УДК 004.681.003

ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОБ'ЄКТА

Юлія Хохлачова
Національний Авіаційний Університет

Анотація: **Розроблено зразковий алгоритм роботи по оцінці інформаційних ризиків; приведено основні правила забезпечення політики безпеки в інформаційній системі; поетапно розглянуто процес аналізу ризиків; проаналізовано ймовірні загрози для інформаційних мереж, які необхідно враховувати при розробці політики інформаційної безпеки; розглянуто підходи, під впливом яких формується стратегія відповідних дій, коли на об'єкт відбувається напад, що загрожує порушенням інформаційної безпеки. Перераховані та розглянуті усі можливі критерії, згідно з якими має доповнюватися і змінюватися політика інформаційної безпеки об'єкта.**
Sammary: **A model algorithm to assess the risk of information, given the basic rules of security policy in the information system; stages describes how risk analysis analyzes the likely threats to information networks that must be considered when developing information security policy; approaches, under whose influence shaped the strategy appropriate action when the object is an attack that threatens a violation of information security. These and considered all possible criteria according to which must be complemented and change policy information security object.**
Ключові слова: **Інформаційна безпека, політика інформаційної безпеки, захист інформації, інформаційна система.**

I Вступ

Інформаційні технології все більш наполегливо проникають в усі сфери людської діяльності, вірніше, людство все більш сміливо інтегрується з інформаційними технологіями. І коли інформація стає провідником у світ людей, коли залежність людської цивілізації від інформаційних потоків (а отже і технологій, що їх обслуговують) не ставиться під сумнів, на перших ролях з'являється інформаційна безпека (ІБ).

Проте сама по собі ПІБ є достатньо абстрактним поняттям. Має бути деякий додаток до ПІБ, тобто необхідні систематизація і правила, що дозволяють зробити технології ПІБ застосовними до реального середовища, де і мусить бути забезпечена безпека інформаційного простору. Наразі й виникає поняття політики ІБ (ПІБ).

Таким чином, розробка ПІБ – процес дуже важливий і суто практичного характеру, що безпосередньо застосовує знання і методи абсолютно всіх розділів інформаційної безпеки в конкретній ситуації. Метою є створення каркасу інформаційної безпеки, тобто конкретних правил і рекомендацій, що регламентують функціонування всіх рівнів ІБ.

Розробка ПІБ – це питання не тривіальне. Від ретельності її опрацювання залежатиме дієвість решти всіх рівнів забезпечення ПІБ – процедурного і програмно-технічного. Складність розробки ПІБ визначається проблематичністю використання чужого досвіду, оскільки ПІБ ґрунтується на виробничих ресурсах і функціональних залежностях усередині об'єкта [1].

Необхідність розробки ПІБ пояснюється необхідністю формування основ планування і управління ПІБ. Мета розробки ПІБ – мінімізація ризиків бізнесу шляхом захисту інтересів об'єктів в інформаційній сфері, планування і підтримка безперервності функціонування, зниження витрат і підвищення ефективності інвестицій в захист інформації.

ПІБ містить вимоги до персоналу та технічних служб. Основні напрями розробки ПІБ [1]:

- визначення, які данні і наскільки серйозно необхідно захищати;
- визначення, хто і який збиток може завдати об'єкту в інформаційному аспекті;
- оцінки ризиків і визначення схеми зменшення їх до прийнятної величини.

II Основна частина

Метою розробки офіційної ПІБ конкретного об'єкта в області інформаційної безпеки є визначення правильного способу використання обчислювальних і комунікаційних ресурсів, а також розробка процедур, що запобігають чи реагують на порушення режиму безпеки. Для досягнення цієї мети варто відштовхуватися від стандартних канонів розробки ПІБ, але й, звичайно ж, враховувати специфіку конкретного об'єкта [2].

По-перше, необхідно прийняти до уваги цілі й основні напрямки діяльності об'єкта (на різних об'єктах установлюються різні вимоги до конфіденційності).

По-друге, політика, яка розробляється, має узгоджуватися з існуючими законами, ДСТУ, НД ТЗІ і внутрішньооб'єктовими правилами (бо, найчастіше, локальна мережа об'єкта не є ізольованою, а має вихід у Internet). ПІБ має висвітлювати проблеми, що виникають на локальному комп'ютері через дії віддаленої сторони, а також віддалені проблеми, причиною яких є користувач або зловмисник.

Сукупність керівних принципів, правил, процедур фактичних прийомів, якими об'єкт керується в своїй діяльності складає ПІБ об'єкта.

Сукупність правил, які регулюють керування ресурсами, їх захист та розподіл всередині об'єкту захисту, та які виражаються за допомогою функціональних вимог безпеки, складає політику безпеки об'єкту.

ПІБ повинна стати результатом спільної діяльності технічних фахівців на об'єкті захисту, здатних реалізувати її початкові технічні аспекти, і керівників, зацікавлених в коректній побудові політики з фінансової, законодавчої та технічної сторони, а також персоналу, що зараз та в майбутньому буде стикатися з нормами ПІБ об'єкта та їх дотримуватися.

ПІБ потенційно впливає на роботу всіх користувачів комп'ютерів на об'єкті, причому в декількох аспектах. Якщо ж такий документ (ПІБ об'єкта) передбачається розробляти і втілювати в життя не власними силами, а за допомогою фахівців ззовні, то потрібно, щоб були враховані наступні п'ять критеріїв оцінки політики [1, 2]:

- чи узгоджується ПІБ з існуючим законодавством і обов'язками відносно третіх сторін?
- чи не обмежуються без потреби інтереси працівників, роботодавців чи третіх сторін?
- чи реалістична політика й чи ймовірне її втілення в життя?
- чи зачіпає політика всі види передачі і збереження інформації, які використовуються в об'єкті?
- чи оголошена політика заздалегідь і чи одержала вона схвалення всіх зацікавлених сторін?

Один із головних спонукальних мотивів розробки ПІБ об'єкта полягає в одержанні впевненості, що діяльність з захисту інформації побудована економічно і технічно виправданим способом. Дане положення здається очевидним, але, взагалі, можливі ситуації, коли зусилля прикладаються не там, де потрібно. Наприклад, основною задачею систем захисту інформації припускають захист від зовнішнього зловмисника, а напади в більшості випадків створюються внутрішніми порушеннями.

Політика звичайно складається з двох частин [3]: загальних принципів і конкретних правил роботи.

Загальні принципи визначають підхід до безпеки в Internet, правила регламентують – що дозволено і що заборонено (правила можуть доповнюватися конкретними процедурами і посібниками).

Звичайна політика безпеки регламентує використання основних сервісів мережі і доводить до відома користувачів мережі їхні права доступу, що і є процедурою автентифікації користувачів.

До ПІБ об'єкта, як до регламентуючого документу, варто відноситися серйозно, бо всі інші стратегії захисту будуються на припущенні, що правила політики безпеки неухильно дотримуються.

Інформаційну систему об'єкта захисту можна вважати захищеною, якщо всі операції виконуються згідно зі строго визначеними правилами (рис. 1), що забезпечують безпосередній захист об'єктів, ресурсів і операцій.

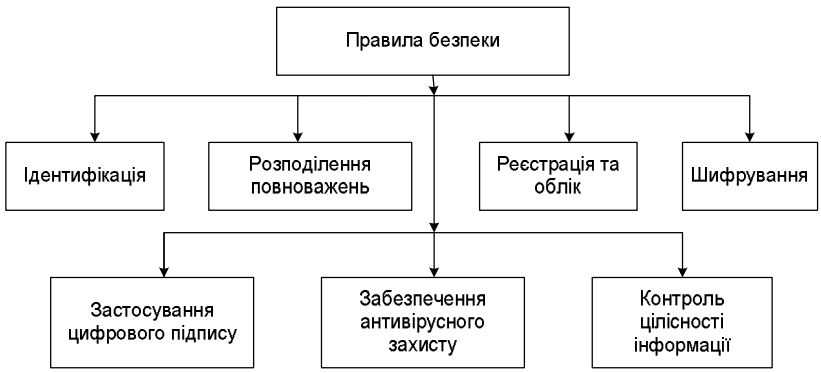

Рисунок 1 – Основні правила забезпечення політики безпеки в інформаційній системі

Основу для формування вимог до захисту складає список загроз. Коли такі вимоги відомі, можуть бути визначені відповідні правила забезпечення захисту, що визначають необхідні функції і засоби захисту. Чим суворіші вимоги до захисту і більше відповідних правил, тим ефективніші її механізми і тим більше захищеною виявляється інформаційна система.

Таким чином, визначаємо, що захист інформації на інформаційному об'єкті – комп'ютерній мережі, буде ефективним, коли проектування та реалізація системи захисту інформаційного об'єкта відбувається згідно з наступними етапами [1]:

1) аналіз ризиків;
2) реалізація політики безпеки;
3) підтримка політики безпеки.

Процес аналізу інформаційних ризиків містить в собі визначення того, що варто захищати, від чого захищати і як це робити. Необхідно розглянути всі можливі ризики і ранжувати їх залежно від потенційного розміру збитку. Цей процес складається з безлічі економічних рішень. Давно визначено, що витрати на захист не повинні перевищувати вартості інформації, що захищається (об'єкта інформації).

Процес аналізу ризиків розділимо на два етапи [3]: ідентифікація активів та ідентифікація загроз. Розглянемо докладніше ці етапи.

1. Ідентифікація активів. Це один з етапів аналізу ризиків. Він складається з ідентифікації всіх об'єктів, що потребують захисту. Необхідно прийняти до уваги все, що може постраждати від порушення режиму безпеки. Тому необхідно спочатку класифікувати активи:

- апаратура: процесори, модулі, клавіатури, термінали, робочі станції, персональні комп'ютери, принтери, дисководи, мережі зв'язку, термінальні сервери, маршрутизатори;
- програмне забезпечення, вихідні тексти, об'єктні модулі, утиліти, діагностичні та комунікаційні програми, операційні системи;
- дані (інформація) безпосередньо доступні, архівовані, оброблювані, збережені у вигляді резервної копії, реєстраційні журнали, бази даних, що передаються комунікаційними мережами;
- люди: користувачі, обслуговуючий персонал;
- документація: програмна, апаратурна, системна, з адміністративних процедур;
- випадкові матеріали: папір, форми, фарбуючи стрічки, магнітні носії.

2. Ідентифікація загроз. Після того, як були виявлені активи, що потребують захисту, необхідно ідентифікувати загрози цим активам і розміри можливого збитку та втрат. Це допоможе зрозуміти, яких загроз ватро побоюватися більше всього.

Типова загроза для більшості об'єктів інформаційного захисту – несанкціонований доступ до інформації на об'єкті, що захищається – може приймати різні форми. Ступінь важливості проблеми несанкціонованого доступу для різних об'єктів різна.

Несанкціоноване (нелегальне) ознайомлення з інформацією – друга поширена загроза. Дуже важливо правильно визначити ступінь конфіденційності інформації, що зберігається в інформаційних системах об'єкта.

Відмовлення в обслуговуванні порушують цілісність системи, виникають з різних причин, і виявляються по-різному. Мережа може прийти в непрацездатний стан від підробленого пакета, від перевантаження чи через відмовлення компонента. Вірус здатний сповільнити чи паралізувати роботу інформаційної системи.

При розробці ПІБ необхідно дати відповіді на декілька питань:

- хто має право використовувати ресурси?
- як правильно використовувати ресурси?
- хто наділений правом давати привілеї і дозволяти використання?
- хто може мати адміністративні привілеї?
- які права й обов'язки користувачів?
- які права й обов'язки системних адміністраторів стосовно звичайних користувачів?
- як працювати з конфіденційною інформацією?

Власне, організаційна ПІБ описує порядок надання і використання прав доступу користувачів, а також вимоги звітності користувачів за свої дії в питаннях безпеки.

Для інформаційних мереж можна виділити наступні ймовірні загрози, які необхідно враховувати при визначенні ПІБ: випадкові та навмисно створювані загрози.

Розглянемо послідовно ці загрози.

До випадкових загроз можна віднести:

- помилки обслуговуючого персоналу та користувачів;
- втрата чи руйнування інформації, обумовлена неправильним збереженням архівних даних на магнітних носіях;
- випадкове знищення чи зміна даних;
- збої устаткування електроживлення;
- збої кабельної системи;
- перебої в електроживленні;

- збої апаратури запису та зйому інформації;
- збої системи архівування даних;
- збої роботи серверів, робочих станцій, мережевих карт і т. п.;
- руйнування файлових структур через некоректну роботу чи програми апаратних засобів;
- зміна даних при помилках у програмному забезпеченні;
- зараження системи вірусами;
- несанкціонований доступ;
- випадкове ознайомлення з конфіденційною інформацією сторонніх осіб.

До випадкових (ненавмисних) загроз мають відношення також випадки руйнації, втрати або зміни даних, конфіденційної інформації або ресурсів під час природних катаклізмів, які не підвладні людині (пожари, землетруси, повені, магнітні бурі, падіння метеоритів та радіоактивні випромінювання).

До навмисно створених загроз слід відносити такі:

- ознайомлення працівників з інформацією, до якої вони не повинні мати доступу;
- несанкціонований доступ сторонніх осіб, що не належать до числа працівників, до конфіденційної інформації і мережевих ресурсів;
- розкриття і модифікація інформації і програм;
- копіювання інформації і програм;
- розкриття чи модифікація або підміна трафіку передачі інформації мережею;
- розробка і поширення комп'ютерних вірусів;
- введення в програмне забезпечення логічних бомб;
- крадіжка магнітних та паперових носіїв, що містять конфіденційну інформацію;
- крадіжка розрахункових документів;
- крадіжка устаткування та апаратури;
- руйнування архівної інформації або навмисне її знищення;
- фальсифікація повідомлень, переданих каналами зв'язку;
- відмовлення від авторства повідомлення, переданого каналами зв'язку;
- відмовлення від факту одержання інформації;
- нав'язування раніше переданого повідомлення;
- перехоплення й ознайомлення з інформацією, передана по каналами зв'язку і т. п.

Головною метою діяльності в області інформаційної безпеки є забезпечення властивостей кожного активу:

- доступності (можливість користування деякими ресурсами інформаційної системи й інформацією в довільний момент);
- конфіденційності (недоступність інформації чи сервісів для користувачів, яким апріорно не надана можливість використання зазначених сервісів або інформації);
- цілісності (незалежність властивостей інформації і ресурсів у будь-який момент часу від моменту їх появи чи введення в систему);
- вірогідності (збереження інформацією своїх семантичних властивостей у будь-який момент часу від моменту введення в систему).

При аналізі загроз варто брати до уваги їхній вплив на активи згідно з чотирма названими напрямками.

На підставі вище зазначеного розроблено зразковий алгоритм роботи з оцінки інформаційних ризиків (рис. 2).

Оцінка ймовірності появи вище перерахованих ймовірних загроз і очікування розмірів втрат – складний і тривалий процес, але коректно визначити вимоги до системи захисту об'єкта ще складніше, тому ПІБ має визначатися наступними мірами:

- ідентифікація користувачів;
- перевірка дійсності та контроль доступу користувачів до об'єкту, що захищається, у приміщення, до ресурсів інформаційної системи;
- поділ повноважень користувачів, що мають доступ до обчислювальних ресурсів;
- реєстрація та облік роботи користувачів;
- реєстрація спроб порушення повноважень;
- шифрування або кодування конфіденційної інформації на основі криптографічних алгоритмів високої стійкості;
- застосування цифрового підпису для передачі інформації каналами зв'язку;
- забезпечення антивірусного захисту та відновлення інформації, зруйнованої вірусними впливами;
- контроль цілісності програмних засобів та інформації, що обробляється;
- відновлення зруйнованої архівної інформації, навіть при значних втратах;

- наявність адміністратора захисту інформації в системі;
- розробка та дотримання необхідних організаційних мір;
- застосування технічних засобів, що забезпечують безперебійну роботу устаткування.

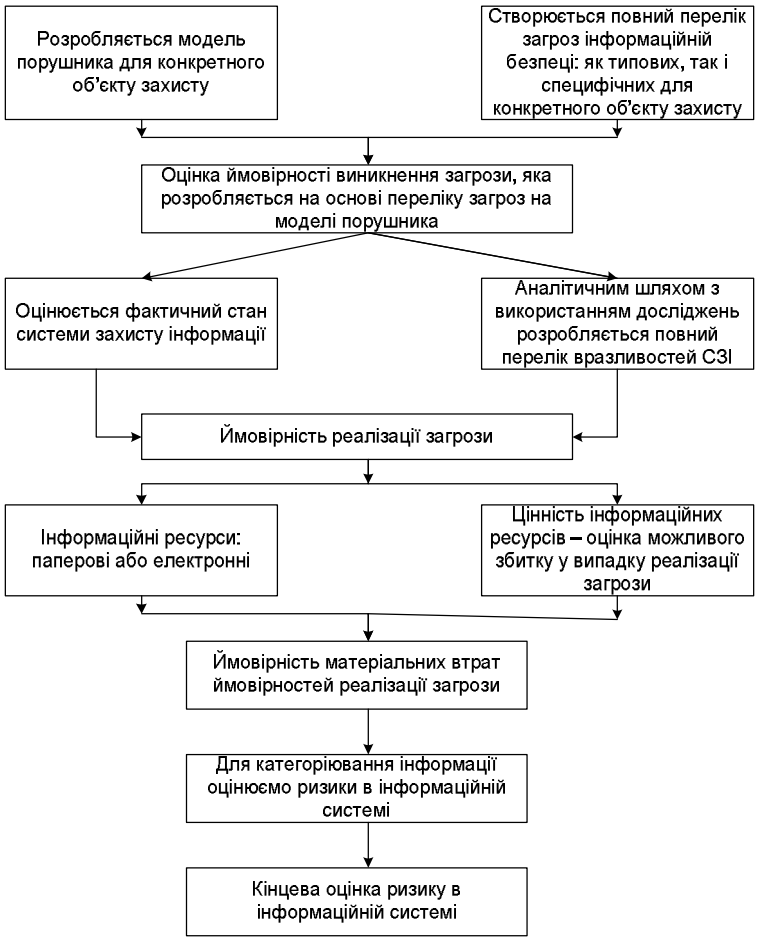

Рисунок 2 – Алгоритм роботи з оцінки ризиків в інформаційній системі

Реалізація ПІБ об'єкта починається з проведення розрахунку фінансових втрат і вибору відповідних засобів для виконання цих задач. При цьому необхідно врахувати такі фактори як безконфліктність роботи обраних засобів, репутація постачальників засобів захисту, можливість одержання повної інформації про механізми захисту і надані гарантії. Також варто враховувати основні положення з безпеки інформації:

- економічна ефективність – вартість засобів захисту має бути меншою, ніж розміри можливого збитку;
- кожен користувач повинний мати мінімальний набір привілеїв, необхідний при роботі;
- простота системи захисту об'єкта – захист буде тим ефективніший, чим легше користувачу з ним працювати;
- відключення захисту при нормальному функціонуванні – захист не повинен відключатися, за винятком особливих випадків, коли співробітник із спеціальними повноваженнями може мати можливість відключити систему захисту;
- відкритість проектування і функціонування механізму захисту (для можливості адекватного реагування обслуговуючого персоналу на виникнення збоїв у системі);
- незалежність системи захисту від суб'єктів захисту – розроблювачами не повинні бути ті, кого вона буде контролювати;
- загальний контроль без будь-яких виключень з безлічі контрольованих суб'єктів;
- звітність і підконтрольність системи захисту;
- відповідальність осіб, що займаються інформаційною безпекою;
- об'єкти захисту доцільно розділити на групи так, щоб порушення захисту в одній групі не впливало на безпеку інших груп;

- відмова від замовчування – при збої засобів захисту доступ до обчислювальних ресурсів повинен бути заборонений;
- система захисту об'єкту має бути цілком специфікована, протестована та погоджена;
- система повинна допускати зміну своїх параметрів адміністратором;
- важливі критичні рішення повинні прийматися людиною, а не комп'ютером;
- система захисту об'єкта повинна проектуватися в розрахунку на вороже оточення і припускати, що користувачі мають найгірші наміри, будуть робити помилки і шукати шляхи обходу механізмів захисту;
- інформація про існування механізмів захисту повинна бути, по можливості, схована від користувачів, робота яких контролюється.

При підтримці ПІБ потрібно постійне спостереження за вторгненнями зловмисників у мережу, виявлення вад і "дір" у системі захисту об'єкта інформації, обліку випадків несанкціонованого доступу до конфіденційних даних.

При цьому основна відповідальність за підтримку ПІБ мережі (об'єкта інформації) лежить на системному адміністраторі, що повинен оперативно реагувати на всі випадки зламу конкретної системи захисту, аналізувати їх і використовувати необхідні апаратні та програмні засоби захисту з урахуванням максимальної економії фінансових засобів.

Очевидно, що будь-яка офіційна політика поза залежністю від її відношення до інформаційної безпеки, час від часу порушується. Порушення може бути наслідком недбалості користувачів, випадкової помилки, відсутності надійної та належної інформації про поточну політику чи її нерозуміння. Можливо, також, що деяка особа – група осіб свідомо роблять дії, що прямо суперечать затвердженій політиці безпеки.

Необхідно заздалегідь визначити характер дій, що починаються у випадку виявлення порушень ПІБ, щоб ці дії були швидкими й правильними. Варто організувати розслідування, щоб зрозуміти, як і чому порушення стало можливим. Після цього потрібно внести корективи в систему захисту. Тип і серйозність коректив залежить від типу порушення, яке сталося.

Політику безпеки можуть порушувати різні особи. Деякі з них є своїми, місцевими користувачами, інші – здійснюють напади ззовні. Корисно визначити самі поняття "свої" і "чужі," виходячи з адміністративних, правових чи політичних положень. Ці положення окреслюють характер санкцій, які можна застосувати до порушника – від письмової догани до притягнення до суду. Таким чином, послідовність відповідних дій залежить не тільки від типу порушення, але й від виду порушника; вона повинна бути продумана задовго до першого інциденту, хоча це і непросто.

Варто пам'ятати, що правильно організоване навчання – кращий захист. Керівництво об'єкта, що захищає свою конфіденційну інформацію, зобов'язано поставити справу так, щоб не тільки внутрішні, але і зовнішні легальні користувачі знали положення ПІБ об'єкта.

Проблеми з нелегальними користувачами, загалом, ті ж самі. Потрібно одержати відповіді на питання про те, як типи користувачів порушують політику, як і навіщо вони це роблять. Залежно від результатів розслідування можна просто закрити "діру" в системі захисту та задовольнитися отриманим уроком чи застосувати жорсткіші міри.

Кожний об'єкт повинен заздалегідь визначити набір адміністративних санкцій, застосованих до місцевих користувачів, які порушують ПІБ сторонньої організації чи об'єкта. Крім того, необхідно подбати про захист від відповідних дій сторонньої організації. При розробці ПІБ варто враховувати всі юридичні положення, які застосовуються до подібних ситуацій.

Політика безпеки об'єкта повинна мати процедури для взаємодії з зовнішніми організаціями, в число яких входять правоохоронні органи, інші організації, команди "швидкого реагування", засоби масової інформації. У процедурах повинно бути визначено, хто має право на такі контакти, і як саме вони відбуваються.

Крім політичних положень, необхідно продумати й описати процедури, що виконуються у випадку виявлення порушень режиму безпеки. Для всіх видів порушень мають бути заготовлені відповідні процедури.

Коли на об'єкт відбувається напад, що загрожує порушенням інформаційної безпеки, стратегія відповідних дій може будуватися під впливом двох протилежних підходів.

1. Якщо керівництво побоюється вразливості об'єкта, воно може віддати перевагу стратегії "захиститися і продовжити". Головною метою подібного підходу є захист інформаційних ресурсів і максимально швидке відновлення нормальної роботи користувачів. Діям порушника виявляється максимальна протидія, подальший доступ забороняється, після чого негайно починається процес оцінки нанесених ушкоджень і відновлення інформації. Можливо, доведеться виключити комп'ютерну систему, закрити доступ до мережі чи почати інші жорсткі міри. Зворотній бік даної моделі полягає в тому, що поки зловмисник невиявлений, він може знову напасти на ту ж саму чи іншу організацію колишнім чи новим способом.

2. Інший підхід, "вистежити і засудити", спирається на інші філософію та систему цілей. Основна мета полягає в тому, щоб дозволити зловмиснику продовжувати свої дії, доки об'єкт не зможе встановити його особистість. Такий підхід подобається правоохоронним органам. Нажаль, ці органи не зможуть звільнити об'єкт від відповідальності, якщо користувачі звернуться до суду з позивом із приводу збитку, нанесеного їхнім програмам та інформації.

III Висновки

Політика інформаційної безпеки об'єкта не може бути ідеальною і довговічною, бо з часом усе змінюється: устрій життя та канони в нормативній базі, модернізується устаткування і змінюється обслуговуючий персонал. Отже, політика інформаційної безпеки об'єкта має доповнюватися і змінюватися згідно з усіма перерахованими критеріями змін і цінності інформації, що підлягає захисту.

Література: ***1.*** *Голубенко О. Л. Політика інформаційної безпеки / Голубенко О. Л., Хорошко В. О., Петров О. С., Головань С. М., Яремчук Ю. Є. – Луганськ: Вид. СНУ ім. В. Даля, 2009. – 300 с.* ***2.*** *Ленков С. В. Методы и средства защиты информации. В 2-х томах / Ленков С. В., Перегудов Д. А., Хорошко В. А. – К.: Арий, 2008.* ***3.*** *Соколов А. В. Защита от комп'ютерного терроризма / Соколов А. В., Степанюк О. М. – СПб: БХВ-Петербург, Арлей, 2002. – 496 с.*

УДК 343.9.02.005.334 (477)

ОЦІНЮВАННЯ РИЗИКІВ ТА ЗАГРОЗ ЗЛОЧИННОСТІ У ЗАБЕЗПЕЧЕННІ КРИМІНОЛОГІЧНОЇ БЕЗПЕКИ

Дарія Прокоф'єва-Янчиленко
Служба безпеки України

Анотація: **Стаття присвячена проблемам та перспективам застосування методології ризик-менеджменту у забезпеченні кримінологічної безпеки.**
Summary: **The article is devoted to the problem & perspectives of using risk-management methodology for criminology security guarantee.**
Ключові слова: **Кримінологічна безпека, злочинність, причинність, управління ризиками, оцінювання ризиків.**

I Вступ

Набуття злочинністю в сучасному світі статусу однієї з найбільш істотних загроз національній безпеці на загальнодержавному та міжнародному рівні вимагає нових підходів у дослідженні злочинності та її конкретизованих проявів, а також нових стратегій протидії зазначеним негативним явищам. Враховуючи, що суспільство фактично існує в умовах ризику злочинності, видається перспективним застосування до оцінки та прогнозування динаміки злочинності методології ризик-менеджменту та превентивного управління системою кримінологічної безпеки, що базується на інформаційному характері детермінації.

II Результати досліджень

Загрози безпеці та стабільності в регіоні ОБСЄ найбільш вірогідні сьогодні у формі негативних, дестабілізуючих наслідків подій, які зачіпають одночасно військово-політичний, економічний, екологічний та людській вимір, радше ніж у формі глобального військового конфлікту. Одним з найбільш суттєвих джерел загроз при цьому є дії терористів та інших злочинних угруповань, які передусім не є проблемою якоїсь однієї конкретної держави, а мають транснаціональний характер.

Глобалізація та науково-технічні досягнення розширюють рамки та збільшують масштаб загрози, що виходить від організованої злочинності. Контрабанда, торгівля людьми, нелегальна міграція, незаконний обіг наркотиків та зброї, а також товарів подвійного призначення та новітніх технологій, корупція – все це злочинна діяльність, здатна порушити стабільність та безпеку як в регіоні ОБСЄ, так і за його межами, а також створити поживне середовище для інших істотних загроз. Отже, підвищеного значення для стабільності та сталого розвитку суспільства набуває «безпека від злочинності», тобто, кримінологічна безпека.

Кримінологічна безпека, як інтегральна складова національної безпеки, являє собою об'єктивний стан захищеності життєво важливих інтересів особи, держави, суспільства та навколишнього природного середовища від кримінальних внутрішніх і зовнішніх загроз засобами кримінологічної профілактики,