УДК 004.056

В.М. Ахрамович

АДМІНІСТРАТИВНИЙ РІВЕНЬ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Досліджені: актуальність проблеми інформаційної безпеки, адміністративні рівні згідно міжнародних стандартів, вказано перелік необхідних документів для забезпечення політики безпеки організації, підприємства з різними за насиченістю засобами захисту, організаційною структурою. Сформовані цілі безпеки, підкреслена важливість участі в розробці політики безпеки перших осіб, та персональної відповідальності співробітників, особливо спеціалістів з області безпеки, дотримання законності. Розкрито основні етапи аналізу ризиків для ІС.

Ключові слова: адміністративний рівень, керівництво, організація, захист, інформація, політика безпеки, рівень, етап, погрози, технології, область застосування, ролі, обов'язки, правила, мета, ціль, ризики, збитки.

Вступ

Під інформаційною безпекою (ІБ) ми розумітимемо захищеність інформації та інфраструктури, що її підтримує, від випадкових або навмисних дій природного або штучного характеру, які можуть завдати неприйнятного збитку суб'єктам інформаційних відносин, зокрема власникам і користувачам інформації та інфраструктури, що її підтримує. Захист інформації - це комплекс заходів, направлених на забезпечення інформаційної безпеки. Таким чином, правильний з методологічної точки зору підхід до проблем інформаційної безпеки починається з виявлення суб'єктів інформаційних відносин та інтересів цих суб'єктів, пов'язаних з використанням інформаційних систем (ІС). Загрози інформаційній безпеці - це зворотна сторона використання інформаційних технологій. До адміністративного рівня інформаційної безпеки відносять дії загального характеру, що вживають керівництвом організації для захисту інформації (забезпеченню безпеки інформації).

Основна частина

Слід зазначити, що на сьогодні в проблемі визначення змісту поняття «інформаційна безпека підприємництва» та виробленню системних заходів щодо усунення загроз інформаційній безпеці підприємництва приділяється недостатня увага.. Це зумовлено тим, до недавнього часу органи державної влади України та підприємці не завжди усвідомлювали усю важливість захисту інформації, у зв’язку з цим на законодавчому рівні та у внутрішніх правилах підприємств не було вироблено дієвих процедур захисту інформації та забезпечення безпеки інформаційної системи підприємств. Це призвело до різкого збільшення кількості злочинів [2], пов’язаних із комп’ютерним несанкціонованим доступом, шахрайством та шпіонажем, набули свого масового поширення рейдерські атаки, які стали можливими, у тому числі, і в результаті отримання незаконного доступу до інформаційних систем підприємств.

Зважаючи на вищевикладене, особливої актуальності набувають питання вироблення дієвого адміністративно-правового механізму забезпечення інформаційної безпеки підприємництва, чого можна буде досягти за умови чіткого усвідомлення сутності інформаційної безпеки підприємництва як об’єкта адміністративно-правової охорони [1].

Головна мета заходів адміністративного рівня – сформувати програму робіт в області інформаційної безпеки й забезпечити її виконання, виділяючи необхідні ресурси й контролюючи стан справ.

Основа адміністративного рівня - політика безпеки (ПБ). що відбиває стратегію організації в області захисту своїх інформаційних активів.

Термін "політика безпеки" є не зовсім точним перекладом англійського словосполучення "security policy", однак у цьому випадку калька краще відбиває зміст цього поняття, чому лінгвістично більш вірні "правила безпеки". Ми будемо мати на увазі не окремі правила або їх набори (такого роду розв'язки виносяться на процедурний рівень), а

стратегію організації в області інформаційної безпеки. Для виробітку стратегії й проведення її в життя потрібні, безсумнівно, політичні розв'язки, прийняті на найвищому рівні.

Під політикою безпеки ми будемо розуміти сукупність документованих розв'язків, прийнятих керівництвом організації й спрямованих на захист інформації й асоційованих з нею ресурсів.

Таке трактування, звичайно, набагато ширше, ніж набір правил розмежування доступу (саме це означав термін "security policy" в "Помаранчевій книзі" і в побудованих на її основі нормативних документах інших країн).

Політика безпеки будується на основі аналізу ризиків, які вважаються реальними для інформаційної системи організації. Коли ризики проаналізовані й стратегія захисту визначена, складається програма забезпечення інформаційної безпеки [1].

Основні етапи аналізу ризиків. Використання інформаційних систем пов'язане з певною сукупністю ризиків, під якими розуміються вартісні вираження подій (звичайно ймовірнісних), ведучих до втрат. Якщо ризик не прийнятний, то необхідно вжити захисні заходи, що не перевищують за вартістю можливий збиток.

Аналіз ризику, головним чином, необхідний для наступного:

- виявлення уразливості ІС і її системи захисту,
- визначення необхідних і достатніх витрат на захист,
- вибору конкретних заходів, методів, засобів і систем захисту,
- підвищення поінформованості й компетентності персоналу ІС.

На початковому етапі методом експертної оцінки вирішуються загальні питання проведення аналізу ризику. Вибираються компоненти ІС і ступінь детальності їх розгляду. Всеосяжний аналіз вимагає розгляду всієї інформаційної інфраструктури. Але на практиці із принципу розумної достатності можуть бути виділені й піддані більшій деталізації окремі найбільш важливі компоненти й служби, у першу чергу, де ризики великі або невідомі. Більш ретельного аналізу зазнають нові й модифіковані компоненти ІС, а також компоненти, у яких були нові інциденти й порушення безпеки.

Далі вибираються методології оцінки ризиків як процесу одержання кількісної або якісної оцінки збитку, який може відбутися у випадку реалізації погроз безпеки ІС. Методології носять приватний характер, властивий організації й ІС, і залежать від конкретної безлічі дестабілізуючих факторів і умов функціонування ІС, можливості їх кількісної оцінки, ступеня їх неточності, неповноти, нечіткості і т.д. На практиці, з обліком припустимої наближеної оцінки ризиків, часто використовують прості наочні методи, засновані на елементах теорії ймовірності і математичної статистики.

Етап ідентифікації активів. Основу процесу аналізу ризику становить визначення: що треба захищати, від кого і як. Для цього виявляються активи (компоненти ІС), що потребують захисту. Деякі активи (наприклад, технічні й програмні засоби) ідентифікуються очевидним чином. Про деякі активи (люди, видаткові матеріали) часто забувають. При ідентифікації активів можуть бути порушені й нематеріальні цінності, здатні, однак, постраждати від порушення режиму безпеки, наприклад: репутація компанії, моральний клімат у колективі.

У деяких специфічних ІС активи, унікальні для організації, можуть бути виділені в окремі групи, наприклад: комунікаційне, алгоритмічне або лінгвістичне забезпечення. Крім того, можуть підлягати захисту частини інфраструктури, зокрема підсистеми електропостачання й ін.

У процесі ідентифікації активів фіксуються технології введення, зберігання, обробки й передачі інформації в системі. Головним результатом процесу ідентифікації активів є одержання детальної інформаційної структури організації й способів використання інформації. Подальші етапи аналізу ризику ґрунтуються саме на даній, зафіксованій на деякий момент часу інформації.

Етап аналізу погроз. Після ідентифікації активів ІС слід розглянути всі можливі погрози зазначеним активам, оцінити ризики й ранжувати їх за ступенем можливого збитку.

Під погрозою звичайно розуміється будь-яка подію (дія), яка потенційно може завдати шкоди ІС шляхом порушення конфіденційності, цілісності або доступності інформації. Погрози можуть бути навмисними, що є наслідком навмисних (зловмисних) дій людей, і ненавмисні, викликані помилками людини або збоями й відмовами роботи технічних і програмних засобів, або стихійними діями.

При аналізі погроз необхідно виявити їхні джерела й умови реалізації. Це допоможе у виборі додаткових засобів захисту. Часто одні погрози можуть бути наслідком або умовою прояву ряду інших погроз. Наприклад, несанкціонований доступ (у різних формах його прояву) до ресурсів полегшуючих реалізацію практично будь-якої погрози: від псування магнітного носія до комплексної віддаленої атаки.

Етап оцінки ризиків. Після ідентифікації погрози необхідно оцінити ризик прояву погрози. У більшості випадків можливо одержати кількісну оцінку ризику. Вона може бути отримана на базі експертного опитування, оцінена статистично або розрахована за деякою математичною залежністю (адекватній конкретній погрозі конкретному активу).

Крім імовірності здійснення погрози, важливий розмір очікуваних втрат. У загальному випадку очікувані втрати розраховуються по наступній формулі: $e = p \cdot v$, де p –імовірнісна оцінка ризику прояву погрози, v – збиток при реалізації погрози. Однак як імовірності погрози, так і очікувані втрати не завжди можна оцінити кількісно. Наприклад, розрахувати заміну комп'ютера досить просто, але важко оцінити потенційний збиток у випадку затримки видачі даних, викривлення інформації, розголошення окремих відомостей і т.д. Деякі інциденти можуть завдати шкоди репутації фірми, викликати соціальну напруженість у колективі, спричинити юридичне переслідування підприємства з боку користувачів і т.д.

Виділяються три рівні політики безпеки [5].

Верхній рівень: розв'язки загального характеру, що зачіпають організацію в цілому: мета формулюється в термінах цілісності, доступності й конфіденційності; чітко окреслена сфера впливу (наприклад, ресурси захисту) є основою підзвітності персоналу

На верхній рівень виноситься мінімум питань. Критерії винесення:

- формулювання цілей, які переслідує організація в галузі інформаційної безпеки, визначення загальних напрямів у досягненні цілей;
- забезпечення бази для дотримання законів і правил;
- визначення загального порядоку робіт у масштабах підприємства;
- можливість забезпечити значну економію засобів;
- розробка планів відновлення після критичних ситуацій і забезпечення безперервності роботи інформаційних систем.

Зачіпаються три аспекти виконавської дисципліни:

- дотримання існуючого законодавства;
- контроль дії осіб, відповідальних за розробку програми безпеки;
- забезпечення ретельності персоналу (система заохочень і покарань).

Типова структура документів верхнього рівня визначається стандартом ISO 17799.

Практичні правила з керування інформаційною безпекою призначені для керівників і співробітників, відповідальних за планування, реалізацію й підтримку системи ІБ. Основні групи заходів щодо забезпечення ІБ:

- політика безпеки;
- загальноорганізаційні аспекти захисту;
- класифікація активів і керування ними;
- безпека персоналу;
- фізична безпека й безпека навколишнього середовища;
- адміністрування систем і мереж;
- керування доступом до систем і мереж;
- розробка й супровід інформаційних систем;

- керування безперебійною роботою організації;
- контроль відповідності вимогам.

Для політики верхнього рівня мети організації в області інформаційної безпеки формулюються в термінах цілісності, доступності й конфіденційності. Якщо організація відповідає, наприклад, за підтримку критично важливих баз даних, на першому плані може стояти зменшення числа втрат, ушкоджень або викривлень даних. Для організації, що займається продажем комп'ютерної техніки, імовірно, важлива актуальність інформації про надавані послуги й ціни їх доступність максимальному числу потенційних покупців. Керівництво режимного підприємства в першу чергу опікується про захист від несанкціонованого доступу, тобто про конфіденційність.

У політиці повинні бути визначені обов'язки посадових осіб з розробки програми безпеки й проведенню її в життя. У цьому змісті політика безпеки є основою підзвітності персоналу [3].

Британський стандарт BS 7799:1995 рекомендує включати в документ, що характеризує політику безпеки організації, наступні розділи:

- вступ, що підтверджує заклопотаність вищого керівництва проблемами інформаційної безпеки;
- організаційний, що містить опис підрозділів, комісій, груп і т.д., відповідальних за роботи в області інформаційної безпеки;
- класифікаційний, що описує наявні в організації матеріальні й інформаційні ресурси й необхідний рівень їх захисту;
- штатний, що характеризує заходу безпеки, що застосовуються до персоналу (опис посад з погляду інформаційної безпеки, організація навчання й перепідготовки персоналу, порядок реагування на порушення режиму безпеки й т.п.);
- розділ, що висвітлює питання фізичного захисту;
- керуючий розділ, що описує підхід до керування комп'ютерами й комп'ютерними мережами;
- розділ, що описує правила розмежування доступу до виробничої інформації;
- розділ, що характеризує порядок розробки й супроводу систем;
- розділ, що описує заходи, спрямовані на забезпечення безперервної роботи організації;
- юридичний розділ, що підтверджує відповідність політики безпеки чинному законодавству.

Середній рівень: питання за окремими аспектами ІБ. важливі для різних систем в організації, що експлуатуються. Наприклад:

- відношення до передових (але. можливо, недостатньо перевірених) технологій;
- доступ в Internet (як сполучити бажання доступу до інформації із захистом від зовнішніх погроз, використання домашніх комп'ютерів;
- застосування користувачами неофіційного програмного забезпечення і т.д.

Політика середнього рівня повинна для кожного аспекту висвітлювати наступні теми:

Опис аспекту. Наприклад, якщо розглянути застосування користувачами неофіційного програмного забезпечення, останнє можна визначити як ПЗ, яке не було схвалено або закуплене на рівні організації.

Область застосування. Слід визначити, де, коли, як, стосовно кого й чому застосовується дана політика безпеки. Наприклад, чи стосується політика, пов'язана з використанням неофіційного програмного забезпечення, організацій-субпідрядників? Чи зачіпає вона співробітників, що користуються портативними й домашніми комп'ютерами й змушених переносити інформацію на виробничі машини?

Позиція організації за даним аспектом. Продовжуючи приклад з неофіційним програмним забезпеченням, можна уявити собі позиції повної заборони, розробки процедури приймання подібного ПЗ й т.п. Позиція може бути сформульована й у набагато більш

загальному виді, як набір цілей, які переслідує організація в даному аспекті. Взагалі стиль документів, що визначають політикові безпеки (як і їхній перелік), у різних організаціях може сильно відрізнятися.

Ролі й обов'язки**.** В документ необхідно включити інформацію про посадових осіб, відповідальних за реалізацію політики безпеки. Наприклад, якщо для використання неофіційного програмного забезпечення співробітникам потрібен дозвіл керівництва, повинно бути відомо, у кого і як його можна одержати. Якщо неофіційне програмне забезпечення використовувати не можна, слід знати, хто стежить за виконанням даного правила.

Законопослушність. Політика повинна містити загальний опис заборонених дій і покарань за них [4].

Повинно бути відомо, куди слід звертатися за роз'ясненнями, допомогою й додатковою інформацією. Зазвичай це певна посадова особа, а не конкретна людина, що займає в цей момент даний пост.

Нижній рівень: питання до конкретних інформаційних сервісів. Включає два аспекти - мета й правила їх досягнення, тому його часом важко відокремити від питань реалізації. Приклади питань, на які слід дати відповідь у політику безпеки нижнього рівня:

- хто має право доступу до об'єктів, що підтримується сервісом?
- при яких умовах можна читати й модифікувати дані?
- як організований дистанційний доступ до сервісу?

На цьому рівні описуються механізми захисту інформації й програмно-технічні засоби, які використовуються для їхньої реалізації (у рамках, звичайно, управлінського рівня, але не технічного).

За політику безпеки нижнього рівня відповідають системні адміністратори.

Висновки

Інформаційна безпека - багатогранна, можна навіть сказати, багатовимірна область діяльності, в якій успіх може принести тільки систематичний, комплексний підхід.

Основний принцип безпеки – витрати на засоби захисту не повинні перевищувати вартості об'єктів, що захищаються. При цьому якщо політика безпеки оформляється у вигляді високорівневого документа, що описує загальну стратегію, то аналіз ризиків (як додаток) оформляється у вигляді списку активів, що потребують захисту.

У цілому, необхідно розв’язання проблем на трьох рівнях та їх узгодженність між собою. Ретельність розробки та виконання кожного рівня безпеки, безпосередня зацікавленість вищого керівництва в забезпеченні інформаційної безпеки, чітка відповідальність персоналу за виконання своїх функцій; передбачення майбутніх планів розвитку організації, появи нових ризиків, бачення перспектив ось далеко не повний перелік складових, що можуть привести до успіху.

Література

1. Ахрамович В.М. Інформаційна безпека: навч. посіб. К.:ДП «Інформ.-аналіт. Агенство», 2009.-276с

2. Грайворонський М. В. Безпека інформаційно-комунікаційних систем / М. В. Грайворонський, О. М. Новіков. – К. : Вид.група BUV, 2009. – 608 с.

3. Домарєв В.В., Швець В.А., Шестакова В.В. Організаційне забезпечення захисту інформації з обмеженим доступом. Навчальний посібник. – К.: НАУ, 2006. – 108 с.

4. Лужецький В. А. Основи інформаційної безпеки : навчальний посібник / В. А. Лужецький, О. Д. Кожухівській, О. П. Войтович, – Черкаси: ЧДТУ, 2008. – 223 с

5. Самохвалов Ю.Я., Темніков В.О., Хорошко В.О. Організаційно-технічне забезпечення захисту інформації / За ред. проф. В.О.Хорошка – К.: Видавництво НАУ, 2002. – 208с.

Надійшла 17.01.2017 р. Рецензент: д.т.н., с.н.с. Наконечний В.С.