льчих та непродовольчих товарів в умовах фінансово-економічної кризи: Постанова Кабінету Міністрів України від 05.03.2009 р. № 278. [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg =278-2009-%EF.

4. Про встановлення повноважень органів виконавчої влади та виконавчих органів міських рад щодо регулювання цін (тарифів): Постанова Кабінету Міністрів України від 25.12.1996 р. № 1548 (з наступними змінами та доповненнями). [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=1548-96-%EF.

5. Про затвердження Порядку розрахунку цін на послуги та оренду торгових приміщень (площ) та їх обслуговування на ринках з продажу продовольчих та непродовольчих товарів: спільний наказ Міністерства економіки України та Державного комітету України з питань регуляторної політики та підприємництва від 30.06.2009 р. № 638/109 (з наступними змінами та доповненнями). [Електронний ресурс]. – Режим доступу: http://me.kmu.gov.ua/control/uk/publish/article?art_id=141955&cat_id=32854.

6. Організація торгівлі: підручник. – 3-тє вид. / [В.В. Апопій, І.П. Міщук, В.М. Ребрицький, С. І. Рудницький, Ю.М. Хомяк]. – К.: Центр учбової літератури, 2009. – 632 с.

7. Економічні системи: монографія. – Т. 1. / за ред. Г.І. Башнянина. – Львів: Вид-во Львівської комерційної академії, 2006. – 484 с.

8. Пустовойт О. Розвиток ринку торговельних послуг / О. Пустовойт // Економіка України: Політико-економічний журнал Міністерства економіки та з питань європейської інтеграції України, Міністерства фінансів України та Національної академії наук України. – 2004. – № 9. – С. 30–36.

УДК 519.7

Т.В. Рудий,
Я.Ф. Кулешик, І.М. Ганич,
І.В. Бичинюк

УПРАВЛІННЯ БЕЗПЕКОЮ В ІНФОРМАЦІЙНИХ СИСТЕМАХ МВС

Розроблення, проектування і впровадження системи управління інформаційною безпекою в інформаційних системах оперативних підрозділів МВС, організаційна структура яких базується на рекомендаціях міжнародних стандартів та чинного законодавства України, надає можливість реалізувати захист інформаційних активів, забезпечити безперервне функціонування інформаційної системи і мінімізувати ризики.

Ключові слова: *інформаційні технології, система управління інформаційною безпекою, інформаційна система, політика інформаційної безпеки, інформаційні активи, ризики безпеки.*

Разработка, проектирование и внедрение системы управления информационной безопасностью в информационных системах оперативных подразделений МВД, организационная структура которых базируется на рекомендациях международных стандартов и действующего законодательства Украины, предоставляет возможность реализовать защиту информационных активов, обеспечить беспрерывное функционирование информационной системы и минимизировать риски.

Ключевые слова: *информационные технологии, система управления информационной безопасностью, информационная система, политика информационной безопасности, информационные активы, риски безопасности.*

It is stated in the article that development, design, implementation and management of information security in information systems of law enforcement operational units, organizational structure which is based on the recommendations of international standards and current legislation of Ukraine, provides an opportunity to realize the protection of information assets, ensure continuous operation of an information system and minimize risks.

Key words: *information technology, information security management system, information system, information security policy, information assets, security risks.*

Постановка проблеми. Система управління інформаційною безпекою (СУІБ) повинна забезпечувати безпечність та надійність функціонування інформаційних систем (ІС) оперативних підрозділів МВС. Впровадження та функціонування СУІБ стосується всіх підрозділів і насамперед керівників. Тому ці посадові особи повинні брати безпосередню участь у вирішенні питань, які належать до сфери їх відповідальності, під час упровадження та функціонування СУІБ.

Цілі СУІБ та заходи безпеки, які вже запроваджені і ті, що будуть додатково впроваджені в разі необхідності, а також відповідна документація, що описує функціонування СУІБ, повинні бути зрозумілими для всіх, кого це стосується. Тому обов'язковою умовою успішного функціонування СУІБ є також проведення відповідних навчань працівників з питань інформаційної безпеки (ІБ).

Стан дослідження. Проблемам створення і функціонування СУІБ присвячено достатньо публікацій як у відкритих, так і закритих літературних джерелах. З доступних для пересічного користувача джерел хочемо відзначити праці таких вчених як М.П. Карпінський, В.П. Захаров, А.О. Ботюк, С.Г. Бабичев, В.П. Горбулін, В.В. Домарьов, В.Ю. Захарченко, В.І. Лазуренко, С.А. Петренко, А.В. Бєляєв та ін. Важливість наукового здобутку та внеску у теорію і практику захисту інформації згаданих вчених важко переоцінити.

Аналіз літературних джерел дає підстави стверджувати, що у процесі проектування, створення і експлуатування СУІБ є певні недоліки, які знижують ефективність їх функціонування. Як правило, керівники підрозділів МВС розглядають проблему засобів інформації (ЗІ) та інформаційних систем переважно з технічної точки зору. Розв'язання проблеми пов'язують з придбанням та інсталяцією програмно-апаратних засобів ЗІ. Однак, для організації ефективного режиму інформаційної безпеки цього недостатньо. Необхідно також обґрунтувати розроблення СУІБ, яка визначає стратегію і тактику системи ЗІ та враховує динаміку зміни загроз інформації.

Мета дослідження полягає у визначенні організаційних принципів і методів управління ІБ в ІС оперативних підрозділів МВС. Тому розглянемо набір принципів, які дозволяють створити ефективну СУІБ. Разом з тим, варто відзначити, що ці принципи є всього лише одним з аспектів стратегії управління інформаційними технологіями (ІТ). Неможливо успішно керувати ІБ в ІС при незадовільному управлінні цими технологіями.

Виклад основних положень. Автори пропонують розробляти організаційну структуру і впроваджувати СУІБ відповідн до рекомендацій міжнародних стандартів та чинного законодавства України [1]. Такими стандартами є:

- ISO/IEC 27002:2005 Інформаційні технології. Методи захисту. Кодекс практики для управління інформаційною безпекою [2].
- ISO/IEC 27003:2010 Інформаційні технології. Методи захисту. Керівництво з застосування системи менеджменту захисту інформації [3].
- ISO/IEC 27004:2009 Інформаційні технології. Методи захисту. Вимірювання [4].
- ISO/IEC 27005:2008 Інформаційні технології. Методи забезпечення безпеки. Управління ризиками інформаційної безпеки [4].
- ISO/IEC 27006:2007 Інформаційні технології. Методи забезпечення безпеки. Вимоги до органів аудиту і сертифікування систем управління інформаційною безпекою [5, 6, 7].

Впровадження стандартів з питань СУІБ не може бути разовою акцією. Це фактично є безперервним процесом розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та вдосконалення системи інформаційної безпеки [8].

Зрозуміло, що для проведення цих робіт потрібні ресурси, у тому числі наявність фахівців з питань ІБ, наявність з боку керівництва

повної підтримки та контролю, а також розуміння проблем, які постійно виникають.

Керівництво підрозділів повинно забезпечити визначення завдань ІБ, їх відповідність вимогам чинного законодавства України, нормативно-правових актів, наказів керівництва МВС, настанов відповідних служб, інтегрованість у суміжні служби, переглядати ефективність впровадження та функціонування СУІБ, надавати ресурси, які потрібні для забезпечення інформаційної безпеки ІС та навчання персоналу. Для розв'язання цих завдань необхідно визначити організаційну структуру системи управління інформаційною безпекою, повноваження та відповідальність щодо розроблення, впровадження та функціонування СУІБ.

Для процесів СУІБ застосована модель «ПВПД» (плануй–виконуй–перевіряй–дій), яка використовує п'ять принципів управління ІБ:

Оцінювання ризиків і визначення потреб.

Встановлення централізованого адміністрування.

Впровадження необхідних політик безпеки і відповідних засобів контролю.

Досягнення необхідного рівня підготовленості працівників.

Контроль і оцінювання ефективності політик безпеки і механізмів контролю.

Істотним чинником ефективного здійснення цих принципів є сполучний цикл діяльності, який гарантує, що СУІБ постійно націлена на поточні ризики. Важливо, щоб керівництво своєчасно оцінило наявність ризиків, пов'язаних з безпекою інформаційних систем. Підставою для розроблення і впровадження політик безпеки та вибору необхідних засобів контролю є оцінювання ризиків. Прийняті кроки дозволять збільшити обізнаність керівництва про ризики і відповідні політики безпеки.

Ефективність засобів контролю полягає в оцінюванні шляхом різних досліджень та аудиторських перевірок. Отримані результати забезпечують підхід до подальшого оцінювання ризиків і визначають необхідні зміни в політиках і засобах контролю. Всі ці дії централізовано адмініструються і координуються відповідною службою або штатом фахівців, що складається з консультантів, представників окремих служб та відділів, керівників підрозділів.

Організаційні принципи управління інформаційною безпекою подано на рисунку.

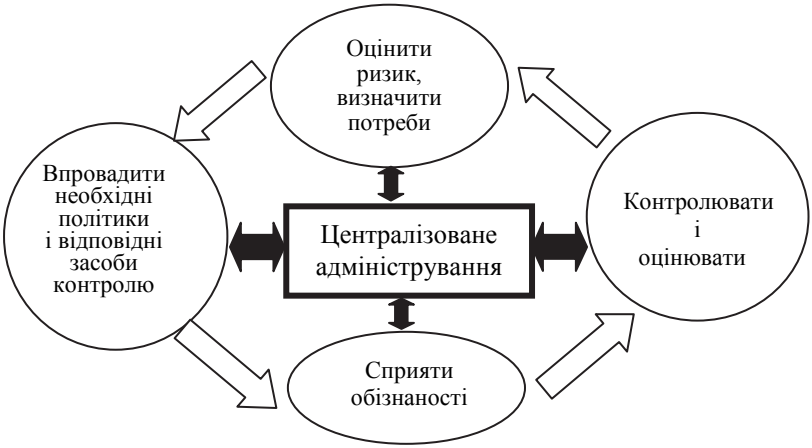

Рис. Організаційні принципи управління інформаційною безпекою

Наступні шістнадцять методів, які використовуються для реалізації п'яти принципів СУІБ, є ключовими для ефективного виконання програми ІБ. Вони є такими:

- визнати інформаційні ресурси як істотні (невід'ємні) активи ІС підрозділів ОВС;
- визначити групу адміністрування для виконання ключових дій;
- надати групі адміністрування незалежний доступ до керівництва;
- обґрунтувати і виділити бюджет та персонал;
- встановити відмінності між політиками і керівними принципами;
- встановити взаємозв'язок політик і ризиків;
- забезпечити супровід політик безпеки групою адміністрування;
- розробити практичні процедури оцінювання ризиків;
- безперервно управляти ризиками;
- контролювати чинники, які впливають на ризики і вказують на ефективність ІБ;
- підвищувати професіоналізм і технічні знання працівників;
- безперервне навчання користувачів та інших працівників на прикладі ризиків та відповідних політик;

- використовувати дружній підхід;
- встановити відповідальність керівників підрозділів і керівників, які беруть участь у програмі забезпечення безпеки;
- використовувати отримані результати для координування майбутніх зусиль і підвищення відповідальності керівництва;
- відслідковувати нові методи та засоби контролю.

Оцінювання ризику є першим кроком реалізації програми забезпечення ІБ. Безпеку розглядатимемо як набір політик безпеки і відповідних засобів контролю, призначених для безпечного функціонування ІС та зменшення відповідних ризиків. Таким чином, визначення ризиків, пов'язаних з інформаційною безпекою, є відправною точкою циклу управління нею.

Політика інформаційної безпеки (ПІБ) – це пакет документів, який описує і регламентує систему управління інформаційною безпекою ІС оперативних підрозділів МВС, відповідає вимогам чинного законодавства України та міжнародних угод, базується на рекомендаціях міжнародних стандартів.

Метою політики інформаційної безпеки є впровадження та ефективне управління системою забезпечення ІБ, спрямованої на захист інформаційних активів, забезпечення безперервного функціонування ІС, мінімізування ризиків, створення позитивної репутації оперативних підрозділів МВС та довірчих відносин з населенням.

Основним завданням впровадження ПІБ є захист інформаційних активів від зовнішніх та внутрішніх навмисних та ненавмисних загроз. Політика розповсюджується на всі аспекти діяльності ІС оперативних підрозділів та застосовується до всіх інформаційних активів, які можуть справляти матеріальний інтерес для кримінальних структур у разі несанкціонованого витоку.

Як основні об'єкти області діяльності інформаційної безпеки, розглядаються наступні види активів:

інформаційні активи: інформація та дані у довільному вигляді, які отримуються, зберігаються, обробляються, передаються, оголошуються (до цього виду необхідно віднести знання працівників, бази даних та системи біометричного ідентифікування, документація, навчальні матеріали, описи процедур, інформація на фізичних носіях);

програмне забезпечення: прикладне програмне забезпечення, системне програмне забезпечення, сервісне програмне забезпечення та довільне інше програмне забезпечення, незалежно від форми отримання (придбання, власного розроблення, вільного розповсюдження), яке

використовується працівниками для роботи та у процесі взаємодії з іншими службами;

фізичні активи: працівники, апаратні засоби інформаційних технологій (корпоративні комп'ютерні мережі (КМ) і мережеві технології, сервери, робочі станції, міжмережеві екрани, телекомунікаційне обладнання, обладнання зв'язку, маршрутизатори, АТС), приміщення, спеціальне обладнання, технічні засоби;

сервісні активи: інформаційні та телекомунікаційні сервіси (сервіси Internet, E-mail, спеціальних каналів зв'язку), інші технічні сервіси (опалення, освітлення, системи сигналізацій та моніторингу), усі послуги, пов'язані з отриманням, наданням, використанням, передаванням та знищенням активів, усі юридичні та фізичні особи, організації, установи та підприємства, а також їх працівники, яким передані певні послуги на ІТ-аутсорсинг [9].

Для кожного активу визначаються можливі ризики та шляхи їх мінімізування, тобто рекомендуємо використати ризик-орієнтований підхід.

Оцінювання можливих ризиків провадиться за чотирма основними критеріями безпеки:

доступність – забезпечення безперервного доступу до інформаційних та супутніх активів ІС, спеціальних КМ та сервісів згідно з наданими працівникам повноваженнями та правами у мінімально необхідному обсязі;

цілісність – захист точності/коректності та повноти активів і методів оброблення інформації;

конфіденційність – забезпечення доступності до ІС, спеціальних КМ, інформації, активів тільки для офіційно авторизованих працівників у мінімально необхідному обсязі;

спостережливість – забезпечення можливості визначення – хто, що і коли робив з тим, або іншим інформаційним активом (забезпечення принципу невідмови від вчинених дій).

Політика регламентує управління доступами та паролями, чіткий розподіл ролей та обов'язків, визначення вимог ІБ для кожного активу. Впровадження ПІБ в інформаційні системи забезпечує підтримку рівня безпеки на належному рівні, що у свою чергу, передбачає:

постійне навчання працівників у сфері ІБ;

проведення контролю безпеки та доступу до ІС;

управління інцидентами, класифікування та забезпечення конфіденційності інформації;

антивірусний захист, резервне копіювання, ліцензійну чистоту програмного забезпечення, вхідний/вихідний контроль за обміном інформацією у ІС;

забезпечення фізичної безпеки та інших аспектів інформаційної безпеки.

Для зменшення ризиків виникнення інцидентів ІБ, пов'язаних з зовнішніми і внутрішніми навмисними та ненавмисними впливами, елементарною необізнаністю працівників необхідно розробити та запровадити систему управління інцидентами інформаційної безпеки (СУІБ), яка є базовою частиною загальної системи управління інформаційною безпекою. Вона дозволяє виявляти, враховувати, реагувати й аналізувати події та інциденти інформаційної безпеки. Без реалізації цих процесів неможливо забезпечити рівень захищеності, який є адекватним до вимог сучасних стандартів і галузевих норм.

Управління інцидентами є важливим процесом, який забезпечує можливість спочатку виявити інцидент, а потім, за допомогою коректно обраних засобів підтримки, якомога швидше його розв'язати.

Основна задача управління інцидентами – відновити нормальну роботу служб та сервісів і звести до мінімуму негативний вплив інциденту на роботу ІС для підтримки якості й доступності служб на максимально можливому рівні. Нормальною вважається робота служб та сервісів, що не виходить за рамки угоди про рівень обслуговування.

Перед СУІБ ставляться наступні цілі:

відновлення нормального функціонування служб та сервісів ІС у найкоротші терміни;

зведення до мінімуму впливу інцидентів на функціонування ІС;

забезпечення злагодженого оброблення всіх інцидентів і запитів обслуговування;

зосередження ресурсів підтримки на найважливіших напрямах;

надання відомостей, які дозволять оптимізувати процеси підтримки, зменшити кількість інцидентів і планувати управління.

Використовуючи найкращі, перевірені часом напрацювання і вирівнювання ІТ-процесів для оброблення збоїв довільних видів, рішення з управління інцидентами дозволяють використовувати ресурси залежно від пріоритетів оперативної діяльності, управляти рівнями обслуговування, а також краще контролювати роботу ІТ-служб.

Для реалізування системи управління інцидентами інформаційної безпеки необхідно виконати наступні роботи:

надати ресурси для розроблення та впровадження системи СУІБ;

здійснити фахову підготованість працівників;

визначити область функціонування СУІБ;

розробити комплекс процесів СУІБ;

впровадити процеси СУІБ та інтегрувати їх з уже функціонуючими процесами, такими як інвентаризування активів, аналіз ризиків та оцінювання ефективності;

розробити архітектуру і комплекс програмно-технічних засобів з автоматизації процесів СУІБ і моніторингу подій.

У результаті проведених робіт буде запроваджена СУІБ, яка розв'язуватиме наступні задачі:

оперативний моніторинг стану ІБ в рамках функціонування ІС;

виявлення, облік, реагування, розслідування та аналіз інцидентів ІБ;

інформування вищого керівництва про поточний стан ІБ.

Таким чином, необхідно реалізувати комплексний підхід щодо розв'язання наступних задач:

виявлення, інформування та облік інцидентів ІБ;

реакція на інциденти, включаючи застосування необхідних засобів для запобігання, зменшення і відновлення завданого збитку;

аналіз реалізованих інцидентів з метою планування превентивних заходів захисту і покращення процесу забезпечення ІБ в цілому.

Для оброблення подій та інцидентів ІБ необхідно організувати процес реагування на інциденти, основними задачами якого є:

забезпечення координування реагування на інцидент;

підтвердження/спростування факту виникнення інциденту;

забезпечення збереження і цілісності доказів виникнення інциденту, створення умов для накопичення і зберігання точної інформації про інциденти, які мали місце;

мінімізування порушень порядку роботи і модифікування даних, відновлення в найкоротші терміни працездатності ІС при її порушенні у результаті інциденту;

мінімізування наслідків порушення режиму конфіденційності, цілісності і доступності інформації у ІС;

захист активів ІС;

створення умов для порушення цивільної або кримінальної справи проти зловмисників;

швидке виявлення та/або попередження подібних інцидентів у майбутньому.

Висновки. Система управління інформаційною безпекою дозволяє виявляти, враховувати, реагувати й аналізувати події та інциденти інформаційної безпеки. Без реалізування цих процесів неможливо забезпечити рівень захищеності, який є адекватним до вимог сучасних стандартів і галузевих норм.

Впровадження політики інформаційної безпеки надає можливість захисту інформаційних активів від зовнішніх та внутрішніх навмисних та ненавмисних загроз, розповсюджується на всі аспекти діяльності ІС оперативних підрозділів та застосовується до всіх інформаційних активів, які можуть справляти матеріальний інтерес для кримінальних структур у разі несанкціонованого витоку.

Для зменшення ризиків виникнення інцидентів ІБ, пов'язаних з зовнішніми і внутрішніми навмисними та ненавмисними впливами, елементарною необізнаністю працівників, необхідно розробити та запровадити систему управління інцидентами інформаційної безпеки, яка є базовою частиною загальної системи управління інформаційною безпекою.

Наостанок відзначимо, що при експлуатуванні систем менеджменту інформаційної безпеки процес управління інцидентами є одним з найважливіших у постачанні даних для аналізу функціонування таких систем, оцінювання ефективності використовуваних заходів, зниження ризиків і планування удосконалення захисту ІС.

1. Про інформацію: Закон України // Відомості Верховної Ради України. – 1992. – № 48 (зі змінами і доповненнями). [Електронний ресурс]. – Режим доступу: http://www.rada.gov.ua.

2. Міжнародний стандарт ISO/IEC 27002. [Електронний ресурс]. – Режим доступу: http://www.wikitntu.org.ua.

3. Міжнародний стандарт ISO/IEC 27003-27004. [Електронний ресурс]. – Режим доступу: http://www.iso27001security.com.

4. Міжнародний стандарт ISO/IEC 27005. [Електронний ресурс]. – Режим доступу: http://www.riskmanagementinsight.com

5. Міжнародний стандарт ISO/IEC 27006. [Електронний ресурс]. – Режим доступу: http://27000.org

6. Когут В.В. Порядок атестування систем технічного захисту інформації / В.В. Когут, Т.В. Рудий, Я.Ф. Кулешник // Проблеми діяльності кримінальної міліції в умовах розбудови правової держави: матеріали науково-звітної конф. фак. кримінальної міліції Львівського державного університету внутрішніх справ (12 березня 2010 р.). – Львів: ЛьвДУВС, 2010. – С. 90–97.

7. Специфіка протидії злочинам у сфері інформаційних технологій / [Т.В. Рудий, В.М. Слижук, І.М. Ганич, А.В. Нечепуренко] / Проблеми діяльно-

сті кримінальної міліції в умовах розбудови правової держави: матеріали V звітної науково-практичної конф. фак. кримінальної міліції Львівського державного університету внутрішніх справ (14 квітня 2011 р.). – Львів: ЛьвДУВС, 2011. – С. 168–176.

8. Кулешник Я.Ф. Модель системи інформаційної безпеки у Windows / Я.Ф. Кулешник, Т.В. Рудий, А.Т. Рудий // Проблеми застосування інформаційних технологій, спеціальних технічних засобів у діяльності ОВС, навчальному процесі, взаємодії з іншими службами: матеріали науково-практичного семінару (4 грудня 2009 р.). – Львів: ЛьвДУВС, 2009. – С. 89–93.

9. Руда О.І. Аутсорсинг у сфері інформаційних технологій / О.І. Руда, І.І. Руда // Проблеми застосування інформаційних технологій, спеціальних технічних засобів у діяльності ОВС, навчальному процесі, взаємодії з іншими службами: матеріали науково-практич. конф. (24 грудня 2010 р.). – Львів: ЛьвДУВС, 2010. – С. 196–200.

УДК 65.012.8:33+338.45

Ю.О. Гершуненко

ВИРОБНИЧО-ЕКСПОРТНИЙ ПОТЕНЦІАЛ У СИСТЕМІ ЗМІЦНЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ КРАЇНИ

Розглянуто сутність та специфіку інноваційного розвитку виробничо-експортного потенціалу, згруповано існуючі підходи до його оцінки.

Ключові слова: *виробничо-експортний потенціал, інвестиції, економічна безпека.*

Рассмотрены понятие и специфика инновационного развития производственно-экспортного потенциала, сгруппированы основные подходы к его оценке.

Ключевые слова: *производственно-экспортный потенциал, инвестиции, экономическая безопасность.*

The essence and specific of innovation development of industrial-export potential are considered in the article and the existing approaches to its evaluation are classified.

Key words: *production and export potential, economic security, system strengthening economic security, investments.*

Постановка проблеми. Економічна безпека держави є складовою національної безпеки на рівні особи, суспільства і держави; здатність держави забезпечувати ефективне задоволення суспільних потреб і стійкого економічного розвитку її забезпечення тісно