Гордєєва-Герасимова Л. Ю.

Дніпровський національний університет імені Олеся Гончара (Україна)

ЗАХИСТ ІНФОРМАЦІЇ – ОДИН ІЗ НАПРЯМІВ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ

Забезпечення економічної безпеки підприємства – це можливість протидії потенційним і реальним зовнішнім та внутрішнім загрозам, запровадження превентивних заходів щодо усунення чи мінімізації яких має забезпечувати суб'єкту господарювання успішність функціонування в умовах ризику. При цьому безпека підприємства повинна забезпечуватися за такими основними напрямами, як економічна, науково-технічна, інформаційна, кадрова, соціальна, екологічна, фізична безпека тощо [1].

В умовах сьогодення інформаційна безпека дедалі більше стосується саме суб'єктів підприємницької діяльності, яким потрібно захищатися від відтоку інформації. Інформаційна безпека – це здатність персоналу підприємства забезпечити захист інформаційних ресурсів та потоків, у тому числі у мережах колективного доступу, від загроз несанкціонованого доступу до них [2].

Потрібно зауважити, що останні десятиліття у зв'язку з бурхливим розвитком Internet і мереж колективного доступу в світі стався якісний стрибок у поширенні і доступності інформації. В наш час все більшого застосування набирає використання віддаленого доступу між територіально рознесеними інформаційними мережами підприємства. Користувачі-підприємства отримали дешеві й доступні канали зв'язку. І прагнучі до економії коштів, підприємства використовують такі канали для передачі критичною комерційної інформації. Однак принципи побудови Internet відкривають зловмисникам можливості крадіжки або навмисного спотворення інформації. Не забезпечений достатньо надійний захист від проникнення порушників у корпоративні та відомчі мережі.

Суттєвим фактором будь-якої передачі даних є безпека інформації. Наразі говорити про те, що інформаційна безпека стала частиною корпоративних мереж підприємств в нашій країні можна з великою обачливістю. Необхідність

забезпечувати надійну безпеку інформації освідомили тільки великі компанії, але й вони до недавнього часу сприймали проблеми тільки з технічної сторони, яка була спрямована на встановлення програмного забезпечення для захисту інформації, такого як антивірусного програмного забезпечення, міжмережевих екранів, програм для моніторингу мереж і виявлення вторгнень, несанкціонованого доступу і віртуальних частин мереж. За рекомендаціями дослідницьких фірм, основним напрямком забезпечення безпеки слід спрямувати на розробку політики безпеки і супутніх їй документів. Політика безпеки є найдешевшим і одночасно найефективнішим засобом забезпечення інформаційної безпеки. Крім того, якщо політика сформульована, то вона є і керівництвом щодо розвитку і вдосконалення системи захисту. Можна сказати, що забезпечення інформаційної безпеки зводиться до трьох основних напрямів – це комбінація технічних, адміністративних і організаційних заходів.

Для ефективної протидії мережевим атакам і забезпечення можливості активного і безпечного використання в бізнесі відкритих мереж активно розвивається концепція побудови захищених віртуальних приватних мереж – VPN (Virtual Private Networks). При використанні технологій VPN безпека передавання інформації через загальнодоступні мережі реалізується за допомогою шифрування, внаслідок чого створюється закритий для сторонніх канал обміну інформацією [3].

Існує декілька захищених протоколів VPN, тому однозначно не можна відповісти на питання, яка з технологій VPN підходить найкраще. При застосуванні відповідного протоколу VPN постає питання про доцільність використання саме такого захисту мережі. Адже при реалізації такого захисту мережі необхідно звертати увагу не лише на переваги VPN, основними з яких є об’єднання розподілених ресурсів, підвищена безпека, прозорість для користувача та зниження затрат за рахунок використання інтернету, але й недоліки, які можуть вступати у протиріччя з нашими вимогами до безпеки мережі. До недоліків VPN слід віднести затрати часу на реалізацію, вірогідність виявленні проблем експлуатації, залежність доступу від інтернет провайдера,

взаємодія між різними протоколами, апаратними та програмними засобами різних виробників.

Крім того, при використанні технологій VPN потрібно враховувати і економічну складову. Існують безкоштовні VPN-сервіси, які можна використовувати. При належній кваліфікації системного адміністратора їх налаштовують з урахуванням особливостей мережі та необхідного ступеню інформаційної безпеки відповідного підприємства. Також існують платні VPN-сервіси, які вважаються більш захищеними та стабільнішими і швидкими. Який сервіс обрати – вирішувати керівництву підприємства виходячи з необхідності підтримання відповідного ступеню інформаційної безпеки та рівня кваліфікації персоналу IT-напряму.

Отже, у сучасному світі використанні Internet-технологій дедалі стає актуальним питання захисту інформації підприємствами від можливості крадіжки або навмисного спотворення її у мережі. Технології VPN – це один із засобів захисту інформації у мережі, які мають свої переваги та недоліки. Доцільність використання такого засобу вирішується керівництвом підприємства, зважаючи на економічну складову використання платного або безкоштовного VPN-сервісу і рівня кваліфікації IT-персоналу та необхідного рівня інформаційної безпеки.

Список використаних джерел:

1. Легомінова С. В. Теоретичні засади інформаційної безпеки підприємства / С. В. Легомінова // «Економіка. Менеджмент. Бізнес». № 3 (13); 2015. С.87-92.
2. Нехай В.А., Нехай В.В. Інформаційна безпека як складова економічної безпеки підприємств. URL: http://www.vestnik-econom.mgu.od.ua/journal/2017/24-2-2017/30.pdf. (Дата звернення 19.03.2020р.)
3. Різновиди мереж VPN та коли потрібно ними користуватися. URL: https://uk.vpnmentor.com/blog/%D1%80%D1%96%D0%B7%D0%BD%D0%BE%D0%B2%D0%B8%D0%B4%D0%B8-%D0%BC%D0%B5%D1%80%D0%B5%D0%B6-vpn-%D1%82%D0%B0-%D0%BA%D0%BE%D0%BB%D0%B8-%D0%BF%D0%BE%D1%82%D1%80%D1%96%D0%B1%D0%BD%D0%BE/ (Дата звернення 19.03.2020р.)