Гуменюк А. В.,
кандидат економічних наук, доцент
Курницький Д.П., здобувач 2 к. 641 гр.
Уманський державний педагогічний
університет імені Павла Тичини
м. Умань, Україна

ІНФОРМАЦІЙНА БЕЗПЕКА ЯК ФАКТОР СТАБІЛЬНОСТІ БІЗНЕС-ПРОЦЕСІВ

У сучасному цифровому світі безпека інформації стає все більш актуальним та критично важливим завданням для організацій у всіх галузях. Впровадження ефективної політики інформаційної безпеки (далі - ІБ) є невід'ємним елементом забезпечення захисту конфіденційності, цілісності та доступності інформації. Розглянемо основні вимоги та принципи, які необхідно враховувати під час розробки та впровадження політики інформаційної безпеки.

Інформаційна безпека - стан захищеності інформаційного середовища суспільства, що забезпечує її формування, використання і розвиток в інтересах громадян, організацій, держав [1].

На думку науковців, інформаційна безпека охоплює процеси не тільки захисту інформації, але й, наприклад, обміну інформацією [2].

Принципи, що враховуються при розробці та впровадженні політики інформаційної безпеки:

- законність. Здійснення захисних заходів відповідно до чинного законодавства в галузі ІБ, іншими нормативними актами, затверджених органами державної влади, застосуванням усіх дозволених методів виявлення та припинення правопорушень.
- системність. Врахування всіх взаємопов'язаних і змінних у часу елементів, умов і чинників, значимих підтримки ІБ в організації, включаючи всі об'єкти захисту та напрями порушень ІБ, уразливості використовуваних систем та високу кваліфікацію зловмисник.
- мультидисциплінарний підхід до розробки політики ІБ. Врахування правових, технічних, адміністративних, організаційних, навчальних, комерційних та функціональних питань.
- багаторівневість оборони та різноманітність захисту коштів. Утруднення дій зловмисника (зловмисник для злому системи повинен володіти різноманітними знаннями та навичками).

Цілеспрямований безперервний процес вжиття відповідних заходів на всіх етапах життєвого циклу організації:

- гнучкість керування та застосування захисних заходів. Забезпечення можливості варіювати рівень захищеності залежно від поточної ситуації та потреби організації ІБ у цей період часу.
- спостережуваність і контрольованість захисних заходів. Результат їх застосування буде явний і може бути оцінено підрозділом організації, які мають відповідні повноваження.

Вимоги, які враховуються при розробці та впровадженні політики інформаційної безпеки:

1. Аналіз загроз та ризиків. Першим і основним кроком при розробці політики ІБ є аналіз загроз та ризиків, з якими може зіткнутися організація. Це дозволяє визначити потенційні вразливості та небезпеки для інформації, а також виявити найбільш істотні активи, які потребують особливого захисту. Аналіз ризиків допомагає оцінити потенційні наслідки інцидентів безпеки та розробити відповідні заходи щодо їх запобігання або мінімізації.

2. Законодавчі вимоги та регуляторні норми. При розроблення політики ІБ необхідно враховувати законодавчі вимоги та регуляторні норми, що регулюють область інформаційну безпеку.

3. Управління доступом. Контроль доступу є важливим складової політики ІБ. Вона визначає правила та процедури для авторизації та аутентифікації користувачів, управління привілеями доступу, а також моніторингу та реєстрації подій у системі. Кожен користувач повинен мати лише ті привілеї, які необхідні для виконання своїх робочих обов'язків, та доступ до конфіденційна інформація повинна бути обмежена і контролюється.

4. Навчання та обізнаність користувачів. Політика ІБ повинна включати програми навчання та обізнаності користувачів про прийняті правила та процедури безпеки. Користувачі є однією зі слабких ланок у ланцюзі інформаційної безпеки, та навчання допомагає їм зрозуміти ризики та загрози, з якими вони можуть зіткнутися і навчитися застосовувати відповідні заходи безпеки.

5. Регулярне оновлення та аудит політики ІБ. Інформаційне середовище та загрози постійно змінюються, тому політика ІБ має бути регулярно оновленою. Оновлення політики ІБ дозволяє впроваджувати нові технології та методи захисту, а також враховувати нові загрози та вимоги безпеки. Аудит політики ІБ допомагає перевірити відповідність політики дійсній практиці та виявити можливі вразливості та прогалини у безпеці.

Особливу увагу під час формування комплексної політики ІБ рекомендується приділяти міжнародним стандартам, зокрема ISO/IEC 27002:2005 та ГОСТ Р ІСО/МЕК 17799-2005, у яких визначено її загальну структуру. Політика ІБ повинна містити:

1. визначення цілей, значущості та сфери дії ІБ;
2. принципи управління інформаційною безпекою, орієнтовані на бізнес-цілі організації та управління ризиками;
3. вимоги та правила щодо відповідності законодавству, захисту від шкідливого ПЗ, відповідальності за порушення тощо;
4. розподіл обов’язків і порядок реагування на інциденти;
5. посилання на додаткові документи з більш детальними процедурами.

Розробка та впровадження політики інформаційної безпеки вимагає обліку низки основних вимог та принципів. Важливо провести аналіз загроз та ризиків, врахувати законодавчі вимоги, залучити зацікавлених сторін та застосувати системний підхід. Ключовими аспектами політики ІБ є управління доступом, навчання користувачів, регулярне оновлення та аудит політики. Метою цих вимог та принципів є створення ефективної системи захисту інформації, що забезпечує конфіденційність, цілісність та доступність даних організації. Впровадження політики ІБ вимагає постійного моніторингу та вдосконалення, щоб бути адаптованою до змін, що змінюються, і технологіям. Сучасні організації повинні усвідомлювати, що інформаційна безпека є безперервним процесом і вимагає участі всіх співробітників, починаючи від вищого керівництва та закінчуючи звичайними користувачами.

Отже, розробка та впровадження політики ІБ – це невід’ємна частина стратегії інформаційної безпеки кожної організації та, коли ці вимоги та принципи застосовуються правильно, вони допомагають мінімізувати ризики та запобігати витокам та порушенням безпеки даних. При цьому організація може забезпечити довіру своїх клієнтів та захистити свою репутацію, що є фундаментом для успішного функціонування у сучасному інформаційному суспільстві.

Література:

1. Якименко Ю. М., Савченко В. А., Легомінова С. В. Системний аналіз інформаційної безпеки: сучасні методи управління: підручник. Київ: Державний університет телекомунікацій, 2022. 308 с.
2.Чубаєвський В., Жук Т. Економічна ефективність інформаційної безпеки підприємств торгівлі. Цифрова економіка. 2022. No 1. С. 106–117. DOI: http://doi.org/10.31617/visnik.knute.2022(141)08