Інформаційна безпека суспільства

Паршукова Л.М.

У сучасному соціумі інформаційна сфера має дві складові: інформаційно-технічну (штучно створений людиною світ техніки, технологій тощо) та інформаційно-психологічну (природний світ живої природи, що включає і самої людини). Відповідно, в загальному випадку інформаційну безпеку суспільства (держави) можна представити двома складовими частинами: інформаційно-технічною безпекою і інформаційно-психологічної (психофізичної) безпекою.

У якості стандартної моделі безпеки часто призводять модель з трьох категорій:

- Конфіденційність - стан інформації, при якому доступ до неї здійснюють тільки суб'єкти, що мають на нього право;
- Цілісність - уникнення несанкціонованої модифікації інформації;
- Доступність - уникнення тимчасового або постійного захування інформації від користувачів, що отримали права доступу.

Виділяють і інші не завжди обов'язкові категорії моделі безпеки:

- Неспростовності - неможливість відмови від авторства;
- Підзвітність - забезпечення ідентифікації суб'єкта доступу та реєстрації його дій;
- Достовірність - властивість відповідності передбаченому поведінки чи результату;
- Автентичність або справжність - властивість, що гарантує, що суб'єкт або ресурс ідентичні заявленим.

Дії, які можуть завдати шкоди інформаційної безпеки організації, можна розділити на декілька категорій:

1. Дії, здійснювані авторизованими користувачами. У цю категорію потрапляють: цілеспрямована крадіжка або знищення даних на робочій

станції або сервері; пошкодження даних користувачів в результаті необережних дій.

2. «Електронні» методи впливу, здійснювані хакерами. Під хакерами розуміються люди, які займаються комп'ютерними злочинами як професійно (у тому числі в рамках конкурентної боротьби), так і просто з цікавості. До таких методів належать: несанкціоноване проникнення в комп'ютерні мережі; DOS-атаки.

Метою несанкціонованого проникнення ззовні в мережу підприємства може бути нанесення шкоди (знищення даних), крадіжка конфіденційної інформації та використання її в незаконних цілях, використання мережевої інфраструктури для організації атак на вузли третіх фірм, крадіжка коштів з рахунків і т.п.

Атака типу DOS (скор. від Denial of Service - «відмова в обслуговуванні») - це зовнішня атака на вузли мережі підприємства, що відповідають за її безпечну і ефективну роботу (файлові, поштові сервера). Зловмисники організують масовану відправку пакетів даних на ці вузли, щоб викликати їх перевантаження і, в підсумку, на якийсь час вивести їх з ладу. Це, як правило, тягне за собою порушення в бізнес-процесах компанії-жертви, втрату клієнтів, збиток репутації тощо.

3. Комп'ютерні віруси. Окрема категорія електронних методів впливу - комп'ютерні віруси та інші шкідливі програми. Вони являють собою реальну небезпеку для сучасного бізнесу, широко використовує комп'ютерні мережі, інтернет і електронну пошту. Проникнення вірусу на вузли корпоративної мережі може призвести до порушення їх функціонування, втрат робочого часу, втрати даних, втрату особистих даних і навіть прямим розкраданням фінансових коштів. Вірусна програма, яка проникла в корпоративну мережу, може надати зловмисникам частковий або повний контроль над діяльністю компанії.

4. Спам. Всього за кілька років спам з незначного дратівної чинника перетворився в одну з серйозних загроз безпеці: електронна пошта останнім

часом стала головним каналом поширення шкідливих програм; спам забирає багато часу на перегляд і подальше видалення повідомлень, викликає у співробітників почуття психологічного дискомфорту; як приватні особи , так і організації стають жертвами шахрайських схем, реалізованих спамерами; разом зі спамом нерідко віддаляється важлива кореспонденція, що може призвести до втрати клієнтів, зриву контрактів і інших неприємних наслідків; небезпека втрати кореспонденції особливо зростає при використанні чорних списків RBL та інших «грубих» методів фільтрації спаму.

5. «Природні» загрози. На інформаційну безпеку компанії можуть впливати різноманітні зовнішні фактори: причиною втрати даних може стати неправильне зберігання, крадіжка комп'ютерів і носіїв, форс-мажорні обставини і т.д.

Таким чином, в сучасних умовах наявність розвиненої системи інформаційної безпеки стає одним з найважливіших умов конкурентоспроможності і навіть життєздатності будь-якої компанії.