PROTECTION OF INFORMATION IN NETWORKS

Hrynyk Yuliya,Vysochanska Bozhena, Golovatyi Roman
Lviv State University of Life Safety

Останнім часом все більш актуальною стає проблема захисту інформації. Чим більше комп'ютеризуються різні сфери нашого життя, тим більше стає областей можливого проникнення зловмисників, конкурентів і просто комп'ютерних хуліганів. Для протидії зовнішнім атакам необхідно не тільки мати засоби захисту інформації, а й розуміти принципи їх функціонування, вміти правильно їх налаштувати, розуміти слабкі місця операційних систем.

Recently, the problem of information security has become increasingly relevant. The more computerized different areas of our lives, the more areas of possible intrusion of intruders, competitors, and just computer bullies. To counteract external attacks, it is necessary not only to have information security tools, but also to understand the principles of their functioning, to be able to configure them correctly, to understand the weaknesses of operating systems.

Ключові слова: захист інформації, комп'ютерні мережі.
Keywords: protection of information in networks

As general observations computers become better understood and more economical, every day brings new applications. Many of these new applications involve both storing information and simultaneous use by several individuals. The key concern in this paper is multiple use [1, 2].

For those applications in which all users should not have identical authority, some scheme is needed to ensure that the computer system implements the desired authority structure.

There are a variety of specialized techniques and types of network security you will want to roll out. Cisco, a networking infrastructure company, uses the following schema to break down the different types of network security, and while some of it is informed by their product categories, it's a useful way to think about the different ways to secure a network. Here they are [3]:

- Access control: You should be able to block unauthorized users and devices from accessing your network. Users that are permitted network access should only be able to work with the limited set of resources for which they've been authorized.
- Anti-malware: Viruses, worms, and trojans by definition attempt to spread across a network, and can lurk dormant on infected machines for days or weeks. Your security effort should do its best to prevent initial infection and also root out malware that does make its way onto your network.
- Application security: Insecure applications are often the vectors by which attackers get access to your network. You need to employ hardware, software, and security processes to lock those apps down.
- Behavioral analytics: You should know what normal network behavior looks like so that you can spot anomalies or breaches as they happen.
- Data loss prevention: Human beings are inevitably the weakest security link. You need to implement technologies and processes to ensure that staffers don't deliberately or inadvertently send sensitive data outside the network.
- Firewalls: Perhaps the granddaddy of the network security world, they follow the rules you define to permit or deny traffic at the border between your network and the internet, establishing a barrier between your trusted zone and the wild west outside. They don't preclude the need for a defense-in-depth strategy, but they're still a must-have.
- VPN: A tool (typically based on IPsec or SSL) that authenticates the communication between a device and a secure network, creating a secure, encrypted "tunnel" across the open internet.
- Web security: You need to be able to control internal staff's web use in order to block web-based threats from using browsers as a vector to infect your network. And others network security methods.

In reviewing the extent to which protection mechanisms are systematically understood (which is not a large extent) and the current state of the art [4, 5]. As in the case of all programming systems,

it will be necessary for protection systems to be used and analyzed and for their users to propose different, better views of the necessary and sufficient semantics to support information protection.

Finally, one may wish to extend dynamically the range of objects protected [6, 7]. Such a goal might be reached by making the type field large enough to contain an additional unique identifier, and allowing for software interpretation of the access to typed objects. This observation brings us to the subject of user-programmed controls on sharing and the implementation of protected objects and protected subsystems. We shall not attempt to examine this topic in depth, but rather only enough to learn what problems are encountered.

Reference:

1. Fruhlinger J. What is network security? Definition, methods, jobs & salaries [Електронний ресурс] / Josh Fruhlinger // CSOonline. – 2018. – Режим доступу до ресурсу: https://www.csoonline.com/article/3285651/what-is-network-security-definition-methods-jobs-and-salaries.html.
2. Зачко О. Б. Імітаційне моделювання потоку відвідувачів торгово-розважального центру / О. Б. Зачко, Р. Р. Головатий // Управління проектами: стан та перспективи: матер. XII міжнар. наук.-прак. конф. – Миколаїв: МНУК, 2016 - С. 96 – 98.
3. Jerome S. the protection of information in computer systems [Електронний ресурс] / Saltzer Jerome. – 1975. – Режим доступу до ресурсу: http://web.cs.wpi.edu/~guttman/cs557_website/papers/saltzer1975.pdf.
4. Зачко О. Б. Управління безпекою на стадії планування проектів з масовим перебуванням людей з врахуванням категорії складності / О. Б. Зачко, Д. С. Кобилкін, Р. Р. Головатий // Вісник НТУ «ХПІ». Серія: Стратегічне управління, управління портфелями, програмами та проектами. – Х. : НТУ «ХПІ», 2018. – № 2 (1278). – С. 53–58. – Бібліогр.: 17 назв. – ISSN 2311–4738.
5. Купчак М. І., Смотр О. О., Купчак М. Я. Тенденції та проблеми впровадження інформаційних технологій в управління підрозділами університету. Вісник Львівського державного університету безпеки життєдіяльності. 2013. № 7. С. 28–32.
6. Рак Ю. П. Формування проектів методом візуалізації інформації для підвищення стану безпеки торгово-розважальних центрів / 123 Ю. П. Рак, Р. Р. Головатий // Управління проектами у розвитку суспільства: зб. тез доповідей XII Міжнар. конф. – Київ: КНУБА, 2015. – С. 226 – 228
7. Рак Ю. П., Головатий Р. Р. Сервісна модель проектів створення об’єктів з масовим перебуванням людей. Управління проектами у розвитку суспільства: зб. тез доповідей XIII Міжнар. конф. Київ: КНУБА, 2016. С. 207 – 208.