: Запобігти втратам, пошкодженню, крадіжці або компрометації ресурсів СУІБ та перериванню діяльності організації.

11.2.1 ***Розміщення та захист обладнання***

Заходи безпеки

Обладнання має бути розміщено чи захищено так, щоб зменшити ризики інфраструктурних загроз і небезпек та можливого несанкціонованого доступу.

Настанова щодо впровадження

Для захисту обладнання треба розглянути наведені нижче настанови:

a) обладнання має бути розміщено так, щоб мінімізувати непотрібний доступ до робочих зон;

b) засоби оброблення інформації, що обробляють конфіденційні дані, має бути розташовано з осторогою для зниження ризику спостереження інформації особами, які не мають на це санкцій, під час її використання;

c) треба убезпечити засоби зберігання для уникнення несанкціонованого доступу;

d) елементи, що потребують спеціального захисту, має бути ізольовано для зменшення загального рівня необхідного захисту;

e) має бути узгоджено заходи безпеки для мінімізації ризику потенційних фізичних загроз і загроз навколишнього середовища, наприклад крадіжки, вогню, вибухів, диму, води (або відмови постачання води), пилу, вібрації, хімічних впливів, завад електроживлення, комунікаційних завад, електромагнітного випромінювання та вандалізму;

f) має бути розроблено настанови щодо приймання їжі та напоїв, а також паління поблизу засобів оброблення інформації;

g) треба здійснювати моніторинг умов довкілля, таких як температура та вологість, які можуть негативно вплинути на функціонування засобів оброблення інформації;

h) для всіх будівель треба застосовувати захист від блискавки, а до всіх вхідних ліній енергопостачання та комунікацій має бути вбудовано фільтри захисту від блискавки;

i) для обладнання в промисловому оточенні необхідно розглянути застосування спеціальних методів захисту, таких як оболонки на клавіатуру;

j) треба захистити обладнання оброблення конфіденційної інформації для мінімізації ризику витоку інформації внаслідок випромінювання.

11.2.2 *Допоміжні комунальні служби*

Заходи безпеки

Обладнання має бути захищено від аварійних відімкнень живлення та інших порушень, внаслідок аварій засобів життєзабезпечення.

Настанова щодо впровадження

Усі засоби життєзабезпечення (наприклад, електрика, телекомунікації, водопостачання, водовідведення, газ, вентиляція та кондиціювання повітря) мають:

a) відповідати специфікаціям виробника обладнання та вимогам законодавства;

b) регулярно оцінюватися їх потужності для того, щоб відповідати росту бізнесу та вимогам локального законодавства;

c) регулярно оглядатися й тестуватися для забезпечення їх належного функціонування;

d) за потреби, обладнати тривожними сигналами в разі виявлення неправильного функціонування;

e) за потреби, мати кілька фідерів з різними фізичними шляхами.

Аварійне освітлення та комунікації мають бути наявними. Аварійні вимикачі та клапани для відімкнення електроживлення, води, газу та іншого обладнання має бути розміщено поруч з аварійними виходами або кімнатами з обладнанням.

Додаткова інформація

Додаткове резервування для мережевих з'єднань може бути отримано за допомогою різних маршрутів від більш ніж одного провайдера.

11.2.3 *Безпека кабельних мереж*

Заходи безпеки

Силові та телекомунікаційні кабельні мережі передачі даних або підтримки інформаційних послуг має бути захищено від перехоплювання, взаємного впливу чи пошкоджень.

Настанова щодо впровадження

Має бути розглянуто наведені нижче настанови щодо безпеки кабельної мережі:

a) силові й телекомунікаційні лінії у засобах оброблення інформації мають, де можливо, бути уземлені або забезпечені відповідним альтернативним захистом;

b) силові кабелі має бути відокремлено від телекомунікаційних кабелів, щоб запобігти взаємному впливу;

c) кабельну мережу має бути захищено від несанкціонованого перехоплення або пошкодження, наприклад використанням кабелепроводу або уникненням маршрутів через загальнодоступні зони;

d) для важливих або критичних систем необхідно розглянути додаткові заходи безпеки, які охоплюють:

1) використання захищеного кабелепроводу й кімнат або шаф, які замикаються, у точках вимірювання та приєднання зовнішнього провідника;
2) використання електромагнітного екранування для захисту кабелів;
3) введення технічних засобів та фізичних обстежень щодо несанкціонованих пристроїв, приєднаних до кабелів;
4) контрольований доступ до комутаційних панелей та кабельних приміщень.

11.2.4 *Обслуговування обладнання*

Заходи безпеки

Обладнання потрібно правильно обслуговувати, щоб забезпечити його постійну доступність і цілісність.

Настанова щодо впровадження

Треба розглянути наведені нижче настанови щодо обслуговування обладнання:

a) обслуговування обладнання потрібно виконувати відповідно до рекомендованих постачальником специфікацій та періодів обслуговування;

b) ремонт та обслуговування обладнання повинен виконувати лише персонал, який має санкцію на обслуговування;

c) потрібно зберігати записи стосовно всіх очікуваних або фактичних несправностей та всього запобіжного й коригувального обслуговування;

d) планування обслуговування обладнання має передбачати впровадження належних заходів безпеки, беручи до уваги, чи виконує таке обслуговування внутрішній персонал організації, чи зовнішній; за потреби, конфіденційну інформацію потрібно буде вивантажити з обладнання або персонал має бути достатньо проінструктовано;

e) мають задовольнятися всі вимоги, накладені політиками страхування;

f) перед вводом обладнання повторно в експлуатацію після його обслуговування, його має бути перевірено, щоб гарантувати, що це обладнання не було змінено і працює правильно.

11.2.5 *Переміщення майна*

Заходи безпеки

Обладнання, інформацію чи програмне забезпечення не потрібно виносити назовні без попередньої санкції на ці дії.

Настанова щодо впровадження

Треба розглянути наведені нижче настанови:

a) найманий персонал та користувачі зовнішніх сторін, які мають повноваження дозволяти переміщення ресурсів СУІБ назовні, має бути чітко ідентифіковано;

b) має бути встановлено обмеження на термін переміщення обладнання, треба перевірити відповідність йому під час повернення обладнання;

c) там, де це потрібно і передбачено, обладнання має бути зареєстровано як таке, що переміщується, і зареєстровано після повернення;

d) ідентичність, роль та належність до організації будь-кого, хто працює з ресурсами СУІБ або використовує їх, має бути задокументовано і цю документацію повертають разом з обладнанням, інформацією чи програмним забезпеченням.

Додаткова інформація

Вибіркові перевірки, вжиті для виявлення несанкціонованого переміщення майна, можна також виконувати для виявлення несанкціонованих пристроїв записування, зброї тощо і запобігання внесенню їх в організацію. Такі вибіркові перевірки потрібно виконувати відповідно до законодавства та нормативів. Осіб має бути поінформовано щодо проведення вибіркових перевірок, і перевірки потрібно виконувати лише за санкцією, якої вимагає законодавство та нормативи.

11.2.6 *Безпека обладнання та ресурсів СУІБ поза службовими приміщеннями*

Заходи безпеки

До ресурсів СУІБ поза службовими приміщеннями має бути застосовний захист з урахуванням різних ризиків роботи поза службовими приміщеннями організації.

Настанова щодо впровадження

Незалежно від власника, використання будь-якого обладнання збереження та оброблення інформації поза приміщеннями організації має бути санкціоновано керівництвом. Це застосовують для обладнання, яке є власністю організації, і до такого обладнання, яке перебуває в приватній власності та його використовують на користь організації.

Для захисту обладнання поза приміщеннями організації треба розглянути наведені нижче настанови:

a) обладнання та носії, винесені зі службових приміщень організації, не повинні залишатися без нагляду в загальнодоступних місцях;

b) завжди треба дотримуватися інструкцій виробника щодо захисту обладнання, наприклад захисту від впливу сильних електромагнітних полів;

c) заходи безпеки для місць поза приміщеннями організації, таких як роботи вдома, віддаленої роботи й тимчасових місць перебування потрібно визначати за допомогою оцінки ризиків і відповідні заходи безпеки потрібно застосовувати належним чином, наприклад шафи для документів, що замикаються, політика чистого стола, контролі доступу до комп'ютерів і безпечні комунікації з офісом (див. також ISO/IEC 27033 [15], [16], [17], [18], [19]);

d) якщо обладнання поза приміщеннями організації передається між різними особами чи зовнішніми сторонами, потрібно підтримувати журнал аудиту, у якому визначено послідовність передавання між утримувачами обладнання, зокрема й хоча б прізвище та організації, що відповідали за це обладнання.

Ризики безпеки, наприклад, пошкодження, крадіжки або підслуховування, можуть суттєво відрізнятися залежно від місцезнаходження, їх треба брати до уваги під час визначання найбільш придатних заходів безпеки.

Додаткова інформація

Обладнання збереження та оброблення інформації охоплює всі види персональних комп'ютерів, органайзерів, мобільних телефонів, смарт-карт, паперу тощо, які тримають для роботи вдома чи виносять зі звичайного місця роботи.

Більше інформації щодо інших аспектів захисту мобільного обладнання можна знайти в 6.2.

Може бути доцільним для зменшення ризиків заборонити певним працівникам працювати поза приміщеннями організації чи обмежити використання ними портативного IT-обладнання.

11.2.7 *Безпечне вилучення або повторне використання обладнання*

Заходи безпеки

Усі елементи обладнання, які містять носії пам'яті, має бути перевірено для забезпечення того, що будь-які конфіденційні дані або ліцензійне програмне забезпечення було видалено чи безпечним чином перезаписано до вилучення або повторного використання.

Настанова щодо впровадження

Обладнання має бути перевірено для того, щоб впевнитися, чи містять носії пам'яті інформацію перед вилученням або повторним використанням.

Пристрої, які містять конфіденційну або ліцензійну інформацію, мають бути фізично зруйновані або інформацію має бути зруйновано, видалено чи перезаписано з використанням методів, які забезпечують, щоб початкову інформацію не можна було відновити, а не з використанням стандартних функцій видалення чи форматування.

Додаткова інформація

Пошкоджені пристрої, що містять конфіденційні дані, можуть потребувати оцінки ризику для визначення, що краще: фізично зруйнувати елементи чи надіслати в ремонт або списати. Інформацію може бути скомпрометовано внаслідок недбалого вилучення або повторного використання обладнання.

Додатково до безпечного знищення інформації на диску шифрування всього диска зменшує ризик розкриття конфіденційної інформації, коли обладнання вилучено або його повторно використовують за умови, що:

a) процес шифрування є досить стійким та шифрування охоплює весь диск (зокрема й незаповнені місця, файли підкачування тощо);

b) ключі шифрування мають довжину, достатню для запобігання атак злому;

c) самі ключі шифрування зберігаються конфіденційно (наприклад, їх ніколи не зберігають на тому самому диску).

Для подальшого аналізу шифрування див. розділ 10.

Методи для безпечного перезаписування носіїв зберігання інформації відрізняються відповідно до технології зберігання інформації на носіях. Треба проаналізувати інструменти перезаписування для того, щоб упевнитися, що вони придатні для носіїв зберігання інформації, що їх використовують.

11.2.8 ***Обладнання користувачів, залишене без нагляду***

Заходи безпеки

Користувачі повинні забезпечити, щоб залишене без нагляду обладнання було належним чином захищено.

Настанова щодо впровадження

Усі користувачі повинні бути поінформовані стосовно вимог щодо безпеки та процедур захисту залишеного без нагляду обладнання та їх відповідальності за впровадження такого захисту. Користувачам треба рекомендувати:

a) припиняти активні сеанси після закінчення, доки їх не буде убезпечено відповідним блокувальним механізмом, наприклад екранною заставкою, захищеною паролем;

b) від'єднуватися від прикладних програм або мережевих сервісів, коли закінчується потреба в цьому;

c) захищати комп'ютери чи мобільне обладнання від несанкціонованого використання за допомогою блокування клавіатури або еквівалентним заходом безпеки, наприклад парольним доступом, коли їх не використовують.

11.2.9 ***Політика чистого стола та чистого екрана***

Заходи безпеки

Має бути ухвалено політику чистого стола щодо паперів і змінних носіїв інформації та політику чистого екрана щодо засобів оброблення інформації.

Настанова щодо впровадження

Політика чистого стола та чистого екрана має брати до уваги класифікацію інформації (див. 8.2), правові та контрактні вимоги (див. 18.1) і відповідні ризики та культурні аспекти організації. Треба розглянути наведені нижче настанови:

a) носії конфіденційної або критичної інформації, наприклад папери або змінні носії пам'яті має бути замкнено (краще, якщо в сейфі, шафі або інших видах захищених меблів), коли вони не потрібні, особливо коли в офісі нікого немає;

b) комп'ютери й термінали мають перебувати у стані завершення сеансу чи бути захищені механізмом блокування екрана та клавіатури, який контролюється паролем, токеном чи подібним механізмом автентифікації користувача, якщо їх залишають без нагляду, і мають бути захищені блокуванням клавіатури, паролями або іншими заходами безпеки, якщо їх не використовують;

c) треба запобігати несанкціонованому використанню фотокопіювальної та іншої розмножувальної техніки (наприклад, сканерів, цифрових камер);

d) документи, що містять конфіденційну або класифіковану інформацію, повинні видаляти з принтерів негайно.

Додаткова інформація

Політика чистого стола/чистого екрана знижує ризики несанкціонованого доступу, втрати чи пошкодження інформації протягом та після звичайного робочого часу. Сейфи та інші види засобів безпечного зберігання можуть також захищати інформацію, яку в них зберігають, від таких лих як пожежа, землетрус, повінь чи вибух.

Рекомендовано розглянути використання принтерів з функцією пін-коду, тоді лише ініціатори друку зможуть отримати віддруковані матеріали і лише перебуваючи поруч із принтером.

12 БЕЗПЕКА ЕКСПЛУАТАЦІЇ

12.1 Процедури експлуатації та відповідальності

Ціль: Забезпечити коректне та безпечне функціонування засобів оброблення інформації.

12.1.1 ***Документовані процедури експлуатації***

Заходи захисту

Процедури експлуатації має бути задокументовано та зроблено доступними для всіх користувачів, що їх потребують.

Настанова щодо впровадження

Має бути підготовлено документовані процедури стосовно діяльності з експлуатації, пов'язаної із засобами оброблення інформації та комунікаціями, такі як процедури запуску і завершення процедур, резервного копіювання, обслуговування обладнання, поводження з носіями, управління комп'ютерними приміщеннями й обробленням пошти та безпеки.

Процедури експлуатації мають визначати докладні інструкції, включаючи:

a) інсталяцію та конфігурацію систем;

b) оброблення та поводження з інформацією як автоматичне, так і в ручному режимі;

c) резервне копіювання (див. 12.3);

d) вимоги диспетчеризації, зокрема й взаємозв'язок з іншими системами, час самого раннього початку і самого пізнього завершення роботи;

e) інструкції щодо поводження з помилками або іншими надзвичайними обставинами, які можуть виникати протягом виконання роботи, включаючи обмеження на використання системних утиліт (див. 9.4.4);

f) підтримка та ескалація контактів, включаючи зовнішні контакти підтримки, у разі неочікуваних технічних проблем або проблем експлуатації;

g) певні інструкції щодо поводження з вихідними даними й носіями, такі як використання певного паперу чи управління конфіденційними вихідними даними, охоплюючи процедури безпечного вилучення вихідних даних із завдань, що відмовили (див. 8.3 та 11.2.7);

h) процедури перезапуску та відновлення роботи системи для використання в разі відмови системи;

i) управління журналом аудиту та інформацією реєстраційного журналу системи (див. 12.4);

j) процедури моніторингу.

Процедури експлуатації та задокументовані процедури щодо роботи системи потрібно розглядати як санкціоновані керівництвом офіційно оформлені документи і зміни. Там, де це технічно можливо, управління інформаційними системами повинно бути однаковим, з використанням однакових процедур, інструментів і утиліт.

12.1.2 *Управління змінами*

Заходи безпеки

Зміни в організації, бізнес-процесах, засобах оброблення інформації та системах, які впливають на інформаційну безпеку, мають бути контрольованими.

Настанова щодо впровадження

Зокрема, треба розглянути наведені нижче елементи, як от:

a) ідентифікація й реєстрація значних змін;

b) планування й тестування змін;

c) оцінка потенційних впливів, включаючи впливи таких змін на безпеку;

d) процедура офіційного оформлення затвердження запропонованих змін;

e) перевірка того, що вимоги інформаційної безпеки виконуються;

f) доведення до відома всіх відповідних осіб подробиць зміни;

g) процедури нейтралізації несправностей, включаючи процедури й відповідальності щодо припинення та відновлення після невдалих змін і непередбачуваних подій;

h) наявність аварійної процедури внесення змін для забезпечення можливості швидкого та контрольованого впровадження змін, необхідних для усунення інциденту (див. 16.1).

На місцях має бути офіційно оформлено процедури для забезпечення задовільного контролю всіх змін, які стосуються обладнання, програмного забезпечення або процедур. Після проведення змін потрібно протягом тривалого часу зберігати журнал реєстрації аудиту, який містить усю суттєву інформацію.

Додаткова інформація

Недостатній контроль змін до засобів оброблення інформації та систем зазвичай призводить до збоїв систем та порушення безпеки. Зміни операційного середовища, особливо під час переходу системи від етапу розроблення до етапу промислової експлуатації, можуть вплинути на надійність прикладних програм (див. також 14.2.2).

12.1.3 *Управління потужністю*

Заходи безпеки

Для забезпечення потрібної продуктивності системи необхідно здійснювати моніторинг та регулювати використання ресурсів і проектувати вимоги до майбутньої потужності.

Настанова щодо впровадження

Вимоги щодо потужності систем, яких це стосується, має бути визначено з урахуванням критичності бізнесу. Для забезпечення і, за потреби, поліпшення доступності та ефективності систем потрібно застосовувати налаштування та моніторинг систем. Для вчасного виявлення проблем мають бути наявними відповідні заходи безпеки. Під час проектування майбутніх вимог до потужності потрібно брати до уваги нові вимоги бізнесу та систем і поточні та прогнозовані тенденції щодо можливостей оброблення інформації організації.

Особливу увагу треба звернути на ті ресурси, які потребують тривалої процедури закупівлі або великих витрат; тому керівники повинні здійснювати моніторинг використання основних ресурсів системи. Вони повинні ідентифікувати тенденції використання, особливо стосовно бізнесових прикладних програм та інструментів управління інформаційними системами.

Керівники повинні використовувати цю інформацію для ідентифікації та уникнення потенційних вузьких місць і залежності від основного персоналу, який може становити загрозу для безпеки системи чи послуг, і планувати належні заходи.

Забезпечення достатньої потужності може бути досягнуто за допомогою підвищення потужності або зменшення необхідності. Приклади управління необхідності потужності охоплюють:

a) знищення даних, які вже не використовують (дисковий простір);

b) перегляд прикладних програм, систем, баз даних або інфраструктури;

c) оптимізацію процесів та процедур групування;

d) оптимізацію логічних запитів і запитів баз даних для прикладних програм;

e) відміну чи обмеження для ресурсоємних сервісів з широкою полосою, якщо вони є некритичними для бізнесу (наприклад, відеотранслювання).

Має бути розглянуто задокументований план управління потужністю для завдань критичних систем.

Додаткова інформація

Ці заходи безпеки також відносять до потужності людських ресурсів, а також офісів та обладнання.

12.1.4 *Відокремлення засобів розробки, тестування та експлуатації*

Заходи безпеки

Засоби розроблення, тестування та експлуатації має бути відокремлено для зменшення ризиків несанкціонованого доступу чи змін в операційному середовищі.

Настанова щодо впровадження

Треба ідентифікувати рівень відокремлення середовищ: експлуатації, тестування та розроблення, необхідний для запобігання проблемам експлуатації, і впровадити належні заходи безпеки.

Треба розглянути наведені нижче елементи:

a) має бути визначено й задокументовано правила переведення програмного забезпечення з етапу розроблення до етапу експлуатації;

b) програмне забезпечення, яке розробляють та яке перебуває в експлуатації, потрібно запускати на різних системах або комп'ютерних процесорах і в різних доменах або директоріях;

c) зміни в системах, які перебувають в експлуатації, і прикладних програмах має бути протестовано в тестовому або інсценованому середовищі до того, як буде запроваджено в експлуатацію;

d) тестування не потрібно здійснювати на системах, які перебувають в експлуатації, окрім екстремальних випадків;

e) компілятори, редактори та інші інструменти розробляння або системні утиліти не повинні бути доступними із систем, які перебувають в експлуатації, коли це не потрібно;

f) для зниження ризику помилки користувачі повинні використовувати різні користувацькі профілі доступу для систем, які працюють у промисловій експлуатації, і тестових систем, меню має виводити на екран належні ідентифікаційні повідомлення;

g) конфіденційні дані не потрібно копіювати в середовище тестової системи до того, як еквівалентні заходи безпеки не буде запроваджено для систем, що їх тестують (див. 14.3).

Додаткова інформація

Діяльність з розроблення й тестування може спричинити серйозні проблеми, наприклад небажану модифікацію файлів або середовища системи, або відмову системи. У цьому разі є потреба підтримувати відоме та стабільне середовища, у якому здійснювати повнофункціональне тестування і запобігати неналежному доступу розробника до середовища промислової експлуатації.

Там, де персонал, який розробляє й тестує, має доступ до системи, яка перебуває в експлуатації, та її інформації, він може внести код, що не санкціоновано та не протестовано, або змінити експлуатаційні дані. У деяких системах такою можливістю можуть зловживати для вчинення шахрайства чи внесення непротестованого або зловмисного коду, який може спричинити серйозні проблеми експлуатації.

Розробники й тестувальники також ставлять під загрозу конфіденційність оброблюваної інформації. Діяльність з розроблення й тестування може спричинити ненавмисні зміни в програмному забезпеченні або інформації, якщо спільно використовувати те саме комп'ютерне середовище. Тому бажаним є відокремлення засобів розроблення, тестування та експлуатації для зменшення ризику випадкової зміни або несанкціонованого доступу до програмного забезпечення, що перебуває в експлуатації, та бізнес-даних (див. також 14.3 стосовно захисту даних тестування).

12.2 Захист від зловмисного коду

Ціль: Гарантувати, що інформація та засоби оброблення інформації захищені проти зловмисного коду.

12.2.1 *Заходи безпеки проти зловмисного коду*

Заходи безпеки

Має бути впроваджено заходи безпеки щодо виявлення, запобігання та відновлення для захисту від зловмисного коду і належні процедури поінформування користувачів.

Настанова щодо впровадження

Захист від зловмисного коду має базуватися на виявленні зловмисного коду і виправленні програмного забезпечення, поінформуванні щодо безпеки, належному доступі до системи та контролі управління змінами. Треба розглянути наведені нижче настанови:

a) розроблення офіційно оформленої політики, яка не допускає використання несанкціонованого програмного забезпечення (див. 12.6.2 та 14.2);

b) запровадження заходів безпеки, які запобігають чи виявляють використання несанкціонованого програмного забезпечення (наприклад, білий список прикладного програмного забезпечення);

c) запровадження заходів безпеки, які запобігають чи виявляють використання відомих чи очікувано зловмисних веб-сайтів (наприклад, чорний список);

d) розроблення офіційної оформленої політики захисту від ризиків, пов'язаних з отриманням файлів і програмного забезпечення від або через зовнішні мережі чи на будь-якому іншому носієві, із зазначенням того, які саме заходи захисту треба вжити;

e) зменшення вразливостей, які можуть бути використані зловмисним кодом, наприклад управління технічними вразливостями (див. 12.6);

f) проведення регулярних переглядів програмного забезпечення та вмісту даних систем, які підтримують критичні бізнес-процеси; наявність будь-яких непогоджених файлів або несанкціонованих поправок потрібно розслідувати з офіційним оформленням;

g) інсталяцію та регулярне оновлення програмного забезпечення виявлення та знищення зловмисного коду для сканування комп'ютерів та носіїв як превентивного заходу безпеки або у звичайному порядку; перевірки, які виконують, мають містити:

1) перевірку на зловмисний код будь-яких файлів на електронному або оптичному носії та файлів, одержаних через мережі, до застосування;
2) перевірку завантажуваних та приєднаних до електронної пошти файлів на зловмисний код до застосування; цю перевірку потрібно виконувати в різних місцях, наприклад на серверах електронної пошти, настільних комп'ютерах і на вході в мережу організації;
3) перевірку веб-сторінок на зловмисний код;

h) визначення управлінських процедур і відповідальностей щодо захисту систем від зловмисного коду, навчання використанню систем, звітування та відновлення після атак зловмисного коду;

i) підготовка відповідних планів безперервності бізнесу для відновлення після атак зловмисного коду, охоплюючи всі необхідні резервні копіювання даних і програмного забезпечення та заходи з відновлення (див. 12.3);

j) впровадження процедур для регулярного збирання інформації, таких як підписка на списки розсилання та/або перевірка веб-сайтів, які надають інформацію щодо нових зловмисних кодів;

k) впровадження процедур для верифікації інформації, пов'язаної зі зловмисним кодом, і гарантування, що попереджувальні бюлетені є точними та інформативними; керівники повинні гарантувати,

що для визначення різниці між містифікацією та справжнім зловмисним кодом використовують компетентні джерела, наприклад журнали з гарною репутацією, достовірні Інтернет-сайти або постачальники, які надають програмне забезпечення, що захищає від зловмисного коду; усі користувачі повинні бути поінформовані щодо проблеми містифікацій і що робити в разі їх отримання;

l) ізоляція середовищ, де можуть виникати катастрофічні наслідки.

Додаткова інформація

Використання двох або більше програмних продуктів, які захищають середовище оброблення інформації від зловмисного коду і отримані від різних виробників, може покращити ефективність захисту від зловмисного коду.

Треба потурбуватися щодо захисту проти внесення зловмисного коду під час виконання процедур обслуговування та аварійних дій, які можуть обходити звичайні заходи безпеки проти зловмисного коду.

Захист проти зловмисного коду може спричинити пошкодження під час експлуатації в певних випадках.

Використання лише виявлення зловмисного коду та відновлення програмного забезпечення як заходів безпеки проти зловмисного коду зазвичай буває недостатнім і часто потребує доповнення операційними процедурами, які попереджають внесення зловмисного коду.

12.3 Резервне копіювання

Ціль: Захистити від втрати даних.

12.3.1 *Резервне копіювання інформації*

Заходи безпеки

Згідно із затвердженою політикою резервного копіювання треба регулярно робити і в подальшому тестувати резервні копії інформації, програмного забезпечення та образів систем.

Настанова щодо впровадження

Політика резервного копіювання має визначати вимоги організації до резервування інформації, програмного забезпечення та систем.

Політика резервного копіювання має визначати вимоги щодо зберігання та захисту.

Має бути надано відповідні засоби резервного копіювання для забезпечення того, що вся важлива інформація і програмне забезпечення можуть бути відновлені після стихійного лиха чи відмови носія.

Під час створення плану резервного копіювання треба розглянути наведені нижче елементи:

a) має бути зроблено точні й повні записи щодо резервних копій і задокументовано процедури поновлення з резервних копій;

b) обсяг (наприклад, повне чи диференційоване резервне копіювання) і частоту резервних копіювань мають враховувати бізнес-вимоги організації, вимоги щодо безпеки стосовно залученої інформації та критичність інформації для безперервного функціонування організації;

c) резервні копії потрібно зберігати у віддаленому місці, на достатній відстані, щоб уникнути будь-якого пошкодження від стихійного лиха в основному приміщенні;

d) резервним копіям інформації треба надати належний рівень фізичного та інфраструктурного захисту (див. розділ 11), який не суперечить стандартам, що застосовують в основному приміщенні;

e) носії резервних копій потрібно регулярно тестувати для забезпечення того, що їм, за потреби, можна довіряти в разі аварійних дій; ці тести потрібно виконувати разом із тестом процедур відновлення інформації і перевіркою стосовно потрібного часу відновлення. Тестування можливості відновлення резервних даних потрібно виконувати на спеціальних тестових носіях, без перезаписування первинних носіїв у разі, коли процес резервування чи відновлення був невдалим і спричинив невідновлюване пошкодження або втрату даних;

f) у ситуаціях, коли важливою є конфіденційність, резервні копії має бути захищено засобами шифрування.

Операційні процедури мають контролювати резервне копіювання та виправляти помилки регулярних процедур резервного копіювання для гарантування повноти резервних копій відповідно до політики резервного копіювання.

Заходи резервного копіювання для окремих систем та сервісів потрібно регулярно тестувати для гарантування того, що вони задовольняють вимоги планів безперервності бізнесу. Для критичних сис-

тем та сервісів заходи резервного копіювання мають охоплювати всю системну інформацію, прикладні програми й дані, необхідні для відновлення системи в цілому в разі лиха.

Треба визначити період тривалого зберігання важливої бізнес-інформації, беручи до уваги всі вимоги до архівних копій, які потрібно постійно зберігати.

12.4 Ведення журналів аудиту та моніторинг

Ціль: Записувати події та генерувати докази.

12.4.1 *Журнал аудиту подій*

Заходи безпеки

Журнал аудиту подій, у якому записується діяльність користувачів, винятки, збої та події інформаційної безпеки, потрібно вести, зберігати й регулярно переглядати.

Настанова щодо впровадження

Журнали аудиту подій мають містити, за потреби:

a) ID (ідентифікатор) користувача;

b) діяльність системи;

c) дати, час та подробиці основних подій, наприклад входу в систему та виходу з неї;

d) ідентифікацію термінала чи його розміщення, за можливості, та ідентифікацію системи;

e) записи успішних та відхилених спроб доступу до системи;

f) записи успішних та відхилених спроб доступу до даних та іншого ресурсу;

g) зміни конфігурації системи;

h) використання привілейованих прав доступу;

i) використання системних утиліт і прикладних програм;

j) файли, які були доступними, та вид доступу;

k) мережеві адреси й протоколи;

l) тривожні сигнали системи контролю доступу;

m) активацію та деактивацію систем захисту, таких як антивірусні системи та системи виявлення вторгнення;

n) записи транзакцій, які було здійснено користувачами в прикладному програмному забезпеченні.

Журнали аудиту подій встановлюють основу для автоматизованих систем моніторингу, які спроможні генерувати консолідовані звіти й попередження про безпеку системи.

Додаткова інформація

Журнали аудиту можуть містити конфіденційні та персональні дані. Треба вжити належних заходів захисту їх конфіденційності (див. 18.1.4).

За можливості, системні адміністратори не повинні мати повноваження стирати або деактивувати журнали реєстрації їх власної діяльності (див. 12.4.3).

12.4.2 *Захист інформації журналів реєстрації*

Заходи безпеки

Засоби реєстрування та інформацію реєстрації має бути захищено від фальсифікації та несанкціонованого доступу.

Настанова щодо впровадження

Ціллю заходів безпеки має бути захист від несанкціонованих змін в інформації журналів аудиту та проблем експлуатації за допомогою засобів реєстрування, охоплюючи:

a) зміни типів записуваних повідомлень;

b) редагування та видалення файлів реєстрації;

c) перевищення місткості пам'яті носія файлів журналів аудиту, яке призводить до відмови щодо записування подій або до перезаписування поверх минулих записаних подій.

Може бути потрібно архівування деяких журналів аудиту, якщо це є частиною політики тривалого збереження записів або вимогами збирання й тривалого зберігання доказів (див. також 16.1.7).

Додаткова інформація

Системний журнал часто містить великий обсяг інформації, більшість якої не стосується моніторингу інформаційної безпеки. Щоб допомогти виділити важливі для цілей моніторингу безпеки події, треба розглянути автоматичне копіювання належних типів повідомлень у другий журнал реєстрації та/або використання відповідних системних утиліт чи інструментів аудиту для виконання опитування файлу та вдосконалення.

Системні журнали потребують захисту, оскільки, якщо дані можуть бути модифіковані або дані в них знищені, їх існування може створити помилкове розуміння безпеки. Для захисту журналів аудиту може бути запроваджене копіювання в реальному часі журналів аудиту на систему, що перебуває поза межами контролю системного адміністратора чи оператора.

12.4.3 *Журнали реєстрації адміністратора та оператора*

Заходи безпеки

Діяльність системного адміністратора та системного оператора має реєструватися і журнали аудиту мають бути захищені та регулярно переглядатися.

Настанова щодо впровадження

Користувачі з привілейованими правами доступу можуть мати можливість маніпулювати журналами аудиту на засобах оброблення інформації, що перебуває під їх безпосереднім контролем, тому треба захистити й переглядати ці журнали аудиту для підтримки можливості реєстрації дій привілейованих користувачів.

Додаткова інформація

Система виявлення вторгнення, якою управляють поза межами контролю системного адміністратора та адміністратора мережі, можна використовувати для моніторингу діяльності системного адміністратора та адміністратора мережі щодо їх відповідності.

12.4.4 *Синхронізація годинників*

Заходи безпеки

Годинники всіх важливих систем оброблення інформації в організації або домені безпеки має бути синхронізовано з джерелом часу погодженої точності.

Настанова щодо впровадження

Має бути задокументовано зовнішні та внутрішні вимоги стосовно подання часу, синхронізації й точності часу. Такі вимоги може бути визначено на рівні законодавства, регулятора, контракту, відповідності стандартам чи вимогами для внутрішнього моніторингу. Має бути визначено стандартне еталонне джерело часу для використання всередині організації.

Має бути задокументовано та впроваджено підходи організації до отримання еталонного часу від зовнішніх джерел та відповідну синхронізацію внутрішніх годинників.

Додаткова інформація

Правильна установка комп'ютерного годинника важлива для забезпечення точності журналів аудиту, необхідних для розслідування або як доказ у правових або дисциплінарних випадках. Неточні журнали аудитів можуть заважати таким розслідуванням і підірвати довіру до такого доказу. Годинник, зв'язаний з широкомовним розсиланням радіо-часу від національного атомного годинника, можна використовувати як еталонний годинник для систем реєстрації. Часовий мережевий протокол можна використовувати для утримування всіх серверів у режимі синхронізації із цим еталонним годинником.

12.5 Контроль програмного забезпечення, що перебуває в експлуатації

Ціль: Гарантувати цілісність систем, що перебувають в експлуатації.

12.5.1 *Інсталяція програмного забезпечення в системах, що перебувають в експлуатації*

Заходи безпеки

Мають бути наявними процедури контролю інсталяції програмного забезпечення в системах, що перебувають в експлуатації.

Настанова щодо впровадження

Має бути розглянуто наведені нижче настанови щодо контролю змін програмного забезпечення в системах, що перебувають в експлуатації:

a) оновлення програмного забезпечення, що перебуває в експлуатації, прикладних програм та бібліотек програм потрібно здійснювати лише адміністраторам, які пройшли навчання, після надання їм відповідної санкції керівництва (див. 9.4.5);

b) системи, що перебувають в експлуатації, мають містити лише затверджений виконуваний код, а не розроблений код чи компілятори;

c) прикладні програми та програмне забезпечення систем, що перебуває в експлуатації, потрібно запроваджувати лише після всебічного та успішного тестування; тести повинні містити тестування на простоту використання, безпеку, вплив на інші системи та зручність для користувачів і їх треба виконувати на відокремлених системах (див. також 12.1.4); треба гарантувати, що всі відповідні бібліотеки початкових програм оновлено;

d) для додержання контролю як над усім впровадженим програмним забезпеченням, так і над усією системною документацією треба використовувати систему контролю конфігурації;

e) стратегія повернення програми до попереднього стану має бути наявною до впровадження змін;

f) для всіх оновлень бібліотек програм, що перебувають в експлуатації, потрібно підтримувати журнал аудиту;

g) як захід на випадок непередбачуваних обставин потрібно підтримувати попередні версії прикладного програмного забезпечення;

h) старі версії програмного забезпечення потрібно зберігати в архіві разом з усією необхідною інформацією та параметрами, процедурами, подробицями щодо конфігурації та програмами підтримки, стільки часу, скільки в архіві зберігають дані.

Програмне забезпечення систем, що перебувають в експлуатації, яке постачає виробник, потрібно обслуговувати на рівні, який підтримує постачальник. Через певний час виробники програмного забезпечення припиняють підтримувати попередні версії програмного забезпечення. Організація повинна розглянути ризики залежності від непідтримуваного програмного забезпечення.

Будь-яке рішення щодо переходу на нову версію має враховувати бізнес-вимоги щодо зміни та безпеку версії, наприклад введення нової функціональності безпеки або кількості та серйозності проблем безпеки, які впливають на цю версію. Виправлення програмного забезпечення потрібно застосовувати, якщо вони можуть допомогти усунути або зменшити слабкі місця безпеки (див. 12.6).

Фізичний або логічний доступ потрібно надавати постачальникам лише за потреби та для підтримки й після затвердження керівництвом. Потрібно здійснювати моніторинг діяльності постачальників (див. 15.2.1).

Програмне забезпечення може залежати від програмного забезпечення та модулів, які постачають ззовні та які треба моніторити й контролювати, щоб уникнути несанкціонованих змін, які можуть привнести слабкі місця безпеки.

12.6 Управління технічною вразливістю

Ціль: Запобігати використанню технічних вразливостей.

12.6.1 *Управління технічною вразливістю*

Заходи безпеки

Треба отримувати своєчасну інформацію щодо технічних вразливостей інформаційних систем, які використовують, оцінювати підвладність організації таким вразливостям і вживати належних заходів, щоб урахувати пов'язаний з цим ризик.

Настанова щодо впровадження

Актуальний та повний інвентарний опис ресурсів СУІБ (див. розділ 8) є передумовою ефективного управління технічною вразливістю. Спеціальна інформація, необхідна для підтримки управління технічною вразливістю, включає виробника програмного забезпечення, номери версій, поточний стан розміщення (наприклад, яке програмне забезпечення інстальоване в яких системах) і особу (осіб) в організації, відповідальну(-их) за програмне забезпечення.

У відповідь на ідентифікацію потенційних технічних вразливостей потрібно вживати належних і своєчасних дій. Для розроблення ефективного процесу управління технічними вразливостями треба слідувати наведеній нижче настанові:

a) організація повинна визначити та встановити ролі та обов'язки, пов'язані з управлінням технічною вразливістю, враховуючи моніторинг вразливості, оцінку ризику вразливості, виправлення, відстежуваність ресурсу СУІБ, і всі необхідні обов'язки щодо координації;

b) інформаційні ресурси, які будуть використовувати для ідентифікації важливих технічних вразливостей і підтримки поінформованості щодо них, має бути ідентифіковано для програмного забезпечення та інших технологій (на основі інвентарного опису ресурсів СУІБ, див. 8.1.1); ці інформаційні ресурси потрібно оновлювати на основі змін в інвентарному описі або якщо знайдено інші нові чи корисні ресурси;

c) має бути визначено часову шкалу реагування на сповіщення щодо потенційно важливих технічних вразливостей;

d) як тільки потенційну технічну вразливість ідентифіковано, організація повинна ідентифікувати пов'язані з нею ризики й дії, яких треба вжити; така дія може залучати виправлення у вразливих системах і/або застосування інших заходів безпеки;

e) залежно від того, наскільки терміново треба врахувати технічну вразливість, вжиті дії потрібно здійснювати відповідно до контролів, пов'язаних з управлінням змінами (див. 12.1.2), або згідно з процедурами відповіді на інциденти інформаційної безпеки (див. 16.1.5);

f) якщо виправлення доступне, треба оцінити ризики, пов'язані з інсталяцією виправлення (ризики, спричинені вразливістю, має бути порівняно з ризиком від інсталяції виправлення);

g) виправлення має бути протестовано й оцінено до їх інсталяції для забезпечення того, що вони ефективні і не спричинюють побічні неприпустимі ефекти; якщо виправлення недоступні, треба розглянути інші заходи безпеки, такі як:

1) відключити послуги чи можливості, пов'язані з вразливістю;
2) пристосувати чи додати контролі доступу, наприклад міжмережеві екрани на межах мережі (див. 13.1);
3) посилити моніторинг для виявлення чи запобігання реальним атакам;
4) покращити поінформованість щодо вразливості;

h) для всіх вжитих процедур треба підтримувати журнал аудиту;

i) потрібно постійно здійснювати моніторинг та оцінювання процесу управління технічною вразливістю, щоб забезпечити його результативність та ефективність;

j) системи з високим ризиком потрібно розглядати першими;

k) ефективний процес управління технічною вразливістю має бути пов'язаний з діями з управління інцидентами для виявлення зв'язку даних стосовно вразливостей з функцією усунення інциденту та забезпечувати процедури, які потрібно проводити в разі виникнення інциденту;

l) визначити процедуру, яку застосовують в ситуації, коли вразливість ідентифіковано, але немає відповідних контрзаходів. У цій ситуації організація повинна оцінити ризики, пов'язані з відомою вразливістю, і визначити відповідні дії щодо виявлення та корекції.

Додаткова інформація

Управління технічною вразливістю можна розглядати як підфункцію управління змінами і як таку, що може одержувати ефект від процесів та процедур управління змінами (див. 12.1.2 та 14.2.2).

На виробників часто чинять значний тиск, щоб вони випускали виправлення якомога скоріше. Тому існує можливість, що виправлення може не врахувати проблеми адекватно і може спричинити негативний побічний ефект. До того ж у деяких випадках, якщо виправлення було застосовано, деінсталювати його може бути важко.

Якщо адекватне тестування виправлень неможливе, наприклад, через вартість або недостатність ресурсів, можна розглянути відкладення виправлення, доки на основі досвіду, описаного іншими користувачами, буде оцінено пов'язані ризики.

12.6.2 *Обмеження на інсталяцію програмного забезпечення*

Заходи безпеки

Має бути розроблено та впроваджено правила стосовно інсталяції програмного забезпечення користувачами.

Настанова щодо впровадження

Організація повинна визначити й чітко підтримувати сувору політику стосовно того, які типи програмного забезпечення може інсталювати користувач.

Має бути застосовано принцип надання найменших привілеїв. Якщо користувачам надано деякі привілеї, вони мають можливість інсталювати програмне забезпечення. Організація повинна ідентифікувати, які типи інсталяцій програмного забезпечення дозволено (наприклад, оновлення та виправлення безпеки для наявного програмного забезпечення), а також, які типи інсталяцій заборонено (наприклад, програмне забезпечення, яке призначено лише для персонального використання, і програмне забезпечення, джерела якого щодо наявності потенціального зловмисного коду невідомі чи викликають підозру. Такі привілеї потрібно призначати відповідно до ролей, які виконує користувач.

Додаткова інформація

Неконтрольована інсталяція програмного забезпечення на комп'ютерній техніці може призвести до внесення вразливостей і в подальшому до витоку інформації, втрати цілісності або іншим інцидентам інформаційної безпеки, чи втрати прав інтелектуальної власності.

12.7 Розгляд аудиту інформаційних систем

Ціль: Мінімізувати вплив аудиту на системи, які перебувають у промисловій експлуатації.

12.7.1 *Заходи безпеки аудиту інформаційних систем*

Заходи безпеки

Вимоги аудиту та діяльність, що охоплює перевірки систем, які перебувають в експлуатації, має бути ретельно сплановано та погоджено, щоб мінімізувати ризик порушення бізнес-процесів.

Настанова щодо впровадження

Треба звернути увагу на наведені нижче настанови:

a) вимоги аудиту стосовно доступу до систем і даних має бути погоджено з відповідним керівництвом;

b) сфера застосування перевірок має бути погодженою та контрольованою;

c) перевірки потрібно обмежувати доступом до програмного забезпечення й даних лише для читання;

d) доступ не лише для читання потрібно дозволяти лише до окремих копій системних файлів, які після завершення аудиту треба знищувати, або їм потрібно надавати належний захист, якщо є зобов'язання щодо зберігання таких файлів згідно з вимогами до документування аудитів;

e) вимоги щодо спеціального чи додаткового оброблення має бути визначено та погоджено;

f) тести аудиту, що можуть впливати на доступність системи, треба запускати за межами бізнес-часу;

g) треба здійснювати моніторинг усякого доступу та реєструвати його для генерації журналу аудиту доступу.

13 БЕЗПЕКА КОМУНІКАЦІЙ

13.1 Управління безпекою мережі

Ціль: Забезпечити захист інформації в мережах та захист засобів оброблення інформації, що їх підтримує.

13.1.1 *Заходи безпеки мережі*

Заходи безпеки

Треба відповідним чином управляти й захищати мережі для захисту інформації в системах і прикладних програмах.

Настанова щодо впровадження

Заходи безпеки має бути впроваджено для гарантування безпеки інформації в мережах і захисту підключених послуг від несанкціонованого доступу. Зокрема, треба розглянути наведені нижче елементи:

a) має бути встановлено відповідальності й процедури управління віддаленим обладнанням;

b) відповідальність за експлуатацію мереж має бути, за можливості, відокремлено від відповідальності за експлуатацію комп'ютерів (див. 6.1.2);

c) треба розробити певні заходи безпеки для захисту конфіденційності й цілісності даних, що проходять у загальнодоступних чи бездротових мережах, і для захисту підключених систем і прикладних програм (див. розділ 10 і 13.2); певні заходи безпеки можуть бути необхідними також для підтримання доступності послуг мережі та підключених комп'ютерів;

d) для уможливлення запису та виявлення дій, які можуть впливати чи бути пов'язані з інформаційною безпекою, треба застосувати належні реєстрацію та моніторинг;

e) керівництво повинно ретельно скоординувати дії як для оптимізації обслуговування організації, так і для забезпечення того, що заходи безпеки узгоджено застосовують по всій інфраструктурі оброблення інформації;

f) системи в мережі має бути автентифіковано;

g) зв'язок систем з мережею має бути обмеженим.

Додаткова інформація

Додаткову інформацію щодо безпеки мережі наведено в ISO/IEC 27033 [15], [16], [17], [18], [19].

13.1.2 *Безпека послуг мережі*

Заходи безпеки

Характеристики безпеки, рівні послуг, а також вимоги управління всіма послугами мережі має бути ідентифіковано й міститися в будь-якій угоді щодо послуг мережі як для послуг, які надає сама організація, так і для аутсорсингових послуг.

Настанова щодо впровадження

Треба визначити й регулярно здійснювати моніторинг здатності постачальника послуг мережі, управляти погодженими послугами в безпечний спосіб, при цьому має бути погоджено право проведення аудиту.

Має бути ідентифіковано заходи безпеки, необхідні для окремих послуг, такі як характеристики безпеки, рівні обслуговування та вимоги щодо управління. Організація повинна забезпечити, щоб постачальники послуг мережі впровадили ці заходи.

Послуги мережі охоплюють надання підключень, приватні послуги мережі та мережі з доданою вартістю, а також рішення щодо управління безпекою мережі, такі як міжмережеві екрани та системи виявлення вторгнення. Ці послуги можуть різнитися від простої смуги пропускання без управління до складних пропозицій з доданою вартістю.

Характеристиками безпеки послуг мережі можуть бути:

a) технології, застосовані для безпеки послуг мережі, такі як автентифікація, шифрування та контролі мережевих підключень;

b) технічні параметри, потрібні для безпечного підключення до послуг мережі відповідно до правил безпеки та підключень мережі;

c) процедури використання послуг мережі для обмеження доступу до послуг мережі або прикладних програм, якщо це необхідно.

13.1.3 *Сегментація в мережах*

Заходи безпеки

У мережі мають бути сегментовані групи інформаційних послуг, користувачів, а також інформаційні системи.

Настанова щодо впровадження

Одним з методів контролювання безпеки великих мереж є розділення їх на окремі логічні мережеві домени. Домени може бути обрано на основі рівнів довіри (наприклад, домен публічного доступу, домен робочих станцій, домен серверів), з урахуванням організаційних одиниць (наприклад, управління персоналом, фінанси, маркетинг) чи будь-якої комбінації (наприклад, домен серверів, який зв'язує різні організаційні одиниці). Сегментацію може бути здійснено з використанням фізично різних мереж або з використанням різних логічних мереж (наприклад, віртуальних мереж).

Периметр кожного домену має бути чітко визначений. Доступ між доменами мережі дозволений, але повинен контролюватися на периметрі з використанням міжмережевих шлюзів (наприклад, брандмауер, роутер-фільтр). Критерії для сегментації мереж на домени й доступ, який дозволено крізь міжмережеві шлюзи, потрібно визначати на основі оцінки вимог щодо безпеки для кожного домену. Оцінку потрібно виконувати відповідно до політики контролю доступу (див. 9.1.1), вимог доступу, цінності та класифікації інформації, яку обробляють, а також брати до уваги відносну вартість і вплив продуктивності вбудовування придатної технології шлюзів.

Бездротові мережі потребують спеціального поводження через погано визначений периметр мережі. Для чутливого середовища треба уважно розглянути всі бездротові доступи як зовнішні з'єднання і відділити ці доступи від внутрішніх мереж, доки цей доступ не буде здійснений крізь міжмережевий шлюз згідно з політикою контролю доступу до мережі (див. 13.1.1) перед наданням дозволеного доступу до внутрішніх систем.

Автентифікація, шифрування й технології контролю доступу до мережі на рівні користувачів для сучасних, основаних на стандартах бездротових мереж можуть бути достатньо ефективними для прямого з'єднання з внутрішньою мережею організації, якщо їх відповідним чином запроваджено.

Додаткова інформація

Мережі все більше розширюються за межі організації, оскільки формуються бізнес-спільноти, які можуть потребувати з'єднання або спільного використання засобів оброблення інформації та обслуговування

мережі. Таке розширення може збільшити ризик несанкціонованого доступу до інформаційних систем організації, які користуються мережею, причому деякі з них можуть потребувати захисту від користувачів іншої мережі через свою конфіденційність або критичність.

13.2 Обмін інформацією

Ціль: Підтримувати безпеку інформації, якою обмінюються всередині організації та з зовнішнім об'єктом.

13.2.1 *Політики та процедури обміну інформацією*

Заходи безпеки

Мають бути наявними офіційно оформлені політики, процедури та заходи безпеки для захисту обміну інформацією з використанням усіх видів засобів комунікації.

Настанова щодо впровадження

Процедури та заходи безпеки, яких треба дотримуватися під час використання засобів комунікації для обміну інформацією, мають стосуватися наведеного нижче переліку:

a) процедури, спроектовані для захисту обмінюваної інформації від перехоплення, копіювання, модифікації, неправильної маршрутизації та знищення;

b) процедури виявлення та захисту від зловмисного коду, який може бути переданий за допомогою використання електронних комунікацій (див. 12.2.1);

c) процедури захисту переданої чутливої електронної інформації у формі приєднаних файлів;

d) політика чи настанови, що визначають придатне використання електронних засобів комунікації (див. 8.1.3);

e) відповідальності найманого персоналу, зовнішніх сторін та будь-яких інших користувачів щодо неприпустимості компрометації організації, наприклад через наклеп, кривдження, запозичення прав, переадресування ланцюгових листів, несанкціоновані закупівлі тощо;

f) застосування криптографічних методів, наприклад, для захисту конфіденційності, цілісності й автентичності інформації (див. розділ 10);

g) настанови щодо тривалого зберігання та вилучення згідно з національними й місцевими законодавством та нормами всієї бізнес-кореспонденції, зокрема й повідомлень;

h) заходи безпеки та обмеження, пов'язані з використанням засобів комунікації, наприклад автоматичне переадресування електронних повідомлень на зовнішні адреси пошти;

i) нагадування персоналу про необхідність вжиття належних запобіжних заходів для того, щоб не розкривати конфіденційної інформації;

j) неприпустимість залишення на автовідповідачі повідомлень, які містять конфіденційну інформацію, оскільки їх може бути відтворено особами, які не мають на це санкції; ці повідомлення можуть зберігатися у спільних системах або зберігатися некоректно через неправильне набирання номера;

k) нагадування персоналу щодо проблем використання факсимільних апаратів або послуг, а саме:

1) несанкціонований доступ до вбудованої пам'яті для повідомлень для їх відновлення;

2) навмисне чи випадкове програмування апаратів для надсилання повідомлень на певні номери;

3) надсилання документів та повідомлень на неправильний номер або через неправильне набирання номера, або використання збереженого неправильного номера.

Крім того, персоналу треба нагадувати, що вони не повинні вести конфіденційних розмов у громадських місцях або через незахищені комунікаційні канали, у відкритих офісах чи місцях для нарад.

Засоби обміну інформацією мають відповідати всім чинним правовим вимогам (див. 18.1).

Додаткова інформація

Обмін інформацією можна здійснювати з використанням багатьох різних видів засобів комунікації, включаючи електронну пошту, голос, факсимільні апарати та відео.

Обмін програмним забезпеченням можна здійснювати через багато різних видів носіїв, зокрема й завантаження з Інтернету та придбання у виробників, які продають серійні продукти.

Треба розглянути вимоги до заходів безпеки й наслідки — бізнесові, правові та щодо безпеки, пов'язані з електронним обміном даними, електронною комерцією та електронною комунікацією.

13.2.2 *Угоди щодо обміну інформацією*

Заходи безпеки

Між організацією та зовнішніми сторонами повинні бути укладені угоди щодо безпечного обміну бізнес-інформацією.

Настанова щодо впровадження

Угоди щодо обміну інформацією мають містити наведене нижче:

a) відповідальності керівництва щодо контролю та сповіщення стосовно передавання, відсилання та приймання;

b) процедури забезпечення простежуваності та неспростовності;

c) мінімальні вимоги технічних стандартів щодо пакетування та передавання;

d) угоди щодо умовного депонування документів;

e) стандарти ідентифікації кур'єра;

f) відповідальності та зобов'язання в разі інциденту інформаційної безпеки, наприклад втрати даних;

g) використання погодженої системи позначень для конфіденційної або критичної інформації, яка гарантує, що позначення є зрозумілими і що інформація захищена належним чином (див. 8.2);

h) технічні стандарти щодо записування та зчитування інформації та програмного забезпечення;

i) будь-які спеціальні заходи безпеки, які можуть знадобитися для захисту конфіденційних елементів, таких як криптографічні ключі (див. розділ 10);

j) підтримку можливості відслідкування ланцюжка отримувачів інформації під час її передавання;

k) прийнятні рівні контролю доступу.

Для захисту інформації та фізичних носіїв під час передавання мають бути розроблені та підтримуватися політики, процедури та стандарти (див. 8.3.3), на них треба посилатися в угодах щодо обміну.

Зміст будь-якої угоди, який стосується безпеки, має відображати конфіденційність залученої бізнес-інформації.

Додаткова інформація

Угоди можуть бути в електронному вигляді або складені вручну і можуть мати форму офіційно оформлених контрактів. Стосовно конфіденційної інформації спеціальні механізми, які використовують для обміну такою інформацією, мають бути несуперечливими для всіх організацій та всіх типів угод.

13.2.3 *Електронний обмін повідомленнями*

Заходи безпеки

Інформація, яка міститься в електронних повідомленнях, має бути захищена належним чином.

Настанова щодо впровадження

Міркування безпеки щодо електронного обміну повідомленнями мають включати:

a) захист повідомлень від несанкціонованого доступу, модифікації або відмови в обслуговуванні;

b) забезпечення коректного адресування та передавання повідомлення;

c) загальну надійність і доступність послуги;

d) правові вимоги, наприклад вимоги до електронних підписів;

e) отримання погодження перед використанням загальнодоступних зовнішніх послуг, таких як засоби оперативного пересилання повідомлень або спільне використання файлів;

f) більш жорсткі рівні автентифікації, яка контролює доступ із загальнодоступних мереж.

Додаткова інформація

Існує велика кількість типів електронного обміну повідомленнями, таких як електронна пошта, електронний обмін даними (Electronic Data Interchange — EDI) та соціальні мережі, які відіграють все більш важливу роль у бізнес-комунікаціях.

13.2.4 *Угоди щодо конфіденційності або нерозголошення*

Заходи безпеки

Вимоги до угод щодо конфіденційності або нерозголошення, які відображають потреби організації в захисті інформації, мають бути ідентифіковані, задокументовані та регулярно переглядатися.

Настанова щодо впровадження

Угоди щодо конфіденційності або нерозголошення мають ураховувати вимоги захисту конфіденційної інформації з використанням наявних правових норм. Угоди щодо конфіденційності або нерозголошення застосовують до зовнішніх сторін або працівників організації. Має бути визначено або долучено до розгляду елементи типів іншої сторони і їх дозволений доступ або дозволене оброблення конфіденційної інформації. Для ідентифікації вимог до угод щодо конфіденційності або нерозголошення треба розглянути наведені нижче елементи:

a) визначення інформації, яка має бути захищена (наприклад, конфіденційна інформація);

b) очікувана тривалість угоди, зокрема й випадки, коли конфіденційність потрібно підтримувати необмежено;

c) необхідні дії після припинення угоди;

d) відповідальності та дії сторін, що підписали угоду, для запобігання несанкціонованому розголошенню інформації;

e) право власності на інформацію, секрети виробництва та інтелектуальна власність і як вони пов'язані із захистом конфіденційної інформації;

f) дозволене використання конфіденційної інформації і права сторони, яка підписала угоду, користуватися інформацією;

g) право аудиту і моніторингу діяльності, пов'язаної з конфіденційною інформацією;

h) процес сповіщення та звітування щодо несанкціонованого розголошення чи витоку конфіденційної інформації;

i) терміни повернення або руйнування інформації в разі припинення угоди;

j) очікувані дії, яких треба вжити в разі порушення угоди.

Виходячи з вимог щодо безпеки організації, може виникнути необхідність долучати в угоду щодо конфіденційності або нерозголошення також інші елементи.

Угоди щодо конфіденційності та нерозголошення мають відповідати всім чинним законам і нормам для юрисдикції, де їх використовують, (див. 18.1).

Вимоги до угод щодо конфіденційності та нерозголошення треба переглядати періодично, і в разі змін, які впливають на ці вимоги.

Додаткова інформація

Угоди щодо конфіденційності та нерозголошення захищають інформацію організації та інформують сторони, які підписали угоди, про їх відповідальність щодо захисту, використання та розголошення інформації лише у відповідальний та санкціонований спосіб.

В організації може виникнути необхідність використовувати різні форми угод щодо конфіденційності та нерозголошення за різних обставин.

14 ПРИДБАННЯ, РОЗРОБЛЕННЯ ТА ПІДТРИМКА ІНФОРМАЦІЙНИХ СИСТЕМ

14.1 Вимоги щодо безпеки для інформаційних систем

Ціль: Забезпечити, що безпека є невід'ємною частиною інформаційних систем протягом всього життєвого циклу. Це також включає вимоги для інформаційних систем, які забезпечують надання послуг з використанням публічних (загальнодоступних) мереж.

14.1.1 *Аналіз та специфікація вимог щодо інформаційної безпеки*

Заходи безпеки

Вимоги щодо інформаційної безпеки має бути долучено в положення щодо бізнес-вимог до нових інформаційних систем або модернізацій до наявних інформаційних систем.

Настанова щодо впровадження

Вимоги щодо інформаційної безпеки має бути ідентифіковано з урахуванням різних методів, таких як виконання вимог відповідності політикам і регуляторним вимогам, моделювання загроз, перегляд інцидентів або використання загроз від наявних вразливостей. Результати цієї ідентифікації має бути задокументовано і переглянуто всіма акціонерами.

Вимоги щодо безпеки та заходи безпеки мають відображати цінність для бізнесу охоплюваних інформаційних ресурсів (див. 8.2) і потенційну шкоду бізнесу, яка може бути наслідком відмови або відсутності безпеки.

Ідентифікація та управління вимогами до інформаційної безпеки та процеси запровадження безпеки має бути інтегровано на початкових стадіях проектування інформаційної системи. Ранній розгляд вимог щодо інформаційної безпеки, а саме на етапі проектування, може призвести до більш ефективних та дешевих рішень.

Вимоги щодо інформаційної безпеки мають також розглядати:

a) рівень конфіденційності, який потрібний для заявленої ідентичності користувачів, для визначення вимог стосовно автентифікації користувачів;

b) процедури надання доступу та процедури авторизації для бізнес-користувачів, а також для привілейованих або технічних користувачів;

c) інформування користувачів та операторів стосовно їх обов'язків та відповідальності;

d) сервіси безпеки, потрібні для ресурсів СУІБ, які використовують, зокрема стосовно доступності, конфіденційності, цілісності;

e) вимоги, які походять з бізнес-процесів, такі як журнали аудиту й моніторингу транзакцій, вимоги щодо неспростовності;

f) вимоги, визначені іншими заходами безпеки, наприклад інтерфейсами до систем аудиту й моніторингу або системами виявлення витоків інформації.

Для прикладних систем, які забезпечують надання послуг через публічні мережі або в яких використовують транзакції, має бути розглянуто відповідні заходи безпеки 14.1.2. та 14.1.3.

Якщо продукти купують, треба слідувати офіційно оформленій процедурі тестування та придбання. Контракти з постачальником мають враховувати ідентифіковані вимоги щодо безпеки. Якщо функціональність безпеки запропонованого продукту не задовольняє встановлені вимоги, то до придбання продукту має бути переглянуто нові внесені ризики й відповідні заходи безпеки.

Має бути розроблено та впроваджено придатні настанови щодо безпечної конфігурації продукту для фінальної версії програмного забезпечення/набору сервісів такої системи.

Має бути визначено критерії приймання продуктів, наприклад у термінах їх функціональності, які будуть надавати гарантії, що ідентифіковані вимоги щодо безпеки виконано. Продукти потрібно оцінювати відповідно до цих критеріїв перед їх придбанням. Додаткову функціональність має бути переглянуто для оцінки того, що вона не буде вносити додаткових небажаних ризиків.

Додаткова інформація

ISO/IEC 27005 [11] та ISO 31000 [27] надають настанови щодо використання процесів управління ризиками для ідентифікації заходів безпеки, які забезпечують виконання вимог щодо інформаційної безпеки.

14.1.2 *Безпечні прикладні сервіси в публічних мережах*

Заходи безпеки

Інформація в прикладних сервісах, яку передають через публічні мережі, має бути захищеною від шахрайської діяльності, контрактних суперечок, несанкціонованого розголошення та модифікації.

Настанова щодо впровадження

Розгляд інформаційної безпеки для прикладних сервісів, які передаються через публічні мережі, має охоплювати наведене нижче:

a) рівень конфіденційності, необхідний кожній стороні в кожній іншій заявленій тотожності, наприклад за допомогою автентифікації;

b) процес призначення осіб, які мають право затверджувати вміст документа або підписувати транзакційні документи;

c) забезпечення того, що партнери по комунікації повністю поінформовані стосовно наданих їм прав з надання чи використання сервісу;

d) визначення та виконання вимог щодо конфіденційності, цілісності, доказів відсилання й одержання основних документів, неспростовність контрактів, наприклад, пов'язаних з тендерами та контрактними процесами;

e) рівень довіри, потрібний для цілісності основних документів;

f) вимоги стосовно захисту будь-якої конфіденційної інформації;

g) конфіденційність і цілісність для будь-яких документів-замовлень, платіжної інформації, деталей адрес доставки та квитанцій підтвердження отримання;

h) ступінь верифікації, призначений для підтвердження платіжної інформації, яку надає отримувач;

i) вибір найбільш придатної форми платежів для захисту від шахрайства;

j) рівень захисту, потрібний для підтримання конфіденційності та цілісності іншої інформації;

k) уникнення втрат або дублювання інформації транзакцій;

l) зобов'язання, пов'язані з будь-якими недостовірними транзакціями;

m) вимоги до страхування.

Багато з наведених вище питань може бути вирішено, застосовуючи криптографічні засоби безпеки (див. розділ 10) з урахуванням відповідності вимогам законодавства (див. розділ 18, звертаючи особливу увагу на легалізації криптографії — див. 18.1.5).

Структуру прикладних сервісів між сторонами має підтримувати задокументована угода, яка задовольняє обидві сторони для погодження термінів надання сервісів, включаючи подробиці щодо призначення (див. пункт b) вище).

Має бути розглянуто вимоги стійкості проти атак, які містять вимоги стосовно захисту використовуваних серверів прикладних програм або гарантії доступності мережевих з'єднань, що забезпечують доставку сервісу.

Додаткова інформація

Прикладні програми, доступні через публічні мережі, є вразливими для багатьох мережевих загроз, таких як шахрайська діяльність, контрактні суперечки і розголошення або модифікація інформації. Тому необхідними є детальна оцінка ризиків та відповідний вибір заходів безпеки. Потрібні заходи безпеки часто містять криптографічні методи для автентифікації та безпечного передавання даних.

Прикладні сервіси можуть використовувати безпечні методи автентифікації, наприклад криптографію відкритих ключів і цифрові підписи (див. розділ 10) для зменшення ризиків. Також там, де такі послуги потрібні, можна використовувати третю довірчу сторону.

14.1.3 *Захист транзакцій прикладних сервісів*

Заходи безпеки

Інформація, залучена в транзакції прикладних сервісів, має бути захищена для запобігання неповній передачі, неправильній маршрутизації, несанкціонованій зміні повідомлення, несанкціонованому розголошенню, несанкціонованому дублюванню повідомлення чи його повторенню.

Настанова щодо впровадження

Міркування щодо безпеки для транзакцій прикладних сервісів мають включати наведене нижче:

a) застосування електронних підписів кожною стороною, залученою в транзакцію;

b) усі аспекти транзакції, тобто забезпечення того, що:

1) таємна інформація автентифікації користувачів усіх сторін є дійсна та верифікована;

2) транзакція залишається конфіденційною; та

3) зберігається приватність усіх залучених сторін;

c) комунікаційні канали між усіма залученими сторонами зашифровані;

d) убезпечені протоколи, які використовують для комунікацій між усіма залученими сторонами;

e) забезпечення, що зберігання подробиць транзакції розміщено поза будь-якою загальнодоступною інфраструктурою, наприклад на запам'ятовувальній платформі, яка існує у внутрішній (Intranet) мережі організації, і тривало не зберігається і не відображається на носії даних, безпосередньо доступному з Інтернету;

f) там, де використовують довірчу повноважну організацію (наприклад, для випуску та підтримки цифрового підпису та/або цифрових сертифікатів), безпека має бути комплексною та вбудованою в єдиний з кінця-в-кінець процес управління сертифікатом/підписом.

Додаткова інформація

Необхідно, щоб обсяг прийнятих заходів безпеки відповідав рівню ризику, пов'язаного з кожною формою транзакції прикладного сервісу.

Транзакції можуть потребувати відповідності законодавчим та регуляторним вимогам, у юрисдикції яких транзакція створена, обробляється, закінчується чи зберігається.

14.2 Безпека в процесах розроблення та підтримки

Ціль: Гарантувати, що інформаційну безпеку проектують та впроваджують протягом життєвого циклу розроблення інформаційних систем.

14.2.1 *Політика безпечного розроблення*

Заходи безпеки

Потрібно встановлювати й застосовувати до розробників всередині організації правила для розроблення програмного забезпечення та систем.

Настанова щодо впровадження

Безпечне розроблення є вимогою стосовно побудови безпечних сервісів, архітектури, програмного забезпечення та системи. У межах політики безпечного розроблення потрібно брати до уваги наведені нижче аспекти:

a) безпеку середовища розроблення;

b) настанову щодо безпеки протягом життєвого циклу розроблення програмного забезпечення:

1) безпеку методології розроблення програмного забезпечення;

2) настанови щодо безпечного кодування для кожної мови програмування, які використовують;

c) вимоги щодо безпеки на стадії проектування;

d) контрольні точки з безпеки в плані проектування;

e) безпечні репозитарії;

f) безпеку під час контролю версій;

g) потрібні знання безпеки прикладних модулів;

h) можливість уникнення, знаходження та фіксації вразливостей з боку розробників.

Методики безпечного програмування потрібно використовувати як для нових розробок, так і під час повторного використання в коді сценаріїв, де стандарти, які використовують під час розроблення, могли бути невідомими або не відповідали сучасним кращим практикам. Стандарти безпечного кодування мають бути розглянутими та бути обов'язковими для використання там, де це можливо. Розробники повинні тренуватися в їх використанні й тестуванні; перегляд кодів має підтвердити їх використання.

Якщо розроблення виконують на умовах аутсорсингу, організація має отримати гарантії, що зовнішня сторона виконує ці правила для безпечного розроблення (див. 14.2.7).

Додаткова інформація

Розроблення може також здійснюватися всередині додатків, таких як офісні прикладні програми, шрифти, браузери та бази даних.

14.2.2 *Процедури контролю змін системи*

Заходи безпеки

Зміни в системах всередині життєвого циклу розроблення мають бути контрольованими за допомогою офіційно оформлених процедур контролю змін.

Настанова щодо впровадження

Офіційно оформлені процедури контролю змін мають бути задокументовані та здійснюватися примусово для гарантії цілісності системи, прикладних програм і продуктів з початкових стадій проектування протягом усіх послідовних зусиль стосовно підтримки.

Введення нових систем та великих змін до наявних систем повинні слідувати за офіційно оформленим процесом документування, специфікацій, тестування, контролю якості та впровадження, яким управляють.

Цей процес має містити оцінку ризику, аналіз впливу змін і специфікацію необхідних заходів безпеки. Також цей процес має забезпечувати, що наявні процедури безпеки та контролювання не скомпрометовано, програмістам надано доступ лише до тих частин системи, які необхідно обслуговувати, і для будь-яких змін отримано офіційно оформлені угоди та затвердження.

Всюди, де це можливо, процедури контролю змін прикладних програм і експлуатації має бути об'єднано (див. також 12.1.2). Процедури змін мають включати:

a) підтримування запису щодо погоджених рівнів санкціонованого доступу;

b) забезпечення, що зміни подають користувачі, які мають на це санкцію;

c) перегляд заходів безпеки та процедур цілісності для забезпечення того, що вони не будуть цими змінами скомпрометовані;

d) ідентифікацію всього програмного забезпечення, інформації, компонентів баз даних та апаратних засобів, які потребують корекції;

e) ідентифікацію та перевірку безпечності критичного коду для зведення до мінімуму ймовірності появи відомих слабких місць;

f) отримання до початку роботи офіційно оформленого затвердження докладних пропозицій;

g) забезпечення того, щоб користувачі, які мають на це санкцію, прийняли зміни до їх впровадження;

h) забезпечення того, що комплект системної документації оновлюється після завершення кожної зміни і стара документація архівується або вилучається;

i) підтримання контролю версій для всіх оновлень програмного забезпечення;

j) підтримання журналу аудиту всіх запитів на зміни;

k) забезпечення того, що експлуатаційна документація (див. 12.1.1) і користувацькі процедури, за потреби, змінюються для того, щоб залишатися належними;

l) забезпечення, що впровадження змін має місце в потрібний час і не порушує залучені бізнес-процеси.

Додаткова інформація

Заміна програмного забезпечення може вплинути на операційне середовище.

Хорошою практикою є тестування нового програмного забезпечення в середовищі, відокремленому як від промислового обладнання, так і від середовища розробки (див. також 12.1.4). Це забезпечує засоби контролю над новим програмним забезпеченням і надає додатковий захист експлуатаційній інформації, яку використовують для тестування. Такий підхід має охоплювати виправлення, пакети оновлення та інші оновлення.

Якщо розглядають можливість автоматичного оновлення, необхідно порівняти цілісність і доступність системи й переваги швидкого встановлення оновлень. Автоматичні оновлення не потрібно використовувати на критичних системах, оскільки деякі оновлення можуть спричинити відмову критичних прикладних програм.

14.2.3 ***Технічний перегляд прикладних програм після змін операційної платформи***

Заходи безпеки

Коли операційні платформи змінено, критичні для бізнесу прикладні програми має бути переглянуто й протестовано, щоб забезпечити відсутність негативного впливу на функціонування та безпеку організації.

Настанова щодо впровадження

Ця процедура має включати:

a) перегляд процедур контролювання та цілісності прикладних програм для забезпечення того, що їх не було скомпрометовано змінами операційної платформи;

b) забезпечення, що сповіщення щодо змін операційної платформи надано вчасно для уможливлення проведення до впровадження належного тестування й переглядів;

c) забезпечення, що зроблено належні зміни до плану безперервності бізнесу (див. розділ 17).

Додаткова інформація

Операційна платформа охоплює операційні системи, бази даних і міжплатформне зв'язувальне програмне забезпечення. Потрібно також здійснювати контроль змін прикладних програм.

14.2.4 ***Обмеження на зміни до пакетів програмного забезпечення***

Заходи безпеки

Модифікації пакетів програмного забезпечення не повинні заохочуватися, бути обмеженими найнеобхіднішими змінами і всі зміни потрібно суворо контролювати.

Настанова щодо впровадження

Наскільки це можливо й практично застосовно, пакети програмного забезпечення, поставлені виробником, потрібно використовувати без модифікацій. У тих випадках, коли пакети програмного забезпечення потребують модифікації, треба розглянути наведені нижче пункти:

a) ризик компрометації вбудованих заходів безпеки та процесів контролю цілісності;

b) чи треба отримати згоду виробника;

c) можливість отримання необхідних змін від виробника як стандартних оновлень програми;

d) вплив того, що організація внаслідок змін стає відповідальною за майбутню підтримку програмного забезпечення;

e) сумісність з іншим програмним забезпеченням, яке використовують.

Якщо зміни необхідні, оригінальне програмне забезпечення має бути збережено, а зміни застосовані до чітко визначеної копії. Має бути впроваджено процес управління оновленням програмного забезпечення, щоб гарантувати, що найновіші затверджені виправлення й оновлення прикладних програм інстальовані на всьому санкціонованому програмному забезпеченні (див. 12.6.1). Усі зміни має бути повністю протестовано й задокументовано, щоб їх можна було повторно застосовувати, за потреби, до майбутніх модернізацій програмного забезпечення. Якщо це потрібно, модифікації має бути протестовано та затверджено незалежним органом з оцінювання.

14.2.5 ***Принципи проектування безпечної системи***

Заходи безпеки

Принципи проектування безпечних систем потрібно розробити, задокументувати, виконувати та використовувати для будь-яких зусиль щодо реалізації інформаційних систем.

Настанова щодо впровадження

Принципи проектування безпечних систем, які базуються на принципах проектування безпеки, має бути розроблено, задокументовано, виконувати та використовувати для будь-яких зусиль щодо внутрішнього проектування інформаційних систем. Безпеку потрібно розробляти в усіх архітектурних шарах (бізнес, дані, прикладні програми та технології) з урахування балансу між потребами інформаційної безпеки та потребами можливості доступу. Нові технології має бути проаналізовано на предмет ризиків безпеки і проект потрібно переглядати з урахуванням відомих характеристик атак.

Ці принципи та визначені процедури проектування треба регулярно переглядати для гарантії того, що вони ефективно використовують посилені стандарти безпеки в процесі проектування. Їх треба також регулярно переглядати для гарантії того, що вони залишаються сучасними в термінах боротьби з будь-якими потенційними загрозами й залишають можливість для вдосконалення технологій та рішень, які будуть використовувати.

Визначені принципи безпечного проектування треба використовувати, де це можливо, для аутсорсингового розроблення інформаційних систем через контракти та інші угоди, які укладають між організацією та постачальником, який є аутсорсером. Організація має підтвердити, що суворість принципів проектування безпеки постачальників порівняні з їх власними.

Додаткова інформація

Процедури розроблення прикладних програм мають використовувати методики безпечного проектування під час розроблення прикладних програм, які мають вхідні та вихідні інтерфейси. Методики проектування безпеки надають настанови стосовно методів автентифікації користувачів, контролю безпечних сесій та підтвердження даних, виявленню та вилученню кодів налагодження.

14.2.6 *Безпечне середовище розроблення*

Заходи безпеки

Організації повинні запровадити та відповідним чином захистити безпечне середовище проектування для розроблення систем та інтеграції зусиль, що покривають повний життєвий цикл розроблення системи.

Настанова щодо впровадження

Безпечне середовище розроблення охоплює персонал, процеси й технології, пов'язані з розробленням та інтеграцією системи.

Організації повинні оцінювати ризики, пов'язані із зусиллями стосовно розроблення окремої системи, та запровадити безпечні середовища розроблення для розроблення специфічних систем, беручи до уваги таке:

a) конфіденційність даних, які будуть оброблятися, зберігатися та передаватися системою;

b) застосування зовнішніх та внутрішніх вимог, наприклад з регуляторних актів або політик;

c) засоби безпеки, які вже запроваджено організацією стосовно розроблення системи;

d) надійність персоналу, який працює в цьому середовищі (див. 7.1.1);

e) ступінь аутсорсингу щодо розроблення системи;

f) потребу ізоляції між різними середовищами розроблення;

g) контроль доступу до середовища розроблення;

h) моніторинг змін у середовищі та кодів, які зберігають;

i) резервні копії (бекапи) зберігають у безпечних віддалених місцях;

j) контроль за переміщенням даних з цього середовища та до нього.

Якщо визначено рівень захисту для специфічного середовища розроблення, організація повинна задокументувати відповідні процеси в процедурах безпечного розроблення та забезпечувати ними всіх працівників, хто потребує цього.

14.2.7 *Аутсорсингове розроблення*

Заходи безпеки

Організація повинна здійснювати нагляд над аутсорсинговим розробленням систем та його моніторинг.

Настанова щодо впровадження

Там, де є аутсорсингове розроблення систем, треба розглянути наведені нижче пункти:

a) ліцензійні угоди, права власності на коди та права інтелектуальної власності (див. 18.1.2);

b) контрактні вимоги стосовно безпечного проектування, кодування та практик тестування (див. 14.2.1);

c) надання зовнішньому розробнику затвердженої моделі загроз;

d) приймальне тестування якості й точності виконуваних робіт;

e) надання доказів, що були використані критичні рівні безпеки для досягнення мінімальних прийнятних рівнів безпеки та якості конфіденційності;

f) надання доказів, що було виконано достатнє тестування для захисту від навмисного та ненавмисного зловмисного контенту під час постачання;

g) надання доказів, що виконано достатнє тестування для захисту від наявності вразливостей;

h) угоди умовного депонування, наприклад якщо первинні коди більше недоступні;

i) контрактні права доступу для аудиту процесів розроблення та заходів безпеки;

j) ефективне документування середовища, яке використовують для розроблення;

k) організація залишається відповідальною за відповідність законодавству, яке використовують, і підтвердження ефективності заходів безпеки.

Додаткова інформація

Більш докладну інформацію стосовно взаємовідносин з постачальниками наведено в ISO/IEC 27036 [21], [22], [23].

14.2.8 *Тестування безпеки системи*

Заходи безпеки

Тестування функціональності безпеки потрібно виконувати протягом розроблення.

Настанова щодо впровадження

Нові та оновлені системи потребують ретельного тестування та перевірки протягом процесу розроблення, охоплюючи підготовку детальних процедур діяльності й тестових вхідних та очікуваних вихідних даних у діапазоні умов дії систем. Для внутрішніх розробок такі тести первинно повинна виконувати команда розробників. Після цього треба виконувати незалежне приймальне тестування (як для внутрішніх розробок, так і для аутсорсингових розробників) для гарантії того, що система працює як очікували і не інакше (див. 14.1.1 та 14.1.9). Тривалість тестування має бути пропорційною важливості та природи системи.

14.2.9 *Приймальне тестування системи*

Заходи безпеки

Програми приймального тестування та відповідні критерії має бути визначено для нових інформаційних систем, оновлень та нових версій.

Настанова щодо впровадження

Приймальне тестування має включати тестування вимог щодо інформаційної безпеки (див. 14.1.1 і 14.1.2) і дотримання практик безпечного розроблення систем (див. 14.2.1). Тестування потрібно також здійснювати для компонент, які отримують, і системи в цілому. Організація може використовувати автоматичні засоби, такі як засоби аналізу коду чи сканери вразливостей, і має підтверджувати усунуті дефекти, пов'язані з безпекою.

Тестування потрібно здійснювати в реалістичному тестовому середовищі для гарантії, що система не буде вносити вразливостей в середовище організації, і що тести є надійними.

14.3 Дані для тестування системи

Ціль: Забезпечити захист даних, які використовують для тестування.

14.3.1 *Захист даних для тестування системи*

Заходи безпеки

Дані для тестування має бути ретельно відібрано, захищено та контрольовано.

Настанова щодо впровадження

Треба уникати використання для цілей тестування баз даних, які перебувають в експлуатації, містять персональну інформацію чи будь-яку іншу конфіденційну інформацію. Якщо персональну чи будь-яку іншу конфіденційну інформацію використовують для цілей тестування, усі конфіденційні подробиці та вміст має бути видалено чи модифіковано до використання (див. ISO/IEC 29101 [26]).

Для захисту експлуатаційних даних у разі їх використання для цілей тестування потрібно застосовувати наведені нижче настанови:

a) процедури контролю доступу, які застосовують до прикладних систем, що перебувають в експлуатації, потрібно також застосовувати до прикладних систем, які тестують;

b) копіювання експлуатаційної інформації для прикладної системи, яку тестують, треба санкціонувати кожного разу окремо;

c) експлуатаційну інформацію потрібно видаляти з тестового середовища негайно після завершення тестування;

d) копіювання та використання експлуатаційної інформації потрібно реєструвати для формування журналу аудиту.

Додаткова інформація

Приймальне тестування й тестування системи зазвичай потребує значних обсягів тестових даних, найближчих до експлуатаційних даних, наскільки це можливо.

15 ВЗАЄМОВІДНОСИНИ З ПОСТАЧАЛЬНИКАМИ

15.1 Інформаційна безпека у взаємовідносинах з постачальниками

Ціль: Гарантувати захист ресурсів СУІБ організації, які можуть бути доступні постачальникам.

15.1.1 *Політика інформаційної безпеки для взаємовідносин з постачальниками*

Заходи безпеки

Вимоги інформаційної безпеки для послаблення ризиків, пов'язаних із доступом постачальників до ресурсів СУІБ організації має бути погоджено з постачальником та задокументовано.

Настанова щодо впровадження

Організація повинна ідентифікувати в політиці та ввести заходи інформаційної безпеки для специфічних адрес постачальника, який має доступ до інформації організації. Ці заходи безпеки мають бути задіяні в процесах і процедурах, які мають бути впроваджені організацією, а також у тих процесах і процедурах, які організація повинна вимагати під час впровадження постачальником, включаючи:

a) ідентифікацію й документування типів постачальників, наприклад, IT-послуги, послуги логістики, фінансові послуги;

b) стандартизований процес і життєвий цикл для управління взаємовідносинами з постачальником;

c) визначення типів доступу до інформації, який буде дозволено різним типам постачальників; моніторинг і контроль цього доступу;

d) мінімальні вимоги щодо інформаційної безпеки для кожного типу інформації і типу доступу для збереження як основи для окремих угод з індивідуальними постачальниками, основаних на потребах бізнесу організації та її профілях ризиків;

e) процеси та процедури для моніторингу дотримання встановленим вимогам щодо інформаційної безпеки для кожного типу постачальника й типу доступу, включаючи перевірку зовнішньою стороною та сертифікацію продукту;

f) точність і повноту заходів безпеки для гарантії цілісності інформації чи оброблення інформації, яке здійснює інша сторона;

g) типи зобов'язань, які можуть бути прийнятими постачальниками для захисту інформації організації;

h) оброблення інцидентів інформаційної безпеки та випадків, пов'язаних із доступом постачальника, охоплюючи відповідальності як організації, так і постачальника;

i) домовленості стосовно життєздатності та, за потреби, відновлення й потенційних ушкоджень для гарантії доступності інформації чи оброблення інформації, яке здійснює інша сторона;

j) навчальні тренінги для персоналу організації, який залучено до процесу придбання, стосовно політик, процесів та процедур;

k) навчальні тренінги для персоналу організації, який взаємодіє з персоналом постачальника, стосовно відповідних правил угод і поведінки з урахуванням типу постачальника та рівня доступу постачальника до систем та інформації організації;

l) умови, на яких вимоги щодо інформаційної безпеки та засоби безпеки, буде задокументовано в угоді, яку підписує кожна сторона;

m) управління необхідними передаваннями інформації, обладнання для оброблення інформації та будь-чого, що може бути передано, і гарантія, що інформаційна безпека буде виконуватися протягом періоду передавання.

Додаткова інформація

Інформація може бути піддана ризику постачальниками з невідповідним управлінням інформаційною безпекою. Для адміністрування доступу постачальників до засобів оброблення інформації має бути ідентифіковано та застосовано заходи безпеки. Наприклад, якщо є певна потреба конфіденційності інформації, може бути використано угоди щодо нерозголошення. Іншим прикладом є ризики захисту даних у разі, коли угода з постачальником включає передавання даних чи доступ до інформації через кордони. Організація повинна бути поінформована, що законодавча чи контрактна відповідальність за інформацію, яку захищають, залишається в організації.

15.1.2 ***Урахування безпеки в угодах з постачальниками***

Заходи безпеки

Усі відповідні вимоги щодо інформаційної безпеки має бути встановлено та погоджено з кожним постачальником, який може мати доступ, обробляти, зберігати, передавати чи надавати компоненти IT-інфраструктури для інформації організації.

Настанова щодо впровадження

Угоди з постачальниками має бути запроваджено та задокументовано, щоб гарантувати уникнення непорозумінь між організацією та постачальником, враховуючи зобов'язання обох сторін для того, щоб задовольнити відповідні вимоги щодо інформаційної безпеки.

Треба розглянути доцільність включення в угоди таких питань для того, щоб задовольнити визначені вимоги щодо інформаційної безпеки, а саме:

a) опис інформації, яку будуть надавати чи доступ до якої буде надано, і методів надання чи доступу до інформації;

b) класифікація інформації відповідно до схеми класифікації організації (див. 8.2); за потреби також таблиця відповідності між схемою класифікації організації та схемою класифікації постачальника;

c) законодавчі та регуляторні вимоги, охоплюючи захист даних, права інтелектуальної власності й копіювання, а також опис того, як буде гарантовано їх виконання;

d) зобов'язання кожної зі сторін контракту впроваджувати погоджений набір заходів безпеки, зокрема й контроль доступу, перегляд продуктивності, моніторинг, звітність та аудит;

e) правила прийнятного використання інформації, зокрема й небажане використання, за потреби;

f) докладний перелік персоналу постачальника, якого санкціоновано для доступу до інформації або для отримання інформації організації, чи процедури, чи умови санкціонування, або відкликання санкції персоналу постачальника для доступу до інформації чи для отримання інформації організації;

g) політики інформаційної безпеки, важливі для цього специфічного контракту;

h) вимоги та процедури управління інцидентами (особливо повідомлення та співпраця під час усунення інциденту);

i) тренінги та вимоги до розуміння специфічних процедур і вимог щодо інформаційної безпеки, наприклад реагування на інцидент, процедури санкціонування;

j) відповідні правила до субпідрядників, включаючи заходи безпеки, які необхідно впровадити;

k) важливі угоди з партнерами, включаючи контактних осіб для обговорення інформаційної безпеки;

l) вимоги щодо захисту, якщо є, для персоналу постачальника, включаючи осіб, відповідальних за проведення процедур захисту та сповіщення, якщо захист не було завершено або результати викликають сумніви чи занепокоєння;

m) права аудиту процедур і заходів безпеки постачальника, пов'язаних із цією угодою;

n) процедури усунення дефектів та розв'язання конфліктів;

o) зобов'язання постачальника стосовно періодичного надання незалежного звіту щодо ефективності заходів безпеки та погодження на своєчасну корекцію важливих ситуацій, визначених у цьому звіті;

p) зобов'язання постачальника відповідати вимогам щодо безпеки організації.

Додаткова інформація

Для різних організацій та різних типів постачальників угоди можуть значно відрізнятися. Тому треба звернути увагу на охоплення угодою всіх ідентифікованих ризиків і вимог щодо безпеки. Угоди постачальника можуть також залучати інші сторони (наприклад, субпідрядників).

Щоб уникнути будь-якої затримки в розміщенні замінюваних продуктів чи послуг, в угоді має бути розглянуто процедури для продовження обробки, коли третя сторона стає нездатною постачати свої продукти чи послуги.

15.1.3 ***Ланцюг постачання інформаційних та комунікаційних технологій***

Заходи безпеки

Угоди з постачальниками мають містити вимоги стосовно адресації ризиків інформаційної безпеки, пов'язаних з ланцюгом постачання продуктів та послуг інформаційних і комунікаційних технологій.

Настанова щодо впровадження

Має бути розглянуто такі питання для долучення до угод з постачальниками, які стосуються безпеки ланцюга постачання:

a) визначення вимог щодо інформаційної безпеки для врахування до продуктів чи послуг інформаційних і комунікаційних технологій, які планують придбати, додатково до загальних вимог щодо інформаційної безпеки для взаємозв'язків із постачальником;

b) для послуг інформаційних і комунікаційних технологій вимога того, щоб постачальники поширювали вимоги щодо інформаційної безпеки організації вздовж ланцюга постачання, якщо постачальник має субконтракти із зовнішніми сторонами для частин послуг інформаційних і комунікаційних технологій, які він надає організації;

c) для продуктів інформаційних і комунікаційних технологій вимога того, щоб постачальники поширювали вимоги інформаційної безпеки організації вздовж ланцюга постачання, якщо постачальник має субконтракти із зовнішніми сторонами для частин продуктів інформаційних і комунікаційних технологій, які він надає організації;

d) запровадження процесу моніторингу та прийнятних методів для підтвердження, що продукти і послуги інформаційних і комунікаційних технологій, які надають, дотримують визначені вимоги щодо безпеки;

e) запровадження процесу для ідентифікації компонент продукту чи послуг, які є критичними для підтримання функціональності, і тому потребують посиленої уваги й докладної перевірки, якщо їх формують за межами організації, особливо якщо верхній постачальник з ланцюга постачання передає на аутсорсинг іншим постачальникам елементи компонент продукту чи послуги;

f) отримання гарантії, що критичні компоненти і їх джерело може бути відслідковано вздовж ланцюга постачання;

g) отримання гарантії, що продукти інформаційних і комунікаційних технологій, які постачають, функціонують, як очікують, без будь-яких неочікуваних чи небажаних особливостей;

h) визначення ролей для розподілу інформації вздовж ланцюга постачання та будь-яких потенційних витоків і компромісів між організацією та постачальником;

i) запровадження специфічних процесів для управління життєвим циклом і доступністю компонент інформаційних і комунікаційних технологій та пов'язаними з цим ризиками безпеки.

Додаткова інформація

Специфічні практики управління ризиком ланцюга постачання інформаційних і комунікаційних технологій побудовано на узагальненні загального управління інформаційною безпекою, якістю, проектами і практик системного інжинірингу, але не замінюють їх.

Організації повинні консультуватися з постачальниками для розуміння ланцюга постачання інформаційних і комунікаційних технологій та будь-яких питань, які мають важливий вплив на продукти й послуги, які надаватимуть. Організації можуть впливати на практики інформаційної безпеки ланцюга постачання інформаційних і комунікаційних технологій за допомогою чіткого визначення в угодах з їх постачальниками питань, які повинні бути адресованими іншим постачальникам у ланцюгу постачання інформаційних і комунікаційних технологій.

Ланцюг постачання інформаційних і комунікаційних технологій, описаний тут, включає хмарні комп'ютерні послуги.

15.2 Управління наданням послуг постачальником

Ціль: Підтримувати належний рівень інформаційної безпеки та надання послуг відповідно до угод з постачальниками.

15.2.1 *Моніторинг та перегляд послуг постачальника*

Заходи безпеки

Організація повинна регулярно проводити моніторинг, перегляд та аудит отримання послуг постачальника.

Настанова щодо впровадження

Моніторинг та перегляд послуг постачальника повинні забезпечувати, що дотримано терміни й умови угод щодо інформаційної безпеки та управління інцидентами інформаційної безпеки та проблемами здійснюють належним чином.

Це повинне охоплювати процес взаємодії управління послугою між організацією та постачальником щодо:

a) моніторингу рівнів продуктивності послуг для перевірки дотримання угоди;

b) перегляду звітів стосовно послуг, наданих третьою стороною, і проведення регулярних нарад щодо виконання робіт згідно з вимогами угоди;

c) проведення аудиту постачальників разом із переглядом звітів незалежних аудиторів за їх наявності та відслідковуючи ідентифіковані в угоді питання;

d) надання інформації про інциденти інформаційної безпеки та перегляд цієї інформації згідно з угодою та будь-якими настановами й процедурами, що її підтримують;

e) перегляду журналів аудиту постачальника та записів про події безпеки, проблеми експлуатації та відмови, відстежування недоліків та порушень, пов'язаних з надаваною послугою;

f) вирішення та управління всіма ідентифікованими проблемами;

g) перегляду аспектів інформаційної безпеки взаємозв'язків постачальника з його власними постачальниками (партнерами);

h) гарантування того, що постачальник підтримує достатню дієздатність послуг разом із працездатністю планів, розроблених для гарантії того, що погоджені рівні безперервності послуги підтримуються після збоїв послуги або катастрофи (див. розділ 17).

Відповідальність щодо управління взаємодією з постачальником має бути покладено на особу чи групу управління послугою. Крім того, організація повинна забезпечити, щоб постачальник визначив відповідальності щодо перевірки відповідності та примусового застосування вимог угоди. Для моніторингу цих вимог угоди мають бути наявними достатні технічні навички та ресурси, особливо мають задовольнятися вимоги щодо інформаційної безпеки. Якщо помічено недоліки в наданні послуги, треба вжити належні дії.

Організація повинна підтримувати достатній загальний контроль та спостережність усіх аспектів безпеки щодо конфіденційної або критичної інформації чи засобів оброблення інформації, які доступні, обробляються або управляються постачальником. Організація повинна забезпечити збереження спостережності діяльності щодо безпеки, такої як управління змінами, ідентифікація вразливостей та звітування/реагування щодо інциденту безпеки відповідно до визначеного процесу, формату та структури звітування.

15.2.2 *Управління змінами в послугах постачальника*

Заходи безпеки

Зміни в наданні послуг постачальника, зокрема й підтримування та вдосконалювання наявних політик інформаційної безпеки, процедур і заходів безпеки, мають управлятися з урахуванням критичності залучених бізнес-систем і процесів та переоцінки ризиків.

Настанова щодо впровадження

Наведені нижче аспекти потребують урахування:

a) змін в угодах з постачальником;

b) змін, зроблених організацією, для впровадження:

1) покращень поточних запропонованих послуг;

2) розроблення будь-яких нових прикладних програм і систем;

3) модифікації чи оновлення політик та процедур організації;

4) нових або змінених заходів безпеки для розв'язання інцидентів безпеки та вдосконалення безпеки;

c) змін у послугах постачальника для впровадження:

1) змін та покращень у мережах;

2) використання нових технологій;

3) погодження нових продуктів або новіших версій/варіантів реалізації;

4) нових інструментів та середовища розробки;

5) змін фізичного розташування засобів надання послуги;

6) змін постачальників.

16 УПРАВЛІННЯ ІНЦИДЕНТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

16.1 Управління інцидентами інформаційної безпеки та вдосконаленням

Ціль: Гарантувати послідовний та ефективний підхід до управління інцидентами інформаційної безпеки, охоплюючи поширення інформації про події безпеки та слабкі місця.

16.1.1 *Відповідальності та процедури*

Заходи безпеки

Має бути визначено відповідальності керівництва та процедури для забезпечення швидкого, ефективного і правильного реагування на інциденти інформаційної безпеки.

Настанова щодо впровадження

Треба розглянути наведені нижче настанови щодо відповідальностей керівництва та процедур управління інцидентами інформаційної безпеки:

a) має бути визначено відповідальності керівництва для гарантування, що наступні процедури буде розроблено та поширено належним чином всередині організації:

1) процедури для планування та підготовки реагування на інцидент;
2) процедури моніторингу, виявлення, аналізу та звітування про події та інциденти інформаційної безпеки;
3) процедури реєстрації діяльності щодо управління інцидентами;
4) процедури збирання судових доказів;
5) процедури оцінювання й прийняття рішення щодо подій інформаційної безпеки та оцінювання слабких місць інформаційної безпеки;
6) процедури реагування, включаючи процедури ескалації, контрольного відновлення після інциденту та інформування внутрішнього та зовнішнього персоналу чи організацій;

b) визначені процедури мають гарантувати, що:

1) компетентний персонал може обробляти питання, пов'язані з інцидентами інформаційної безпеки всередині організації;
2) запроваджена точка контакту для виявлення та звітування про інциденти інформаційної безпеки;
3) підтримуються відповідні контакти з регуляторними органами, зовнішніми зацікавленими групами або форумами, які аналізують питання, пов'язані з інцидентами інформаційної безпеки;

c) процедури звітування мають включати:

1) розроблення форм звітування про події інформаційної безпеки для підтримки діяльності зі звітування й для допомоги персоналу нагадати всі потрібні дії в разі події інформаційної безпеки;
2) процедуру, яку має бути застосовано в разі події інформаційної безпеки, наприклад, негайну реєстрацію всіх деталей, таких як тип невідповідності чи порушення, відмова, що сталася, повідомлення на екрані та негайна реєстрація в точці контакту і виконання лише скоординованих дій;
3) посилання на затверджений формальний дисциплінарний процес стосовно персоналу, який вчинив порушення безпеки;
4) відповідні процеси зворотного зв'язку для гарантування, що персонал, який повідомив про подію інформаційної безпеки, поінформований про результати після того, як це питання проаналізовано та закрито.

Цілі управління інцидентами інформаційної безпеки має бути погоджено з керівництвом, і треба забезпечити, що особи, відповідальні за управління інцидентами інформаційної безпеки, розуміють пріоритети організації щодо обробки інцидентів інформаційної безпеки.

Додаткова інформація

Інциденти інформаційної безпеки можуть виходити за межі організації та державні кордони. Щоб реагувати на такі інциденти існує потреба, що постійно збільшується, координувати дії у відповідь і спільно використовувати інформацію щодо цих інцидентів з відповідними зовнішніми організаціями.

Докладні настанови стосовно управління інцидентами інформаційної безпеки викладено в ISO/IEC 27035 [20].

16.1.2 *Звітування про події інформаційної безпеки*

Заходи безпеки

Необхідно якнайшвидше звітувати стосовно подій інформаційної безпеки через належні канали управління.

Настанова щодо впровадження

Весь найманий персонал та підрядники повинні бути поінформовані щодо їх відповідальності якнайшвидше звітувати про будь-які події інформаційної безпеки. Вони також повинні бути поінформовані щодо процедури звітування про події інформаційної безпеки і місце контакту, де вони повинні звітувати про події.

Ситуації, які треба розглядати для звітування про події інформаційної безпеки, мають включати:

a) неефективність заходів безпеки;
b) порушення цілісності, конфіденційності або очікуваної доступності;
c) людські помилки;
d) невідповідності політиці чи настановам;
e) порушення заходів фізичної безпеки;
f) неконтрольовані зміни системи;
g) збій програмного забезпечення чи апаратних засобів;
h) порушення доступу.

Додаткова інформація

Збої або інша аномальна поведінка системи можуть бути показником атаки на безпеку або фактичного порушення безпеки, і тому про них треба завжди звітувати як про подію інформаційної безпеки.

16.1.3 *Звітування щодо слабких місць інформаційної безпеки*

Заходи безпеки

Треба вимагати від усього найманого персоналу та підрядників, які користуються інформаційними системами та послугами, звертати увагу та звітувати щодо будь-яких спостережених або очікуваних слабких місць у системах чи послугах.

Настанова щодо впровадження

Увесь найманий персонал та підрядники якнайшвидше повинні звітувати про це в місці контакту, щоб запобігти інцидентам інформаційної безпеки. Процес звітування має бути якомога простішим, доступнішим і досяжним.

Додаткова інформація

Найманому персоналу та підрядникам треба рекомендувати не намагатися знайти підтвердження очікуваного слабкого місця безпеки. Тестування слабких місць можна розцінювати як потенційне зловживання системою і воно може також нашкодити інформаційній системі чи послузі та призвести до правових наслідків для особи, яка здійснює тестування.

16.1.4 *Оцінювання та прийняття рішення стосовно подій інформаційної безпеки*

Заходи безпеки

Події інформаційної безпеки має бути оцінено та прийнято рішення стосовно віднесення їх до інцидентів інформаційної безпеки.

Настанова щодо впровадження

У місці контакту повинні оцінювати кожну подію інформаційної безпеки з використанням узгодженої класифікації подій та інцидентів інформаційної безпеки й вирішувати, чи треба цю подію класифікувати як інцидент інформаційної безпеки. Класифікація та пріоритезація може надати допомогу в ідентифікації впливу та розповсюдженні інциденту.

Якщо організація має команду реагування на інциденти інформаційної безпеки (ISIRT), оцінювання та прийняття рішення може бути переспрямовано до цієї команди (ISIRT) для підтвердження чи переоцінювання.

Результати оцінювання та прийняття рішення має бути детально записано для цілей подальшого посилання й підтвердження.

16.1.5 *Реагування на інциденти інформаційної безпеки*

Заходи безпеки

Реагування на інциденти інформаційної безпеки має здійснюватися відповідно до задокументованої процедури.

Настанова щодо впровадження

Реагування на інциденти інформаційної безпеки має здійснюватися у визначеному місці контакту та іншими призначеними особами організації чи зовнішніх сторін (див. 16.1.1).

Реагування має включати таке:

a) якнайшвидше збирання доказів після виникнення інциденту;
b) виконання судового аналізу інформаційної безпеки, за потреби (див. 16.1.7);
c) ескалацію, за потреби;
d) гарантію, що всю діяльність щодо реагування відповідним чином зареєстровано для подальшого аналізу;
e) повідомлення існування інциденту інформаційної безпеки чи будь-яких пов'язаних із цим деталей іншим внутрішнім і зовнішнім особам чи організаціям, які мають знати про це;

f) визначення зв'язку зі слабкими місцями інформаційної безпеки, які можуть бути причиною або сприяти цьому інциденту;

g) коли інцидент успішно оброблено, формальне закриття та звітування про нього.

За потреби, можна проводити аналіз після інциденту для ідентифікації джерела цього інциденту.

Додаткова інформація

Основною метою реагування на інцидент є повернення до «нормального рівня безпеки» і після цього — ініціація необхідного відновлення.

16.1.6 *Знання з вивчення інцидентів інформаційної безпеки*

Заходи безпеки

Знання, отримані з аналізу та розв'язання інцидентів інформаційної безпеки, мають використовувати для зменшення ймовірності чи впливу майбутніх інцидентів.

Настанова щодо впровадження

Мають існувати механізми, які дозволяють кількісно оцінити й відслідкувати типи, обсяги й вартість інцидентів інформаційної безпеки. Інформацію, отриману від зіставляння інцидентів інформаційної безпеки, потрібно використовувати для ідентифікації інцидентів, які повторюються чи мають значний вплив.

Додаткова інформація

Зіставляння інцидентів інформаційної безпеки може вказати на потребу в удосконалених або додаткових заходах безпеки для обмеження частоти, пошкодження та вартості майбутніх інцидентів або може бути взято до уваги в процесі перегляду політики безпеки (див. 5.1.2).

З міркувань конфіденційності короткі історії (анекдоти) з реальних інцидентів інформаційної безпеки можна використовувати в тренінгах користувачів з питань безпеки (див. 7.2.2) як приклади того, що може трапитися, як реагувати на такі інциденти та як уникати їх в майбутньому.

16.1.7 *Збирання доказів*

Заходи безпеки

Організація повинна визначити і використовувати процедури для ідентифікації, збирання, отримання і зберігання інформації, яку можна використовувати як докази.

Настанова щодо впровадження

Мають бути розроблені та виконуватися внутрішні процедури збирання доказів для дисциплінарних цілей та юридичних дій.

Загалом процедури щодо доказів мають забезпечувати ідентифікацію, збір, зберігання й надання доказів відповідно до різних типів середовища, обладнання та статусу обладнання, наприклад увімкнено чи вимкнено. Ці процедури мають включати:

a) ланцюг охорони;

b) безпеку доказів;

c) безпеку персоналу;

d) ролі та відповідальності персоналу, якого це стосується;

e) компетентність персоналу;

f) документування;

g) інструктаж.

Там, де це можливо, сертифікація або інші доречні засоби підтвердження кваліфікації персоналу має бути розглянуто для посилення значення збережених доказів.

Докази можуть виходити за межі організації та/чи юрисдикції. У таких випадках треба забезпечити, щоб організація мала право збирати необхідну інформацію як судовий доказ. Щоб максимально збільшити можливості визнання за межами відповідної юрисдикції, має також бути розглянуто вимоги різних юрисдикцій.

Додаткова інформація

Ідентифікація — це процес, який охоплює пошук, розпізнавання й документування потенційних доказів. Збирання — це процес комплектування фізичних об'єктів, які можуть містити потенційні докази. Отримання — це процес створення копій даних у межах визначеного набору. Зберігання — це процес підтримки та охорони цілісності й первинного стану потенційних доказів.

Якщо подію інформаційної безпеки виявлено вперше, може бути неочевидним, чи може ця подія призвести до судовий дій. Тому може існувати загроза, що необхідні докази буде знищено навмисно чи випадково до того, як серйозність інциденту буде зрозумілою. Доцільно долучати адвоката чи поліцію одразу в будь-яку юридичну дію, яку планують зробити, і отримати консультацію стосовно потрібних доказів.

Настанови щодо ідентифікації, збирання, отримання та зберігання цифрових доказів описано в ISO/IEC 27037 [24].

17 АСПЕКТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УПРАВЛІННЯ БЕЗПЕРЕРВНІСТЮ БІЗНЕСУ

17.1 Безперервність інформаційної безпеки

Ціль: Безперервність інформаційної безпеки має бути залучено в системи управління безперервністю бізнесу організації.

17.1.1 *Планування безперервності інформаційної безпеки*

Заходи безпеки

Організація повинна визначити свої вимоги щодо інформаційної безпеки та безперервності управління інформаційною безпекою в надзвичайних ситуаціях, наприклад під час кризи чи катастрофи.

Настанова щодо впровадження

Організація повинна визначити, чи приділяти увагу безперервності інформаційної безпеки всередині процесу управління безперервністю бізнесу або процесу управління відновленням після катастрофи. Вимоги щодо інформаційної безпеки має бути визначено під час планування безперервності бізнесу та відновлення після катастрофи.

За відсутності формальних планів безперервності бізнесу та відновлення після катастрофи процес управління інформаційною безпекою має передбачати, що вимоги щодо інформаційної безпеки залишаються такими самими в надзвичайних ситуаціях, як і під час нормальних операційних умов роботи. Іншим вибором буде таке: організація може виконати аналіз впливу на бізнес аспектів інформаційної безпеки для визначення вимог щодо інформаційної безпеки, які можна запроваджувати для надзвичайних ситуацій.

Додаткова інформація

Для зменшення часу та зусиль на виконання «додаткового» аналізу впливу на бізнес для інформаційної безпеки рекомендовано розглядати аспекти інформаційної безпеки разом з нормальним управлінням безперервністю бізнесу чи аналізом впливу на бізнес управління відновлення після катастроф. Це призведе до точного формулювання вимог щодо інформаційної безпеки в процесах управління безперервністю бізнесу чи управління відновленням робіт після катастроф.

Інформацію стосовно управління безперервністю бізнесу наведено в ISO/IEC 27031 [14], ISO 22313 [9] та ISO 22301 [8].

17.1.2 *Реалізація безперервності інформаційної безпеки*

Заходи безпеки

Організація повинна розробити, задокументувати, реалізувати та підтримувати процеси, процедури та заходи безпеки для гарантування необхідного рівня безперервності щодо інформаційної безпеки під час надзвичайної ситуації.

Настанова щодо впровадження

Організація повинна гарантувати, що:

a) адекватна структура управління підготовлена для пом'якшення та реагування на руйнівну подію за допомогою персоналу з потрібними правами, досвідом і компетенцією;

b) визначений персонал для реагування на інциденти з потрібними повноваженнями, правами і компетенцією для управління інцидентом та підтримування інформаційної безпеки;

c) розроблено та запроваджено задокументовані плани, процедури реагування та відновлення, які деталізують, як будуть управляти організацією в надзвичайних ситуаціях і будуть підтримувати свою інформаційну безпеку на заздалегідь визначеному рівні, базуючись на затверджених керівництвом цілях безперервності інформаційної безпеки (див. 17.1.1).

Відповідно до вимог безперервності інформаційної безпеки організація повинна розробити, задокументувати, впровадити та підтримувати:

a) заходи безпеки всередині процесів, процедур і систем підтримки й інструментів для безперервності бізнесу та відновлення роботи після катастроф;

b) процеси, процедури та зміни здійснення реалізації для підтримування наявних заходів безпеки протягом надзвичайного періоду;

c) додаткові заходи для заходів безпеки, які не може бути підтримано протягом надзвичайної ситуації.

Додаткова інформація

Має бути визначено специфічні процеси та процедури в контексті безперервності бізнесу чи відновлення після катастрофи. Інформація, яку обробляють у цих процесах та процедурах чи всередині задіяних інформаційних систем для їхньої підтримки має бути захищено. Тому організація повинна

залучати спеціалістів з інформаційної безпеки під час розроблення, впровадження та підтримування процесів і процедур безперервності бізнесу чи відновлення після катастроф.

Заходи безпеки, які було впроваджено, мають діяти протягом надзвичайної ситуації. Якщо заходи безпеки не можуть продовжувати убезпечувати, мають бути розроблені, впроваджені та підтримуватися інші заходи безпеки для забезпечення припустимого рівня інформаційної безпеки.

17.1.3 *Верифікація, перегляд та оцінювання безперервності інформаційної безпеки*

Заходи безпеки

Організація повинна підтверджувати розроблені та впроваджені заходи безперервності інформаційної безпеки через регулярні інтервали часу для гарантування, що вони дійсні та ефективні протягом надзвичайних ситуацій.

Настанова щодо впровадження

Організаційні, технічні, процедурні та процесні зміни як у контексті операційної діяльності, так і в контексті безперервності бізнесу, можуть призвести до змін у вимогах безперервності інформаційної безпеки. У такому разі процеси, процедури і заходи для інформаційної безпеки має бути переглянуто з урахуванням цих змінених вимог.

Організація повинна підтверджувати свою безперервність управління інформаційною безпекою за допомогою:

a) перевірки й тестування функціональності процесів, процедур і заходів безперервності інформаційної безпеки для гарантії, що вони відповідають цілям безперервності інформаційної безпеки;

b) перевірки й тестування знань та планів дій для виконання процесів, процедур та заходів безперервності інформаційної безпеки для гарантії, що їх продуктивність відповідає цілям безперервності інформаційної безпеки;

c) переглядів підтвердження та ефективності заходів безперервності інформаційної безпеки в разі змін в інформаційних системах, процесах, процедурах і заходах інформаційної безпеки чи процесах та рішеннях з управління безперервності бізнесу/управління відновлення роботи після катастроф.

Додаткова інформація

Підтвердження заходів безперервності інформаційної безпеки відрізняється від загального тестування й підтвердження інформаційної безпеки та має виконуватися за межами тестування змін. Якщо це можливо, найкраще інтегрувати підтвердження заходів безперервності інформаційної безпеки з тестуваннями організацією безперервності бізнесу чи відновлення роботи після катастроф.

17.2 Резервне обладнання

Ціль: Гарантувати доступність обладнання для оброблення інформації.

17.2.1 *Доступність обладнання для оброблення інформації*

Заходи безпеки

Обладнання оброблення інформації має бути впроваджено з резервуванням, достатнім для того, щоб відповідати вимогам доступності.

Настанова щодо впровадження

Організація повинна ідентифікувати бізнес-вимоги для доступності інформаційних систем. Якщо доступність не може бути гарантовано з використанням наявної архітектури систем, має бути розглянуто резервні компоненти чи архітектури.

Резервні інформаційні системи в разі їх використання має бути протестовано для гарантії, що перехід з одного компонента на інший працює, як передбачено.

Додаткова інформація

Впровадження резервного обладнання може спричинити ризики цілісності або конфіденційності інформації та інформаційних систем, які потрібно розглянути під час створення інформаційних систем.

18 ВІДПОВІДНІСТЬ

18.1 Відповідність правовим та контрактним вимогам

Ціль: Уникнути порушень будь-якого закону, вимог, що діють на підставі закону, нормативних або контрактних зобов'язань, пов'язаних з інформаційною безпекою та будь-якими вимогами щодо безпеки.

18.1.1 ***Ідентифікація застосовного законодавства та контрактних вимог***

Заходи безпеки

Усі важливі вимоги, що діють на підставі закону, нормативні чи контрактні вимоги та підхід організації до задоволення цих вимог має бути чітко визначено, задокументовано й актуалізовано для кожної інформаційної системи та організації.

Настанова щодо впровадження

Аналогічно має бути визначено та задокументовано певні заходи безпеки та індивідуальні обов'язки для задоволення цих вимог.

Менеджери повинні ідентифікувати всі вимоги застосовного до їх організації законодавства для того, щоб відповідати вимогам до їх типу бізнесу. Якщо організація займається бізнесом в інших країнах, менеджери повинні розглянути відповідність у всіх цих країнах.

18.1.2 ***Права інтелектуальної власності***

Заходи безпеки

Має бути впроваджено належні процедури забезпечення відповідності законодавчим, нормативним і контрактним вимогам щодо прав інтелектуальної власності та щодо використання запатентованих продуктів програмного забезпечення.

Настанова щодо впровадження

Для захисту будь-яких матеріалів, які можна вважати інтелектуальною власністю, треба розглядати наведені нижче настанови:

a) публікація політики відповідності правам інтелектуальної власності, яка визначає правове використання програмного забезпечення та інформаційних продуктів;

b) придбання програмного забезпечення лише через відомі та визнані джерела для забезпечення того, що авторські права не порушуються;

c) підтримка поінформованості щодо політики захисту прав інтелектуальної власності та надання попередження про намір вжиття дисциплінарних дій проти персоналу, який їх порушує;

d) підтримка відповідних реєстрів ресурсів СУІБ та ідентифікація всіх ресурсів СУІБ з вимогами захисту прав інтелектуальної власності;

e) підтримка доказів та свідоцтв володіння ліцензіями, майстер-дисків, настанов тощо;

f) запровадження заходів безпеки для забезпечення того, щоб не було перевищено будь-якої кількості дозволених користувачів;

g) виконання перевірок, що інстальовано лише санкціоноване програмне забезпечення та ліцензовані продукти;

h) надання політики підтримки належних умов ліцензування;

i) надання політики вилучення чи передавання програмного забезпечення іншим;

j) відповідність термінам та умовам щодо програмного забезпечення та інформації, отриманих із загальнодоступних мереж;

k) відсутність відмінного від дозволеного авторським правом дублювання, перетворення в інший формат або виділення з комерційних записів (кіно, аудіо);

l) недопущення відмінного від дозволеного авторським правом повного або часткового копіювання книг, статей, звітів або інших документів.

Додаткова інформація

Права інтелектуальної власності охоплюють авторське право на програмне забезпечення чи документ на авторське право, права на промисловий зразок, торгові марки, патенти й ліцензії на початковий текст.

Патентований програмний продукт зазвичай постачають згідно з ліцензійною угодою, яка визначає терміни та умови ліцензії, наприклад, обмеження використання продуктів визначеними комп'ютерами або обмеження копіювання створенням лише резервних копій. Важливість та обізнаність щодо прав інтелектуальної власності має бути пояснено персоналу стосовно програмного забезпечення, розробленого організацією.

Законодавчі, регуляторні та контрактні вимоги можуть накладати обмеження на копіювання патентованих матеріалів. Зокрема, вони можуть вимагати, що можна використовувати лише матеріал, розроблений організацією або який ліцензовано чи надано організації розробником. Порушення авторського права може призвести до судового позову, який може залучати кримінальне переслідування.

18.1.3 *Захист організаційних записів*

Заходи безпеки

Відповідно до законодавчих, регуляторних, контрактних і бізнес-вимог важливі записи має бути захищено від втрати, знищення, фальсифікації, несанкціонованого доступу та несанкціонованого використання.

Настанова щодо впровадження

Під час вирішення питання щодо захисту специфічних організаційних записів має бути розглянуто відповідну їх класифікацію, основану на схемі класифікації організації. Записи має бути класифіковано за типами, наприклад облікові записи, записи баз даних, журнали транзакцій, журнали аудиту та експлуатаційних процедур, кожна з подробицями щодо періоду зберігання й типу носія пам'яті, наприклад папір, мікрофіш, магнітний, оптичний. Будь-які відповідні криптографічні ключові дані, а також програми, пов'язані із зашифрованими архівами або цифровими підписами (див. розділ 10), для уможливлення розшифрування записів потрібно також зберігати протягом строку зберігання записів.

Треба розглянути можливість псування носіїв, використаних для зберігання записів. Процедури зберігання та оброблення треба запроваджувати відповідно до рекомендацій виробника.

Там, де вибрано електронні засоби зберігання, для захисту від втрат через майбутні заміни техніки мають бути наявними процедури забезпечення доступу до даних (до зчитування як носіїв, так і формату) протягом періоду тривалого зберігання.

Системи зберігання даних потрібно обирати так, щоб необхідні дані можна було віднайти у прийнятному форматі за прийнятний період часу та залежно від вимог, які мають виконуватися.

Система зберігання та оброблення має забезпечувати чітку ідентифікацію записів та періоду їх тривалого зберігання, як визначено застосовним національним або регіональним законодавством чи нормативами. Ця система має дозволяти відповідне знищення записів після цього періоду, якщо вони не потрібні організації.

Для досягнення цих цілей захисту записів в організації треба виконувати наведені нижче кроки:

a) має бути видано настанови щодо тривалого зберігання, оброблення й вилучення записів та інформації;

b) має бути складено графік тривалого зберігання, який ідентифікує записи й період часу, протягом якого їх треба тривало зберігати;

c) треба підтримувати інвентарні описи джерел ключової інформації.

Додаткова інформація

Деякі записи можуть потребувати безпечного тривалого зберігання для задоволення законодавчих, регуляторних або контрактних вимог, а також для підтримки основної бізнес-діяльності. Прикладами є записи, які можуть бути потрібні як докази функціонування організації в межах законодавчих або регуляторних правил, щоб забезпечити захист від потенційних громадянських чи кримінальних позовів, чи для підтвердження фінансового стану організації відносно акціонерів, зовнішніх сторін та аудиторів. Період часу та вміст даних для тривалого зберігання інформації може встановлювати національний закон або нормативи.

Подальшу інформацію стосовно управління організаційними записами можна знайти в ISO 15489-1 [5].

18.1.4 *Захист даних та конфіденційність персональних даних*

Заходи безпеки

Конфіденційність і захист даних, що ідентифікують особу, має бути забезпечено згідно з вимогами відповідного законодавства та регуляторними вимогами, за наявності.

Настанова щодо впровадження

Має бути розроблено й запроваджено політику організації щодо конфіденційності та захисту персональних даних. Цю політику має бути доведено до відома всіх осіб, залучених до оброблення персональної інформації.

Відповідність цієї політики всьому чинному законодавству й регуляторним вимогам щодо захисту персональних даних вимагає відповідної структури управління та контролю. Часто найкраще цього досягають призначенням відповідальної особи, як наприклад, службовця із захисту персональних даних, який повинен надавати настанови для керівників, користувачів і постачальників послуг щодо їх особистої відповідальності і певних процедур, яким треба слідувати. Відповідальність за оброблення персональних даних та забезпечення поінформованості щодо принципів захисту персональних даних має здійснюватися згідно з відповідним законодавством та регуляторними вимогами. Має бути запроваджено відповідні технічні та організаційні заходи для захисту персональних даних.

Додаткова інформація

В ISO/IEC 29100 [25] описано загальні настанови стосовно захисту персональних даних в інформаційних і телекомунікаційних системах. Багато країн ввело законодавство, яке встановлює заходи безпеки на збирання, оброблення та передавання персональних даних (взагалі інформацію щодо наявних осіб, які може бути ідентифіковано за цією інформацією). Залежно від відповідного національного законодавства такі заходи безпеки можуть накладати обов'язки на тих, хто збирає, обробляє та поширює персональні дані, і можуть також обмежувати можливість передавання таких даних до інших країн.

18.1.5 *Нормативи щодо криптографічних засобів*

Заходи безпеки

Криптографічні засоби потрібно використовувати відповідно до всіх застосовних угод, законів та регуляторних вимог.

Настанова щодо впровадження

Для відповідності всім застосовним угодам, законам та регуляторним вимогам треба розглянути наведені нижче позиції:

a) обмеження імпорту та експорту комп'ютерних апаратних засобів та програмного забезпечення для виконання криптографічних функцій;

b) обмеження імпорту та експорту комп'ютерних апаратних засобів та програмного забезпечення, розроблених для долучення в них криптографічних функцій;

c) обмеження використання шифрування;

d) обов'язкові чи віддані на розсуд методи доступу повноважних органів країни до інформації, зашифрованої за допомогою апаратних або програмних засобів для забезпечення конфіденційності вмісту.

Для забезпечення відповідності національним законам та регуляторним вимогам має бути отримано правові рекомендації. До того, як передати зашифровану інформацію або криптографічні засоби до іншої країни крізь кордони юрисдикції, також має бути отримано правові рекомендації.

18.2 Перевірки інформаційної безпеки

Ціль: Гарантувати, що інформаційна безпека впроваджена та працює відповідно до організаційних політик та процедур.

18.2.1 *Незалежні перевірки інформаційної безпеки*

Заходи безпеки

Підходи організації до управління інформаційною безпекою та її впровадження (тобто цілі заходів безпеки, заходи безпеки, політики, процеси й процедури для інформаційної безпеки) мають незалежно перевірятися через заплановані інтервали або коли відбуваються значні зміни.

Настанова щодо впровадження

Керівники повинні ініціювати незалежні перевірки. Такі незалежні перевірки потрібні для гарантування постійної придатності, адекватності та ефективності підходу організації до управління інформаційною безпекою. Перевірка має охоплювати оцінку можливості для покращення й потребу у змінах підходу до безпеки, зокрема й політики та цілей заходів безпеки.

Такі перевірки повинні виконувати особи, незалежні від сфери діяльності, яку перевіряють, наприклад функція внутрішнього аудиту, незалежний менеджер або зовнішні організації, які спеціалізуються на таких перевірках. Особи, які здійснюють такі перевірки, повинні мати відповідні навички й досвід.

Результати незалежних перевірок має бути записано й доведено до керівництва, яке ініціювало цю перевірку. Ці записи має бути збережено.

Якщо незалежна перевірка показала, що підхід організації та впровадження управління інформаційною безпекою є неадекватними, наприклад, задокументовані цілі та вимоги не виконують або не відповідають напрямкам інформаційної безпеки, визначеним у політиках інформаційної безпеки (див. 5.1.1), керівництво повинно запровадити коригувальні дії.

Додаткова інформація

В ISO/IEC 27007 [12] «Guidelines for information security management systems auditing» та ISO/IEC TR 27008 [13] «Guidelines for auditors on information security controls» також надано настанови стосовно виконання незалежних перевірок.

18.2.2 *Відповідність політикам і стандартам безпеки*

Заходи безпеки

Керівники повинні регулярно перевіряти відповідність оброблення інформації та процедур у межах сфери їх відповідальності належним політикам, стандартам та іншим вимогам щодо безпеки.

Настанова щодо впровадження

Керівники повинні визначити, як перевіряти, що вимоги щодо інформаційної безпеки, зазначені в політиках, стандартах та інших відповідних нормативних документах, виконуються. Для ефективних регулярних перевірок потрібно розглядати засоби автоматизованого вимірювання та звітування.

Якщо в результаті перегляду виявлено будь-яку невідповідність, керівники повинні:

a) визначити причини невідповідності;

b) оцінити потребу в діях для забезпечення відповідності;

c) визначити та впровадити належну коригувальну дію;

d) здійснити перевірку вжитої коригувальної дії для підтвердження її ефективності та визначити будь-які відхилення чи слабкі місця.

Результати перевірок і коригувальних дій, виконаних керівниками, потрібно реєструвати, а ці записи треба підтримувати. Керівники повинні звітувати про результати особам, які проводять незалежні перевірки (див. 18.2.1), якщо незалежна перевірка є у сфері їх відповідальності.

Додаткова інформація

Експлуатаційний моніторинг використання системи наведено у 12.4.

18.2.3 *Перевірка технічної відповідності*

Заходи безпеки

Інформаційні системи потрібно регулярно перевіряти на відповідність політикам і стандартам інформаційної безпеки організації.

Настанова щодо впровадження

Перевіряти технічну відповідність потрібно переважно за допомогою автоматизованого інструментарію, який формує технічні звіти для їх подальшої інтерпретації технічними спеціалістами. Як альтернативний спосіб, перевірки може проводити вручну (за підтримки, якщо потрібно, належних інструментів програмного забезпечення) досвідчений системний інженер.

Якщо використовують тестування на проникнення чи оцінку вразливості, має бути проявлено обачність, оскільки такі дії можуть призвести до компрометації безпеки системи. Такі тестування має бути заплановано, задокументовано та повторювано.

Будь-яку перевірку технічної відповідності треба виконувати лише компетентним санкціонованим особам або під наглядом таких осіб.

Додаткова інформація

Перевірка технічної відповідності включає обстеження систем, що перебувають в експлуатації, щоб забезпечити, що заходи безпеки апаратного та програмного забезпечення впроваджено коректно. Такий вид перевірки відповідності потребує експертизи технічного спеціаліста.

Перевірка відповідності також включає, наприклад, тестування на проникнення та оцінку вразливостей, які може виконувати незалежний експерт, з яким укладено контракт спеціально для цих цілей. Це може бути корисним у разі виявлення вразливостей в системі та для перевірки того, наскільки ефективними є заходи безпеки для запобігання несанкціонованому доступу внаслідок цих вразливостей.

Тестування на проникнення та оцінка вразливостей надає миттєвий знімок системи в певному стані в певний час. Миттєвий знімок обмежено тими частинами системи, які дійсно тестували під час спроб(и) проникнення. Тестування на проникнення та оцінка вразливостей не замінює оцінювання ризику.

У технічному регламенті ISO/IEC TR 27008 [13] надано специфічну настанову стосовно перевіряння технічної відповідності.

БІБЛІОГРАФІЯ

1 ISO/IEC Directives, Part 2

2 ISO/IEC 11770-1 Information technology — Security techniques — Key management — Part 1: Framework

3 ISO/IEC 11770-2 Information technology — Security techniques — Key management — Part 2: Mechanisms using symmetric techniques

4 ISO/IEC 11770-3 Information technology — Security techniques — Key management — Part 3: Mechanisms using asymmetric techniques

5 ISO 15489-1 Information and documentation — Records management — Part 1: General

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

7 ISO/IEC 20000-2[1)] Information technology — Service management — Part 2: Guidance on application of service management systems

8 ISO/IEC 22301 Societal security — Business continuity management systems — Requirements

9 ISO/IEC 22313 Societal security — Business continuity management systems — Guidance

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

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

12 ISO/IEC 27007 Information technology — Security techniques — Guidelines for information security management systems auditing

13 ISO/IEC TR 27008 Information technology — Security techniques — Guidelines for auditors on information security controls

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

15 ISO/IEC 27033-1 Information technology — Security techniques — Network security — Part 1: Overview and concepts

16 ISO/IEC 27033-2 Information technology — Security techniques — Network security — Part 2: Guidelines for design and implementation of network security

17 ISO/IEC 27033-3 Information technology — Security techniques — Network security — Part 3: Reference networking scenarios — Threats, design techniques and control issues

18 ISO/IEC 27033-4 Information technology — Security techniques — Network security — Part 4: Securing communications between networks using security gateways

19 ISO/IEC 27033-5 Information technology — Security techniques — Network security — Part 5: Securing communications across networks using Virtual Private Networks (VPNs)

20 ISO/IEC 27035 Information technology — Security techniques — Informaton security incident management

21 ISO/IEC 27036-1 Information technology — Security techniques — Information security for supplier relationships — Part 1: Overview and concepts

22 ISO/IEC 27036-2 Information technology — Security techniques — Information security for supplier relationships — Part 2: Common requirements

23 ISO/IEC 27036-3 Information technology — Security techniques — Information security for supplier relationships — Part 3: Guidelines for ICT supply chain security

24 ISO/IEC 27037 Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence

25 ISO/IEC 29100 Information technology — Security techniques — Privacy framework

26 ISO/IEC 29101 Information technology — Security techniques — Privacy architecture framework

27 ISO 31000 Risk management — Principles and guidelines.

НАЦІОНАЛЬНЕ ПОЯСНЕННЯ

1 ISO/IEC Директиви. Частина 2

2 ISO/IEC 11770-1 Інформаційні технології. Методи захисту. Керування ключами. Частина 1. Основні положення

3 ISO/IEC 11770-2 Інформаційні технології. Методи захисту. Керування ключами. Частина 2. Механізми з використанням симетричних алгоритмів

4 ISO/IEC 11770-3 Інформаційні технології. Методи захисту. Керування ключами. Частина 3. Механізми з використанням асиметричних алгоритмів

5 ISO 15489-1 Інформація та документація. Керування записами. Частина 1. Загальні положення

[1)] ISO/IEC 20000-2:2005 скасовано та замінено на ISO/IEC 20000-2:2012 Інформаційні технології. Керування послугами. Частина 2. Настанови щодо застосування систем керування послугами.

6 ISO/IEC 20000-1 Інформаційні технології. Керування послугами. Частина 1. Вимоги до системи керування послугами

7 ISO/IEC 20000-2[1)] Інформаційні технології. Керування послугами. Частина 2. Настанови щодо застосування систем керування послугами

8 ISO 22301 Соціальна безпека. Системи управління безперервністю бізнесу. Вимоги

9 ISO 22313 Соціальна безпека. Системи управління безперервністю бізнесу. Настанова

10 ISO/IEC 27001 Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги

11 ISO/IEC 27005 Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки

12 ISO/IEC 27007 Інформаційні технології. Методи захисту. Настанови для аудиту систем управління інформаційною безпекою

13 ISO/IEC TR 27008 Інформаційні технології. Методи захисту. Настанови для аудиторів заходів інформаційної безпеки

14 ISO/IEC 27031 Інформаційні технології. Методи захисту. Настанови для інформаційних і телекомунікаційних технологій стосовно готовності до забезпечення безперервності бізнесу

15 ISO/IEC 27033-1 Інформаційні технології. Методи захисту. Безпека мережі. Частини 1. Огляд та концепції

16 ISO/IEC 27033-2 Інформаційні технології. Методи захисту. Безпека мережі. Частина 2. Настанови щодо проектування та впровадження безпеки мереж

17 ISO/IEC 27033-3 Інформаційні технології. Методи захисту. Безпека мережі. Частина 3. Рекомендовані сценарії мереж. Загрози, методи проектування та заходи безпеки

18 ISO/IEC 27033-4 Інформаційні технології. Методи захисту. Безпека мережі. Частина 4. Убезпечення міжмережевих комунікацій з використанням шлюзів безпеки

19 ISO/IEC 27033-5 Інформаційні технології. Методи захисту. Безпека мережі. Частина 5. Убезпечення комунікацій в мережах з використанням віртуальної приватної мережі (VPNs)

20 ISO/IEC 27035 Інформаційні технології. Методи захисту. Управління інцидентами інформаційної безпеки

21 ISO/IEC 27036-1 Інформаційні технології. Методи захисту. Інформаційна безпека для взаємовідносин з постачальниками. Частина 1. Огляд та концепції

22 ISO/IEC 27036-2 Інформаційні технології. Методи захисту. Інформаційна безпека щодо взаємовідносин з постачальниками. Частина 2. Загальні вимоги

23 ISO/IEC 27036-3 Інформаційні технології. Методи захисту. Інформаційна безпека щодо взаємовідносин з постачальниками. Частина 3. Настанови щодо безпеки ланцюгів постачання ІКТ

24 ISO/IEC 27037 Інформаційні технології. Методи захисту. Настанови щодо ідентифікації, збирання, отримання та зберігання цифрових доказів

25 ISO/IEC 29100 Інформаційні технології. Методи захисту. Основні положення щодо приватності

26 ISO/IEC 29101 Інформаційні технології. Методи захисту. Основні положення щодо архітектури приватності

27 ISO/IEC 31000 Управління ризиками. Принципи та настанови.

ДОДАТОК НА
(довідковий)

ПЕРЕЛІК НАЦІОНАЛЬНИХ СТАНДАРТІВ УКРАЇНИ, ІДЕНТИЧНИХ З МІЖНАРОДНИМИ СТАНДАРТАМИ, ПОСИЛАННЯ НА ЯКІ Є В ЦЬОМУ СТАНДАРТІ

ДСТУ ISO/IEC 11770-1:2015 Інформаційні технології. Методи захисту. Керування ключами. Частина 1. Основні положення (ISO/IEC 11770-1:2010, IDT)

ДСТУ ISO/IEC 11770-2:2015 Інформаційні технології. Методи захисту. Керування ключами. Частина 2. Механізми з використанням симетричних методів (ISO/IEC 11770-2:2008; Cor 1:2009, IDT);

ДСТУ ISO/IEC 11770-3:2015 Інформаційні технології. Методи захисту. Керування ключами. Частина 3. Механізми з використанням асиметричних методів (ISO/IEC 11770-3:2008; Cor 1:2009, IDT);

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

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

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

Код УКНД 35.040

Ключові слова: безпека віддаленої роботи, безпека людських ресурсів, відповідальність, відповідність, заходи безпеки, інформаційна безпека, інформаційні технології, інцидент інформаційної безпеки, криптографічний захист, методи захисту, політика інформаційної безпеки, правила доступу, ресурси СУІБ, ризики інформаційної безпеки, система управління інформаційною безпекою, фізична безпека.

Редактор **І. Дьячкова**

Верстальник **С. Неділько**

Підписано до друку 29.08.2016. Формат 60 × 84 1/8.
Ум. друк. арк. 8,37. Зам. 1776 Ціна договірна.

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

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