Дячков Д. В.
к.е.н., доцент кафедри менеджменту
Полтавської державної аграрної академії

ОСОБЛИВОСТІ ЗАХИСТУ ЛОКАЛЬНОГО ТА «ХМАРНОГО» ІТ-ОТОЧЕННЯ СУЧАСНОЇ ОРГАНІЗАЦІЇ

В умовах глобальної інформатизації соціально-економічних систем актуальною залишається проблема забезпечення їх інформаційної безпеки. Досвід використання інформаційних систем в різних сферах життєдіяльності вказує на різноплановість та реальність загроз втрати інформації, що, як наслідок, призводить до економічних збитків.

У зв'язку з цим, основними завданнями розробки, вдосконалення та впровадження технологій захисту інформації повинні відбуватися в наступних напрямах:

- формування нових стандартів електронно-цифрового підпису;
- розвиток масштабності системи електронних цифрових сертифікатів з використанням центрів довіри;
- вдосконалення криптографічного захисту корпоративних (віртуальних) комп'ютерних мереж і засобів міжмережевого екранування;
- застосування засобів антивірусного захисту та засобів захисту від несанкціонованого доступу до інформації для неоднорідних розподілених інформаційних систем;
- моніторинг та аудит безпеки мережевих інформаційних ресурсів;
- захист програмно-апаратних засобів для IP-телефонії;
- захист мереж мобільного зв'язку та персональних комунікацій;
- біометрична ідентифікація, застосування засобів аутентифікації на базі інтелектуальних карт та інших малогабаритних технічних засобів обробки інформації [2].

Розвиток зазначених перспективних технологій захисту інформації вимагає, з одного боку, застосування нових математичних і криптографічних рішень, а з

іншого боку, залежить від розвитку мікропроцесорних, алгоритмічних, програмних та інших суміжних технічних рішень.

Перспективні технології захисту інформації повинні синтезувати тільки високотехнологічні розробки інтелектуальних систем аналізу інформації, які інтегрують передові досягнення лінгвістичного аналізу, мовних технологій, візуалізації даних, програмно-технічних рішень.

Для вітчизняних підприємств характерним є те, що у корпоративних інформаційних системах підприємства взаємодія здійснюється за допомогою локальних, глобальних мереж та «хмарних» технологій.

Підприємства, що використовують для доступу до корпоративних систем виключно паролі, ставлять під загрозу стабільність бізнесу, піддаючи свої інформаційні активи таким ризикам, як фішинг, MITM («людина посередині»), соціальна інженерія, підбір пароля, крадіжка облікових даних. І як наслідок, несанкціонований доступ до корпоративних ресурсів, що призводить до розголошення комерційної таємниці, фінансових і репутаційних втрат.

Деякі організації дозволяють доступ до своїх інфраструктур тільки всередині периметра корпоративного захисту, іншим же компаніям, навпаки, потрібно дозволити доступ поза межами контрольованої зони зовнішнім консультантам, партнерам або віддаленим співробітникам. Тому організація безпечної і надійної передачі даних, захист від зовнішніх і внутрішніх загроз, захист конфіденційності даних є складним завданням [1].

Тонкі клієнти, нульові клієнти, сервери, ноутбуки, планшети і мобільні пристрої, так чи інакше беруть участь в корпоративному житті користувача на підприємстві та вимагають уніфікованої і незалежної від пристрою політики безпеки. ІТ-служби та служби інформаційної безпеки організації повинні вирішити складне завдання – одночасно зберегти унікальні можливості різних типів пристроїв і забезпечити їх достатньо високим рівнем безпеки.

Все це призводить до того, що посилений контроль за доступом користувачів з різних пристроїв і з будь-якого місця стає дуже важливим завданням і частиною інформаційної системи.

VDI-клієнти, як заміна традиційним ПК і перехід до централізованих обчислень, підвищують продуктивність, надають колосальні та можливості для зростання. Спільне використання тонких клієнтів і рішень з безпеки підприємства з легкістю може усунути описані складності і отримати всі переваги централізованих обчислень, зокрема:

– двофакторна аутентифікація користувачів в корпоративній системі в різних сценаріях: термінальних сеансах, VPN-з'єднаннях, доступі до «хмарних» платформ VDI;

– блокування термінального сеансу при від'єднанні токена або смарт-карти;

– можливість використання електронного підпису в прикладних програмах;

– карта-пропуск в приміщення (наявність RFID-мітки), також може бути платіжною (MasterCard або Visa) або транспортною картою з корпоративним стилем організації;

– наявність сертифікату ФСТЕК дозволяє відповідати вимогам регуляторів ринку інформаційної безпеки і спрощує атестацію інформаційної системи;

– вбудована підтримка SSL VPN;

– інтеграція з більшістю популярних вітчизняних чи західних програмних рішень [3].

Таким чином, сучасні підприємства здійснюють перехід до використання різносторонньої інформаційної інфраструктури, яка об'єднує як локальне, так і «хмарне» IT-оточення. Тому для зниження бізнес-ризиків в сфері інформаційної безпеки велике значення має вибір вірного рішення для аутентифікації. Очевидно, що найкращі рішення підтримують саму широку лінійку аутентифікаторів і можуть забезпечити захист як «cloud», так і локальних програм, а також будь-яку мережу, доступ до якої здійснюється з будь-якого пристрою.

Список використаних джерел:

1. Варгин В. Г. Использование онтологии при управлении доступом к интеллектуальным ресурсам [Электронный ресурс] / В. Г. Варгин,

Семерханов И. А. // Информационная безопасность, проектирование, технология элементов и узлов компьютерных систем. – Режим доступа: http://www.sworld.com.ua/konfer27/419

2. Современные технологии обеспечения информационной безопасности [Электронный ресурс]. – Режим доступа : http://www.biometrics.ru/

3. ТОНКости безопасности [Электронный ресурс] / Современные информационные системы CIS. – 2017. – №1 – Режим доступа: http://100pdf.net/cis-1-2017