УДК 681.518

Долгушев Є.В., Резніченко В.А.
Кіровоградський національний технічний університет

Шляхи вирішення проблем інформаційної безпеки

Для пошуку рішень проблем інформаційної безпеки при роботі у мережі Інтернет був створений незалежний консорціум ISTF (Internet Security Task Force) – громадська організація, що складається з представників і експертів компаній-постачальників засобів інформаційної безпеки, електронного бізнесу і провайдерів інтернет-інфраструктури. Ціль цього консорціуму – розробка технічних, організаційних і операційних посібників з безпеки діяльності в Інтернеті.

Консорціум ISTF виділив дванадцять дванадцять областей інформаційної безпеки, на яких в першу чергу повинні сконцентрувати свою увагу творці електронного бізнесу, щоб забезпечити його працездатність. Цей список, зокрема, включає наступні пункти: автентифікація (механізм об'єктивного підтвердження ідентифікуючої інформації), право на приватну, персональну інформацію (забезпечення конфіденційності інформації), визначення подій безпеки (Security Events), захист корпоративного периметру, визначення атак, контроль за потенційно небезпечним вмістом (Malicious Content), контроль доступу, адміністрування, реакція на події.

Рекомендації ISTF призначені для існуючих або знову утворених компаній електронної комерції та електронного бізнесу. Ці рекомендації допомагають визначити потенційні проломи в їх комп'ютерних мережах, які, якщо не звернути на них належної уваги, можуть використовуватися хакерами. Це може привести до атак на систему електронної комерції, збитків і навіть до краху електронного бізнесу. Консорціум ISTF настійно рекомендував скористатися його напрацюваннями ще до початку організації компанії, має намір зайнятися електронною комерцією і бізнесом.

Реалізація рекомендацій консорціуму ISTF означає, що захист інформації в системі електронного бізнесу повинна бути комплексною.

Згідно з рекомендаціями ISTF і класифікації «рубежів оборони» Hurwitz Group першим і найважливішим етапом розробки системи інформаційної безпеки електронного бізнесу є механізми управління доступом до мереж загального користування та з них, а також механізми безпечних комунікацій, реалізовані між мережевими екранами і продуктами приватних захищених віртуальних мереж (VPN).

Супроводжуючи їх засобами інтеграції і управління всією ключовий інформацією системи захисту (PKI - інфраструктура відкритих ключів), можна отримати цілісну, централізовано керовану систему інформаційної безпеки.

Наступний рубіж включає в себе інтегровані в загальну структуру засоби контролю доступу користувачів в систему разом з системою одноразового входу і авторизації (Single Sign-On).

Антивірусний захист, засоби аудиту та запобігання атак, по суті, завершують створення інтегрованої цілісної системи безпеки, якщо мова не йде про роботу з конфіденційними даними.

Застосування комплексу засобів захисту на всіх рівнях корпоративної системи дозволяє побудувати ефективну і надійну систему забезпечення інформаційної безпеки.

Список використаних джерел

1. *Шаньгін В.Ф. «Захист інформації в комп'ютерних системах і мережах» - М.: ДМК Прес, 2012 – 592 с.*