УДК 004.056.57

Івчук Д.О.

Забезпечення захисту інформаційної системи підприємства з віддаленим доступом на основі технології VPN та протоколу SSTP

Вінницький національний технічний університет

Анотація

Дана робота присвячена вивченню та аналізу існуючих методів захисту інформаційних систем, а також розробці способу віддаленого доступу до інформаційної системи підприємства. Новизна даного способу захисту полягає у використанні власноруч сформованих сертифікатів SSTP та системи перевірки їх приналежності .

Ключові слова: інформаційна система, віддалений доступ, безпека інформаційних і комунікаційних систем, комутатор, локальна мережа, глобальна мережа.

Abstract

This work is devoted to the study and analysis of existing methods for the protection of information systems, as well as the development of a way of remote access to the enterprise information system. The novelty of this method of protection is the use of self-generated SSTP certificates and systems for verifying their belongings.

Keywords: information system, remote access, security of information and communication systems, switch, local area network, global network.

Вступ

Щороку у світі стає все більше і більше компаній, які турбуються про власну інформаційну безпеку. Це зумовлено автоматизацією усіх виробничих та бізнес-процесів. Так як більшість підприємств/компаній мають територіально віддалені підрозділи, постає питання про об’єднання їх у єдину інформаційну систему.

У даній роботі розглядається розробка інформаційної системи підприємства, до якої буде відбуватись віддалене підключення працівників за допомогою технології VPN.

Основна частина

У роботі розглянуто різновиди атак на комп’ютерні системи, їх класифікацію та ступені загроз. Також, розглянуто способи віддаленого підключення до інформаційних систем, дано оцінку їх швидкодії та захищеності. Поставлено задачу створення захищеної інформаційної системи з віддаленим доступом на основі технології VPN на основі персонально сформованого протоколу SSTP для користувача.

Було розглянуто загрози інформаційній системі як в середині локальної мережі так і з глобальної мережі. Під час аналізу загроз було виявлено що одну з найбільших загроз несуть зловмисники, які під виглядом користувача цієї системи намагаються заволодіти або пошкодити інформацію підприємства.

Для того щоб запобігти несанкціонованому доступу з боку зловмисника та зробити віддалений доступ більш безпечним було розроблено модель локальної мережі підприємства. Налаштовано адресацію, комутацію та firewall на мережевому обладнанні.

Також розроблено програмне забезпечення для формування SSTP-протоколів.

Результати та висновки

Мережа даної інформаційної системи була емульована у програмному середовищі GNS3, де й було проведено налаштування мережевого обладнання.

Програмний додаток формування SSTP-протоколів було розроблено у середовищі Visual Studio 2016 за допомогою мови програмування C# та розроблено його графічний інтерфейс.

Список використаної літератури

1. Sukhov, A.M. Active flows in diagnostic of troubleshooting on backbone links / A.A. Galtsev, A.M.Sukhov, D.I. Sidelnikov, A.P. Platonov, M.V. Strizhov // Journal of High Speed Networks . – 2011. – Vol. 18. – №. 1. – P. 69-81.
2. Котенко И.В., Степашкин М.В., Дойникова Е.В. Анализ защищенности автоматизированных систем с учетом социоинженерных атак // Проблемы информационной безопасности. Компьютерные системы. 2011 – №3 – С.40–57.
3. Mahammad-oglu Alguliev Rasim, Irada Yavar-kizi Alakbarova Порівняльний аналіз інформаційних атак в інтернеті / Інформаційні технології та комп'ютерна інженерія – Вінниця: Видавництво Вінницького національного технічного університету, 2010. – Том 3 – № 19. https://vxheaven.org/lib/pdf/Signature%20Generation%20and%20Detection%20of%20Malware%20Families.pdf
4. Новіков О. М. Безпека Інформаційно-Комунікаційних Систем / О. М. Новіков, М. В. Грайворонський. – Київ: BHV, 2009. – 608 с. – (Підручник).
5. Sun H. API Monitoring System for Defeating Worms and Exploits in MS-Windows System/ H. Sun, Y. Lin, M. Wu. – Hsinchu Taiwan: Department of Computer Science National Tsing-Hua University, 2006. – 4058 с.
6. Analysis of Computer Intrusions Using Sequences of Function Calls [Електронний ресурс]/ P.Sean, B. Matt, K. Sidney, M. Keith. – 2007. – Режим доступу до ресурсу: http://web.cs.ucdavis.edu/~peisert/research/PBKM-IEEETDSC-FunctionCalls.pdf

Івчук Дмитро Олегович – студента групи УБ-14б, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: fm.ub14.ivchuk@gmail.com

Науковий керівник: ***Карпінець Василь Васильович*** - кандидат технічних наук, доцент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця.

Ivchuk Dmytro Olehovich - student of UB-14b group, faculty of management and information security, Vinnytsia national technical university, Vinnytsia, e-mail: fm.ub14.ivchuk@gmail.com

Supervisor: ***Karpinets Vasyl Vasylovych*** - candidate of technichal Sciences, associate Professor of management and security of information systems, Vinnytsia national technical University, Vinnytsia.