УДК 004.939

**Т. В. Рудий,**
**О. В. Захарова, В. В. Сеник,**
**С. В. Сеник, М. І. Ізьо**

# ОРГАНІЗАЦІЙНО-ПРАВОВИЙ СУПРОВІД ЗАХИСТУ ІНФОРМАЦІЙНИХ СИСТЕМ ПІДРОЗДІЛІВ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ НА ОСНОВІ МІЖНАРОДНИХ СТАНДАРТІВ

*Означено проблеми захисту інформації, які не можуть бути розв'язаними без створення нових законодавчих актів і запровадження нової політики у сфері інформатизації, тобто заналізовано інформаційні відносини з огляду на об'єкт правового регулювання.*

*Роз'яснено і обґрунтовано потребу розроблення організаційно-правових засад, які визначають стратегію, тактику системи захисту інформаційних систем підрозділів Національної поліції України з урахуванням динаміки зміни загроз інформаційним активам на основі положень міжнародних стандартів ISO/IEC серії 27000.*

**Ключові слова:** *інформаційна система, захист інформації, інформаційні загрози, нормативно-правові чинники, міжнародні стандарти.*

**Постановка проблеми**. Підвищення рівня захищеності інформаційного середовища підрозділів Національної поліції України є сьогодні надактуальним завданням суспільства. З-поміж визначальних у цьому аспекті є нормативно-правові чинники – закони, стандарти, галузеві нормативні документи, рішення тощо. Мета в них одна – забезпечити виконання організаційно-технічних заходів зі захисту інформації (ЗІ), що дасть змогу підняти рівень захищеності спеціалізованих інформаційних систем (ІС).

В умовах повномасштабної інформаційної війни, яка ведеться проти нашої країни, забезпечення безпеки ІС підрозділів Національної поліції (НП) України, безумовно, має стати державним завданням. Особливої уваги вимагає захист критичних активів, а також централізованих баз даних.

Несанкціонований доступ до інформаційних активів може істотно ускладнювати виконання завдань оперативними підрозділами НП, тому проблема створення ефективної системи ЗІ набуває неабиякого значення. Автори вважають, що така система ЗІ повинна бути найперше комплексною і адаптивною.

**Стан дослідження.** Проблемам організаційно-правового супроводу створення і функціонування систем ЗІ присвячено достатньо публікацій у відкритих літературних джерелах. Багато з них торкаються проблеми ЗІ, яка не може бути розв'язаною без упровадження нових законодавчих, нормативно-правових актів і нової політики у сфері інформатизації, тобто без висвітлення інформаційних відносин з огляду на об'єкт правового регулювання.

Назагал, незважаючи на позитивні зміни у законодавчому регулюванні інформаційних відносин, обмеженість національного законодавства і відсутність єдиної правової бази правоохоронних органів у протидії порушенням безпеки ІС, залишаються одними з головних причин зростання кількості і високого рівня латентності злочинів, пов'язаних із порушеннями інформаційної безпеки (ІБ).

Важливою проблемою є й відсутність системного підходу до формування правової політики держави в інформаційній сфері, про що наголошують у своїх публікаціях відомі у цій галузі науковці [1; 2; 3; 4].

З розвитком інформаційних технологій (ІТ) і систем ЗІ виникла потреба уніфікувати вимоги до їх проектування та впровадження, забезпечивши належний рівень стандартизації. Одним з найважливіших напрямів цієї роботи визнано адаптування міжнародного стандарту ISO/IEC серії 27000.

Аналіз літературних джерел дає підстави стверджувати, що у процесі проектування, створення й експлуатування систем ЗІ існують суттєві недоліки, які знижують ефективність їхнього функціонування. Тож слід обґрунтувати розроблення організаційно-правових засад ЗІ, які визначать стратегію, тактику системи ЗІ, врахувавши динаміку зміни загроз інформаційним активам ІС.

Тимчасом чинне законодавство України в інформаційній сфері недостатньо враховує вимог міжнародних стандартів, які надають дещо ширший спектр послуг і профілів захищеності.

Дотримання принципів стандартів ISO/IEC серії 27000 забезпечує керування і контроль доступом, розроблення та обслуговування апаратно-програмних комплексів, керування безперервністю інформаційних процесів.

Відповідність вимогам стандартів ISO/IEC серії 27000 і дотримання національних правових норм з інформаційної безпеки є запорукою створення ефективної системи ЗІ.

**Мета** статті полягає у тому, щоб окреслити організаційно-правову структуру системи ЗІ в ІС підрозділів НП України з урахуванням вимог міжнародних стандартів ISO/IEC серії 27000, попри те що

це є лиш одним з аспектів стратегії системи управління інформаційними технологіями у підрозділах НП України.

**Виклад основних положень**. Інкорпорацію законодавства України та структуру нормативно-правових актів України у галузі технічного захисту інформації, обов'язкових до виконання, на рівні правової доктрини можна подати так:

– Конституція України;

– закони України;

– укази та розпорядження Президента України;

– постанови та розпорядження Кабінету Міністрів України;

– нормативно-правові акти Служби безпеки України, Державної служби спеціального зв'язку та захисту інформації (ДССЗТЗІ) України;

– міжнародні угоди України з питань технічного захисту інформації, згода на обов'язковість виконання яких надана Верховною Радою України.

Регулятивно-правову основу забезпечення ЗІ в ІС підрозділів НП України становлять: Конституція України; Постанова Верховної Ради України «Про концепцію національної безпеки України»; закони України «Про інформацію», «Про науково-технічну інформацію», «Про державну таємницю», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про доступ до публічної інформації», «Про захист персональних даних»; Постанова Кабінету Міністрів України «Про затвердження правил захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах».

В Україні розроблено серію нормативних документів системи технічного захисту інформації, основним з яких є НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації комп'ютерних систем від несанкціонованого доступу». Цей документ використовується під час проектування та створення комплексних систем захисту інформації (КСЗІ) державних інформаційних ресурсів, а також ІС, в яких обробляється інформація з обмеженим доступом, вимогу щодо захисту якої визначено законом.

Однак довільно використовувана в проектуванні КСЗІ методологія мусить бути сумісною з основними сучасними стандартами, такими як ISO/IEC серії 27000.

Тому організаційно-правові засади системи ЗІ в ІС підрозділів Національної поліції України повинні формуватися відповідно до рекомендацій міжнародних стандартів та з дотриманням положень чинного законодавства України.

Такими стандартами є: ISO/IEC 27001:2013 Інформаційні технології. Методи захисту. Системи менеджменту інформаційною безпекою; ISO/IEC 27002:2005 Інформаційні технології. Методи захисту. Кодекс практики для менеджменту інформаційною безпекою; ISO/IEC 27003:2010 Інформаційні технології. Методи захисту. Керівництво з застосування системи менеджменту захисту інформації; ISO/IEC 27004:2009 Інформаційні технології. Методи захисту. Вимірювання; ISO/IEC 27005:2008 Інформаційні технології. Методи забезпечення безпеки. Управління ризиками інформаційної безпеки; ISO/IEC 27006:2007 Інформаційні технології. Методи забезпечення безпеки. Вимоги до органів аудиту і сертифікування систем менеджменту інформаційної безпеки [5, 6, 7, 8, 9].

У світовій практиці паралельно з розвитком технічних систем ЗІ розвивався напрямок стандартизації у частині менеджменту інформаційної безпеки. Результатом стало затвердження міжнародного стандарту ISO/IEC 27001:2005, а пізніше ISO/IEC 27001:2013 Впровадження системи менеджменту інформаційної безпеки (СМІБ). Стандарт дає змогу правильно організувати процес захисту інформаційних активів і управління ризиками для цих активів. Для контролю якості процесу менеджменту інформаційної безпеки було запроваджено інститут сертифікування. Сертифікат має міжнародний статус.

Відповідно до вимог стандарту, процес розроблення СМІБ охоплює такі етапи: етап планування – забезпечує правильне завдання контексту і масштабу СМІБ, оцінюються ризики, пропонується відповідний план оброблення цих ризиків; етап реалізування – впроваджує ухвалені рішення, які були визначені на етапі планування; аналіз захищеності – етап оцінювання ефективності та надійності функціонування створеної СМІБ, проведення аудиту ІБ, виявлення недоліків; реагування – етап виконання коригувальних дій з покращення функціонування СМІБ, реагування вимагає первісного інвестування, документування діяльності, формалізування підходу до управління ризиками, визначення методів аналізу.

Як основні об’єкти області функціонування СМІБ, розглядаються такі види активів:

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

– ***програмне забезпечення***: прикладне програмне забезпечення, системне програмне забезпечення, сервісне програмне забезпечен-

ня та довільне інше програмне забезпечення незалежно від форми отримання (придбання, власного розроблення, таке, що вільно розповсюджується), яке використовується працівниками для роботи та у процесі взаємодії з іншими службами;

– ***фізичні активи***: працівники, апаратні засоби комп'ютерних мереж і мережеві технології (сервери, робочі станції, міжмережеві екрани, телекомунікаційне обладнання, обладнання зв'язку), приміщення, виробниче обладнання, технічні засоби;

– ***сервісні активи***: інформаційні та комунікаційні сервіси (корпоративні комп'ютерні мережі спеціального призначення, Internet, E-mail, спеціальні канали зв'язку), інші технічні сервіси (опалення, освітлення, системи сигналізацій та моніторингу), усі послуги, пов'язані з отриманням, наданням, використанням, передаванням і знищенням активів, усі юридичні та фізичні особи, організації, установи й підприємства (а також їхні працівники), яким передано певні послуги на ІТ-аутсорсинг.

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

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

1. Встановлення централізованого адміністрування.
2. Автентифікування об'єктів, суб'єктів і активів ІС.
3. Авторизування об'єктів, суб'єктів і активів ІС.
4. Аналіз ризиків і формування керуючих впливів.
5. Досягнення необхідного рівня підготованості працівників.

Істотним чинником ефективного втілення цих принципів є сполучний цикл діяльності, який гарантує, що СМІБ постійно спрямована на поточні ризики. Важливо своєчасно оцінити наявність ризиків, пов'язаних із безпекою ІС.

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 політиці безпеки і засобах контролю. Всі ці дії централізовано адмініструються і координуються. Тобто у СМІБ інформаційних систем реалізовано адміністративне керування доступом.

Організаційні принципи реалізування СМІБ наведено на рисунку.

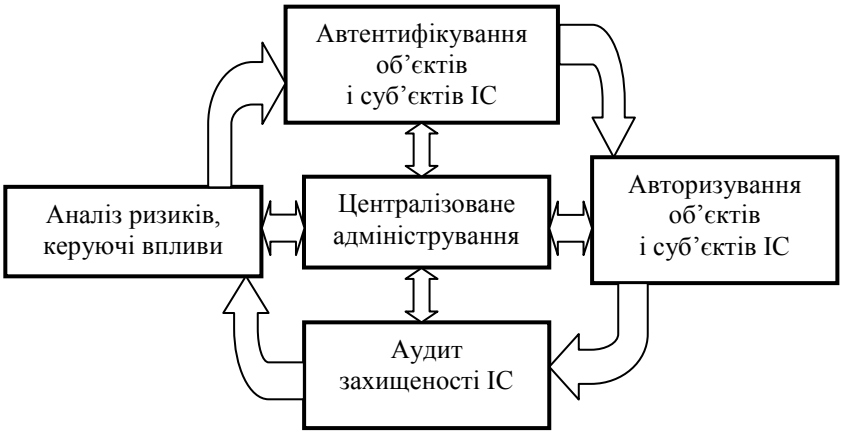


*Рис. Організаційні принципи реалізування системи менеджменту інформаційної безпеки*

Оцінювання ризиків, на думку авторів, повинно провадитися за чотирма основними критеріями безпеки – це:

- ***доступність*** – забезпечення безперервного доступу до інформаційних і супутніх активів ІС, сервісів згідно з наданими користувачам повноваженнями та правами у мінімально необхідному обсязі;
- ***цілісність*** – захист точності/коректності та повноти активів і методів оброблення інформації;
- ***конфіденційність*** – забезпечення доступності до інформаційних активів тільки для офіційно авторизованих користувачів у мінімально необхідному обсязі;
- ***спостережність*** – забезпечення можливості визначення – хто, що і коли робив з тим чи іншим інформаційним активом (забезпечення принципу невідмови від учинених дій).

Це означає, що керування інформаційними потоками між користувачами, процесами, об'єктами та суб'єктами здійснюють тільки спеціально авторизовані користувачі (адміністратори). Звичайні користувачі змінювати права доступу користувачів до процесів і пасивних об'єктів, а також виконувати довільні інші функції керування засобами СМІБ не можуть.

Слід зазначити, що хоча всі засоби СМІБ у стандартах та нормативних документах є важливими, але застосування засобів управління повинно відповідати ризикам і можливим загрозам для конкретної ІС.

Всі процедури забезпечення СМІБ мають бути адресними, тобто для кожної процедури мусить бути визначений перелік користувачів, виконавців, а також перелік інформаційних активів ІС, для яких потрібне їх застосування.

Оцінювання ефективності процедур СМІБ, як правило, виконується за результатами аудиту безпеки та перевірок, якість і періодичність яких може суттєво вплинути на функціонування всієї ІС.

Впроваджуючи інформаційну стратегію при розробленні СМІБ, вважаємо за необхідне вдатися до теорії та практики інформаційного аудиту, що дає можливість отримати цілісну й об'єктивну картину стану всієї ІС та її окремих елементів, локалізувати наявні проблеми з метою створення ефективної і оптимальної програми розвитку забезпечення ІБ.

В умовах упровадження технології систем з відкритою архітектурою, які вирізняються складною взаємодією ІС різного походження (інтероперабельністю), існуванням проблем перенесення прикладних програм між різними платформами (мобільністю) та іншими особливостями, питання впровадження СМІБ набуває все більшої ваги.

Тривалий час аудит безпеки ІС тлумачився як окремий незалежний сервіс, який супроводжувався створенням і впровадженням стандартів аудиторської діяльності у сфері інформаційних технологій. Як правило, це закриті стандарти.

Такий підхід не відповідає одному з головних завдань аудиту, а саме: результати аудиту повинні бути об'єктивними, неупередженими і такими, що можуть бути повторені та відтворені довільним аудитом, найкраще – зовнішнім, який використовуватиме таку ж методику аудиту.

На відміну від закритих стандартів аудиту, існують відкриті стандарти аудиту безпеки ІС, які окреслюють організаційно-правову структуру аудиту ІБ. Відкриті стандарти пов'язують ІТ і дії аудиторів, об'єднують і погоджують багато критеріїв у єдиний ресурс, що дають можливість на сучасному рівні впроваджувати систему менеджменту інформаційною безпекою в ІС, враховують практично всі особливості ІС (на програмно-апаратному рівні) довільного масштабу і складності.

Неможливо обійти увагою новий стандарт ISO/IEC 27035:2011 Інформаційні технології. Методи забезпечення безпеки. Управління інцидентами інформаційної безпеки [10], який надає практичні рекомендації з виявлення, реєстрування та оцінювання випадків порушення інформаційної безпеки в ІС.

Він допоможе реагувати на інциденти ІБ, зокрема, вводити відповідні інструменти контролю для їхнього запобігання та відновлення

у разі реалізування загроз, покращувати загальний підхід до проектування технічних систем ЗІ.

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

Управління інцидентами – це важливий процес, 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 і сервісів, що не виходить за рамки угоди про рівень обслуговування.

Цілі, які ставлять перед СУІІБ, охоплюють:

– 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.

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

Для реалізування системи управління інцидентами інформаційної безпеки потрібно виконати такі роботи:

– надати ресурси для розроблення та впровадження системи СУІІБ;

– здійснити фахову підготовку працівників;

– визначити область функціонування СУІІБ;

– 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 моніторингу подій.

Унаслідок проведених робіт буде запроваджена СУІБ, яка буде розв'язуватиме такі задачі:

– оперативний моніторинг стану ІБ в рамках функціонування ІС;

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

– інформування вищого керівництва про поточний стан ІБ;

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

– аналіз реалізованих інцидентів з метою планування превентивних заходів захисту і покращення процесу забезпечення ІБ загалом.

Для оброблення подій та інцидентів ІБ доцільно організувати процес реагування на інциденти. Основними задачами процесу реагування на інциденти ІБ 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 сталися;

– мінімізування порушень порядку роботи і модифікування даних, відновлення в найкоротші терміни працездатності ІС в разі її порушення через інцидент;

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

– захист активів ІС;

– створення умов для порушення цивільної або кримінальної справи проти зловмисників;

– швидке виявлення та/або попередження подібних інцидентів у подальшому.

Також слід наголосити, що під час експлуатування системи менеджменту інформаційної безпеки процес управління інцидентами є одним із найважливіших у постачанні даних для аналізу функціонування таких систем, оцінювання ефективності використовуваних заходів, зниження ризиків і планування удосконалення роботи ІС.

В Україні тільки перша версія ISO/IEC 27001:2005 частково отримала статус державного стандарту. Питання його практичного застосування залишається актуальним. Стандарт з урахуванням галузевих особливостей є обов'язковим у банківській сфері – СОУ Н НБУ 65.1 СУІБ 1.0: 2010.

Існує правова колізія, відповідно до якої міжнародні стандарти ISO/IEC серії 27000 в Україні не адаптовані, а «Критерії оцінки захищеності інформації комп'ютерних систем від несанкціонованого доступу» 1999 року є застарілими (ІТ та технології ЗІ, на відміну від чинного законодавства, інтенсивно розвивалися), – і вона має тенденцію до загострення за найгіршим сценарієм.

Спробуємо з'ясувати головні причини виникнення такої ситуації. Отже, замовник своїми силами або із залученням підрядників розробляє технічне завдання (ТЗ) на КСЗІ, погоджує його з ДССЗТЗІ, а потім, на підставі ТЗ проектує, реалізовує КСЗІ за допомогою сукупності організаційних, програмно-апаратних та інженерних засобів і вводить у дослідну експлуатацію. Далі, на підставі отриманої заявки ДССЗТЗІ визначає компанію-ліцензіата, що виступає організатором державної експертизи КСЗІ.

Організатор експертизи володіє штатом кваліфікованих експертів, розробляє програму та методику експертних випробувань, проводить їх і подає результати своєї роботи у вигляді проекту експертного висновку на розгляд експертної ради з питань технічного захисту інформації ДССЗТЗІ. У разі позитивного рішення КСЗІ отримує атестат відповідності вимогам системи технічного захисту інформації (ТЗІ).

Сучасній системі проектування КСЗІ притаманні й інші недоліки. Скажімо, для ІС з різною архітектурою, різними вимогами щодо забезпечення ЗІ, що ґрунтуються, зокрема, і на різних категоріях доступу до інформації, існують стандартні функціональні профілі захищеності, тобто деякі фіксовані набори послуг безпеки. Водночас розробник КСЗІ, формуючи ТЗ, самостійно визначає об'єкти захисту, на які ці послуги поширюються. Експерти з ДССЗТЗІ в процесі узгодження ТЗ перевіряють специфікації послуг, однак складно визначити рівень адекватності висунутих вимог до умов функціонування існуючих ІС.

Наступний етап контролю за відповідністю ТЗ створеній КСЗІ – експертиза. Зазвичай експертиза полягає лише у перевірці якості реалізування заявлених послуг безпеки в ІС та комплектність документації на КСЗІ.

Практично ніколи експертами якість впровадженої КСЗІ не перевіряється тестуванням на несанкціонований доступ (НСД) до активів ІС. По-перше, цього не вимагає нормативно-правова база, а по-друге, для проведення таких робіт потрібен високий фаховий рівень експертів [11].

Недостатнє бюджетне фінансування при закупівлі відповідних програмно-технічних засобів захисту накладає додаткові обмеження на технічну складову КСЗІ в ІС підрозділів НП України.

Фахівці можуть розробити та запровадити ідеальний варіант КСЗІ, відповідні служби та експерти виконають усі належні експертизи та заходи з атестування, а відсутність кваліфікованих фахівців зведе нанівець усі попередні зусилля. Тож для забезпечення якісного функціонування КСЗІ керівництву НП необхідно терміново переглянути посадові оклади працівникам служб захисту інформації, аби залучити потрібних фахівців.

У всіх аспектах забезпечення ЗІ основним елементом є аналіз можливих загроз стосовно порушення роботи ІС, тобто загроз, які підвищують уразливість інформації, призводять до її витоку, випадкового або навмисного компрометування, знищення.

Інтегрування системи управління інцидентами інформаційної безпеки у КСЗІ гарантує низку переваг:

– підвищення загального рівня інформаційної безпеки;

– зменшення негативних наслідків реалізування загроз та часу відновлення штатних режимів функціонування ІС;

– посилення акценту на попередження інцидентів інформаційної безпеки;

– призначення пріоритетів і збору даних;

– внесок в обґрунтування рішень щодо формування бюджету та ресурсів;

– надання додаткової інформації для розроблення політики інформаційної безпеки та супровідної документації.

Розглядаючи загальні принципи ЗІ в ІС, доцільно наголосити, що комплексний ЗІ в ІС має у своїй основі використання організаційних і програмно-апаратних засобів ЗІ. Такі засоби повинні забезпечувати ідентифікування та автентифікування користувачів, розподіл повноважень доступу до активів ІС, реєстрування та облік спроб НСД [12].

**Висновки.** 1. На підставі проведеного аналізу автори вважають, що сучасна нормативно-правова база, яка, поза всім, не встановлює вимог до розроблення політики інформаційної безпеки та оцінювання ризиків в ІС, має бути істотно доповненою. Для цього потрібно: або

адаптувати стандарти ISO/IEC серії 27000, що унеможливить легальну участь у державному чи приватному сертифікуванні систем ТЗІ, або – розробити власні, якісно нові стандарти безпеки для державних силових структур.

2. Міжнародні стандарти ISO/IEC серії 27000, на відміну від нормативних документів в Україні, об'єктом захисту передбачають процес оброблення, доступу та збереження інформації, а не КСЗІ.

1. Олійник О. В. Нормативно-правове забезпечення інформаційної безпеки в Україні / О. В. Олійник // Право і суспільство. – 2012. – № 3. – С. 132–137 [Електронний ресурс]. – Режим доступу: http://nbuv.gov.ua/UJRN/Pis_2012_3_30.

2. Karpinski M. Information Security / M. Karpinski. – Warsawa: Measurements, Automation and Monitoring. – 2012. – 280 p.

3. Цимбалюк В. С. Інституціоналізація інформаційної безпеки в інформаційному праві України / В. С. Цимбалюк // Бюлетень Мін'юсту України. – 2007. – № 8. – С. 45–53.

4. Тарасенко Р. Б. Інформаційне право: навч.-метод. посібник / Р. Б. Тарасенко; МВС України, Луган. держ. ун-т внутр. справ ім. Е. О. Дідоренка. – Луганськ: РВВ ЛДУВС ім. Е. О. Дідоренка, 2010. – 512 с.

5. Міжнародний стандарт ISO/IEC 27001 [Електронний ресурс]. – Режим доступу: http://www.iso.org

6. Міжнародний стандарт ISO/IEC 27002 [Електронний ресурс]. – Режим доступу: http://www.iso.org

7. Міжнародний стандарт ISO/IEC 27003-27004 [Електронний ресурс]. – Режим доступу: http://www.iso.org

8. Міжнародний стандарт ISO/IEC 27005 [Електронний ресурс]. – Режим доступу: http://www.iso.org

9. Міжнародний стандарт ISO/IEC 27006 [Електронний ресурс]. – Режим доступу: http://www.iso.org

10. Міжнародний стандарт ISO/IEC 27035 [Електронний ресурс]. – Режим доступу: http://www.iso.org

11. 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 конференції факультету кримінальної міліції Львівського державного університету внутрішніх справ (м. Львів, 12 березня 2010 р.). – Львів: ЛьвДУВС, 2010. – С. 90–97.

12. Рудий Т. В. Політика інформаційної безпеки в інформаційних системах спеціального призначення / Т. В. Рудий, О. В. Захарова, А. Т. Рудий // Проблеми застосування інформаційних технологій, спеціальних технічних засобів у діяльності ОВС та в навчальному процесі: збірник наукових статей за матеріалами доповідей науково-практичної конференції (м. Львів, 27 грудня 2013 року). – Львів: ЛьвДУВС, 2014. – С. 21–26.

**Рудый Т. В., Захарова А. В., Сеник В. В., Сеник С. В., Изьо М. И. Организационно-правовое сопровождение защиты информационных систем подразделений Национальной полиции Украины на основании международных стандартов**

*Определены проблемы защиты информации, которые не могут быть развязаны без создания новых законодательных актов и внедрения новой политики в сфере информатизации, то есть проанализированы информационные отношения с точки зрения объекта правового регулирования. Разъяснена и аргументирована необходимость разработки организационно-правовых принципов, определяющих стратегию, тактику системы защиты информационных систем подразделений Национальной полиции Украины с учётом динамики изменения угроз информационным активам на основании положений международных стандартов ISO/IEC серии 27000.*

**Ключевые слова:** *информационная система, защита информации, информационные угрозы, нормативно-правовые факторы, международные стандарты.*

**Rudyy T. V., Zakharova O. V., Senyk V. V., Senyk S. V., Izyo M. I. Organizational support legal defense information systems Ukraine units National police based on international standards**

*Definite problem of information security that can not be resolved without the introduction of new legislation and new policy in the field of information, that analyzes information relations from the point sight of the object of legal regulation.*

*Considered and reasonably treatment institutional and legal framework that determine strategy, tactics of system to protect information systems divisions of the National Police of Ukraine taking into account the dynamics of the threats to information assets on the basis of international standards ISO / IEC 27000 series.*

*Commitment to standards ISO / IEC 27000 series provides control and monitoring of access, development and maintenance of hardware and software systems, continuity management information processes. Compliance with standards ISO / IEC 27000 series and compliance with the nation-tional legal standards in information security is the key to creating an effective information security system state information assets. In all aspects of information security basic element is the analysis of possible threats of violation of information system, threats that increase the vulnerability of information assets, resulting in leakage of unauthorized, accidental or compromising deliberate, destruction. Considering the general principles of the protection of information in information systems is worth noting that a comprehensive data protection in information systems is based on the use of institutional and legal software and hardware. Such facilities should secure of identification and authenticity users distribution commission admission assets to information systems, recording and accounting of access attempts. International standards ISO / IEC 27000 series as opposed to the regulations in Ukraine subject protection process involving handling, access and preservation of government information assets, rather than a comprehensive system of protection of state information assets.*

**Key words:** *information system, information security, information threats, regulatory factors, international standards.*

*Стаття надійшла 3 березня 2017 р.*