**УДК 004.056.57**

**Олександр Едуардович Шорский,**
*студент Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут»*

**Володимир Якович Пєвнєв,**
*кандидат технічних наук, доцент, доцент кафедри комп'ютерних систем, мереж та кібербезпеки Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут»*

# Антивірусний захист локальної мережі як засіб боротьби з правопорушеннями в кіберпросторі

В умовах інформатизації суспільства, застосування засобів інформаційних і комунікаційних технологій стає все більш актуальною проблема забезпечення інформаційної безпеки (ІБ) людини, підприємства, організації, громади, суспільства та держави.

Згідно з [1], кібербезпека – це захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі.

Одночасно з розвитком комп'ютерної техніки виникли та продовжують розвиватися шкідливі програми, серед яких виділяються комп'ютерні віруси. Комп'ютерний вірус – це невелика, складна, ретельно складена і небезпечна програма, яка може самостійно розмножатися, переноситися на диски, прикріплюватися до програм, передаватися через мережу, порушують роботу комп'ютера. При цьому вона намагається виконати приховане самокопіювання в різні області виконуваних кодів інших програм, максимально захищається від виявлення і по завершенню «інкубаційного» періоду заявляє про себе не прогнозованими руйнівними діями [2].

В грудні 2015 року відбулася кібератака на енергетичні компанії України. Найбільше постраждали споживачі «Прикарпаттяобленерго»: було вимкнено близько 30 підстанцій, близько 230 тисяч мешканців залишались без світла протягом однієї-шести годин. Атака відбувалась із використанням троянської програми BlackEnergy. Водночас синхронних атак зазнали «Чернівціобленерго» та «Київобленерго», але з меншими наслідками. Загальний недовідпуск електричної енергії становив – 73 МВт•год (0.015 % від добового обсягу споживання України) [3].

Кібератака з використанням вірусу, який спочатку був названий Petya.A (пізніше – NotPetya), відбулася наприкінці червня 2017 року. Департамент кіберполіції стверджує, що хакерська атака за допомогою вірусу Petya почалася в Україні через оновлення програми M.E.Doc, яке вийшло о 10:30 27 червня[4]. За підрахунками спеціалістів збитки України в результаті кібератаки вірусу Petya склали 0,4 % ВВП України, що є більше за 300 млн. доларів [4].

З роками розвинулась індустрія антивірусного програмного забезпечення, і про вірусні атаки звичайним користувачам вже можна менше хвилюватися. Антивірус – це програма, яка виявляє й знешкоджує комп'ютерні віруси. Слід зауважити, що віруси у своєму розвиткові випереджають антивірусні програми, тому навіть у випадку регулярного користування антивірусів немає 100% гарантії безпеки [5].

Розробники антивірусів активно впроваджують нові технології антівірусобудування: Hostbased Intrusion Prevention System (HIPS), Sandbox, Virtual-based Intrusion Prevention System (VIPS). Ці технології дозволяють користувачеві активно моніторити процеси в системі і приймати рішення про допуск їх до різних функцій ОС.

На сьогодні все більш популярними стають методи проактивного захисту: HIPS та пісочниця. Ці дві конкуруючі технології активно інтегрують в своє ПЗ найпопулярніші антивіруси: NOD32 і Kaspersky Anti-Virus використовують HIPS, Avast Antivirus – пісочницю. Проактивні методи захисту є високоефективним засобом захисту від шкідливого ПЗ і можуть скласти вагому конкуренцію класичним, реактивним методам захисту, а в поєднанні з ними можуть значно підвищити ефективність антивірусних систем.

4 Cyberpolice Ukraine (2017-06-27): Це ПЗ має вбудовану функцію оновлення, яка періодично звертається до серверу http://upd.me-doc.com.ua за допомогою User Agent «medoc1001189». URL: https://twitter.com/cyberpoliceua/status/879772963658235904 (дата звернення: 20.10.2019).

В доповіді розглянуті проблеми захисту локальних мереж від вірусного програмного забезпечення. Антивірусний захист локальної мережі є складною проблемою, яка не зводиться до простого налаштування антивірусних продуктів. Як правило, потрібне створення окремої підсистеми. З технічної точки зору при розв'язанні даної проблеми особливу увагу слід приділити тестуванню придбаного антивірусного ПЗ, а також установці антивірусних пакетів на поштові сервери. Для забезпечення антивірусного захисту локальної мережі доцільно використовувати комбіновані системи (міжмережний екран, антивірус, пісочниця). Такий метод дозволить максимально зменшити вірогідність проникнення вірусів в локальну мережу та забезпечити безпеку даних, що зберігаються на персональних комп'ютерах.

**Список бібліографічних посилань**

1. Про основні засади забезпечення кібербезпеки України : ракон України від 05.10.2017 № 2163-VIII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 20.10.2019).
2. Ленков С. В., Перегудов Д. А., Хорошко В. А. Методы и средства защиты информации : в 2 т. / под ред. В. А. Хорошко. Киев : Арий, 2008. Т. 1 : Несанкционированное получение информации. 464 с.
3. Zetter K. The Ukrainian Power Grid Was Hacked Again // Vice. Jan 10, 2017. URL: https://www.vice.com/en_us/article/bmvkn4/ukrainian-power-station-hacking-december-2016-report (дата звернення: 20.10.2019).
4. Аналіз регуляторного впливу // Державна служба спеціального зв'язку та захисту інформації України : офіц. сайт. 03.04.2018. URL: http://195.78.68.84/dsszzi/control/uk/publish/article?showHidden=1&art_id=288142&cat_id=38837&ctime=1522850564776 (дата звернення: 21.10.2019).
5. ТОП-10 комп'ютерних вірусів в історії. Ч. 2. URL: https://zillya.ua/top-10-kompyuternikh-virusiv-v-istori-chastina-2 (дата звернення: 21.10.2019).

*Одержано 22.10.2019*