

ДЕЯКІ ПРОБЛЕМИ БЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ В ОРГАНІЗАЦІЯХ

*Рудяк М.В., к.ф.-м.н., доцент, Бойович О.В.
Одеський національний університет ім. І. І. Мечникова (Одеса, Україна)*

I. Безпека електронної системи - це її здатність протидіяти спробам нанести збитки власникам та користувачам систем при появі різноманітних збуджуючих (навмисних і ненавмисних) впливів на неї. Природа впливів може бути різноманітною: спроба проникнення зловмисника, помилки персоналу, стихійні лиха (ураган, пожежа і інші), вихід з ладу окремих ресурсів. Розрізняють внутрішню і зовнішню безпеку. *Зовнішня безпека* враховує захист від стихійного лиха, від проникнення зловмисника, отримання доступу до носіїв інформації чи виходу системи з ладу. Предметом *внутрішньої безпеки* є забезпечення надійної і коректної роботи *системи*, цілісності її програм і даних.

Існує два підходи до *забезпечення безпеки електронних систем*: *фрагментарний підхід* - проводиться протибачення строго визначеним загрозам при певних умовах (спеціалізовані антивірусні засоби, автономні засоби шифрування, тощо);

- *комплексний підхід* - передбачається створення середовища обробки інформації, яке об'єднує різноманітні (правові, організаційні, програмно-технічні) заходи для протидії загрозам.

Комплексний підхід, як правило, використовується для *захисту великих систем*. В цьому випадку необхідно забезпечити виконання *наступних заходів*:

- організаційні заходи по контролю за персоналом, який має високий рівень повноважень на дії в системі (за програмістами, адміністраторами баз даних мережі і т.д.); організаційні та технічні заходи по резервуванню критично важливої інформації; організаційні заходи по відновленню працездатності системи у випадку виникнення нештатних ситуацій;
- організаційні та технічні заходи по *управлінню доступом* в приміщеннях, в яких знаходиться *обчислювальна техніка*;
- організаційні та технічні заходи по фізичному захисту приміщень, в яких знаходиться *обчислювальна техніка і носії даних*, від стихійних лих, масових безпорядків і т.д.

П. В 1985 році Національний центр комп'ютерної безпеки Міністерства оборони США опублікував так звану «*Оранжеву книгу*» («Критерії достовірності обчислювальних систем Міністерства оборони»). В ній були наведені основні положення, згідно з якими американське відомство оборони визначало ступінь захищеності *інформаційно-обчислювальних систем*. В ній в систематизованому вигляді наводились *основні поняття, рекомендації і класифікація видів загроз безпеці інформаційних систем і методи захисту від та*. Вона стала настільною книгою для спеціалістів в галузі *захисту інформації*, а запропонована в ній методологія по суті стала загальноприйнятною і в тій чи іншій мірі увійшла в національні стандарти.

Системний підхід згідно з «Оранжевою книгою» вимагає:

- прийняття принципів рішень в галузі безпеки на основі поточного стану *інформаційної системи*;
- прогнозування можливих загроз і аналізу пов'язаного з ними ризику для *інформаційної системи*;
- планування заходів по запобіганню виникнення критичних ситуацій;
- планування заходів по виходу з критичних ситуацій на випадок, якщо вони виникнуть.

В «Оранжевій книзі» було введено важливе поняття «*політика безпеки*». **Політика безпеки** - це сукупність норм, правил і методик, на основі яких у подальшому буде вестись діяльність *інформаційної системи* в галузі обробки, зберігання і розподілення критичної інформації. При цьому під *інформаційною системою* розуміється як апаратно-програмний комплекс, так і обслуговуючий персонал.

III. Політика безпеки формується на основі аналізу поточного стану і перспективи розвитку інформаційної системи, можливих загроз. Вона визначає:

- мету, задані і пріоритети системи безпеки;
- галузь дії окремих підсистем;
- гарантований мінімальний рівень захисту; обов'язки персоналу по забезпеченню захисту; санкції за порушення захисту.

Якщо виконання політики безпеки проводиться не в повній мірі або непослідовно, тоді імовірність порушення захисту інформації різко зростає.

Захист інформації означає комплекс заходів, який забезпечує:

- збереження конфіденційності інформації - запобігання ознайомлення з інформацією не вповноважених осіб;
- збереження інформації - запобігання пошкодження чи знищення інформації внаслідок свідомих дій зловмисника, помилок персоналу, стихійного лиха;
- прозорість - наявність системи безпеки не повинна створювати перешкод для нормальної роботи системи.

IV. Визначення політики безпеки неможливе без аналізу ризику. Аналіз ризику підвищує рівень поінформованості про слабкі та сильні сторони захисту, створює базу для підготовки і прийняття рішень, оптимізує розмір затрат на захист, оскільки більша частина ресурсів спрямовується на блокування загроз, що можуть принести найбільшу шкоду. Аналіз ризику складається з наступних основних етапів:

- опис складу системи: апаратних засобів, програмного забезпечення, даних, документації, персоналу;
- визначення слабких місць по кожному елементу системи з оцінкою можливих загроз;
- оцінка імовірності реалізації загроз;
- оцінка очікуваних розмірів втрат (цей етап складний, оскільки не завжди можлива кількісна оцінка даного показника);
- аналіз можливих методів і засобів захисту;
- оцінка вигаду від прийнятих заходів; якщо очікувані втрати більші допустимого рівня, необхідно посилити заходи безпеки.

Аналіз ризику завертається прийняттям політики безпеки і складанням плану захисту з наступними розділами:

- поточний стан: опис статусу системи безпеки в момент підготовки плану;
- рекомендації: вибір основних засобів захисту, що реалізують політику безпеки;
- відповідальність: список відповідальних працівників і зон відповідальності;
- розклад: визначення порядку роботи механізмів, в тому числі і засобів контролю;
- перегляд положень плану, які повинні періодично переглядатися.

V. Основним питанням початкового етапу впровадження системи безпеки в організації є призначення відповідальній особі за безпеку і розмежування сфер їх впливу. При вирішенні питань розподілу відповідальності за безпеку комп'ютерної системи необхідно враховувати наступні положення:

- тільки керівництво організації може прийняти основоположні рішення в галузі політики комп'ютерної безпеки;
- тільки спеціалісти зможуть забезпечити правильне функціонування системи безпеки;
- ніяка зовнішня організація чи її група спеціалістів життєво не зацікавлена в економічній ефективності заходів безпеки «чужої» організації.

Організаційні заходи безпеки інформаційних систем прямо чи опосередковано пов'язані з адміністративним управлінням і відносяться до рішень і дій, які застосовуються керівництвом для створення таких умов експлуатації, які зведуть до мінімуму слабкість захисту. Дії адміністрації можна регламентувати по наступних напрямках: 1) заходи фізичного захисту комп'ютерних систем; 2) регламентація технологічних процесів; 3) регламентація роботи з конфіденційною інформацією; 4) регламентація процедур резервування; 5) регламентація внесення змін; б) регламентація роботи персоналу і користувачів; 7) підбір та підготовка кадрів; 8) заходи контролю і спостереження.

До галузі стратегічних рішень при створенні системи комп'ютерної безпеки, повинні бути віднесена розробка загальних вимог до класифікації даних, що зберігаються і

обробляються в системі. На практиці найчастіше використовуються наступні категорії інформації: важлива інформація; корисна інформація; конфіденційна інформація; відкрита інформація.

Керівництво організації повинно приймати рішення про те, хто і яким чином буде визначати степінь конфіденційності і важливості інформації.

VI. Під загрозою безпеки розуміють потенційні дії або події, які можуть прямо чи опосередковано принести втрати - привести до розладу, спотворення чи несанкціонованого використання ресурсів мережі, включаючи інформацію, що зберігається, передається або обробляється, а також програмні і апаратні засоби.

Не існує єдиної загальноприйнятої класифікації загроз безпеки, хоча існує багато її варіантів. Однією із подібних класифікацій є наступний перелік: 1) по цілі реалізації; 2) по принципу дії на систему; 3) по характеру впливу на систему; 4) по причині появи помилки захисту; 5) по способу дії атаки на об'єкт; б) по об'єкту атаки; 7) по використовуваних засобах атаки; 8) по етапу об'єкту атаки.

Загрози прийнято ділити на випадкові і навмисні. Джерелом випадкових загроз можуть бути помилки в програмному забезпеченні, виходи з ладу апаратних засобів, неправильні дії користувачів або адміністрації локальної обчислювальної мережі (ЛОМ) і т.д. Навмисні загрози, на відміну від випадкових, прагнуть нанести шкоду користувачам (абонентам) ЛОМ і, в свою чергу, діляться на активні та пасивні. Пасивні загрози, як правило, спрямовані на несанкціоноване використання інформаційних ресурсів ЛОМ, не впливаючи при цьому на її функціонування. Пасивною загрозою є, наприклад, спроба отримання інформації, що циркулює в каналах передачі даної ЛОМ, шляхом підслуховування. Активні загрози прагнуть порушити нормальне функціонування ЛОМ шляхом цілеспрямованого впливу на її апаратні, програмні і інформаційні ресурси. До активних загроз відносяться, наприклад, порушення або радіоелектронне заглушення ліній зв'язку ЛОМ, вивід з ладу ЕОМ або її операційної системи, спотворення відомостей в користувацьких базах даних або системної інформації ЛОМ і т.д. Джерелами активних загроз можуть бути безпосередні дії зловмисників, програмні віруси, тощо.

До основних загроз безпеки інформації відносяться: 1) розкриття конфіденційної інформації; 2) компрометація інформації; 3) несанкціоноване використання ресурсів ЛОМ; 4) помилкове використання її ресурсів; 5) несанкціонований обмін інформацією; б) відмова від інформації; 7) відмова в обслуговуванні.

VII. Система захисту інформації - це організована сукупність спеціальних установ, засобів, методів і заходів, що забезпечують захист інформації від внутрішніх і зовнішніх загроз.

В загальній системі забезпечення безпеки захист інформації відіграє значну роль. Виділяють наступні основні форми захисту інформації: 1) фізичні; 2) законодавчі; 3) управління доступом; 4) криптографічне закріплення.

Фізичні способи захисту ґрунтуються на фізичних перешкодах для зловмисника, закриваючи шлях до захищеної інформації (строга система допуску). До законодавчих способів захисту відносяться законодавчі акти, які регламентують правіша використання і обробки інформації і встановлюють міру відповідальності за порушення цих правил. Під управлінням доступом розуміють захист інформації шляхом регулювання доступу до всіх ресурсів системи. В комп'ютерних системах найефективнішими є криптографічні способи захисту інформації, що характеризуються найкращим рівнем захисту.