Розділ 20. Аудит інформаційної та/або кібербезпеки

20.1. Етапи проведення аудиту.
20.2. Аудит на основі аналізу ризиків.
20.3. Аудит на основі стандартів інформаційної безпеки (ІБ).
20.4. Аудит на основі експертних досліджень інформаційних систем (ІС).
20.5. Забезпечення безперервності бізнес-процесів: Поняття бізнес-процесу. Модель бізнес-процесу.
20.6. Розробка політик інформаційної безпеки під час забезпечення бізнес-процесів.
20.7. Дотримання політик інформаційної безпеки під час забезпечення бізнес-процесів.

20.1. Етапи проведення аудиту

Аудит інформаційної безпеки – системний процес отримання об'єктивних якісних та кількісних оцінок про поточний стан інформаційної безпеки автоматизованої системи відповідно до певних критеріїв та показників безпеки.

Інформаційна безпека (ІБ) – стан збереження інформаційних ресурсів та захищеності законних прав особистості та суспільства в інформаційній сфері.

Аудит дозволяє оцінити поточну безпеку функціонування інформаційної системи, оцінити та прогнозувати ризики, керувати їх впливом на бізнес-процеси фірми, коректно та обґрунтовано підійти до питання забезпечення безпеки її інформаційних активів, стратегічних планів розвитку, маркетингових програм, фінансових та бухгалтерських відомостей, вмісту корпоративних баз. даних. Зрештою, грамотно проведений аудит безпеки інформаційної системи дозволяє досягти максимальної віддачі від коштів, що інвестуються у створення та обслуговування системи безпеки фірми.

В Україні використовується наступний стандарт: **ДСТУ ISO/IEC 27007:2018 Інформаційні технології. Методи захисту. Настанова щодо аудиту систем управління інформаційною безпекою (ISO/IEC 27007:2017, IDT)** – Цей документ містить вказівки щодо управління програмою аудиту системи управління інформаційною безпекою (СУІБ), щодо проведення аудитів та компетентності аудиторів СУІБ, на додаток до вказівок, що містяться в ISO 19011. Цей документ стосується тих, хто потребує розуміння чи проведення внутрішніх чи зовнішніх аудитів СУІБ або управління програмою аудиту СУІБ.

Крім того, важливу роль стандартизації критеріїв грає асоціація **ISACA** (Information Systems Audit and Control Association). Ця асоціація заснована в 1969 році і в даний час об'єднує близько 20 тисяч членів із понад 100 країн. Вона підтримує діяльність більш як 12 тисяч аудиторів інформаційних систем. На допомогу професійним аудиторам, адміністраторам та зацікавленим користувачам асоціацією ISACA із залученням фахівців із провідних світових

консалтингових компаній було розроблено стандарт **CoBIT**. Цей стандарт в даний час доступний для застосування всіма бажаючими, причому ISACA (www.isaca.org) сприяє створенню організаціями свого персонального варіанту застосування стандарту (так званого **myCoBit**).

Основні напрямки діяльності в галузі аудиту безпеки інформації

Основні напрями аудиту інформаційної безпеки деталізуються такі: атестацію; контроль захищеності інформації; спеціальні дослідження технічних засобів та проектування об'єктів у захищеному виконанні.

1. Атестація об'єктів інформатизації щодо вимог безпеки інформації:

– атестація автоматизованих систем, засобів зв'язку, обробки та передачі інформації;

– атестація приміщень, призначених для проведення конфіденційних переговорів;

– атестація технічних засобів, встановлених у виділених приміщеннях.

2. Контроль захищеності інформації обмеженого доступу:

– виявлення технічних каналів витоку інформації та способів несанкціонованого доступу до неї;

– контроль ефективності засобів захисту інформації.

3. Спеціальні дослідження технічних засобів на наявність побічних електромагнітних випромінювань та наведень (ПЕМВН):

– персональні ЕОМ, засоби зв'язку та обробки інформації;

– локальні обчислювальні системи;

– оформлення результатів досліджень відповідно до вимог відповідних органів.

4. Проектування об'єктів у захищеному виконанні:

– розробка концепції інформаційної безпеки;

– проектування автоматизованих систем, засобів зв'язку, обробки та передачі в захищеному виконанні;

– проектування приміщень, призначених для проведення конфіденційних переговорів.

Види та цілі аудиту

Розрізняють зовнішній та внутрішній аудит.

Зовнішній аудит – це, як правило, разовий захід, який проводиться за ініціативою керівництва організації або акціонерів. Зовнішній аудит рекомендується (а для низки фінансових установ та акціонерних товариств потрібно) проводити регулярно. Цей вид аудиту проводиться в основному "поза" компанією та, як правило, спеціалізованими організаціями. У цьому випадку аналізуються заходи ризику від зовнішніх атак, атак із боку (навіть якщо організація захищена міжмережевими екранами). Під час проведення зовнішнього аудиту експерт здійснює:

– сканування портів, пошук уразливостей у мережевому та прикладному програмному забезпеченні,;

– спроби взаємодії з web-, поштовими та файловими серверами;

– спроби вторгнення в локальні мережі організації.

За бажанням керівництва організації, може бути здійснений спеціальний вид зовнішнього аудиту, так званий **Ethical Hacking**. У цьому випадку спеціальна організація (у світі це широко поширена практика, такі підрозділи мають спеціальну назву: “tiger team”) здійснює певні замовником види атак на сервери, сайти та хости організації.

Внутрішній аудит є безперервною діяльністю, що здійснюється на підставі документа, який зазвичай має назву «Положення про внутрішній аудит», і відповідно до плану, підготовка якого здійснюється підрозділом внутрішнього аудиту і затверджується керівництвом організації. Аудит безпеки інформаційних систем є однією із складових IT-аудиту. Внутрішній аудит зазвичай проводиться спеціальною командою з числа персоналу організації. Його завданням є оцінка ризику існуючої технології застосування інформаційної системи. Цей вид аудиту виконується із залученням засобів автоматизації аудиту, які реалізують будь-який стандарт.

Внутрішній аудит проводиться усередині мережного простору, обмеженого міжмережевим екраном організації. Він також включає сканування портів і вразливостей внутрішніх хостів організації. Крім того, аналізується організація та виконання встановленої політики безпеки, контроль та управління доступом до ресурсів, парольна політика персоналу організації та її виконання. Цей вид аудиту доповнює стандартні методики проведення аудиту вичерпнішим розглядом мережевих уразливостей.

Цілями проведення аудиту безпеки є:

– отримання об'єктивних доказів, аналіз ризиків, пов'язаних з можливістю здійснення загроз безпеці щодо ресурсів інформаційних систем (ІС);

– оцінка поточного рівня захищеності ІС;

– локалізація «вузьких місць» у системі захисту ІС;

– оцінка відповідності ІС існуючим стандартам у сфері інформаційної безпеки (ІБ);

– інвентаризація ресурсів інформаційної системи та визначення матеріалів для розробки організаційних документів, формулярів завдань та ресурсів, списків користувачів, оптимізації прав користувачів тощо;

– інвентаризація всіх видів створюваної, оброблюваної, прийнятої, переданої та ін. інформації, визначення (при необхідності уточнення) вимог забезпечення основних властивостей безпеки (конфіденційності, цілісності, доступності, спостереження) для кожного виду інформації;

– збирання даних для оцінки ефективності вживаних заходів та засобів захисту інформації;

– аналіз ефективності заходів захисту;

– аналіз складу та характеристик ресурсів (технічних та програмних), технологій обробки та передачі інформації в системі;

– аналіз телекомунікаційної складової інформаційної системи, включаючи топологію мережі, характеристики технічних та програмних засобів телекомунікацій;

– аналіз порядку допуску працівників до роботи з інформаційною системою;

– виявлення “мертвих душ” (облікових записів співробітників, звільнених із роботи, чиї облікові записи з якоїсь причини були видалені);

– аналіз існуючого порядку придбання, встановлення, оновлення та налаштування програмних засобів.

– розробка пропозицій щодо вдосконалення системи захисту інформації;

– вироблення рекомендацій щодо впровадження нових та підвищення ефективності існуючих механізмів безпеки ІС;

В результаті аудиту необхідно отримати:

– характеристику інформаційної системи як об'єкта захисту;

– формуляри робочих місць користувачів;

– формуляри завдань, які вирішуються в інформаційній системі;

– перелік завдань, які вирішуються в інформаційній системі;

– перелік видів інформації, що використовується під час вирішення завдань.

Представлені Аудитору рапорти про **інциденти системи інформаційної безпеки (СІБ)** повинні містити документацію про т.з. "слабких точках" СІБ.

До додаткових завдань, що стоять перед внутрішнім аудитором, крім надання допомоги зовнішнім аудиторам, можуть також входити:

– розробка політик безпеки та інших організаційно-розпорядчих документів щодо захисту інформації та участь у їх впровадженні в роботу організації;

– постановка завдань для IT – персоналу, що стосуються забезпечення захисту інформації;

– участь у навчанні користувачів та обслуговуючого персоналу ІС з питань забезпечення інформаційної безпеки;

– участь у розборі інцидентів, пов'язаних з порушенням інформаційної безпеки;

– інші завдання.

Основні етапи аудиту безпеки

Роботи з аудиту безпеки ІС включають ряд послідовних етапів, які в цілому відповідають етапам проведення комплексного IT-аудиту автоматизованої системи, що включає в себе:

– ініціювання процедури аудиту;

– збирання інформації аудиту;

– аналіз даних аудиту;

– вироблення рекомендацій;

– підготовку аудиторського звіту

Розглянемо ці етапи більш детально.

Ініціація процедури аудиту

Аудит повинен ініціюватися керівництвом компанії, а не відділом аудиту (аудитором). Це пов'язано з тим, що в ході аудиту буде задіяна велика кількість співробітників із різних підрозділів, при цьому дії людей мають бути скоординовані. На етапі ***ініціювання процедури аудиту*** мають бути вирішені такі організаційні питання:

– права та обов'язки аудитора мають бути чітко визначені та документально закріплені у його посадових інструкціях, а також у положенні про внутрішній (зовнішній) аудит;

– аудитором має бути підготовлений та погоджений з керівництвом план проведення аудиту;

– у положенні про внутрішній аудит має бути закріплено, зокрема, що співробітники компанії зобов'язані сприяти аудитору та надавати всю необхідну для проведення аудиту інформацію.

Для проведення обстеження формується спеціальна робоча група. До її складу входять фахівців відділів IT, а також інформаційної безпеки. Після цього видається наказ на підприємстві, у якому даються вказівки начальникам підрозділів про надання групі необхідної допомоги.

На етапі ініціювання процедури аудиту мають бути визначені межі проведення обстеження. План та межі проведення аудиту обговорюються на робочих зборах, у яких беруть участь аудитори, керівництво компанії та керівники структурних підрозділів.

Збір інформації аудиту

Етап ***збору інформації аудиту*** є найбільш складним та тривалим. Це пов'язано в основному з відсутністю необхідної документації на інформаційну систему та необхідністю щільної взаємодії аудитора з багатьма посадовими особами організації. Для отримання інформації аудитор проводить спеціальні інтерв'ю, а також досліджує інформаційну систему за допомогою спеціалізованого інструментарію.

Щоб зібрати необхідний обсяг якісної інформації для аналізу, необхідно отримати опис організаційної структури користувачів системи та обслуговуючих підрозділів. Для збору цих даних можна використовувати схеми організаційної структури користувачів та відповідних підрозділів.

В ході інтерв'ю аудитор повинен отримати відповіді на запитання про те, хто є власником інформації, хто є користувачем інформації, хто є провайдером послуг, які послуги та яким чином надаються кінцевим користувачам, які види програм функціонують у системі, скільки користувачів задіюють ці програми.

Крім того, аудитору потрібна інформація про структуру самої системи. У ході опитування аудитор повинен дізнатися, з яких компонентів складається система, якою є їх функціональність, де проходять межі корпоративної системи, як вона взаємодіє з іншими елементами IT-інфраструктури.

При цьому аудитору потрібна структурна схема системи, інформаційних потоків, опис структури інформаційного забезпечення, розміщення компонентів системи. На жаль, як правило, підготовка значної частини документації здійснюється під час аудиту.

Аналіз даних аудиту

Методи аналізу даних, що використовуються аудиторами, визначаються обраними підходами до проведення аудиту, які можуть істотно відрізнятися.

Перший підхід, найскладніший, базується на аналізі ризиків. Спираючись на методи аналізу ризиків, аудитор визначає для обстежуваної ІС індивідуальний набір вимог безпеки, що найбільше враховує особливості даної ІС, середовища її функціонування та існуючі в цьому середовищі загрози безпеці.

Другий підхід, найпрактичніший, спирається на використання стандартів інформаційної безпеки. Стандарти визначають базовий набір вимог безпеки для широкого класу ІС, що формується внаслідок узагальнення світової практики. Стандарти можуть визначати різні набори вимог безпеки, залежно від рівня захищеності ІС, який потрібно забезпечити, її приналежності (комерційна організація чи державна установа), а також призначення (фінанси, промисловість, зв'язок тощо). Від аудитора у разі потрібно правильно визначити набір вимог стандарту, відповідність яким потрібно забезпечити.

Третій підхід, найефективніший, передбачає комбінування перших двох. Базовий набір вимог безпеки, що пред'являються ІС, визначається стандартом. Додаткові вимоги, які максимально враховують особливості функціонування даної ІС, формуються на основі аналізу ризиків.

Вироблення рекомендацій аудиту

Рекомендації, що видаються аудитором за результатами аналізу стану ІС, визначаються підходом, особливостями обстежуваної ІС, станом справ з інформаційною безпекою і ступенем деталізації, що використовується при проведенні аудиту. У будь-якому разі, рекомендації аудитора повинні бути конкретними та застосовними до цієї ІС, економічно обґрунтованими, аргументованими (підкріпленими результатами аналізу) та відсортованими за ступенем важливості. При цьому заходи щодо захисту організаційного рівня практично завжди мають пріоритет над конкретними програмно-технічними методами захисту. Водночас наївно очікувати від аудитора, як результат проведення аудиту, видачі технічного проекту підсистеми інформаційної безпеки, або детальних рекомендацій щодо впровадження конкретних програмно-технічних засобів захисту інформації.

Підготовка аудиторського звіту

Аудиторський звіт є основним результатом аудиту. Його якість характеризує якість роботи аудитора. Він повинен, принаймні, містити:

– опис цілей проведення аудиту;

– характеристику обстежуваної ІС;

– вказівку меж проведення аудиту та використовуваних методів;

– результати аналізу даних аудиту;

– висновки, що узагальнюють ці результати та містять оцінку рівня захищеності автоматизованої системи (АС) або відповідність її вимогам стандартів;

– рекомендації аудитора щодо усунення існуючих недоліків та вдосконалення системи захисту.

20.2. Аудит на основі аналізу ризиків

Базовим поняттям аудиту на основі аналізу ризиків є **Система менеджменту інформаційної безпеки (СМІБ, ISMS)** – частина загальної системи менеджменту, що ґрунтується на оцінці ділових ризиків з метою створити, впровадити, експлуатувати, постійно контролювати, аналізувати, підтримувати в робочому стані і покращувати захист інформації (ЗІ).

Система менеджменту складається з організаційної структури, політики, діяльності щодо планування, відповідальності, практик, процедур, процесів та ресурсів.

В якості об'єкта аудиту може виступати як інформаційно-телекомунікаційна система (ІТС) організації в цілому, так і її окремі складові, що забезпечують обробку інформації, яка підлягає захисту.

Варіанти аудиту СМІБ:

– плановий внутрішній аудит;

– позаплановий внутрішній аудит;

– пошук загроз;

– моделювання загроз.

Система менеджменту інцидентів інформаційної безпеки (СМІІБ) є базовою складовою загальної СМІБ і дозволяє виявляти, враховувати, реагувати і аналізувати події та інциденти інформаційної безпеки. Без реалізації цих процесів неможливо забезпечити рівень захищеності, адекватний сучасним стандартам і галузевим нормам. Для найбільш ефективної реалізації СМІІБ необхідно спиратись на вимоги міжнародних і галузевих стандартів, таких як **ISO/IEC 27001:2013** «Information security management systems. Requirements», **ITU-T X-1051** «Information security management systems. Requirements for telecommunications», а також **ISO/IEC 27035:2011** «Information technology. Security techniques. Information security incident management».

Оцінка рівня безпеки ІС за допомогою визначення ризиків інформаційної безпеки

Після збору необхідної інформації проводиться її аналіз з метою оцінки поточного рівня захищеності системи. У процесі такого аналізу визначаються ризики інформаційної безпеки, яким схильна компанія. Фактично ризик являє собою інтегральну оцінку того, наскільки ефективно існуючі засоби захисту здатні протистояти інформаційним атакам.

Зазвичай виділяють дві основні групи методів розрахунку ризиків безпеки.

Перша група дозволяє встановити рівень ризику шляхом оцінки ступеня відповідності певним набором вимог до інформаційної безпеки. Як джерела таких вимог можуть виступати:

– нормативно-правові документи підприємства, що стосуються питань інформаційної безпеки (політика безпеки, регламенти, накази, розпорядження);

– вимоги чинного українського законодавства;

– рекомендації міжнародних стандартів – ISO 17799, OCTAVE, CoBIT, BS 7799-2 і т. д.;

– рекомендації компаній-виробників програмного і апаратного забезпечення – Microsoft, Oracle, Cisco і т. д.

Друга група методів оцінки ризиків інформаційної безпеки базується на визначенні ймовірності реалізації атак, а також рівнів їх збитку.

Значення ризику обчислюється окремо для кожної атаки і в загальному випадку є як добуток імовірності проведення атаки а на величину можливого збитку від цієї атаки:

$$Ризик\ (a) = P\ (a) \bullet Збиток\ (a).$$

Значення шкоди визначається власником інформаційного ресурсу, а ймовірність атаки обчислюється групою експертів, які проводять процедуру аудиту. Імовірність в даному випадку розглядається як міра того, що в результаті проведення атаки порушники досягли своїх цілей і завдали шкоди компанії.

Методи обох груп можуть використовувати **кількісні** або **якісні** шкали для визначення величини ризику інформаційної безпеки.

У першому випадку **(кількісна шкала**) для ризику і всіх його параметрів беруться чисельні вираження. Наприклад, при використанні кількісних шкал ймовірність проведення атаки P (a) може виражатися числом в інтервалі [0,1], а збиток від атаки – задаватися у вигляді грошового еквівалента матеріальних втрат, які може понести організація в разі успішної атаки. При використанні якісних шкал числові значення замінюються на еквівалентні їм понятійні рівні. Кожному понятійному рівню в цьому випадку буде відповідати певний інтервал кількісної шкали оцінки. Кількість рівнів може варіюватися в залежності від застосовуваних методик оцінки ризиків.

Для обчислення рівня ризику за **якісними шкалами** застосовуються спеціальні таблиці, в яких в першому стовпці задаються понятійні рівні збитку, а в першому рядку – рівні ймовірності атаки. Осередки же таблиці, розташовані на перетині відповідних рядків і стовпців, містять рівень ризику безпеки. Розмірність таблиці залежить від кількості концептуальних рівнів ймовірності атаки і шкоди.

При розрахунку значень ймовірності атаки, а також рівня можливого збитку використовують статистичні методи, експертні оцінки або елементи теорії прийняття рішень. Статистичні методи передбачають аналіз вже накопичених даних про реально траплялися інциденти, пов’язані з порушенням інформаційної безпеки. На основі результатів такого аналізу будуються припущення про ймовірність проведення атак і рівнях збитку від них в інших ІС. Однак статистичні методи не завжди вдається застосувати через нестачу статистичних даних про раніше проведених атаках на ресурси ІС, аналогічної тій, яка виступає в якості об’єкта оцінки.

Активний аудит інформаційних систем

Одним з найпоширеніших видів аудиту є активний аудит. Він полягає у дослідженні стану захищеності ІС з точки зору зловмисника (або зловмисника, що володіє високою кваліфікацією в галузі ІТ).

Найчастіше компанії-постачальники послуг активного аудиту іменують його **інструментальним аналізом захищеності**, щоб відокремити даний вид аудиту від інших.

Сутність активного аудиту полягає в тому, що за допомогою спеціального програмного забезпечення (у тому числі систем аналізу захищеності) і спеціальних методів, здійснюється збір інформації про стан системи мережевого захисту. Під станом системи мережевого захисту розуміють лише ті параметри і налаштування, використання яких допомагає зловмисникові проникнути в мережі і нанести збитки компанії.

При здійсненні даного виду аудиту система мережевого захисту піддається якомога більшій кількості мережевих атак, які може виконати зловмисник. При цьому аудитор штучно ставиться саме в ті умови, в яких працює зловмисник. Йому надається мінімум інформації, тільки та, яку можна здобути у відкритих джерелах.

Атаки тільки моделюються і не завдають будь-якого деструктивного впливу ІС. Їх різноманітність залежить від використовуваних систем аналізу захищеності і кваліфікації аудитора.

Активний аудит умовно можна розділити на два види – зовнішній і внутрішній.

При **зовнішньому активному** аудиті фахівці моделюють дії зовнішнього зловмисника. У даному випадку проводяться наступні процедури:

–визначення доступних із зовнішніх мереж IP-адрес підприємства;

–сканування даних адрес з метою визначення працюючих сервісів і служб, а також призначення відсканованих хостів;

–визначення версій сервісів і служб хостів, що скануються;

–вивчення маршрутів проходження трафіку до хостів замовника;

–збір інформації про ІС замовника з відкритих джерел;

–аналіз отриманих даних з метою виявлення уразливостей.

Внутрішній активний аудит за складом робіт аналогічний зовнішньому, однак при його проведенні за допомогою спеціальних програмних засобів моделюються дії «внутрішнього» зловмисника.

Даний розподіл активного аудиту на «зовнішній» і «внутрішній» актуальний для підприємства в таких випадках:

–існують фінансові обмеження на придбання послуг і продуктів ЗІ;

–модель зловмисника, яка існує, не містить «внутрішніх» зловмисників;

–розслідується факт обходу системи мережевого захисту.

Найчастіше організація у своїй ІС використовує спеціалізоване програмне забезпечення (ПЗ) власної розробки, призначене для вирішення нестандартних завдань (наприклад, корпоративний інформаційний портал, різні бухгалтерські системи або системи документообігу). Подібні ПЗ унікальні, тому яких-небудь готових засобів і технологій для аналізу їх захищеності та відмовостійкості не існує. У даному випадку проводяться спеціалізовані дослідження, спрямовані на оцінку рівня захищеності конкретного ПЗ.

Також під час активного аудиту здійснюється **дослідження виробленості і стабільності системи, або стрес-тестування**. Воно спрямоване на визначення

критичних точок навантаження, при якій система внаслідок атаки на відмову в обслуговуванні або підвищеної завантаженості перестає адекватно реагувати на легітимні (визначені політикою безпеки) запити користувачів.

Стрес-тест дозволить виявити «вузькі» місця у процесі формування та передачі інформації і визначити ті умови, за яких нормальна робота системи неможлива. Таке тестування передбачає моделювання атак на відмову в обслуговуванні запитів користувача до системи і загальний аналіз її продуктивності.

Результатом активного аудиту є інформація про всі уразливості, ступені їх критичності і методи усунення, відомості про загальнодоступну інформацію (інформацію, доступну будь-якому потенційному порушнику) мережі замовника.

За результатами активного аудиту надаються рекомендації з модернізації системи мережевого захисту, які дозволяють усунути небезпечні уразливості, і таким чином підвищити рівень захищеності ІС від дій «зовнішнього» зловмисника при мінімальних витратах на ІБ.

Однак без проведення інших видів аудиту ці рекомендації можуть виявитися недостатніми для створення «ідеальної» системи мережевого захисту. Наприклад, за результатами даного виду аудиту неможливо зробити висновок про коректність, з точки зору безпеки, проекту ІС.

20.3. Аудит на основі стандартів ІБ

Аудит на основі стандартів ІБ – аудит ІБ на відповідність міжнародним стандартам, наприклад, стандарту **ISO/IEC 27001** «Інформаційні технології. Методи забезпечення безпеки. Системи менеджменту інформаційної безпеки. Вимоги», розробленому Міжнародною організацією зі стандартизації (ISO) і Міжнародною електротехнічною комісією (IEC) на основі британського стандарту **BS 7799-2:2002** «Системи управління інформаційною безпекою. Специфікація і керівництво по застосуванню».

При проведенні цього виду аудиту реальний стан ІБ компанії порівнюється з вимогами щодо безпеки, описаними в обраному стандарті.

Звіт, складений за результатами проведення даного виду аудиту, має містити таку інформацію:

– ступінь відповідності ІТС, що перевіряється, обраному стандарту;

– ступінь відповідності внутрішнім вимогам компанії з питань ІБ;

– кількість і категорії отриманих невідповідностей і зауважень;

– рекомендації з побудови або модифікації системи забезпечення ІБ, які дозволяють привести її у відповідність до даного стандарту;

– детальне посилання на основні документи підприємства, включаючи політику безпеки, опис процедур забезпечення ІБ, додаткові обов'язкові і необов'язкові стандарти і норми, які застосовуються у даній компанії;

– перелік політик, інструкцій, посібників, положень, необхідність яких визначена в стандартах та рекомендації щодо їх розробки.

Після вибору виду аудиту необхідно приділити увагу **вибору аудитора**. Аудитором повинна бути організація, що має багаторічний досвід проведення аудитів, професіоналізм виконавця, підтверджений кваліфікацією його співробітників. Помилковою є думка, що аудит може бути проведений «своїми силами», тобто співробітниками організації, оскільки це не дасть необхідного рівня об'єктивності, і навряд чи співробітники компанії мають необхідний досвід, навички та кваліфікацію.

Підводячи підсумки, необхідно зазначити, що аудит особливо необхідний компаніям які розвиваються, з огляду на те, що він забезпечить своєчасне виявлення загроз ІБ, каналів витоку інформації та відповідні заходи реагування на виявлені уразливості. Вчасно проведений аудит ІБ допоможе уникнути збитків та негативних наслідків.

Діагностичний аналіз СМІБ за вимогами ISO/IEC 27001

Одним із етапів впровадження СМІБ є первинний аналіз. Виконання даного аналізу – це основа для побудови чіткого і зрозумілого плану робіт. Тільки після проведення первинного аналізу СМІБ можна говорити про конкретний алгоритм дій, які належить реалізувати у процесі аудиту.

Результатами первинного аналізу є:

– уявлення про існуючий рівень управління ІБ підприємства;

– перелік робіт з приведення СМІБ у відповідність до стандарту ISO/IEC 27001.

Для того, щоб визначити існуючий рівень СМІБ, необхідно мати чіткі критерії – **вимоги стандарту**. Перелік вимог надає можливість провести діагностичний аналіз СМІБ з певною точністю. Відповідно до цих вимог необхідно скласти опитувальник з варіантами відповідей, який має охоплювати всі розділи і пункти стандарту, містити чіткі, зрозумілі і прості питання. Наприклад: «Чи існує документована методика управління ризиками?». У даному випадку можуть бути варіанти відповідей «Так» або «Ні». Якщо є документ з такою назвою, відповідь має бути позитивною. Разом з тим, це питання не розкриває повністю виконання вимог стандарту. Тому необхідні й так звані «складні» питання.

Складання опитувальника досить трудомісткий і тривалий процес. З огляду на це, австралійською компанією **Bridge Point розроблено типовий опитувальник** та запропоновано використовувати його фахівцям, які проводять діагностичний аналіз СМІБ за вимогами **ISO/IEC 27001**.

Переваги даного опитувальника:

1. Безкоштовно доступний на сайті компанії Bridge Point.
2. Оновлюється, а значить вдосконалюється.
3. Дозволяє з достатньо високим ступенем адекватності оцінити поточний стан СМІБ.
4. Структурований відповідно до розділів стандарту (напрямків безпеки).
5. Простий у використанні.
6. Враховує важливість (вагу, значущість) кожного питання.
7. Автоматизований, надає можливість зручно реєструвати відповіді.
8. Автоматично розраховує результати.
9. Автоматично надає результат аналізу в зручному вигляді.
10. Дозволяє фіксувати і порівнювати стан СМІБ через інтервали часу.

20.4. Аудит на основі експертних досліджень ІС

Експертний аудит можна умовно представити як порівняння стану ІБ з «ідеальним» описом, що передбачає:

– вимоги, які були висунуті керівництвом у процесі проведення аудиту;

– опис «ідеальної» системи безпеки, заснованої на акумульованому у компанії-аудитора загальновідомому та власному досвіді.

При виконанні експертного аудиту проводяться наступні види робіт:

– збір первинних даних про систему ІБ, про її функції й особливості, використовувані технології автоматизованої обробки та передачі даних (з урахуванням найближчих перспектив розвитку);

– збір інформації про наявні організаційно-розпорядчі документи щодо забезпечення ІБ і їх аналіз;

– визначення точок відповідальності систем, пристроїв і серверів ІС;

– формування переліку підсистем кожного підрозділу компанії з категоруванням критичної інформації та схемами інформаційних потоків.

Одним із найбільших за обсягом видом робіт серед тих, які проводяться при експертному аудиті, є збір даних про ІС шляхом інтерв'ювання представників замовника і заповнення ними спеціальних анкет.

Основна мета інтерв'ювання технічних фахівців – збір інформації про функціонування мережі, а керівного складу компанії – з’ясування вимог, які висуваються до системи ІБ.

20.5. Забезпечення безперервності бізнес-процесів: Поняття бізнес-процесу. Модель бізнес-процесу

Бі́знес-проце́с (англ. *Business Process*) – будь-яка діяльність, що має вхідний продукт, додає вартість до нього, та забезпечує вихідний продукт для внутрішнього або зовнішнього споживача.

Існують три види бізнес-процесів:

– **процеси управління** – бізнес-процеси, які управляють функціонуванням системи. Прикладом керувального процесу може служити корпоративне управління та стратегічний менеджмент.

– **основні** – бізнес-процеси, які складають основний бізнес компанії і створюють основний потік доходів. Прикладами операційних бізнес-процесів є постачання, виробництво, маркетинг та збут.

– **забезпечувальні** – бізнес-процеси, які обслуговують основний бізнес. Наприклад, бухгалтерський облік, кадрове, інформаційне забезпечення.

Бізнес-процес починається з попиту споживача і закінчується його задоволенням.

Таблиця 20.1 – Приблизна схема і дефініція бізнес-процесів банку

Об'єкт управління	**Бізнес-процес**
Бізнес-система	Вироблення узгоджених умов діяльності
Технологія	Розробка нових і модифікація наявних продуктів
Клієнт	Продаж активних продуктів
Постачальники фінансових ресурсів	Залучення ресурсів
Персонал	Відтворення персоналу
Технологічні засоби	Відтворення технологічних засобів
Фінанси і стійкість банку	Управління фінансами
Розпорядження на проведення операцій	Операційна діяльність

Власник бізнес-процесу

Власник бізнес-процесу (англ. *Process Owner*) – роль, яку виконує особа, яка несе постійну відповідальність й звітує за успішне проектування, розробку, виконання і ефективність усього наскрізного (крос-функціонального) бізнес-процесу. Ця функція може бути оформлена у вигляді посади на повну ставку або у вигляді додаткових обов'язків для когось з основної або допоміжної служби. Володілець процесу з лав керівництва (володільці процесів рівня підприємства й директор з бізнес-процесів) зазвичай несуть фінансову відповідальність за групи бізнес-процесів. Вони первісно зацікавлені в успішному виконані крос-функціональних бізнес-процесів, які мають ключове значення для успіху компанії.

Наявність власника – необхідна умова успішності бізнес-процесу. Бізнес-процес без власника, який має серйозний вплив в організації, подібен кораблю без штурвала, гвинта і вітрил – такий процес не буде виконуватися у найбільш ефективний і результативний спосіб.

Компоненти бізнес-процесу

Входи бізнес-процесу

Ресурси або дані, які мають бути, й тригери (різні типи подій), які ініціюють процес.

Виходи бізнес-процесу

Виходи – це результати діяння на входи механізмів, які управляються згідно з регулюваннями. В ідеалі виходи – продукція або послуги, які відповідають або перевершують очікування замовинків по термінах, якості і вартості. Це також можуть бути події, які запускають інші процеси у цій самій або у іншій організації.

Механізми бізнес-процесу

Механізми бізнес-процесу – це "інструменти", включаючи машини, системи і людей, які запускаються входами і виконують дії над входами.

Контрольні точки бізнес-процесу

Контрольні точки – це вимоги, обов'язкові дії, інструкції і обмеження, а також закони, положення, регламенти, правила і установки, які структурують і визначають дії над входами. Механізми і контрольні точки можуть бути одним й тим самим, наприклад, регламенти, фінанси і люди[2].

Моделювання та симуляція

Бізнес-процеси можуть бути унаочнені діаграмами бізнес-процесу – наприклад, у позначеннях BPMN. Бізнес-процеси можна моделювати з допомогою програмних засобів, наприклад ARIS.

Симуляція бізнес процесів в сучасних умовах займає особливе місце і в першу чергу в освітньому процесі. Симуляція застосовує методику learning by doing (навчання дією), що надає можливість:

– приймати конкретні економічні та управлінські рішення, що мають реальні наслідки для подальшої діяльності підприємства;

– отримувати орієнтири для набуття нових знань;

– навчитися виявляти причинно-наслідкові зв'язки управління економічними процесами на підприємстві в конкурентному ринковому середовищі.

Автоматизація та комп'ютеризація бізнес-процесів

Автоматизація бізнес-процесів – широкий клас завдань, що не обмежується рухом і обробкою документа, а до складу їх входять різні операції, що виконуються співробітниками, і покрокову автоматичну обробку даних. У ході бізнес-процесу можуть оброблятися різні документи і відбуватися взаємодія з зовнішніми IT-системами. Як правило, автоматизуються ключові бізнес-процеси діяльності підприємства: формування замовлень, виконання заявок клієнтів, розробка і запуск нової продукції і т. д., а також інші нескладні, але численні і рутинні процеси.

Таблиця 20.2 – Охоплення завдань автоматизації та комп'ютеризації бізнес-процесів

Специфікація	**Аудиторія**	**Суть (зміст завдань, що ставляться перед системою)**
описи типових бізнес-процесів	керівники підрозділів автоматизації; консультанти і технічні фахівці, що здійснюють впровадження комплексу	модель предметної області, закладена в основу комплексу; бізнес-процеси, в розрахунку на які комплекс був спроектований
типові технологічні інструкції		рекомендований порядок виконання операцій персоналом при використанні комплексу в складі автоматизованої системи

Ключовий процес

Ключови́й проце́с (англ. *Core or Key Process*) – бізнес-процес, який є життєво необхідним для успіху та життєдіяльності організації.

Моделювання бізнес-процесів

Моделюва́ння бі́знес-проце́сів (англ. *Business process modeling* – BPM) – формалізований і виконаний за певними правилами опис послідовності дій фахівців у формі логічних блок-схем, що визначають вибір подальших дій, виходячи з ситуативного факту. Наприклад: «якщо всі документи для формування страхового акта є в наявності, то формуємо цей документ. Якщо немає, то вживаємо заходів для отримання документів, яких не вистачає». У моделі бізнес-процесів певні послідовності окремих дій об'єднуються у відповідні процедури і сценарії бізнес-процесів. Описується взаємодія фахівців різних підрозділів в рамках одного бізнес-процесу.

Моделювання бізнес-процесів – це процесове відображення (як правило, графічне) діяльності підприємства з тим, щоб в подальшому дані процеси можна було аналізувати і вдосконалювати.

Цілі

Метою моделювання бізнес-процесів як правило є:

1. Документація бізнесу компанії:
   - Для отримання знання про бізнес.
   - Формування карти підрозділів.
   - Переведення бізнесу в інші місця.
   - Для задоволення потреб бізнес-партнерів або об'єднань (наприклад, з метою сертифікації).
   - Для навчання співробітників (передачі знань).
   - Для впровадження (підтримки системи менеджменту якості) та екологічного менеджменту.
2. Підготовка бізнес-процесів (який зазвичай починається з аналізу фактичного стану):
   - З метою впровадження нових організаційних структур.
   - Впровадження аутсорсингу.
3. Підготовка і автоматизації IT-підтримки бізнес систем.
4. Визначення показників процесу.
5. Бенчмаркінг.
6. Найкраща практика.
7. Організаційні зміни:
   - При підготовці до продажу бізнесу.
   - При підготовці до інтеграції компаній або їх частин.
   - Введення або зміна IT-систем та/або організаційних структур.
8. Участь у конкурсах (наприклад, Європейський фонд управління якістю).
9. Удосконалення внутрішніх процесів.

Використання

Моделювання бізнес-процесів, як правило, здійснюється та використовується бізнес-аналітиками і менеджерами, які прагнуть підвищити ефективність процесу та їх якість. В крупних компаніях без формалізації і опису бізнес-процесів складно забезпечити належний рівень виконавської і технологічної дисципліни. Формалізація і опис бізнес-процесів є ключовою умовою для їх автоматизації. Взаємозв'язана система бізнес-процесів зображає

весь комплекс завдань і функцій структурних підрозділів, виконання яких необхідно забезпечити в процесі діяльності компанії. Моделювання бізнес-процесів дозволяє, незалежно від актуальної чисельності персоналу компанії, на будь-якому етапі її еволюційного розвитку, дозволяє закріпити ті або інші функції не тільки за конкретними структурними підрозділами, але і за конкретними фахівцями. В міру збільшення чисельності персоналу, створення нових структурних підрозділів можна гнучко перерозподіляти функції і завдання структурних підрозділів.

Графічний опис бізнес-процесів та їх імітація це методи аналізу бізнес-процесів, ефективність яких доведена багаторічною практикою використання та численними дослідженнями.

Мови графічного моделювання

На сьогодні найвідомішими мовами (нотаціями) графічного моделювання бізнес-процесів є UML, ARIS, IDEF (IDEF0, IDEF3 у програмній інтерпретації BPwin), BPMN.

Абревіатура BPM

Моделювання бізнес-процесів відіграє величезну роль в управлінні бізнес-процесами. Необхідно відзначити, що в англійському перекладі обидва види діяльності мають однакову абревіатуру BPM (Business Process Modeling та Business Process Management, відповідно), що часто призводить до плутанини. Цей факт необхідно враховувати, тому що більшість літератури з даного предмету видано англійською мовою.

20.6. Розробка політик інформаційної безпеки під час забезпечення бізнес-процесів

Політика інформаційної безпеки виступає як документ або багаторівнева система документів, які визначають вимоги безпеки, систему заходів або порядок дій, відповідальність співробітників та механізми контролю задля забезпечення інформаційної безпеки підприємства. У документ **політики безпеки** рекомендовано вносити **наступні розділи**:

– Вступний розділ, що підтверджує стурбованість керівництва проблемами інформаційної безпеки.

– Організаційний розділ, що описує підрозділи, комісії, групи осіб, відповідальні за роботи в області інформаційної безпеки.

– Класифікаційний розділ, що описує матеріальні та інформаційні ресурси підприємства та необхідний рівень їх захисту.

– Штатний розділ, що характеризує заходи безпеки щодо персоналу.

– Розділ, що висвітлює питання фізичного захисту інформації.

– Розділ управління, що описує підхід до управління комп'ютерами та комп'ютерними мережами пересилання даних.

– Розділ, що зазначає правила розмежування доступу до інформації.

– Розділ, що описує заходи, спрямовані на забезпечення безперервної роботи підприємства (доступності інформації).

В даний час для захисту інформації потрібна не просто розробка приватних механізмів захисту, а реалізація системного підходу, що включає комплекс взаємопов'язаних заходів (використання спеціальних технічних і програмних засобів, організаційних заходів, нормативно-правових актів і т.д.). Головною метою будь-якої системи забезпечення інформаційної безпеки є створення умов функціонування підприємства, запобігання загроз його безпеки, захист законних інтересів підприємства від протиправних посягань, недопущення розкрадання фінансових засобів, розголошення, втрати, витоку, спотворення і знищення службової інформації, забезпечення в рамках виробничої діяльності всіх підрозділів підприємства.

Ефективна політика інформаційної безпеки визначає необхідний та достатній набір вимог безпеки. Вона мінімально впливає на продуктивність праці, враховує особливості бізнес-процесів підприємства, підтримується керівництвом, позитивно сприймається й виконується співробітниками підприємства.

Політика інформаційної безпеки (організаційно-технічні і режимні заходи)

Визначення політики інформаційної безпеки

При прийнятті рішень адміністратори ІС зіштовхуються з проблемою вибору варіантів рішень по організації ЗІ на основі обліку принципів діяльності організації, співвідношення важливості цілей і наявності ресурсів. Ці рішення включають визначення того, як будуть захищатися технічні й інформаційні ресурси, а також як повинні поводитися службовці в тих чи інших ситуаціях.

Політика інформаційної безпеки (ПІБ) – набір законів, правил і практичних рекомендацій і практичного досвіду, що визначають управлінські і проектні рішення в області ЗІ. На основі ПІБ будується керування, захист і розподіл критичної інформації в системі. Вона повинна охоплювати всі особливості процесу обробки інформації, визначаючи поводження ІС у різних ситуаціях.

Відповідно до запропонованого підходу політика (заходи) інформаційної безпеки реалізується відповідною структурою органів на основі нормативно-методичної бази з використанням програмно-технічних методів і засобів, що визначають архітектуру системи захисту.

Для конкретної ІС політика безпеки повинна бути індивідуальної. Вона залежить від технології обробки інформації, використовуваних програмних і технічних засобів, структури організації т.д.

Для того щоб описати ПІБ для конкретної ІС, адміністратори спочатку повинні визначити саму область обмежень і умов у зрозумілих усьому термінах. Корисно вказати чи мета причини розробки ПІБ – це допоможе домогтися дотримання політики.

Інформація, що циркулює в рамках ІС, є критично важливої. ІС дозволяє користувачам розділяти програми і дані, що збільшує ризик. Отже, кожний з комп'ютерів, що входять у мережу, має потребу в більш сильному захисті.

ПІБ переслідує дві головні цілі – продемонструвати співробітникам важливість захисту мережного середовища, описати їхня роль у забезпеченні безпеки, а також розподілити конкретні обов'язки по захисту інформації, що циркулює в мережі, так само як і самої мережі.

У відношенні політики безпеки в Internet організації може знадобитися уточнення, чи охоплює ця політика всі з'єднання, через які ведеться робота з Internet (чи прямо опосредованно) чи власне з'єднання Internet. Ця політика також може визначати, чи враховуються інші аспекти роботи в Internet, що не мають відносини до безпеки, такі як персональне використання з'єднань з Internet.

Принципи політики безпеки бізнес-процесів

Політика безпеки визначається як сукупність документованих управлінських рішень, спрямованих на захист інформації й асоційованих з нею ресурсів.

При розробці і проведенні її в життя доцільно керуватися наступними засадами:

- неможливість минати захисні засоби;
- посилення самої слабкої ланки;
- неприпустимість переходу у відкритий стан;
- мінімізація привілеїв;
- поділ обов'язків;
- багаторівневий захист;
- розмаїтість захисних засобів;
- простота і керованість інформаційної системи;
- забезпечення загальної підтримки заходів безпеки.

Пояснимо зміст перерахованих принципів.

Стосовно до межмережевих екранів *принцип неможливості минати захисні засоби* означає, що всі інформаційні потоки в мережу, що захищається, і з її повинні проходити через екран. Не повинно бути «таємних» модемних чи входів тестових ліній, що йдуть в обхід екрана.

Надійність будь-якої оборони визначається самою *слабкою ланкою*. Часто самою слабкою ланкою виявляється не чи комп'ютер програма, а людина, і тоді проблема забезпечення інформаційної безпеки здобуває нетехнічний характер.

Принцип неприпустимості переходу у відкритий стан означає, що при будь-яких обставинах (у тому числі позаштатних), СЗІ або цілком виконує свої функції, або повинна цілком блокувати доступ.

Принцип мінімізації привілеїв наказує виділяти користувачам і адміністраторам тільки ті права доступу, що необхідні їм для виконання службових обов'язків.

Принцип поділу обов'язків припускає такий розподіл ролей і відповідальності, при якому одна людина не може порушити критично важливий

для організації процес. Це особливо важливо, щоб запобігти зловмисні чи некваліфіковані дії системного адміністратора.

Принцип багаторівневого захисту наказує не покладатися на один захисний рубіж, яким би надійним він ні здавався. За засобами фізичного захисту повинні випливати програмно-технічні засоби, за ідентифікацією й автентифікацією – керування доступом і, як останній рубіж, – протоколювання й аудит. Ешелонована оборона здатна принаймні затримати зловмисника, а наявність такого рубежу, як протоколювання й аудит, істотно утрудняє непомітне виконання злочинних дій.

Принцип розмаїтості захисних засобів рекомендує організовувати різні за своїм характером оборонні рубежі, щоб від потенційного зловмисника було потрібно оволодіння різноманітними і, по можливості, несумісними між собою навичками подолання СЗІ.

Принцип простоти і керованості інформаційної системи в цілому і СЗІ особливо визначає можливість формального чи неформально доказу коректності реалізації механізмів захисту. Тільки в простій і керованій системі можна перевірити погодженість конфігурації різних компонентів і здійснити централізоване адміністрування.

Принцип загальної підтримки заходів безпеки – носить нетехнічний характер. Рекомендується із самого початку передбачити комплекс заходів, спрямований на забезпечення лояльності персоналу, на постійне навчання, теоретичне і, головне, практичне.

Види політики безпеки

Основу політики безпеки складає спосіб керування доступом, що визначає порядок доступу суб'єктів системи до об'єктів системи. Назва цього способу, як правило, визначає назва політики безпеки.

Для вивчення **властивостей способу керування доступом** створюється його формальний опис – **математична модель**. При цьому модель повинна відбивати стан всієї системи, її переходи з одного стану в інший, а також враховувати, які стани і переходи можна вважати безпечними в змісті даного керування. Без цього говорити про яких-небудь властивості системи, і тим більше гарантувати їх, щонайменше некоректно.

В даний час найкраще вивчені **два види політики безпеки**: **виборча** і **повноважна**, засновані, відповідно на виборчому і повноважному способах керування доступом. Крім того, існує набір вимог, що підсилює дію цих політик і призначений для керування інформаційними потоками в системі.

Слід зазначити, що засоби захисту, призначені для реалізації якого-небудь з названих способу керування доступом, тільки надають можливості надійного керування чи доступом інформаційними потоками.

Визначення прав доступу суб'єктів до об'єктів і/чи інформаційним потокам (повноважень суб'єктів і атрибутів об'єктів, присвоєння міток критичності і т.д.) входить у компетенцію адміністрації системи.

Основою виборчої політики безпеки є виборче керування доступом, що має на увазі, що:

– усі суб'єкти й об'єкти системи повинні бути ідентифіковані;

– права доступу суб'єкта до об'єкта системи визначаються на підставі деякого правила (властивість вибірковості).

Для опису властивостей виборчого керування доступом застосовується **модель системи на основі матриці доступу (МД),** іноді неї називають матрицею контролю доступу. Така модель одержала назву матричної.

Матриця доступу являє собою прямокутну матрицю, у якій об'єкту системи відповідає рядок, а суб'єкту стовпець. На перетинанні стовпця і рядка матриці вказується тип дозволеного доступу суб'єкта до об'єкта. Звичайно виділяють такі типи доступу суб'єкта до об'єкта, як "доступ на читання", "доступ на запис", "доступ на виконання" і ін.

Безліч об'єктів і типів доступу до них суб'єкта може змінюватися відповідно до деяких правил, що існують у даній системі. Визначення і зміна цих правил також є задачею МД.

Рішення на доступ суб'єкта до об'єкта приймається відповідно до типу доступу, зазначеним у відповідній осередку матриці доступу. Звичайно виборче керування доступом реалізує принцип "що не дозволено, те заборонено", що припускає явний дозвіл доступу суб'єкта до об'єкта. Матриця доступу – найбільш простий підхід до моделювання систем доступу.

Виборча політика безпеки найбільше широко застосовується в комерційному секторі, тому що її реалізація на практиці відповідає вимогам комерційних організацій по розмежуванню доступу і підзвітності, а також має прийнятну вартість і невеликі накладні витрати.

Основу повноважної політики безпеки складає повноважне керування доступом, що має на увазі, що:

– усі суб'єкти й об'єкти системи повинні бути однозначно ідентифіковані;

– кожному об'єкту системи привласнена мітка критичності, що визначає цінність інформації, що міститься в ньому;

– кожному суб'єкту системи привласнений рівень прозорості, що визначає максимальне значення мітки критичності об'єктів, до яких суб'єкт має доступ.

У тому випадку, коли сукупність міток має однакові значення, говорять, що вони належать до одного рівня безпеки. Організація міток має ієрархічну структуру і, таким чином, у системі можна реалізувати ієрархічно спадний потік інформації (наприклад, від рядових виконавців до керівництва). Чим важливіший об'єкт чи суб'єкт, тим вище його мітка критичності. Тому найбільш захищеними виявляються об'єкти з найбільш високими значеннями мітки критичності. Кожен суб'єкт, крім рівня прозорості, має поточне значення рівня безпеки, що може змінюватися від деякого мінімального значення до значення його рівня прозорості.

Основне призначення повноважної політики безпеки – регулювання доступу суб'єктів системи до об'єктів з різним рівнем критичності і запобігання витоку інформації з верхніх рівнів посадової ієрархії на нижні, а також блокування можливого проникнення з нижніх рівнів на верхні. При цьому вона функціонує на тлі виборчої політики, додаючи її вимогам ієрархічно упорядкований характер (відповідно до рівнів безпеки).

Склад та зміст основних заходів щодо розробки політики інформаційної безпеки

Організація заходів щодо захисту інформації

Не можна приступати до впровадження захисту інформації, поки користувачі не придбають навичок, необхідних для їхнього дотримання. Безпека вимагає не тільки знань, але і дій. Усі користувачі повинні знати, що потрібно почати і чого робити не коштує, коли вони зіштовхуються з чи порушенням можливістю його виникнення; до кого потрібно звертатися при виникненні підозр. Користувачі повинні бути упевнені в тому, що заходу для забезпечення безпеки приймаються в їхніх же інтересах, а не по інших розуміннях.

Подумайте про запрошення **кваліфікованого консультанта з безпеки**, що міг би дати вашим користувачам знання з інформаційної безпеки. Якщо консультант досить кваліфікований і ваша організація може собі це дозволити, запросите його на наступні збори групи як наставника при розробці правил. Незважаючи на те, що залучення консультанта для самостійної розробки правил може знизити витрати, ви втратите інтерес і увагу рядового користувача.

Працюючи таким способом, ви створите **правила безпеки**, до яких буде мати відношення кожен співробітник. Незважаючи на те, що в результаті може з'явитися і не самий зроблений документ, ефективність правил підвищиться відчутно. Забезпечте користувачів **керівництвом**, у якому викладений матеріал прийнятного обсягу. Навіть якщо користувачі засвоїли правила, то в них може виникнути питання, як ці правила впровадити. Надавайте разом із усіма правилами **модельні процедури впровадження і приклади**. Записуйте питання співробітників (разом з вашими відповідями і поясненнями) у супровідній документації до правил. Повідомляйте користувачам про ці доповнення.

Доповнюйте правила модельними процедурами і прикладами реалізації. Переконаєтеся, що ваші правила присвячені захисту від дійсних небезпек – від тих, імовірність виникнення яких досить реальна і дійсно представляють для вас погрозу.

У загальному виді сукупність заходів, спрямованих на запобігання погроз, визначається в такий спосіб:

– уведення надвикористання технічних засобів, ПЗ і масивів даних, тобто непотрібне дублювання або використання не за призначенням;

– резервування технічних засобів;

– регулювання доступу до технічних засобів, ПЗ, масивам інформації;

– регулювання використання програмно-апаратних засобів і масивів інформації;

– криптографічний захист інформації;

– контроль елементів ІС;

– реєстрація зведень;

– своєчасне знищення непотрібної інформації;

– сигналізація;

– своєчасне реагування.

У системному плані безліч і розмаїтість можливих видів захисту інформації визначається **способами впливу** на дестабілізуючі фактори їхні причини, що породжують, на елементи ІС, що захищається інформацію і навколишнє середовище, причому в напрямку, що сприяє підвищенню значень показників захищеності інформації. Ці **способи** можуть бути **класифіковані** в такий спосіб:

– **Фізичні засоби** – механічні, електричні, електромеханічні, електронні, електронно-механічні й інші пристрої і системи, що функціонують автономно, створюючи різного роду перешкоди дестабілізуючим факторам.

– **Апаратні засоби** – різні електронні, електронно-механічні і подібні пристрої, що вбудовуються в апаратуру ІС чи, що сполучаються з нею спеціально для рішення задач захисту інформації.

– **Програмні засоби** – спеціальні пакети чи програм окремі програми, використовувані для рішення задач захисту.

– **Організаційні заходи** – організаційно-технічні заходи, передбачаються спеціально в ІС з метою рішення задач захисту.

– **Правові заходи** – законодавчо-правові акти, що існують у державі, спеціально видавані закони, зв'язані з забезпеченням захисту інформації. Вони регламентують права й обов'язки всіх облич і підрозділів, що мають відношення до функціонування ІС, і установлюють відповідальність за дії, наслідком яких може бути порушення захищеності інформації.

– **Морально-етичні норми** – це сформовані в чи суспільстві колективі моральні норми й етичні правила, дотримання яких сприяє захисту інформації, а порушення їх прирівнюється до недотримання правил поводження в суспільстві.

Для забезпечення ефективності захисту інформації усі використовувані засоби і заходи доцільно об'єднати в систему захисту інформації, що повинна бути функціонально самостійною підсистемою ІС. Головною властивістю побудови системи захисту повинна бути здатність до її пристосування при зміні структури технологічних чи схем умов функціонування ІС.

Іншими принципами можуть бути:

– мінімізація витрат, максимальне використання серійних засобів;
– забезпечення рішення необхідної сукупності задач захисту;
– комплексне використання засобів захисту, оптимізація архітектури;
– зручність для персоналу;
– простота експлуатації.

СЗІ доцільно будувати у виді взаємозалежних підсистем, а саме:

– підсистема криптографічного захисту;
– підсистема забезпечення юридичної значимості електронних документів;
– підсистема захисту від НСД;
– підсистема організаційно-правового захисту;
– підсистема керування СЗІ.

Побудова системи захисту інформації в такому виді дозволить забезпечити комплексність процесу захисту інформації в ІС, керованість процесу і можливість адаптації при зміні умов функціонування ІС:

– *Підсистема криптографічного захисту* поєднує засобу такого захисту інформації і по ряду функцій кооперується з підсистемою захисту від НСД.

– *Підсистема забезпечення юридичної значимості* електронних документів служить для додання юридичного статусу документам в електронному представленні і є визначальним моментом при переході до без паперової технології документообігу. Дану підсистему зручно і доцільно розглядати як частина підсистеми криптографічного захисту.

– *Підсистема захисту від НСД* запобігає доступу несанкціонованих користувачів до ресурсів ІС.

– *Підсистема керування СЗІ* призначена для керування ключовими структурами підсистеми криптографічного захисту, а також контролю і діагностування програмно-апаратних засобів і забезпечення взаємодії всіх підсистем СЗІ.

– *Підсистема організаційно-правового захисту* призначена для регламентації діяльності користувачів ІС і являє собою упорядковану сукупність організаційних рішень, нормативів, законів і правил, що визначають загальну організацію робіт із захисту інформації в ІС.

Система захисту інформації являє собою сукупність автоматизованих робочих місць (АРМ), що входять до складу ІС, і програмно-апаратних засобів, інтегрованих в АРМ користувачів ІС.

Політики безпеки для Internet

Організації повинні відповісти на наступні питання, щоб правильно врахувати можливі наслідки підключення до Internety в області безпеки:

– Чи можуть хакери зруйнувати внутрішні системи?

– Чи може бути скомпрометована (змінена чи прочитана) важлива інформація організації при її передачі по Internet?

– Чи можна перешкодити роботі організації?

Ціль політики безпеки для Internet – прийняти рішення про те, як організація збирається захищатися. ПІБ звичайно складається з двох частин – загальних принципів і конкретних правил роботи (які еквівалентні специфічній політиці, описаної нижче). Загальні принципи визначають підхід до безпеки в Internet. Правила ж визначають що дозволено, а що – заборонено. Правила можуть доповнюватися конкретними процедурами і різними посібниками.

Internet при проектуванні і не задумувалася як захищена мережа, тому його **проблемами в поточній версії TCP/IP** є:

– Легкість перехоплення даних і фальсифікації адрес машин у мережі – основна частина трафіку Internet – це нешифровані дані. E-mail, паролі і файли можуть бути перехоплені, використовуючи легко доступні програми.

– Уразливість засобів TCP/IP – ряд засобів TCP/IP не був спроектований бути захищеними і може бути скомпрометований кваліфікованими зловмисниками; засобу, використовувані для тестування особливо уразливі.

– Відсутність політики – багато хто сайти через незнання сконфигуровані таким чином, що надають широкий доступ до себе з боку Internet, не з огляду на можливість зловживання цим доступом; багато хто сайти дозволяють роботу більшого числа сервісів TCP/IP, чим їм потрібно для роботи і не намагаються обмежити доступ до інформації про свої комп'ютери, що може допомогти зловмисникам.

– Складність конфігурування – засоби керування доступом хоста складні; найчастіше складно правильно зконфігурувати і перевірити ефективність установок. Засоби, що помилково неправильно сконфигуровані, можуть привести до неавторизованого доступу.

Рівні політики безпеки

З практичної точки зору політику безпеки можна умовно розділити на три рівні: верхній, середній і нижній.

До **верхнього рівня** відносяться рішення, що торкаються організацію в цілому. Вони носять дуже загальний характер і, як правило, виходять від керівництва організації.

Зразковий список подібних рішень може містити в собі наступні елементи:

– чи формування перегляд комплексної програми забезпечення інформаційної безпеки, визначення відповідальних за просування програми;

– формулювання цілей, що переслідує організація в області інформаційної безпеки, визначення загальних напрямків у досягненні цих цілей;

– забезпечення бази для дотримання законів і правил;

– формулювання управлінських рішень по тим питанням реалізації програми безпеки, що повинні розглядатися на рівні організації в цілому.

Мети політики верхнього рівня організації в області інформаційної безпеки формулюються в термінах цілісності, приступності і конфіденційності.

Якщо організація відповідає за підтримку критично важливих баз даних, на першому плані може стояти зменшення випадків утрат, чи ушкоджень перекручувань даних. Для організації, що займається продажами, імовірно, важлива актуальність інформації про надані послуги і ціни, а також її приступність максимальному числу потенційних покупців.

Режимна організація в першу чергу піклується про захист від несанкціонованого доступу – конфіденційності.

На верхній рівень виноситься керування захисними ресурсами і координація використання цих ресурсів, виділення спеціального персоналу для захисту критично важливих систем, підтримка контактів з іншими організаціями, що забезпечують чи контролюють режим безпеки.

ПІБ верхнього рівня повинна чітко окреслювати сферу свого впливу. Можливо, це будуть усі комп'ютерні системи чи організації навіть більше, якщо ПІБ регламентує деякі аспекти використання співробітниками своїх домашніх комп'ютерів. Можлива, однак, і така ситуація, коли в сферу впливу включаються лише найбільш важливі системи.

У політику повинні бути визначені обов'язки посадових осіб по виробленню програми безпеки і по проведенню її в життя. У цьому змісті ПІБ є основою підзвітності персоналу.

На верхній рівень варто виносити мінімум питань, що визначають значну економію чи засобів коли інакше надійти просто неможливо.

До **середнього рівня** варто віднести питання, що стосуються окремих аспектів інформаційної безпеки, але важливі для різних систем, експлуатованих організацією. Приклади таких питань – відношення до передового, але ще недостатньо перевіреним технологіям: доступ до Internet (як сполучити волю одержання інформації з захистом від зовнішніх погроз?), використання домашніх комп'ютерів, застосування користувачами неофіційного програмного забезпечення і т.д.

Політика безпеки **нижнього рівня** відноситься до конкретних сервісам. Вона містить у собі два аспекти – мети і правила їхнього досягнення, тому її часом важко відокремити від питань реалізації. На відміну від двох верхніх рівнів, розглянута ПІБ повинна бути набагато детальніше.

Є багато речей, специфічних для окремих сервісів, які не можна єдиним образом регламентувати в рамках всієї організації. У той же час ці речі настільки важливі для забезпечення режиму безпеки, що рішення, що відносяться до них, повинні прийматися на управлінському, а не технічному рівні.

Приведемо кілька прикладів питань, на які варто дати відповідь при проходженні політиці безпеки нижнього рівня:

- хто має право доступу до об'єктів, підтримуваним сервісом?
- при яких умовах можна читати і модифікувати дані?
- як організований віддалений доступ до сервісу?

При формулюванні цілей ПІБ нижнього рівня може виходити з заходів цілісності, приступності і конфіденційності, але вона не повинна на них зупинятися. Її мети повинні бути конкретніше

З цілей виводяться правила безпеки, що описують, хто, що і при яких умовах може робити. Чим детальніше правила, тим більш формально вони викладені, тим простіше підтримати їхнє виконання програмно-технічними заходами. З іншого боку, занадто тверді правила можуть заважати роботі користувачів, імовірно, їх прийдеться часто переглядати.

Керівництву треба знайти розумний компроміс, коли за прийнятну ціну буде забезпечений прийнятний рівень безпеки, а працівники не виявляться занадто скровані.

Основні принципи політики забезпечення інформаційної безпеки підприємства

Основними принципами інформаційної безпеки є:

– забезпечення цілісності і збереження даних, тобто надійне їх зберігання в неспотвореному вигляді;

– дотримання конфіденційності інформації (її недоступність для тих користувачів, які не мають відповідних прав);

– доступність інформації для всіх авторизованих користувачів за умови контролю за всіма процесами використання ними отриманої інформації;

– безперешкодний доступ до інформації в будь-який момент, коли вона може знадобитися підприємству.

Ці принципи неможливо реалізувати без особливої **інтегрованої системи інформаційної безпеки**, що виконує наступні функції:

– вироблення політики інформаційної безпеки;

– аналіз ризиків (тобто ситуацій, в яких може бути порушена нормальна робота інформаційної системи, а також втрачені або розсекречені дані);

– планування заходів щодо забезпечення інформаційної безпеки;

– планування дій в надзвичайних ситуаціях;

– вибір технічних засобів забезпечення інформаційної безпеки.

Отже, етапи проведення робіт із забезпечення інформаційної безпеки підприємства виглядають таким чином:

1. Проведення обстеження підприємства на предмет виявлення реальних загроз несанкціонованого доступу до конфіденційної інформації;
2. Розробка політики безпеки, організаційно-розпорядчих документів і заходів щодо забезпечення інформаційної безпеки системи відповідно до вимог по захищеності технічних і програмних засобів від витоку конфіденційної інформації;
3. Проектування системи інформаційної безпеки;
4. Створення прототипу системи інформаційної безпеки;
5. Розробка зразка системи інформаційної безпеки;
6. Впровадження системи інформаційної безпеки в діючу структуру підприємства;
7. Навчання персоналу;
8. Атестація системи інформаційної безпеки підприємства.

Метою комплексної інформаційної безпеки є збереження інформаційної системи підприємства, захист і гарантування повноти і точності виданої нею інформації, мінімізація руйнувань і модифікація інформації, якщо такі трапляються.

Види моделей розробки політики інформаційної безпеки

Серед моделей ПБ найвідомішими є дискреційна, мандатна та рольова. Перші дві досить давно відомі й детально досліджені, а рольова політика є недавнім досягненням теорії та практики захисту інформації.

Дискреційна політика безпеки

Основою **дискреційної політики безпеки (ДПБ)** є дискреційне управління доступом (Discretionary Access Control – DAC), яке визначається двома властивостями:

– усі суб’єкти й об’єкти мають бути однозначно ідентифіковані;

– права доступу суб’єкта до об’єкта системи визначаються на основі певних зовнішніх відносно системи правил.

Назва пункту є дослівним перекладом з англійської терміна Discretionary policy, ще один варіант перекладу – розмежувальна політика. Ця політика одна з найпоширеніших в світі, в системах по замовчуванню мається на увазі саме ця політика. ДПБ реалізується за допомогою матриці доступу, яка фіксує множину об’єктів та суб’єктів, доступних кожному суб’єкту.

Наведемо приклади варіантів задання матриці доступу:

1. Листи можливостей: для кожного суб'єкта створюється лист (файл) усіх об'єктів, до яких має доступ даний суб'єкт;

2. Листи контролю доступу: для кожного об'єкта створюється список усіх суб'єктів, що мають доступи до цього об'єкта;

До **переваг ДПБ** можна віднести відносно просту реалізацію відповідних механізмів захисту. Саме цим зумовлено той факт, що більшість поширених нині захищених автоматизованих систем забезпечують виконання положень саме ДПБ. Однак багатьох проблем захисту ця політика розв'язати не може.

Наведемо найбільш суттєві **вади ДПБ**:

1. Один з найбільших недоліків цього классу політик – вони не витримують атак за допомогою «Троянського коня». Це, зокрема, означає, що система захисту, яка реалізує ДПБ, погано захищає від проникнення вірусів у систему та інших способів прихованої руйнівної дії.

2. Автоматичне визначення прав. Оскільки об'єктів багато і їх кількість безперервно змінюється, то задати заздалегідь вручну перелік прав кожного суб'єкта на доступ до об'єктів неможливо. Тому матриця доступу різними способами агрегується, наприклад, суб'єктами залишаються тільки користувачі, а у відповідну клітину матриці вставляються формули функцій, обчислення яких визначає права доступу суб'єкта, породженого користувачем, до об'єкта. Звичайно, ці функції можуть змінюватися з часом. Зокрема, можливе вилучення прав після виконання певної події, також можливі модифікації, що залежать від інших параметрів.

3. Контроль поширення прав доступу. Найчастіше буває так, що власник файла передає вміст файла іншому користувачеві і той відповідно набуває права власника на цю інформацію. Отже, права можуть поширюватись, і навіть якщо перший власник не хотів передати доступ іншому суб'єкту до своєї інформації, то після кількох кроків передача прав може відбутися незалежно від його волі. Виникає задача про умови, за якими в такій системі певний суб'єкт рано чи пізно отримає необхідний йому доступ.

4. При використанні ДПБ виникає питання визначення правил поширення прав доступу й аналізу їх впливу на безпеку АС. У загальному випадку при використанні ДПБ органом, який її реалізує і який при санкціонуванні доступу суб'єкта до об'єкта керується певним набором правил, стоїть задача, яку алгоритмічно неможливо розв'язати: перевірити, призведуть його дії до порушень безпеки чи ні. Отже, матриця доступів не є тим механізмом, який дозволив би реалізувати ясну і чітку СЗІ в АС. Більш досконалою ПБ виявилася мандатна ПБ.

Мандатна політика

Основу мандатної (повноважної) політики безпеки (МПБ) становить мандатне управління доступом (Mandatory Access Control – MAC), яке передбачає, що:

– всі суб'єкти й об'єкти повинні бути однозначно ідентифіковані;

– у системі визначено лінійно упорядкований набір міток секретності;

– кожному об’єкту системи надано мітку секретності, яка визначає цінність інформації, що міститься в ньому, – його рівень секретності в АС;

– кожному суб’єкту системи надано мітку секретності, яка визначає рівень довіри до нього в АС, – максимальне значення мітки секретності об’єктів, до яких суб’єкт має доступ; мітка секретності суб’єкта називається його рівнем доступу.

Основна мета МПБ – запобігання витоку інформації від об’єктів з високим рівнем доступу до об’єктів з низьким рівнем доступу, тобто протидія виникненню в КС інформаційних каналів згори вниз. Вона оперує, таким чином, поняттями інформаційного потоку і цінності інформаційних об’єктів. Цінність інформаційних об’єктів (або їх мітки рівня секретності) часто дуже важко визначити. Однак досвід показує, що в будь-якій КС майже завжди для будь-якої пари об’єктів X та *Y* можна сказати, який з них більш цінний.

Тобто, можна вважати, що таким чином фактично визначається деяка однозначна функція *c(X),* яка дозволяє для будь-яких об’єктів *X* і *Y* сказати, що:

– коли *Y* більш цінний об’єкт, ніж *X,* то *c(Y) > c(X).*

– і навпаки, якщо *c(Y) > c(X),* то *Y* – більш цінний об’єкт, ніж *X.*

– тоді потік інформації від *X* до *Y* дозволяється, якщо *c(X) < c(Y),* і не дозволяється, якщо *c(X) > c(Y).*

Отже, МПБ має справу з множиною інформаційних потоків, яка ділиться на дозволені і недозволені за дуже простою умовою – значенням наведеної функції. МПБ у сучасних системах захисту на практиці реалізується мандатним контролем на найнижчому апаратно-програмному рівні, що дає змогу досить ефективно будувати захищене середовище для механізму мандатного контролю.

Пристрій мандатного контролю називають монітором звернень. Мандатний контроль, який ще називають обов’язковим, оскільки його має проходити кожне звернення суб’єкта до об’єкта, організується так:

– монітор звернень порівнює мітки рівня секретності кожного об’єкта з мітками рівня доступу суб’єкта;

– за результатом порівняння міток приймається рішення про допуск.

Найчастіше МПБ описують у термінах, поняттях і визначеннях властивостей **моделі Белла-Лападула**. У рамках цієї моделі доводиться важливе твердження, яке вказує на принципову відмінність систем, що реалізують мандатний захист, від систем з дискреційним захистом: «якщо початковий стан системи безпечний і всі переходи системи зі стану до стану не порушують обмежень, сформульованих ПБ, то будь-який стан системи безпечний».

Наведемо ряд **переваг** МПБ порівняно з ДПБ:

1. Для систем, де реалізовано МПБ, є характерним вищий ступінь надійності. Це пов’язано з тим, що за правилами МПБ відстежуються не тільки правила доступу суб’єктів системи до об’єктів, а й стан самої КС. Таким чином, канали витоку в системах такого типу не закладені первісно (що є в положеннях ДПБ), а можуть виникнути тільки при практичній реалізації систем внаслідок помилок розробника.

2. Правила МПБ ясніші і простіші для розуміння розробниками і користувачами АС, що також є фактором, який позитивно впливає на рівень безпеки системи.

3. МПБ стійка до атак типу «Троянський кінь».

4. МПБ допускає можливість точного математичного доведення, що система в заданих умовах підтримує ПБ.

Однак МПБ має дуже серйозні вади – вона дуже складна для практичної реалізації і вимагає значних ресурсів КС. Це пов'язано з тим, що інформаційних потоків у системі величезна кількість і їх не завжди можна ідентифікувати. Сааме ці вади часто заважають її практичному використанню.

МПБ прийнята всіма розвинутими державами світу. Вона розроблялася, головним чином, для збереження секретності (тобто конфіденційності) інформації у військових організаціях. Питання ж цілісності за її допомогою не розв'язуються або розв'язуються частково, як побічний результат захисту секретності.

Рольова політика безпеки

Рольову політику безпеки (РПБ) (Role Base Access Control – RBAC) не можна віднести ані до дискреційної, ані до мандатної, тому що керування доступом у ній здійснюється як на основі матриці прав доступу для ролей, так і за допомогою правил, які регламентують призначення ролей користувачам та їх активацію під час сеансів. Отже, рольова модель є цілком новим типом політики, яка базується на компромісі між гнучкістю керування доступом, характерною для ДПБ, і жорсткістю правил контролю доступу, що притаманна МПБ.

У РПБ класичне поняття «суб'єкт» заміщується поняттями «користувач» і «роль».

Користувач – це людина, яка працює з системою і виконує певні службові обов'язки.

Роль – це активно діюча в системі абстрактна сутність, з якою пов'язаний обмежений, логічно зв'язаний набір повноважень, необхідних для здійснення певної діяльності.

РПБ застосовується досить широко, тому що вона, на відміну від інших більш строгих і формальних політик, є дуже близькою до реального життя.

Справді, за суттю, користувачі, що працюють у системі, діють не від свого власного імені – вони завжди виконують певні службові обов'язки, тобто виконують деякі ролі, які аж ніяк не пов'язані з їх особистістю. Тому цілком логічно здійснювати керування доступом і призначати повноваження не реальним користувачам, а абстрактним (не персоніфікованим) ролям, які представляють учасників певного процесу обробки інформації. Такий підхід до ПБ дозволяє врахувати розподіл обов'язків і повноважень між учасниками прикладного інформаційного процесу, оскільки з точки зору РПБ має значення не особистість користувача, користувача, що здійснює доступ до інформації, а те, які повноваження йому необхідні для виконання його службових обов'язків.

Наприклад, у реальній системі обробки інформації можуть працювати системний адміністратор, менеджер баз даних і прості користувачі. У такій ситуації РПБ дає змогу розподілити повноваження між цими ролями відповідно

до їх службових обов'язків: ролі адміністратора призначаються спеціальні повноваження, які дозволять йому контролювати роботу системи і керувати її конфігурацією, роль менеджера баз даних дозволяє здійснювати керування сервером БД, а права простих користувачів обмежуються мінімумом, необхідним для запуску прикладних програм. Крім того, кількість ролей у системі може не відповідати кількості реальних користувачів – один користувач, якщо він має різні повноваження, може виконувати (водночас або послідовно) кілька ролей, а кілька користувачів можуть користуватися однією й тією ж роллю, якщо вони виконують однакову роботу. При використанні РПБ керування доступом здійснюється в дві стадії: по-перше, для кожної ролі вказується набір повноважень, що представляють набір прав доступу до об'єктів, і, по-друге, кожному користувачеві призначається список доступних йому ролей. Повноваження призначаються ролям відповідно до принципу найменших привілеїв, з якого випливає, що кожний користувач повинен мати тільки мінімально необхідні для виконання своєї роботи повноваження. У моделі РПБ визначаються множини: множина користувачів, множина ролей, множина повноважень на доступ до об'єктів, наприклад, у вигляді матриці прав доступу, множина сеансів роботи користувачів з системою. Для перелічених множин визначаються відношення, які встановлюють для кожної ролі набір наданих їй повноважень, а також для кожного користувача – набір доступних йому ролей.

Правила керування доступом РПБ визначаються певними функціями, які для кожного сеансу визначають користувачів, набір ролей, що можуть бути одночасно доступні користувачеві в цьому сеансі, а також набір доступних у ньому повноважень, що визначається як сукупність повноважень усіх ролей, що беруть участь у цьому сеансі. Як критерій безпеки рольової моделі використовується правило: «система вважається безпечною, якщо будь-який користувач системи, що працює в певному сеансі, може здійснити дії, які вимагають певних повноважень тільки в тому випадку, коли ці повноваження належать сукупності повноважень усіх ролей, що беруть участь у цьому сеансі».

З формулювання критерію безпеки рольової моделі випливає, що управління доступом здійснюється, головним чином, не за допомогою призначення повноважень ролям, а шляхом встановлення відношення, яке призначає ролі користувачам, і функції, що визначає доступний у сеансі набір ролей. Тому численні інтерпретації рольової моделі відрізняються видом функцій, що визначають правила керування доступом, а також обмеженнями, що накладаються на відношення між множинами. Завдяки гнучкості та широким можливостям РПБ суттєво перевершує інші політики, хоча іноді її певні властивості можуть виявитися негативними. Так, вона практично не гарантує безпеку за допомогою формального доведення, а тільки визначає характер обмежень, виконання яких і є критерієм безпеки системи. Хоча такий підхід дозволяє отримати прості й зрозумілі правила контролю доступу (перевага), які легко застосовувати на практиці, проте позбавляє систему теоретичної доказової бази (вада). У деяких ситуаціях ця обставина утруднює використання РПБ, однак у кожному разі оперувати ролями набагато зручніше, ніж суб'єктами (знову перевага), оскільки це більше відповідає поширеним технологіям обробки

інформації, які передбачають розподіл обов'язків і сфер відповідальності між користувачами. Крім того, РПБ може використовуватися одночасно з іншими ПБ, коли повноваження ролей, що призначаються користувачам, контролюється контролюється ДПБ або МПБ, що дозволяє будувати багаторівневі схеми контролю доступу.

Наведений огляд сучасних ПБ визначає основні принципи їх функціонування, а також підкреслює їх роль і виключну важливість при побудові та експлуатації захищених АС. Додамо, що в багатьох сучасних програмних засобах захисту інформації розглянуті ПБ уже реалізовані. Однак слід зазначити, що це зовсім не означає їх механічного застосування. Зрозуміло, що спочатку в конкретній організації має бути проведений ретельний аналіз процесів обробки інформації, на основі якого потім створюється і застосовується конкретна ПБ. Необхідно також зазначити, що, крім загального опису поняття ПБ, в Українському стандарті з технічного захисту інформації більш конкретних нормативних та методичних матеріалів з розробки ПБ для АС поки що немає. Зауважимо, що, в більшості організацій (як державних, так і недержавних) про поняття ПБ навіть не мають уявлення. Але парадокс якраз полягає в тому, що фактично в будь-якій організації завжди існують конкретні правила, що регламентують процес її функціонування, зокрема і процес захисту інформації, а саме ці правила і є політикою. Отже, фактично в будь-яких АС окремі елементи ПБ завжди наявні.

20.7. Дотримання політик інформаційної безпеки під час забезпечення бізнес-процесів

Кожна компанія, в процесі здійснення своєї діяльності, повинна приділяти значну увагу інформаційній безпеці, що полягає зокрема в розробці різноманітних стратегій управління процесами, створенні інструментів та політик, необхідних для запобігання, виявлення, документування та протидії загрозам цифровій та нецифровій інформації.

Інформаційна безпека в контексті цінності компанії

Інформаційна безпека, в широкому розумінні цього слова є сукупністю технічних та організаційних заходів, а також розроблених документів, основною метою яких є захист та збереження інформації, якою володіє компанія. Разом з тим, інформаційна безпека все ж залишається складовою частиною кібербезпеки, що є значно ширшою категорією та включає в себе не лише захист інформації та даних, а й захист систем, мереж та інше.

До основних цілей інформаційної безпеки також відноситься створення набору бізнес-процесів, які захищатимуть інформаційні активи незалежно від того, як форматується інформація, чи вона перебуває в транзиті, обробляється чи знаходиться в стані спокою, тобто зберігається у відповідних базах даних.

Цінність компанії, на думку деяких експертів, визначається перш за все в тому, яка інформація перебуває у володінні компанії, а також як ця інформація

зберігається. Безпека інформації є вирішальним фактором для забезпечення здійснення ефективних ділових операцій, а також для збереження та завоювання довіри клієнтів, як майбутніх, так і існуючих.

Організація інформаційної безпеки в рамках компанії

Для можливості максимально ефективно забезпечити інформаційну безпеку в рамках компанії, насамперед необхідно визначитися з основною стратегією, якої повинна дотримуватися компанія. Така стратегія повинна визначатися керівництвом компанії, з одночасним залученням спеціалістів з інформаційної безпеки, якими можуть виступати як працівники компанії, так і залучені зовнішні підрядники. Результатом розроблюваної стратегії зазвичай є затверджений проект з інформаційної безпеки, а також шляхи та методи його реалізації.

Після визначення глобальної стратегії, компанія, як правило, створює **спеціалізовану команду спеціалістів з питань інформаційної безпеки (Information security team / IS team)** для впровадження та підтримки проекту з інформаційної безпеки. Зазвичай, цією групою керує **головний співробітник інформаційної безпеки (Chief information security officer/CISO**). Інші ж члени команди повинні обиратися, виходячи з рівня їхньої компетенції та вмінь в питаннях безпеки інформації.

Information security team відповідає за управління ризиками, реалізацію процесів, з допомогою яких постійно оцінюються вразливості та загрози по відношенню до інформації, якою володіє компанія, а також за приймання і застосування відповідних захисних засобів контролю. Разом з тим, команда з інформаційної безпеки повинна реагувати на всі порушення безпеки інформації та оперативно приймати рішення про усунення таких порушення, а також про мінімізацію ризиків для інтересів компанії чи фундаментальних прав, свобод та інтересів фізичних осіб, якщо порушення будь-яким чином стосується персональних даних таких осіб.

Проект з реалізації інформаційної безпеки повинен будуватися навколо основних трьох аспектів безпеки, які полягають в підтримці конфіденційності, цілісності та доступності до інформації, в тому числі в межах IT систем та баз даних компанії. Впровадження таких принципів допоможе забезпечити розкриття конфіденційної інформації лише уповноваженим сторонам (конфіденційність), запобігти несанкціонованому зміненню даних (цілісності) та гарантувати, що до інформації можуть отримати доступ тільки уповноважені сторони (за наявності).

Перший аспект безпеки це **конфіденційність**. Такий аспект зазвичай вимагає використання ключів шифрування та шифрування. Тобто, якщо компанія забезпечує недоступність до інформації шляхом її шифрування, обов'язково повинні бути ключі, зокрема у вигляді паролів, які дають можливість дешифрувати інформацію в її первинний вигляд, для можливості використання інформації для цілей компанії.

Другий аспект безпеки – **цілісність**. Він передбачає, наприклад, що коли інформація завантажується (записується) або надсилається в будь-яке місце, а

потім зчитується чи отримується назад, вона повинна бути точно такою, якою вона була в момент надсилання чи завантаження. Інколи, для більшої гарантії безпеки інформації, компанії може знадобитися надсилання однієї і тієї ж інформації у два різних місця, тобто, створення резервної копії інформації.

Третій аспект безпеки полягає в **доступності** інформації, що означає під собою забезпечення своєчасного використання нової інформації, а також оперативне відновлення інформації протягом прийнятного, в рамках загальноприйнятої практики, строку відновлення, який би не порушував інтереси будь-яких осіб, незалежно від того, юридичні це особи чи фізичні. Мається на увазі, що доступ до інформації повинен бути вільний та безперебійний, але тільки звісно ж тільки для тих осіб, хто має на те право.

Не секрет, що заходи інформаційної безпеки повинні бути також зосереджені на мережевих системах та комп'ютерній інфраструктурі компанії, яка найчастіше всього може стати об'єктом кібератак та інших зловмисних дій, направлених на знищення, крадіжку або пошкодження інформації, що належить або якою користується компанія.

Політики та процедури, які регламентують інформаційну безпеку

В процесі впровадження проекту з інформаційної безпеки, компанія повинна забезпечити наявність відповідних документів, якими повинні керуватися працівники компанії, залучені компанією особи, а також Information security team, забезпечуючи реалізацію тих чи інших заходів. Іншими словами, компанія повинна розробити та провадити ISMS (information security management system), що являє собою набір керівних принципів, політик та процесів, що створений для допомоги компанії в процесі управління безпекою інформації та у випадках, пов'язаних з порушенням даних. Маючи розроблений набір керівних принципів, компанія має можливість мінімізувати ризики в контексті безпеки інформації, а також може забезпечити безперервність роботи у разі зміни персоналу.

Компанія може використовувати шаблонні рішення, які користуються популярністю на ринку. Наприклад, стандарти ISO 27001 є надзвичайно популярною та відомою основою для розроблюваної компанією ISMS. Разом, з тим, компанією повинні враховуватися всі аспекти своєї діяльності, а також інші особливості інформації, якою володіє компанія.

Керівні принципи, процеси та політики інформаційної безпеки зазвичай передбачають розробку та імплементацію фізичних та технічних заходів безпеки для захисту інформації від несанкціонованого доступу, використання, розповсюдження або знищення. Ці заходи можуть включати в себе пастки, систему управління ключами шифрування, мережеві системи виявлення вторгнень, політику паролів, політику управління системою електронних адрес та політику антивірусних заходів.

Немаловажним заходом, який повинен включатися в ISMS, є проведення аудиту існуючих документів та систем компанії на відповідність вимогам, які гарантують максимальний захист інформації. Аудит безпеки повинен проводитися компанією з метою оцінки здатності компанії підтримувати захищеність системи на основі та в рамках встановлених критеріїв.

Основна порада, в процесі забезпечення інформаційної безпеки, полягає в залученні кваліфікованих спеціалістів в сфері інформаційної безпеки в процесі імплементації та реалізації проекту з інформаційної безпеки в рамках компанії.

Також, однією з основних порад буде використання світових визнаних стандартів, які забезпечують основний каркас інформаційної безпеки. Компанії, в свою чергу, залишається тільки пристосувати запропоновані алгоритми до своїх внутрішніх процесів, з допомогою яких забезпечується безпека інформації. Це наприклад стандарти ISO або PCI DSS.

Загалом же, підходьте до питання організації інформаційної безпеки досить виважено та скрупульозно, обов'язково застосовуючи сучасні досягнення в області техніки, комп'ютерних технологій, а також, враховуючи вимоги законодавства, зокрема у сфері захисту персональних даних.