УДК 004.4:656.2(477)

ЩОДО НЕОБХІДНОСТІ ВПРОВАДЖЕННЯ СИСТЕМИ КОМПЛЕКСНОГО ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ ПІДПРИЄМСТВ ТА УСТАНОВ ЗАЛІЗНИЧНОГО ТРАНСПОРТУ

Чередниченко О.Ю., к.е.н., доцент (УкрДАЗТ)

В статті розглядається необхідність впровадження на залізничному транспорті комплексної системи захисту інформаційних ресурсів, роль та місце Головного управління інформаційних технологій «Укрзалізниці» як організуючого та координуючого органу щодо вирішення питань роботи інформаційно-телекомунікаційних систем на залізничному транспорті, надаються рекомендації щодо покращення функціонування відомчої системи захисту інформаційних ресурсів.

Ключові слова: захист інформаційних ресурсів, комплексна система захисту технічної інформації, локальні системи, комп'ютерні ситеми, зловмисні дії.

Постановка проблеми. Залізничний транспорт в Україні має стратегічне значення для держави та на цей час зберігає провідну роль у перевезеннях пасажирів та вантажів. Обсяг перевезень сталевими магістралями в загальній транспортній системі країни становить майже 80% вантажообігу й близько 40% пасажирообороту. Україна входить до світової десятки країн з інтенсивності перевезення вантажів та пасажирів.

Залізнична транспортна система загального користування, без урахування промислового залізничного транспорту, сягає 30,3 тис. кілометрів колії, вантажний вагонний парк налічує 174939 вагонів, для вантажних операцій відкрито 1684 станції. На залізницях держави знаходиться значна кількість товарних вагонів та вантажів, які є власністю інших країн. Обслуговування пасажирів здійснюється на 126 вокзалах, 1684 станціях. Щодобово у русі знаходиться 8429 пасажирських вагонів «Укрзалізниці» та 368 вагонів іноземних країн, а загальний контингент працюючих сягає 300 тис. чоловік. [4]. В останній час на залізницях України широке розповсюдження знаходить використання електронних документів та здійснення електронного документообігу. Тому для збереження вказаних позицій в транспортній системі як країни так і Європейському співтоваристві «Укрзалізниця» повинна постійно працювати над стратегією подальшого розвитку своїх підприємств та установ, впроваджувати нові технології та розробки в області залізничного транспорту, активно займатися комп'ютерізацією, автоматизацією робочих місць, підгалузей та інформаційних ресурсів залізниць і їх захистом. Нині на залізницях вже сформована певна модель ІТ-супроводження майже всіх виробничих процесів[5].

Захист інформації здійснюється у відповідності до діючої нормативно-правової бази України. До цієї бази відносяться: закони України, Укази Президента України, Постанови Кабінету Міністрів, накази Служби безпеки України, нормативні документи з криптографічного та технічного захисту інформації, національні стандарти в галузі захисту інформації, міжнародні та регіональні стандарти в сфері захисту інформації. Однак існуюча в Україні нормативна база ще не досягла необхідного розвитку в даній області.

Аналіз останніх досліджень та виділення невирішених частин загальної проблеми.. Питанням забезпечення економічної безпеки залізничного транспорту її окремих складових присвячені роботи таких вітчизняних вчених як: Ейтутіс Г., Іскарова Н., Кожевников Р., Новікова А., Плєтникова І. , Тимофєєва Т., Шевченко І., Шемаєва Л., Шинкаренко В.Г. та ін.[6-12]. Однак, в сучасних умовах розвитку залізничного транспорту виникає необхідність визначення доцільності впровадження комплексної системи захисту інформаційних ресурсів; ролі та місця Головного управління інформаційних технологій «Укрзалізниці» як організуючого та координуючого органу щодо вирішення вказаних питань в системі залізничного транспорту.

Мета дослідження - звернути увагу фахівців щодо необхідності впровадженя відомчої діючої системи захисту інформаційних ресурсів відповідно до вимог Державної служби спеціального зв'язку та захисту інформації (ДССЗЗІ).

Виклад основного матеріалу. Під безпекою електронної системи розуміють її здатність протидіяти спробам нанести збитки власникам та користувачам систем при появі різноманітних збуджуючих (навмисних і ненавмисних) впливів на неї. Як правило, розрізняють внутрішню і зовнішню безпеку. Згідно з установленими нормами міжнародної практики безпеки, об'єктами захисту з урахуванням їх пріоритетів є матеріальні та інформаційні цінності[13].

Лише за останні роки в «Укрзалізниці» активно впроваджуються автоматизовані системи в рамках прийнятих програм, основними серед яких є:

- програма автоматизації пасажирського господарства на 2011—2012 рр.;

- комплексна програма переходу на продаж електронних проїзних документів у внутрішньому сполученні;
- програма подальшого розвитку автоматизації кадрової роботи на 2011—2012 рр.;
- комплексна програма автоматизації процесів матеріальнотехнічного забезпечення залізничної галузі України (АСК МТЗ УЗ);
- програма розвитку та супроводу автоматизованої системи бухгалтерського обліку АСБО «ФОБОС» і т.інш.

Проводячи аналіз стану інформаційної безпеки різних відомств, організацій та фірм, можна прийти до висновку, що об'єктом захисту, який викликає найбільше занепокоєння і акумулює всі проблеми інформаційної безпеки є інформаційно-телекомунікаційні системи (ІТС), що будуються на базі комп'ютерів. Аналіз підтверджує, що з кожним роком кількість комп'ютерних атак, що здійснюють зловмисники суттєво збільшилась. Велику загрозу складають "хакери-мафіозі". Єдина мета цих хакерів - отримання прибутку. На їх долю приходиться 10 % зловмисних дій. За оцінками експертів США, напади «хакерів» на комп'ютери і мережі федеральних державних систем відбуваються в цій країні не рідше 50-ти раз на день[14].

В 2006 р., наказом «Укрзалізниці» від 01.11.2006 № 392-Ц створено Головне управління інформаційних технологій «Укрзалізниці». Створення Головного управління інформаційних технологій «Укрзалізниці» було обумовлено широким використанням не тільки інформаційних технологій у всіх сферах життя суспільства, а і досить актуальною проблему захисту інформації, її користувачів, інформаційних ресурсів, каналів передачі даних від злочинних зазіхань зловмисників[5].

Згідно вимог закону, вся інформація, що є власністю держави, або інформація з обмеженим доступом, повинна оброблятися в системі із застосуванням комплексного системи захисту інформації з підтвердженою відповідністю. Підтвердження відповідно здійснюється за результатами державної експертизи в порядку, логічних законодавством. Під обробкою інформації в системі розуміється виконання однієї або кількох операцій, зокрема: збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрація, приймання, отримання, передавання, які здійснюються в системі за допомогою технічних і програмних засобів. При цьому обмін інформацією здійснюється з використанням інформаційно-телекомунікаційних систем як внутрішнього так і загального користування, в тому числі при підключенні до міжнародних інформаційно-телекомунікаційних систем через глобальну світову інформаційну інфраструктуру.

Згідно закону України «Про захист інформації в інформаційно-телекомунікаційних системах»:

* інформація, що є власністю держави або інформація з обмеженим доступ, повинна бути захищена шляхом побудови КСЗІ з отриманням «Атестата відповідно-наслідком», який видається ДССЗЗІ;

* інша інформація може бути захищена за допомогою КСЗІ за бажанням власника. Необхідність побудови КСЗІ визначається вимогою нормативних документів або бажанням власника інформаційних ресурсів.

Комплексний підхід, як правило, використовується для захисту великих систем, саме такі системи впроваджуються на залізничному транспорті. В цьому випадку необхідно забезпечити виконання наступних заходів:

- організаційні заходи по контролю за персоналом, який має високий рівень повноважень на дії в системі (за програмістами, адміністраторами баз даних мережі і т.д.);
- організаційні та технічні заходи по резервуванню критично важливої інформації;
- організаційні заходи по відновленню працездатності системи у випадку виникнення нештатних ситуацій;
- організаційні та технічні заходи по управлінню доступом в приміщеннях, в яких знаходиться обчислювальна техніка;
- організаційні та технічні заходи по фізичному захисту приміщень, в яких знаходиться обчислювальна техніка і носії даних, від стихійних лих, масових безпорядків і т.д.

Виконання цієї роботи на залізничному транспорті покладено на фахівців Головного управління інформаційних технологій «Укрзалізниці» та Інформаційно-обчислювальних центрів (ІОЦ) на залізницях. Нині в системі залізничного транспорту існує трьохрівнева система: Головне управління інформаційних технологій, ІОЦ, користувачі. Тобто існуюча вертикальна система забезпечує реалізацію єдиної політики дій в цьому напрямку, єдиних стандартів, норм і вимог. В той же час вона не дозволяє, насамперед із-за браку коштів, самостійно на залізницях реалізовувати заходи з впровадження системи копмлесконого захисту інформаційних ресурсів, ефективно протистояти від нападів «хакерів» на комп'ютери і мережі.

Так, в грудні 2012 року правоохоронними органами було виявлено та задокументовано факт несанкціонованого втручання в роботу офіційних веб-сайтів санаторію Південної залізниці «Мрія», Дорожнього фізкультурно-спортивного клубу «Локомотив» та Інформаційно-обчислювального центру з боку турецького «хакерського» угрупування. При цьому, несанкціоноване втручання в комп'ютерну мережу було реалізовано шляхом використання критичних вразливостей систем

управління змістом (Content management system) зазначених Інтернет-ресурсів, із подальшим розміщенням шкідливих програмних засобів (скриптів). Зазначене втручання стало можливим внаслідок порушень окремими посадовими особами, відповідальними за стан захисту інформації, обов'язкових норм НД ТЗІ 2.5-010-03 «Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу», затвердженого наказом ДСТСЗІ СБ України та пов'язане з відсутністю впроваджених на вказаних інформаційних ресурсах комплексної системи захисту інформації, сертифікованої Державною службою спеціального зв'язку та захисту інформації[5].

Висновки. Реформування залізничного транспорту передбачає розподіл функцій державного управління, що передаються Міністерству транспорту та зв'язку України, і господарського управління залізничним транспортом, що передаються господарюючому суб'єктові – Державній акціонерній компанії ПАТ "Українські залізниці", збереження державного контролю за діяльністю залізничного транспорту, відокремлення у системі залізничного транспорту природно-монопольного і конкурентного секторів, здійснення повного розмежування управлінням інфраструктурою і перевезеннями, створення конкурентного середовища на ринку перевезень, ремонтних та інших послуг.

Бурхливе зростання конфіденційної і комерційної інформації, а також істотне збільшення фактів її розкрадання викликає підвищений інтерес все більшого числа організацій до створення власних захищених інформаційних систем. Проектування захищених інформаційних систем процес досить складний, який припускає наявність відповідних знань і досвіду, у її творців. Залізнична галузь має певний досвід та напрацювання щодо захисту власних інформаційних ресурсів, має підготовлені кадри та взмозі фінансувати роботи з захисту інформаційних ресурсів. Тому, важливо, особливо в період реструктуризації галузі, не тільки зберегти існуючу систему, а й не відставати щодо впровадження від новітніх світових технологій в цьому напрямку.

З метою попередження несанкціонованих втручань в роботу інформаційних ресурсів залізничного транспорту, наслідками яких може бути завдання шкоди стабільному функціонуванню стратегічно-важливого підприємства держави, необхідно суворо дотримуватися порядку функціонування вищевказаних інформаційних ресурсів у відповідність нормативним документам з технічного захисту інформації, забезпечити обов'язкове впровадження комплексної системи захисту інформації для зазначених ресурсів.

Вирішення цих питань необхідно враховувати при створенні нової ситеми залізничного транспорту (створення на базі «Укрзалізниці» принципово нової моделі у вигляді ПАТ).

СПИСОК ЛІТЕРАТУРИ

1. Про залізничний транспорт : Закон України від 4 липня 1996 р. № 273/96-ВР // Відомості Верховної Ради України. – 1996. – № 40.
2. Розпорядження Кабінету Міністрів України від 27 грудня 2006 р. № 651-р "Про схвалення Концепції Державної програми реформування залізничного транспорту" [Електронний ресурс] // Режим доступу : http:// www.zakon1.rada.gov.ua.
3. Наказ ДСТСЗІ СБ України від 02.04.2003 року № 33
4. У полі зору –дирекції / Магістраль. – 2013р. - №11 (1797).
5. «Укрзализниця» побежала впереди паровоза / Тижневик «Коментарі». – 2012р. - № 4 (296).
6. Ейтутіс Г. Оцінка економічної безпеки залізничного транспорту. – Економіст. –2009. - №. – с. 56-59.
7. Іксарова Н.О.Транспорна інфраструктура як компонент економічної безпеки України / Н.О. Іскарова // Економічний простір. –2010. - № 36. Режим доступу до статті:http://www.nbuv.gov.ua/portal/Soc_Gum/Ekpr/2010_36/Zmist/6PDF.pdf.
8. Тимофєєва Т.О. Розробка механізму щодо забезпечення економічної безпеки залізничного транспорту: автореф. дис... канд. екон. наук: 08.00.03 – економіка та управління національним господарством / Т.О. Тимофєєва; Укр. держ. акад. залізн. трансп. — Х., 2009. — 20 с.
9. Шевченко І. Особливості формування економічної безпеки підприємства / І. Шевченко // Наука молода. – 2010. - №10. – С. 178-181.
10. Шемаєва Л.Г. Економічна безпека підприємств у стратегічній взаємодії з суб'єктами зовнішнього середовища: автореф. дис. ... д-ра. екон. наук / Л.Г. Шемаєва. — К., 2010. — 39 с.
11. Шинкаренко В.Г. Економічна безпека автотранспортних підприємств та їхня роль у роботі господарського комплексу України / В.Г. Шинкаренко // Збірник наукових праць НТУ. –2009. Режим доступу до статті: http://www.nbuv.gov.ua/portal/natural/Vntu/2009_19_1/pdf/81.pdf
12. Экономическая безопасность железнодорожного транспорта / Р.А. Кожевников, З.П. Межох, Н.П. Терешина и др.; Под ред. Р.А. Кожевникова, З.П. Межох. – М.: Маршрут, 2005. – 326 с.
13. Баранов В М. Защита информации в системах и средствах информатизации и связи. Учебное пособие. / В.М.Баранов. - СПб.: 1996. -111с.

14. Соколов А.В. Защита от компьютерного терроризма. Справочное пособие./ А.В.Соколов, О.М.Степанюк - СПб.: БХВ - Петербург; Арлит 2002. – 496с.

15. Мельников В.В. Защита информации в компьютерных системах. / В.В.Мельников. - М.: Финансы и статистика. - 1997. - 368с.

Аннотация. В статье рассматривается необходимость внедрения на железнодорожном транспорте комплексной системы защиты информационных ресурсов, роль и место Главного управления информационных технологий «Укрзализныци» как организующего и координирующего органа по решению вопросов работы информационно-телекоммуникационных систем на железнодорожном транспорте, даются рекомендации по улучшению функционирования ведомственной системы защиты информационных ресурсов.

Ключевые слова: защита информационных ресурсов, комплексная система защиты технической информации, локальные системы, компьютерные ситемы, злонамеренные действия.

Summary. In article discusses the need to introduce the railways integrated system of information resources protection, the role and place of the Main Directorate of Information Technology "UZ" as organizing and coordinating body to address issues of information and telecommunication systems on rail transport, recommendations for improving the functioning of the department of security of information resources.

Keywords: protection of information resources, integrated protection system technical information, local systems, computer sitemy, malicious action.

Рецензент *д.е.н., професор УкрДАЗТ Компанієць В.В.*
Експерт редакційної колегії *к.е.н., доцент УкрДАЗТ Токмакова І.В.*

УДК 658.7:656.2

ЗАСТОСУВАННЯ ЛОГІСТИЧНОГО ПІДХОДУ ПРИ ПЛАНУВАННІ РОБОТИ ЗАЛІЗНИЧНОГО ТРАНСПОРТУ

Шевченко А.В., аспірант (УкрДАЗТ)

В статті розглянуто необхідність і можливість корегування оперативного плану роботи підрозділів залізниць та основних показників роботи різних ділянок залізничного транспорту в сфері вантажних перевезень.

Ключові слова: логістика, логістичний підхід, залізничний транспорт, оперативний план.

Постановка проблеми. Безперечно, що ефективне керівництво будь яким підприємством полягає в отриманні найбільш можливої прибутковості, яке дозволяє не тільки балансувати на рівні конкурентоспроможності, але й нарощувати матеріально-технічну базу, завойовувати нові ринки збуту своєї продукції та ін. Залізничний транспорт не є виключенням. Однак на ряду з економічними показниками в роботі підприємств залізниць, широко застосовуються й технічні показники такі як обіг вагонів, вантажообіг, простій вагонів різних категорій, навантаження вивантаження, робота та інші, безумовно важливі і динамічно розкриваючи ефективність роботи підприємств залізниці. На підставі цих показників проводиться оцінка ситуації, розробляється необхідний план дій та виконується аналіз прийнятих рішень по керівництву оперативною роботою. Однак, в ринкових умовах, прийняття рішень в оперативній роботі, завжди пов'язано з економічними витратами, які впливають на загальні економічні показники роботи залізниці та її партнерів (замовників перевезень), і від того наскільки обґрунтованими є дії оперативного керівництва залежить ефективність роботи як окремих підрозділів залізниці, так і всієї системи взагалі. Розглянемо приклад: у другій половині дня 31 грудня на залізничну станцію прибуває декілька вагонів під розвантаження, згідно з порядком прийнятим на залізниці після обов'язкових дій по розкредитуванню вантажу вагони подають під розвантаження, начальник станції приділяє особливу увагу для забезпечення своєчасного вивантаження і передачі порожніх вагонів в регулювання. Вантажоотримувач зобов'язаний вивантажити їх у встановлений термін, або сплатити певні кошти за затримку. У більшості випадків підприємства не утримують штат працівників задіяних на вивантаженні цілодобово і тому перед керівництвом стає питання, яке додаткове фінансове навантаження понести, в одному випадку додаткові перерахування на залізницю, у другому по організації вивантаження у святкові дні. Крім того може виникнути потреба залучення фахівців державних органів митниці, ветеринарної інспекції тощо, і в цьому випадку вивантаження може відкластися на більш тривалий