УДК 338.47:67.012.8

Олексій Ананченко
(аспірант факультету транспортних та інноваційних технологій, Національний транспортний університет)

ПИТАННЯ БЕЗПЕКИ ПРИ ВИКОРИСТАННІ РЕСУРСІВ КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

З кожним роком в економіці України розширюються масштаби використання комп'ютерних мереж, зростає кількість інформації, що вимагає надійного захисту. Поряд з цим зростає кількість загроз порушення мережевої безпеки, що можуть виражатись в розповсюдженні шкідливого програмного забезпечення, розсилки фішингових повідомлень електронною поштою, ураження мережевої інфраструктури і знищення важливих файлів, зламування ключових серверів тощо. В статті конкретизовано розгляд питань безпеки при використанні ресурсів корпоративних інформаційних систем. В роботі уточнюється і уніфікується понятійний апарат для удосконалення або розробки нормативних документів стосовно заходів і засобів забезпечення безпеки корпоративних інформаційних систем, наведено приклади розробки паролів до них тощо.

Ключові слова: *комп'ютерні мережі, паролі, системи виявлення вторгнень, системи запобігання вторгнень, Internet.*

Алексей Ананченко
(аспирант факультета транспортных и инновационных технологий, Национальный транспортный университет)

ВОПРОСЫ БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ РЕСУРСОВ КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

С каждым годом в экономике Украины расширяются масштабы использования компьютерных сетей, возрастает количество информации, требующей надежной защиты. Вместе с тем, возрастает количество угроз нарушения сетевой безопасности, что может выражаться в распространении вредоносного программного обеспечения, рассылки фишинговых сообщений электронной почтой, повреждения сетевой структуры, уничтожения важных файлов, взламывания серверов и т.д.

В статье конкретизировано рассмотрение вопросов безопасности при использовании ресурсов корпоративных информационных систем. В работе уточняется и унифицируется понятийный аппарат для усовершенствования или разработки нормативных документов для мер и средств обеспечения безопасности корпоративных информационных систем, приведены примеры разработки паролей к ним.

Ключевые слова: *компьютерные сети, пароли, системы выявления вторжений, системы предупреждения вторжений, Internet.*

Oleksii Ananchenko
(graduate student of faculty of transport and innovative technologies, National Transport University)

SECURITY ISSUES WHEN USING RESOURCES OF CORPORATE INFORMATION SYSTEMS

Every year, the scale of the computer networks usage expands in the economy of Ukraine, the amount of information that needs protection increases. At the same time, the number of threats to network security is increasing, which can be expressed in the spread of malicious software, phishing e-mail messages sendings, damage to the network structure and the destruction of important files, hacking servers, etc. The article concretizes consideration of safety issues when using resources of corporate information systems. The work clarifies and unifies conceptual apparatus for the improvement or development of regulatory documents for the measures and means to ensure the security of corporate information systems, examples of password development for them are given.

Keywords: *computer networks, passwords, intrusion detection systems, intrusion prevention systems, Internet.*

Постановка проблеми. Недавній вступ України до Світової організації торгівлі офіційно закріпив статус нашої держави з ринковою економікою, що характеризується високим рівнем корпоратизації. В загальному вигляді корпоратизація державної власності – це процес трансформації частки державної власності в акціонерну (колективну) власність і формування на цій основі корпоративного сектору в економіці, зокрема в галузях транспорту і зв'язку. Таким прикладом може слугувати приватизація «Укртелеком». А з 21 жовтня 2015 року Державна адміністрація залізничного транспорту України (Укрзалізниця) законодавчими актами парламенту і уряду трансформувалась у Публічне акціонерне товариство (ПАТ) «Українська Залізниця» із стопроцентним володінням акціями ПАТ державою. Ця подія знаменувала собою фактичне завершення довготривалого процесу корпоратизації залізничної галузі. Створюються вертикально інтегровані філії управління, що об'єктивно вимагає модернізації і посилення корпоративних інформаційних систем, питань безпеки при використанні ресурсів корпоративних інформаційних систем, удосконалення або й розробки внутрішніх нормативних документів стосовно захисту баз даних та інше.

Аналіз останніх досліджень і публікацій. Проблеми інформаційної безпеки, захисту інформації в корпоративних інформаційних системах, попередження несанкціонованого доступу і витоку конфіденційної інформації та іншими питаннями цього напрямку досліджень займаються відомі вчені та фахівці – В. Данчук, В. Кабанов, С. Лістровий, Ю. Лемешко, О. Мельниченко, С. Моцний, С. Приходько, Ю. Тесля і багато інших. В травні 2015 року опубліковано збірник доповідей та тез науково-практичної конференції «Інформаційна безпека України», що була проведена в березні цього року Київським університетом імені Т.Г. Шевченка. Чимало матеріалів стосовно безпеки інформаційного простору викладено на інтернет сайті за результатами парламентських слухань на тему «Реформи галузі інформаційно-комунікаційних технологій та розвиток інформаційного простору України», що відбулися 3 лютого 2016 року в сесійній залі Верховної Ради України. Все це побічно підтверджує актуальність даної статті.

Мета статті. Уточнення та уніфікація понятійного апарату, що може дозволити ідентично удосконалювати та розробляти нормативні документи інформаційної безпеки при використанні ресурсів корпоративних інформаційних систем будь-якого підприємства.

Виклад основного матеріалу дослідження. В загальному вигляді безпека – це стан захищеності певного об'єкта або суб'єкта від різних загроз та наявність комплексу відповідних заходів і технічних засобів для попередження або усунення таких загроз.

Керівництво кожного підприємства повинно визначити основні принципи безпечного використання користувачами ресурсів корпоративної інформаційної системи (КІС). Необхідно мати для користування офіційно затверджений документ, в якому формалізовано вимоги до забезпечення безпеки ресурсів КІС та встановлено відповідальність і сферу застосування в роботі окремих підрозділів і посадових осіб. Цей документ може мати назву «Стандарт», «Інструкція», «Політика», але в ньому мають мати місце найменування та визначення термінів, скорочень та їх розшифрування, посилання на окремі законодавчі та відомчі нормативні акти тощо.

На сьогодні законодавче забезпечення інформаційних систем та мереж телекомунікацій опирається на Закони України «Про інформацію» від 02.10.1992 №2657-XII, «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 №80/94-ВР, «Про телекомунікації» від 18.11.2003 №1280-IV, «Про захист персональних даних» від 01.06.2010 №2297-VI тощо.

Проте, як показують матеріали та рекомендації парламентських слухань, проведених 3 лютого 2016 р. в сесійній залі Верховної Ради України на тему «Реформи галузі інформаційно-комунікаційних технологій та розвиток інформаційного простору України», удосконалення законодавчої бази має актуальне значення і зараз.

Звичайно, визначення термінів та їх скорочень на підприємствах можуть різнитися, але наводимо загальновживані в нормативних документах терміни, скорочення та їх розшифровку, що фактично мають уніфікований характер. Це в першу чергу: інформаційні технології – ІТ, персональний комп'ютер – ПК, інформаційна система – ІС, локальна обчислювальна мережа – ЛОМ, електронна обчислювальна машина – ОЕМ, кишеньковий персональний комп'ютер – КПК тощо. Особа, що отримала відповідно до затвердженого порядку на підприємстві, доступ до ресурсів корпоративної інформаційної системи ідентифікується як «користувач», а до «юридичної особи», з якою у підприємства існують якісь договірні відносини, варто застосовувати термін «стороння організація». До запису, що містить відомості, які

інформаційний сервіс повідомляє про себе певній комп'ютерній системі для проходження процесу ідентифікації, аутентифікації та авторизації, доцільно застосовувати термін «технологічний обліковий запис». Якщо підприємство потужне, має достатній технічний, технологічний та інтелектуальний потенціал, то централізована система, що використовується для управління даними користувачів та для синхронізації між декількома сховищами інформації, які використовуються для зберігання параметрів та ідентифікованої інформації, може мати термін «Identity Manager» або скорочено ІДМ. Для забезпечення інформаційної безпеки КІС встановлюється жорсткий порядок. Так, зокрема всі користувачі при отриманні першого доступу до ресурсів корпоративної інформаційної системи, повинні попередньо ознайомитись з нормативними документами і кожен несе персональну відповідальність за свої дії при роботі з програмними та технічними засобами КІС. При цьому кожному користувачу, допущеному до роботи з конкретною підсистемою або програмою КІС, призначається персональне унікальне ім'я (обліковий запис користувача, що формується системою ІДМ). Одночасно забороняється використовувати з будь-якою метою чужий обліковий запис, передавати будь-кому свої облікові дані (ім'я користувача і пароль), а також засоби аутентифікації. Користувачам також забороняється використовувати технологічні облікові записи для проходження процесів ідентифікації, аутентифікації та авторизації без отримання тимчасового дозволу в системі документообігу, погодженого відповідальною особою. Ресурси КІС надаються користувачу для здійснення ним своїх функціональних обов'язків, пов'язаних з виробничою діяльністю.

Інформація, що циркулює в КІС, створювана і збережена в інформаційних системах, вважається власністю певного підприємства, компанії, акціонерного товариства, які залишають за собою право контролювати дії працівників при обробці інформації в КІС, використання корпоративної пошти та мережі Internet. Користувачі зобов'язуються не розголошувати інформацію про процедури і технічну реалізацію захисту інформації в корпоративних інформаційних системах.

Для попередження несанкціонованого доступу до ресурсів корпоративних інформаційних систем використовуються паролі та апаратні засоби аутентифікації, що зобов'язані забезпечити безпечне зберігання даних, що виключає їх втрату або розголошення. В загальному вигляді варто замінювати паролі з періодичністю приблизно 90 днів, причому нове його значення повинно відрізнятись в декількох позиціях. Створюючи пароль, користувачі повинні дотримуватися певних вимог стосовно інформаційної безпеки, не повідомляти нікому свій пароль для доступу до інформаційних ресурсів КІС.

Бажано, щоб користувач, створюючи свій пароль притримувався певних правил безпеки. Наприклад, він повинен складатись не менше ніж з восьми позицій і не повинен бути таким який можна легко вгадати. Так, пароль не повинен включати повторення послідовності будь-яких символів, приміром «111111», «ааааaа», «12345», «qwerty» або якісь інші легкі символи (імена, прізвища, найменування, дати народження, а також загальновживані скорочення, типу ЕОМ, ЛОМ, КПК). Щоб пароль ефективно виконував свою функцію захисту інформації від несанкціонованого доступу, користувачам доцільно використовувати символи із числа наступних чотирьох категорій:

- Прописні букви англійського алфавіту від A до Z;
- Строчні (рядкові) букви англійського алфавіту від a до z;
- Десятичні цифри від 0 до 9;

- Неалфавітні символи, зокрема $, %, #, !

В сучасних умовах практично всі підприємства, компанії та акціонерні товариства використовують електронну пошту та Інтернет. З метою захисту інформації виокремлено низку вимог. Так, дозволяється використовувати корпоративну електронну пошту та Інтернет виключно для виконання своїх службових обов'язків. Забороняється відправляти поштові повідомлення або відвідувати ресурси Інтернет, де є матеріали протизаконного, ворожого та неетичного характеру. Забороняється самостійно налагоджувати і включати автоматизоване пересилання повідомлень корпоративної електронної пошти на зовнішні адреси електронної пошти.

Для уникнення непорозумінь та витоку інформації забороняється:

- Несанкціоноване розміщення інформації в Інтернет;
- Здійснювати тунелювання мережевого трафіку при зверненні до ресурсів мережі Інтернет через корпоративні проксі-сервери;
- Несанкціоноване використання систем миттєвого обміну інформацією;
- Несанкціоновано завантажувати програми з мережі Інтернет і запускати їх.

І насамкінець про дії персоналу в нестандартних, а іноді і в форс-мажорних ситуаціях. Відповідальні особи за безпеку корпоративних інформаційних систем зобов'язані постійно працювати з персоналом, навчати їх діям у випадках виникнення наступних подій:

- Розголошенню облікових даних, втрат, крадіжки засобів аутентифікації;
- Несанкціонованих змін в конфігурації програмних та апаратних засобів;
- Фактів здійснення спроб несанкціонованого доступу до ресурсів корпоративної інформаційної системи;
- Фактів втрат, крадіжок комп'ютерів або інших носіїв інформації, особливо, якщо вони мали інформацію обмеженого доступу.

Взагалі в будь-яких випадках, коли на думку користувачів або причетного персоналу виникають ризику порушення безпеки інформації, необхідно вживати всіх заходів, передбачених законодавством та відомчими нормативними документами.

Висновки і пропозиції. В матеріалі статті розглянуто питання безпеки при використанні ресурсів корпоративних інформаційних систем. В роботі уточнюється і уніфікується понятійний апарат для удосконалення або розробки нормативних документів стосовно заходів та засобів забезпечення інформаційної безпеки корпоративних інформаційних систем. Встановлено, що в першу чергу захисту потребує інформація, що зберігається та обробляється в КІС; відомості про передані повідомлення в мережах електрозв'язку; програмне забезпечення КІС; засоби зв'язку; інформаційні та телекомунікаційні сервіси, а також працюючий персонал.

ЛІТЕРАТУРА

1. *Лістровий С.В.* Підходи до запобігання загроз у комп'ютерних мережах на основі рішення задачі про найменше покриття /Лістровий С.В., Моцний С.В. // Інформаційно-керуючі системи на залізничному транспорті. – 2013. – Харків. – С. 31-35.

2. *Данчук В.Д.* Удосконалення методів забезпечення інформаційної безпеки корпоративних інформаційних систем / Данчук В.Д., Ананченко В.Є., Ананченко О.Є. // Збірник наукових доповідей та тез науково-технічної конференції «Інформаційна безпека України» Київського національного університету ім. Т.Шевченка 12-13 березня 2015. – Київ. – С. 96-97.

3. *Приходько С.І.* Напрямки проведення інформаційно-технологічної реформи телекомунікаційної мережі Укрзалізниці / Приходько С.І., Калабухін Ю.Є., Жученко О.С., Волков О.С. // Інформаційно-керуючі системи на залізничному транспорті. – 2013. – Харків. – С. 52-55.

4. *Брягин О.В.* Безопасность вашего бизнеса. Системный подход. Аналитические материалы, практические рекомендации. – К.: КНТ, 2006. – 228 с.

5. Офіційний веб-портал Верховної Ради України [Електронний ресурс] – Режим доступу. http://zakon.rada.gov.ua

REFERENCES

1. Listrovoy S.V. Threat Prevention Techniques Used in Computer Networks Based on the Solution of a Minimum Cover Problem / Listrovoy S.V., Motsnyi S.V.// Inforamcijno-keruuci sistemi na zaliznicnomu transporti. – 2013. – Kharkiv. – PP. 31-35.

2. Danchuk V.D. Udoskonalennya metodiv zabezpechennya informaciynoi bezpeki korporativnih informaciinih system./Danchuk V.D., Ananchenko V.E., Ananchenko O.E.//Zbirnik naykovih dopovidei ta tez naykovo-tehnishnoi konferencii «Informaciina bezpeka Ukraini» Kiivskogo nacionalnogo universitetu im.T.Shevchenka 12-13 bereznya 2015.- Kyiv. – P. 96-97.

3. Prihodko S.I. Directions for the development of information technology reform of Ukrzaliznytsya telecommunications network/ Prihodko S.I., Kalabukhin Yu.Ye., Zhuchenko O.S., Volkov O.S.// Inforamcijno-keruuci sistemi na zaliznicnomu transporti. – 2013.– Kharkiv. – PP. 52-55.

4. Bryagin O.V. Bezopasnost vashego biznesa.Sistemni podhod.Analiticheskie materiali, prakticheskie rekomendacii. – K.: KNT, 2006. – 228 p.

5. Ofitsiynyy veb-portal Verkhovnoyi Rady Ukrayiny [Official Web Portal of the Verkhovna Rada of Ukraine]. Available at: http://zakon.rada.gov.ua.