Сергій КУШНІР
здобувач вищої освіти 1 курсу ОС «Бакалавр»
спеціальності 202 «Захист і карантин рослин»
Науковий керівник: **Ірина МУШЕНИК**
канд. екон. наук, доцент кафедри математики,
інформатики та академічного письма
Подільський державний аграрно-технічний університет,
м. Кам'янець-Подільський

АНТИВІРУСНИЙ ЗАХИСТ ІНФОРМАЦІЙ У МЕРЕЖІ

Комп'ютерні віруси, останнім часом, найчастіше проникають в систему через електронну пошту та заражені USB-носії інформації (флеш-карти та ін.).

Сучасний антивірусний захист не може обмежуватись лише встановленням антивірусної програми. Необхідним є застосування спеціалізованих програм одноразової перевірки, які оновлюються щоденно, та контроль автоматизованого запуску з USB-носіїв, наприклад: Dr.Web CureIt!, Kaspersky Virus Removal Tool, Norton Security Scan, Panda USB Vaccine.

Для безпечної роботи в локальній та глобальній інформаційній мережі Інтернет важливим є налаштування параметрів безпеки програми перегляду, а також спостереження за мережевою активністю комп'ютерів мережі з метою своєчасного виявлення та блокування мережевих загроз.

Важливим фактором інформаційної безпеки є також використання ліцензійного та сертифікованого програмного забезпечення, що дозволяє отримувати своєчасні оновлення захисту та забезпечити стале функціонування та розвиток інформаційної системи підприємства.

При підключенні мережі організації до мережі Інтернет необхідно прийняти ряд певних організаційно-технічних заходів щодо її захисту.

При побудові захисту слід виходити з того, що будь-який захист ускладнює використання системи, яка захищається, за прямим призначенням обмежує функціональні можливості, використовує обчислювальні і трудові ресурси, вимагає фінансових витрат на створення та експлуатацію. Чим вищий захист, тим більш дорогою у створенні та обслуговуванні стає система і тим менш зручною для безпосередніх користувачів. Тому, захищаючи мережу, слід

виходити з доцільної вартості захисту. Тобто витрати на захист повинні бути пропорційні цінності ресурсу, що захищається.

Найбільш простою і найбільш дешевою з точки зору захисту є трансляція фіксованої внутрішньої адреси у фіксованій зовнішній. При цьому зловмисник безперешкодно “бачить” такий комп'ютер в зовнішній мережі, оскільки йому однозначно відповідає певна зовнішня адреса. Проте вона необхідна при організації сервера, до якого потрібно забезпечити доступ ззовні.

Список використаних джерел:

1. Півень А. Г., Шевченко І. П. Захист інформації та використання інформаційних технологій в інтелектуальній власності. *SocioEconomic Challenges Journal.* 2011.

2. Семенов С.Г., Подорожняк А.О., Баленко О.І., Гавриленко С.Ю. Захист інформації в комп’ютерних системах та мережах : навч. посіб. Харків : НТУ «ХПІ», 2014. 251 с.

3. Захарченко М.В., Кононович В.Г. Інформаційна безпека інформаційно-комунікаційних систем. Лабораторний практикум. Частина 1 – Комплекси засобів захисту інформації від НСД: навч. посіб. за ред. ак. МАІ М.В. Захарченка.– Одеса: ОНАЗ ім. О.С. Попова, 2011. 168 с.

4. Технології захисту інформації . – 2016. URL до ресурсу. URL: https://www.uzhnu.edu.ua/uk/infocentre/get/4186.

5. Реалізація захисту інформації в ком’ютерних системах та мережах на основі операційної системи freebsd. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. 2017. URL до ресурсу. URL: https://ela.kpi.ua/bitstream/123456789/10673/1/14_p114