воздействий (угроз), что подтверждает формулировку понятия живучести [1]. В дальнейшем, при моделировании структуры СЗИ, предполагается оценить эффективность предложенной методики с учётом методики оценки надёжности СЗИ [7, 10, 11].

Список литературы

1. Горицкий В.М., Павлов И.Н. Формализация понятия живучести систем защиты информации. // Зб. наук. праць. "Спеціальні телекоммунікаційні системи та захист інформації". – К.: 2005. – № 2. – С. 36 – 48
2. Каган Б.М. Электронные вычислительные машины и системы. // – М.: Энергоиздат. – 1985. – 552 с.
3. Додонов А.Г., Горбачик Е.С., Кузнєцова М.Г. О функциональной живучести вычислительных систем. // Таг.Р.: ТРТИ. – 1988. – Вып. 10. С. 64 – 68.
4. Крапивин В.Ф. О теории живучести сложных систем. // – М.: Сов. радио. – 1978. – 235 с.
5. Горбачик Е.С. Подход к количественной оценке живучести вычислительных систем. // – «Теоретические основы живучести информационно-вычислительных и управляющих систем». Материалы. II Всесоюзной. научно-техн. конф. – М.: 1988. – Вип. 1. – С. 205.
6. Кузьмин И.В. Оценка эффективности и оптимизация автоматических систем контроля и управления. // – М.:1972. – 365 с.
7. Горицкий В.М., Павлов И.Н. Оценка вероятности безотказной работы комплексных систем защиты информации. // Зв'язок. – К.: 2005. – № 4. –С. 49 – 54.
8. Ефимов А.И., Пальчун Б.П., Ухлинов Л.М. Методика построения тестов проверки технологической безопасности инструментальных средств автоматизации программирования на основе их функциональных диаграмм // Вопросы защиты информации. – М.: 1995. – №3(30). – С.52 – 54.
9. Гарбарчук В., Минович З., Свиц А., Кибернетический подход к проектированию систем защиты информации. // – К.: 2003. 657 с.
10. Романов О.І., Лівенцев С.П., Павлов І.М. Методика оцінювання надійності комплексних систем захисту інформації в спеціальних телекомунікаційних системах // Зв'язок. – К.: 2005. – № 2. – С. 36 – 38.
11. Павлов И.Н. Методика аналізу надійності комплексних систем захисту інформації в автоматизованих системах. // Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні. – К.: 2005. – Вип. 10. – С. 117 — 121.

Поступила 25.05.2005

УДК 681.003

Е.Т. Дряшкаба

ПРОЕКТУВАННЯ ТА РОЗРОБКА ПОЛІТИКИ БЕЗПЕКИ ОБ'ЄКТІВ

Метою розробки офіційної політики конкретного підприємства в області інформаційної безпеки є визначення правильного (з погляду даної організації) 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 Політики безпеки, але й, звичайно ж, враховувати специфіку конкретного підприємства (об'єкта).

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, повинна узгоджуватися з існуючими ДСТУ, законами і внутрішньооб'єктовими правилами (тому що, найчастіше, локальна мережа

об'єкта не є ізольованою, а має вихід у Internet). Політика безпеки повинна висвітлювати проблеми, що виникають на локальному комп'ютері через дії віддаленої сторони, а також віддалені проблеми, причиною яких є локальний хост чи користувач.

Сукупність керівних принципів, правил, процедурі фактичних прийомів, якими організація керується в своїй діяльності складає політику безпеки організації.

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

Політика безпеки повинна стати результатом спільної діяльності технічних фахівців в області захисту, здатних реалізувати її початкові технічні аспекти, і керівників, зацікавлених в коректній побудові політики з фінансової, законодавчої та технічної сторін, а також персоналу, що в майбутньому буде стикатися з нормами Політики безпеки об'єкта та їх дотримувати.

Політика безпеки потенційно впливає на роботу всіх користувачів комп'ютерів в організації, причому по декількох аспектах. Якщо ж такий документ (Політика безпеки об'єкта) передбачається розробляти і втілювати в життя не власними силами, а фахівцями ззовні, то потрібно, щоб були враховані наступні п'ять критеріїв оцінки подібної політики:

- Чи узгоджується політика з існуючим законодавством і з обов'язками по відношенню до 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 усі види передачі і збереження інформації, які використовуються в організації?

- Чи оголошена політика заздалегідь і чи одержала вона схвалення всіх зацікавлених сторін?

Одним з головних спонукальних мотивів розробки політики безпеки об'єкта полягає в одержанні впевненості, що діяльність по захисту інформації побудована економічно і технічно виправданим образом. Дане положення здається очевидним, але, взагалі, можливі ситуації, коли зусилля прикладаються не там, де потрібно. Наприклад, основною задачею системи захисту інформації припускають захист від зовнішнього зловмисника, а напади в більшості випадків походять від внутрішніх порушників.

Політика звичайно складається з двох частин: 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). Звичайно політика безпеки регламентує використання основних сервісів мережі (різні сайти, електронну пошту і т.д.) і доводить до відома користувачів мережі про їхні права доступу, що і є процедурою автентифікації користувачів.

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

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

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 ефективніше її механізми і тим більше захищеною виявляється інформаційна система.

Таким чином, випливає, що захист інформації в інформаційному об'єкті – комп'ютерній мережі, буде ефективною в тому випадку, коли проектування та реалізація системи захисту інформаційного об'єкта відбувається по наступних етапах: 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 в залежності від потенційного розміру збитку. Цей процес складається з безлічі економічних рішень. Давно замічено, що витрати на захист не повинні перевищувати вартості захищаємої інформації (об'єкта інформації).

Рис. 1. Основні правила забезпечення політики безпеки в інформаційній системі.

Розділимо процес аналізу ризиків на два етапи :

-<u>ідентифікація активів:</u> Один з етапів аналізу ризиків складається з ідентифікації всіх об'єктів, що потребують захисту. Необхідно прийняти до уваги все, що може постраждати від порушень режиму безпеки. Можна спочатку класифікувати активи:

Апаратура: процесори, модулі, клавіатури, термінали, робочі станції, персональні комп'ютери, принтери, дисководи, комунікаційні лінії, термінальні сервери, маршрутизатори.

Програмне забезпечення: вихідні тексти, об'єктні модулі, утиліти, діагностичні та комунікаційні програми, операційні системи.

Дані: безпосередньо доступні, архівовані, оброблювані, збережені у вигляді резервної копії, реєстраційні журнали, бази даних, що передаються по комунікаційних лініях.

Люди: користувачі, обслуговуючий персонал.

Документація: по програмах, по апаратурі, системна, по адміністративних процедурах.

Видаткові матеріали: папір, форми, фарбуюча стрічка, м[illegible]ітні носії.

-<u>ідентифікація загроз:</u> Після того, як були виявлені активи, що потребують захисту, необхідно ідентифікувати загрози цим активам і розміри можливого збитку. Це допоможе зрозуміти, яких загроз варто побоюватися більше всього.

Типова загроза для більшості об'єктів інформаційного захисту – це несанкціонований доступ до комп'ютерних ресурсів, може приймати різні форми. Ступінь важливості проблеми несанкціонованого доступу для різних об'єктів різна.

Нелегальне ознайомлення з інформацією — друга розповсюджена загроза. Дуже важливо правильно визначити ступінь конфіденційності інформації, що зберігається в комп'ютерних системах об'єкта.

Відмовлення в обслуговуванні порушують цілісність системи і виникають по різних причинах 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 комп'ютерної системи.

При розробці політики безпеки необхідно дати відповіді на ряд 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 політика безпеки описує порядок надання і використання прав доступу користувачів, а також вимоги звітності користувачів за свої дії в питаннях безпеки.

Для комп'ютерних мереж можна виділити наступні ймовірні загрози, які необхідно враховувати при визначенні політики безпеки:

• Випадкові загрози:

- помилки обслуговуючого персоналу та користувачів;
- втрата чи руйнування інформації, обумовлені неправильним збереженням архівних даних на магнітних носіях;
- випадкове знищення чи зміна даних;
- збої устаткування електроживлення;
- збої кабельної системи;
- перебої електроживлення;
- збої дискових систем;
- збої систем архівування даних;
- збої роботи серверів, робочих станцій, мережевих карт і т.д.;
- руйнування файлової структури через некоректну роботу чи програм апаратних засобів;
- зміна даних при помилках у програмному забезпеченні;
- зараження системи комп'ютерними 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 та радіоактивні випромінювання).

• Навмисно створювані загрози:

- 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 даних і програм;
- копіювання даних і програм;
- розкриття, чи модифікація підміна трафіка обчислювальної мережі;
- розробка і поширення комп'ютерних вірусів;
- введення в програмне забезпечення логічних бомб;
- крадіжка магнітних та паперових носіїв, що містять конфіденційну інформацію;
- також крадіжка розрахункових документів;
- крадіжка устаткування;
- руйнування архівної інформації чи навмисне її знищення;
- фальсифікація повідомлень, переданих по каналах зв'язку;
- відмовлення від авторства повідомлення, переданого по каналах зв'язку;
- відмовлення від факту одержання інформації;
- нав'язування раніше переданого повідомлення;
- перехоплення й ознайомлення з інформацією, переданої по каналах 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);

вірогідності (збереження інформацією своїх семантичних властивостей у будь-який момент часу від моменту введення в систему);

конфіденційності (неприступність інформації чи сервісів для користувачів, яким апріорно не задана можливість використання зазначених сервісів чи інформації);

цілісності (незмінність властивостей інформації і ресурсів у будь-який момент часу від моменту їх появи чи введення у систему) .

При аналізі загроз варто брати до уваги їхній вплив на активи по чотирьох названих напрямках.

На підставі вищесказаного можна розробити зразковий алгоритм роботи з оцінки інформаційних ризиків (рис. 2).

Оцінка ймовірності появи вище перерахованих ймовірних погроз і очікуваних розмірів втрат – складний і тривалий процес, але коректно визначити вимоги до системи захисту об'єкта ще складніше, тому політика безпеки повинна визначатися наступними мірами:

- ідентифікація користувачів;
- перевірка дійсності і контроль доступу користувачів до об'єкта, що захищається, у приміщення, до ресурсів інформаційної системи;
- поділ повноважень користувачів, що мають доступ до обчислювальних ресурсів;
- реєстрація й облік роботи користувачів;
- реєстрація спроб порушення повноважень;
- шифрування конфіденційної інформації на основі криптографічних алгоритмів високої стійкості;
- застосування цифрового підпису для передачі інформації по каналам зв'язку;
- забезпечення антивірусного захисту та відновлення інформації, зруйнованої вірусними впливами;
- контроль цілісності програмних засобів й 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.

Система інформаційної безпеки (СІБ) об'єкта виявиться ефективної, якщо вона буде надійно підтримувати виконання правил політики безпеки, і навпаки.

Реалізація політики безпеки інформаційного об'єкта починається з проведення розрахунку фінансових витрат 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 по безпеці інформації:

- економічна ефективність – вартість засобів захисту повинна бути менше, ніж розміри можливого збитку;
- кожен користувач повинний мати мінімальний набір привілеїв, необхідний при роботі;
- простота системи захисту об'єкта – захист буде тим більше ефективний, чим легше користувачу з нею працювати;

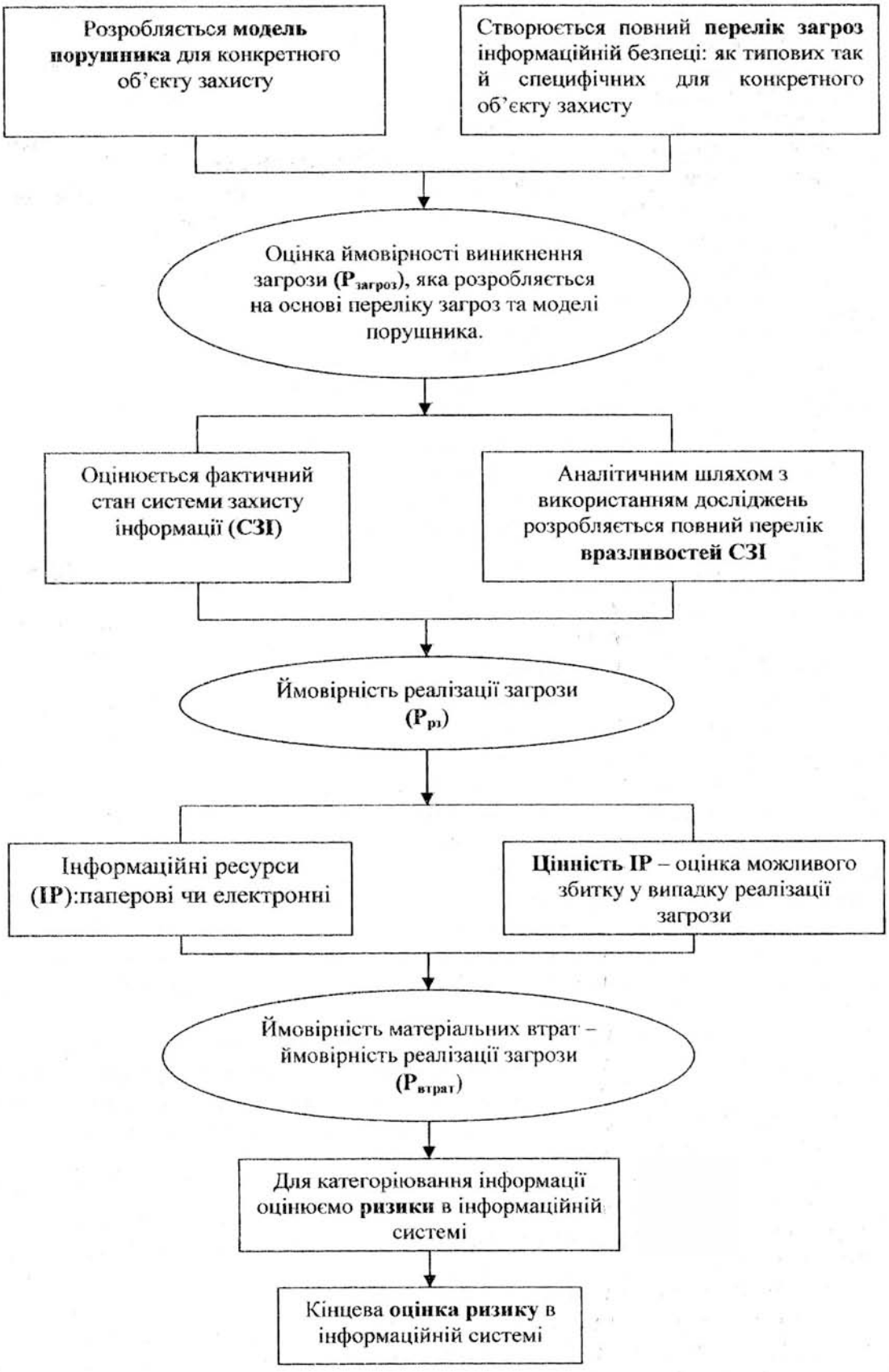

Рис. 2. Зразковий алгоритм роботи з оцінки ризиків в інформаційній системі.

- 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 механізмів 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 яких-небудь виключень з безлічей контрольованих суб'єктів;
- звітність і підконтрольність системи захисту;
- відповідальність осіб, що займаються безпекою інформації;
- об'єкти захисту доцільно розділяти на групи так, щоб порушення захисту в одній групі не впливало на безпеку інших груп;
- відмова за замовчуванням – при збої засобів захисту доступ до обчислювальних ресурсів повинен бути заборонений;
- система захисту об'єкта повинна бути цілком специфікована, протестована та погоджена;
- система повинна допускати зміну своїх параметрів адміністратором;
- важливі критичні рішеннями 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 політики безпеки** потрібно постійне спостереження за вторгненнями зловмисників, які відбуваються, 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 політики безпеки інформаційної мережі (об'єкта інформації) лежить на системному адміністраторі, що повинен оперативно реагувати на всі випадки злому 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 нал жної 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 політики, 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 залежать від типу порушення, яке сталося.

Політику безпеки можуть порушувати дуже різні особи. Деякі з них є своїми, місцевими користувачами, інші нападають 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 залучення 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 підприємства, що захищає свою конфіденційну інформацію, зобов'язано поставити справу

так, щоб не тільки внутрішні, але і зовнішні легальні користувачі знали положення політики безпеки об'єкта.

Проблеми з нелегальними користувачами, загалом, ті ж самі. Потрібно одержати відповіді на питання про те, які типи користувачів порушують політику, як і навіщо вони це роблять. У залежності від результатів розслідування можна просто закрити «діру» у системі захисту та задовольнитися отриманим уроком чи зволіти більш жорстокі міри.

Кожне підприємство повинне заздалегідь визначити набір адміністративних санкцій, застосовуваних до місцевих користувачів, що порушують політику безпеки сторонньої організації. Крім того, необхідно подбати про захист від відповідних дій сторонньої організації. При розробці політики безпеки варто врахувати всі юридичні положення, які застосовуються до подібних ситуацій.

Політика безпеки підприємства повинна містити процедури для взаємодії з зовнішніми організаціями, у число яких входять правоохоронні органи, інші організації, команди "швидкого реагування", засобів масової інформації. У процедурах повинне 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 усіх видів порушень повинні бути заготовлені відповідні процедури.

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

1) Якщо керівництво побоюється вразливості підприємства, 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 запобігається, після чого негайно починається процес оцінки нанесених ушкоджень і відновлення даних. Можливо, при цьому прийдеться виключити комп'ютерну систему, закрити доступ у мережу чи почати інші жорсткі міри. Зворотній бік даної медалі полягає в тому, що поки зловмисник не виявлений, він може знову напасти на цю ж чи іншу організацію колишнім чи новим способом.

2) Інший підхід, "вистежити і засудити", спирається на інші філософію і систему цілей. Основна мета полягає в тому, щоб дозволити зловмиснику продовжувати свої дії, поки організація не зможе встановити його особистість. Такий підхід подобається правоохоронним органам. На жаль, ці органи не зможуть звільнити організацію від відповідальності, якщо користувачі звернуться в суд з позовом із приводу збитку, нанесеного їх програмам і даним.

Судове переслідування — не єдиний можливий результат встановлення особистості порушника. Якщо винним виявився штатний співробітник чи студент, організація може віддати перевагу дисциплінарним мірам. У політиці безпеки повинні бути перераховані припустимі варіанти покарання і критерії вибору одного чи декількох з них у залежності від особистості винного.

Керівництво організації повинне заздалегідь ретельно зважити різні можливості при виборі стратегії відповідних дій. У принципі стратегія може залежати від конкретних обставин нападу. Можливий і вибір єдиної стратегії на усі випадки життя. Потрібно взяти до уваги всі "за" і "проти" та проінформувати користувачів про прийняте рішення, щоб вони в будь-якому випадку усвідомлювали ступінь своєї вразливості.

Після того, як положення політики безпеки затверджені, необхідно почати активний процес, що гарантує сприйнята й обговорення політики . В ідеалі політика повинна дотримувати баланс між безпекою і продуктивністю праці.

Не можна забувати, що політика безпеки об'єкта не може бути ідеальною і довговічною, тому що з часом усе змінюється: міняється устрій життя та канони в нормативній базі, модернізується устаткування і міняється обслуговуючий персонал. Отже,

політика безпеки об'єкта теж повинна доповнюватися і змінюватися у відповідності з усіма перерахованими критеріями та в залежності від змін цінності інформації, що захищається.

Список літератури

1. Информационно-методический журнал «Защита информации. Конфидент», 2002р., Петренко С.А. «Реорганизация корпоративных систем безопасности»;
2. Соколов А.В., Степанюк О.М. «Защита от компьютерного терроризма», Справочное пособие, БХВ-Петербург, «Арлит», 2002;
3. «Выработка официальной политики предприятия в области информационной безопасности», Internet;
4. Щеглов А.Ю. «Защита компьютерной информации от несанкционированного доступа», Санкт-Петербург, «Наука и техника», 2004.

Надійшла 18.06.2005
Після доробки 21.08.2005

УДК 681.3.06

В.К Белошапкін,С.М.Пустовіт, В.Д.Степанов

ФОРМАЛІЗАЦІЯ ПРОБЛЕМИ ОПТИМІЗАЦІЇ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

На сьогодні можна знайти достатньо повний перелік вимог та критеріїв [1-14] , які можуть бути взяті за основу для оцінки ефективності засобів і заходів захисту інформаційних ресурсів (ІР) інформаційно- телекомунікаційних систем.

Аналіз цих документів дозволяє оцінити перспективи використання існуючих розробок на практиці. При цьому такі оцінки важливо зробити з позицій системного підходу..

В [10] викладені основні принципи, які повинні виконуватися в межах системного підходу в ході вирішення довільної складної проблеми. В контексті документів [1-14] ці принципи можна сформулювати наступним чином:

1. Системний аналіз суті проблеми захисту інформації;

2. Розробка і обґрунтування повної, вільної від протиріч концепції і методології вирішення проблеми захисту інформації, в межах якої проблема захисту продукту чи системи в конкретних умовах визначається у вигляді профілю - проекту захисту;

3. Системне використання методів і механізмів захисту інформації при вирішенні задачі синтезу (проектування) безпечних продуктів і систем інформаційних технологій.

Із розгляду зазначених документів видно, що вони спрямовані на вирішення перших двох проблем. В одному з останніх документів - стандарті ISO/IEC 15408 здійснена повна декомпозиція проблеми захисту інформації. Механізми профілю і проекти захисту відображають суть концепції вирішення проблеми захисту інформації.

На сьогодні в нормативних документах відсутня методологія вирішення третьої проблеми -- проблеми синтезу комплексної системи захисту інформації. Функціональні вимоги і вимоги адекватності, як і методологія оцінки безпеки, направлені в першу чергу на рішення задачі оцінки безпеки продукту чи системи. Хоча їх використання, накладає деякий регламентований вплив на проектування, розробку і експлуатацію систем. Тут необхідно забезпечити встановлення відповідності цілям захисту (суть яких виражається через вимоги) множини засобів і механізмів , які маються в розпорядженні.

Стандарт ISO/IEC 15408 передбачає створення електронного каталогу профілів захисту, які пройшли оцінку та сертифікацію, що дозволить розробникам використати відомі профілі захисту при розробці нових систем і продуктів.