Василь Колотило,
студент 1 СТН курсу спеціальності 208 «Агроінженерія»
Науковий керівник: ***Мушеник Ірина Миколаївна***
канд. екон. наук, доцент кафедри математичних дисциплін, інформатики і моделювання,
Подільський державний аграрно-технічний університет,
м. Кам'янець-Подільський

ПРИНЦИПИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

В новітньому суспільстві основною виробничою силою, найважливішим стратегічним ресурсом, який забезпечує подальший його розвиток, є інформація. Саме тому інформація, як і будь які інші ресурси, потребує також особливого захисту. Поруч із терміном "захист інформації" широко застосовується термін "інформаційна безпека". Захист інформації характеризує процес створення обставин, які забезпечують потрібну захищеність інформації, а досягнутий стан такого рівня захищеності відображає інформаційна безпека [1].

Питання інформаційної безпеки набуло особливої значущості в новітніх умовах широкого використання інформаційних автоматизованих систем, заснованих на застосуванні комп'ютерних та телекомунікаційних засобів. Під час забезпечення інформаційної безпеки стали абсолютно імовірними загрози, що породжені навмисними (зловмисними) діями громадян. Перші звістки про несанкціонований доступ до інформації пов'язані були, як правило, з хакерами ("електронними розбійниками"). В останнє десятиріччя порушення захисту інформації зростає разом із застосуванням програмних засобів, а також за допомогою мережі Інтернет.

Дуже розповсюдженою загрозою інформаційної безпеки також є зараження комп'ютерних систем за допомогою комп'ютерних вірусів. Організація системи захисту комп'ютерних мереж ускладнюється тим, що загрози, від яких доводиться захищати мережі та дані, дуже невизначені і носять різноманітний характер. По своєму походженню це можуть бути фактори антропогенні, технічні, технологічні, часові, природні і ін., котрі не

завжди вдається прогнозувати. Тому при проектуванні та впроваджені мереж розробникам необхідно максимально враховувати можливі загрози від яких доводиться захищати мережу і дані, які в ній циркулюють [3].

Доцільно розглядати побудову захисту мережі і даних в ній як комплексну (багатопланову) систему заходів, оскільки непередбачені і навмисні антропогенні загрози можуть виникати в мережі як в людино-машинній автоматизованій системі в різні моменти життєвого циклу мережі і за різних обставин функціонування технічного обладнання, програмного забезпечення, кваліфікації персоналу [5].

Під безпекою електронної системи розуміють 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), вихід з ладу окремих ресурсів, як правило, розрізняють внутрішню і зовнішню безпеку. Внутрішня 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.

Фаєрвол (англ. firewall; fire – вогонь, wall – стіна) – це спеціальний тип програм, який встановлюється на ваш ПК і служить між мережевим фільтром між комп’ютером і мережею Інтернет.

Для того, щоб задовольнити вимогам широкого кола користувачів, існує три типи фаєрволів: мережного рівня, прикладного рівня і рівня з'єднання. Кожен з цих трьох типів використовує свій, відмінний від інших підхід до захисту мережі [2].

Фаєрвол мережного рівня представлений екрануючим маршрутизатором. Він контролює лише дані мережевого і транспортного рівнів службової інформації пакетів. Мінусом таких маршрутизаторів є те, що ще п'ять рівнів залишаються неконтрольованими. Нарешті, адміністратори, які працюють з

екрануючими маршрутизаторами, повинні пам'ятати, що у більшості приладів, що здійснюють фільтрацію пакетів, відсутні механізми аудиту та подачі сигналу тривоги. Іншими словами, маршрутизатори можуть піддаватися атакам і відбивати велику їх кількість, а адміністратори навіть не будуть проінформовані.

Фаєрвол прикладного рівня також відомий як проксі-сервер (сервер-посередник). Фаєрволи прикладного рівня встановлюють певний фізичний поділ між локальною мережею і Internet, тому вони відповідають найвищим вимогам безпеки. Проте, оскільки програма повинна аналізувати пакети і приймати рішення щодо контролю доступу до них, фаєрволи прикладного рівня неминуче зменшують продуктивність мережі, тому в якості сервера-посередника використовуються більш швидкі комп'ютери.

Фаєрвол рівня з'єднання схожий на фаєрвол прикладного рівня тим, що обидва вони є серверами-посередниками. Відмінність полягає в тому, що фаєрволи прикладного рівня вимагають спеціального програмного забезпечення для кожної мережевої служби на зразок FTP або HTTP. Натомість, фаєрволи рівня з'єднання обслуговують велику кількість протоколів [4].

Багато людей путають фаєрвол і антивірус називаючи їх однією програмою, але це не так. Фаєрвол і антивірус це дві різні программи. Антивірусна програма намагається знайти вірус, троян і тому подібне, а далі лікує заражений файл або видаляє (на практиці не завжди знаходить і тим більше лікує).

Брандмауер попросту перекриває доступ в мережу для зараженого файлу або хакерської атаки. Цим він запобігає проникненню зарази в ваш комп’ютер.

Основним завданням фаєрволу є забезпечення невидимості ПК в мережі. Це забезпечується закриттям певних портів, які доступні для злому. Ще в задачі брандмауера входить постійне стеження за всіма встановленими програмами і системними службами. Хакери давно навчилися маскувати

шкідливе ПЗ під безпечні системні файли. Файрвол дозволяє відсікати такі файли, та вони не проникають в операційну систему.

Налаштування будь-якого фаєрволу (брандмауера) дозволяють дозволяти доступ в мережу тільки визначеними програмами. Користувач сам може вирішити, яким програмам дозволяти мережевий доступ. Адже погодьтеся, коли ваш ПК намагається оправити дані без вашого на те дозволу, це як мінімум викликає підозру. Для цього випадку у фаєрволу є певні правила. Користувач може сам вказати довірені додатки, які безперешкодно будуть проходити в Інтернет, занести в чорний список ті, яким доступ буде заборонений. Ще подібні захисники вміють обмежувати мережевий трафік за часом, вести статистику для різних додатків, блокувати рекламу по вмісту або адресою сайту.

Список використаних джерел

1. Боднар І. Р. Роль держави у формуванні інформаційної політики. *Вісник ЛКА,* 2011. Вип. 34. (Серія економічна). С. 291-296.
2. Горбуль Д. В., Мушеник І. М. Сучасні електронні технології як інструменти формування інформаційно-освітнього середовища. *Інформаційне суспільство в умовах глобалізації* : зб. наукових праць Всеукраїнської науково-практичної інтернет-конференції, м. Кам'янець-Подільський, 12 травня 2020 р. Кам'янець-Подільський, 2020. С.152-157.
3. Литвинюк А. А. Основи інформаційної безпеки. Комплексна система захисту інформації: структура, встановлення та підтримка функціонування. URL: http://www.cvk.gov.ua/visnyk/pdf/2008_4/visnik_st_08.pdf
4. Мушеник І. Сучасні реалії і тенденції розвитку інформаційних технологій в освіті. *InterConf.* Вип. 27. 2020. С. 143-146.
5. Сороківська О. А. Інформаційна безпека підприємства: нові загрози та перспективи. *Вісник Хмельницького національного університету*. *Економічні науки.* 2010. № 2. Т. 2. С. 32-35.