УДК 004.056
DOI: https://doi.org/10.53920/ITS-2023-2-9

Юрій Валентинович ДЕМЧЕНКО,
старший викладач,
Державний університет інфраструктури та технологій,
Київський інститут залізничного транспорту,
факультет Інфраструктури та рухомого складу залізниць,
кафедра вагонів та вагонного господарства
ORCID ID: 0009-0007-6058-1264

БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ ВАГОННОГО ГОСПОДАРСТВА

Стаття присвячена опрацюванню питань забезпечення інформаційної безпеки вагоноремонтних підприємств, захисту систем зберігання і обробки комп'ютерних даних, при яких зберігається повна конфіденційність, доступність і цілісність всієї наявної інформації. Головною умовою нормальної роботи повинні бути максимальні знання про всі структурні складові та критерії інформаційної безпеки комп'ютерних даних. Так із кожним наступним роком зростає нагальна роль інформаційної безпеки виробничих процесів, оскільки наше суспільство вступило в нову епоху інформаційних війн, де цінність первинної інформації безперечно має пріоритет. Хоча навіть проста інформація – це не тільки товар, а й значний інструмент для маніпуляції, порушення технологічних процесів, створенню конфліктів, отримання грошової винагороди. Отже, інформаційна безпека – це комплекс захищеності всієї інформації та пов'язаної з нею виробничої інфраструктури, від всіх, як випадкових, так і навмисних дій, внаслідок чого проходить збій у наявній інформації, а також в інфраструктурі підтримки. Метою стороннього проникнення в комп'ютерні мережі підприємства є нанесення шкоди або знищення наявних даних, заволодіння конфіденційною інформацію з можливим подальшим використанням у противоправних цілях.

Ключові слова: *інформаційні системи, інформаційна безпека, сфера обробки інформації, захист, шкідливі програми, конфіденційність, вагонне господарство, антивірусні технології, збитки, заподіяння шкоди, високі технології.*

Yurij ДЕМЧЕНКО
Senior teacher,
State university of infrastructure and technologies
Kyiv institute of railway transport,
faculty of Infrastructure and movable to composition of railways,
department of carriages and carriage economy

SECURITY OF INFORMATION SYSTEMS OF THE CARRIAGE ECONOMY

The article is devoted to the study of the issues of ensuring the information security of railcar repair enterprises, protection of computer data storage and processing systems, which preserve complete confidentiality, availability and integrity of all available information. The main condition for normal operation should be maximum knowledge of all structural components and criteria for information security of computer data. Thus, the role of information security in production processes is growing every year, as our society has entered a new era of information wars, where the value of primary information is undoubtedly of paramount importance. However, even simple information is not only a commodity, but also a significant tool for manipulation, disruption of technological processes, creation of conflicts, and obtaining monetary rewards. Therefore, information security is a security complex of all information and related production infrastructure from all, both accidental and intentional actions, resulting in a failure in the available information and support infrastructure. The purpose of an unauthorized intrusion into an enterprise's computer networks is to damage or destroy existing data, to obtain confidential information with the possible subsequent use for illegal purposes.

Keywords: *information systems, information security, information processing, protection, malware, privacy, railcar industry, anti-virus technologies, losses, damage, high technology.*

Постановка проблеми. У сучасному світі інформаційні системи удосконалюються високими темпами, а інформаційна безпека та політика захисту набувають все більш масштабного характеру, висуваючи цю проблему на перший план. Глобалізація посилюється себе з кожним роком, але окрім позитивних моментів, виникають і дуже серйозні негативні процеси, до яких цивілізований

світ виявився неготовим. Суттєво зросла роль інформаційної безпеки виробничих процесів, оскільки цифрова інформація стала як продуктом, так і сировиною, яку обробляють, виробляють, готують, продають і дуже часто крадуть для отримання прибутку. Нині в основному інформаційну безпеку цифрових технологій визначають через комп'ютерну безпеку. Захист інформації, що знаходиться всередині комп'ютера, є у рази складнішим ніж убезпечення таємниці стандартного листування. Існуючі проблеми інформаційної безпеки актуальні й вимагають більш системного, поглибленого, постійного вивчення, аналізу та удосконаленню. Система інформаційної безпеки транспортної галузі виступає одним із основних елементів у системі національної безпеки. На сьогоднішній день, коли продовжується збройна агресія зі сторони росії, логістична складова нашої держави в основному опирається на залізничний транспорт. У даній статті розглянемо методи забезпечення інформаційної безпеки підприємств вагонного господарства, як одного елементу функціонування транспортної галузі.

Аналіз останніх досліджень і публікацій. У сучасній науковій літературі відсутній єдиний погляд на зміст поняття «інформаційна безпека». Існує необхідність уточнення поняття «інформаційна безпека», що допоможе осмисленню нових її аспектів, дозволить ширше розкрити суть і надати поняттю системного характеру. Провідні спеціалісти з цього питання ведуть публічну дискусію, особливо щодо характеристик існуючих небезпек, їхньої внутрішньої структури. Принципи побудови системи забезпечення національної безпеки висвітлюється в працях В. Богуша та О. Юдина «Інформаційна безпека держави» [1]. Автори висвітлюють загальні принципи побудови системи інформаційної безпеки без детальних вказівок на її впровадження на підприємствах, насамперед транспортної галузі. Система інформаційної безпеки підприємств вагонного господарства повинна в повній мірі відображати захищеність будь-яких корпоративних інтересів в існуючій інформаційній сфері від внутрішніх і зовнішніх загроз. Цікаві напрацювання стосовно інформаційної безпеки підприємств вагонного господарства викладені в роботах провідних вчених, а саме Черняка Г.Ю., Щербини Ю.В [2, 3], Обуховського В.В., Іщенко В.М., Щербини Ю.В. [4].

Мета статті. Аналіз методів забезпечення інформаційної безпеки підприємств вагонного господарства.

Виклад основного матеріалу дослідження. Інформаційна безпека будь-якої організації – це стан захищеності інформаційного середовища цієї організації, що забезпечує її формування, використання і розвиток. У сучасному соціумі інформаційна сфера має дві складові: інформаційно-технічну (штучно створений людиною світ техніки, технологій тощо) та інформаційно-психологічну (природний світ живої природи, що включає і саму людину). Інформаційну безпеку зазвичай можна розділити на дві складові частини: інформаційно-технічну та інформаційно-психологічну (психофізичну) безпеки.

Типова модель інформаційної безпеки складається з трьох категорій: конфіденційність (це стан будь-якої інформації, при якому доступ до неї здійснюють суб'єкти, які мають на це право); цілісність (недопущення недозволеної модифікації наявної інформації); доступність (недопущення тимчасового чи постійного приховування цієї інформації від працівників, які мали на це право доступу).

Існують й інші необов'язкові категорії безпеки: неспростовність (неможливість відмови від авторства); підзвітність (отримання повного співпадіння суб'єкта доступу та індикації всіх його дій); достовірність (відповідності передбаченому результату); автентичність або справжність (показує, що суб'єкт аналогічний заявленому).

Виділяється декілька категорій дій, що завдають шкоди інформаційній безпеці підприємства.

Перше, це дії, здійснювані авторизованими користувачами. Під цю категорію потрапляють цілеспрямована крадіжка або знищення даних на сервері, або робочій станції.

Друге, це методи впливу, що здійснюються різними хакерами, тобто людьми, які скоюють комп'ютерні злочини, у тому числі під час будь-якої конкурентної боротьби між компаніями. До цих методів відносять проникнення без дозволу в чужі комп'ютерні мережі або DoS-атаки. DoS-атака (від англ. Denial of Service – відмова в обслуговуванні) і DDoS-атака (від англ. Distributed Denial of Service – розподілена атака типу «відмова в обслуговуванні») – атака на обчислювальну систему з метою довести її до відмови, тобто створення таких умов, при яких легітимні (правомірні) користувачі системи не можуть одержати доступ до надаваємих системою ресурсів, або цей доступ стає ускладнений [5]. Іншими

словами це зовнішня атака на комп'ютерні мережі, що відповідають за ефективну роботу підприємства. Злочинці організовують лавинну, цілеспрямовану відправку даних на вузли інформаційних систем для їх перевантаження і виведення на якийсь час із ладу. У результаті це тягне за собою порушення або припинення роботи в бізнес-процесах компанії, на яку організована атака, та втрату її клієнтів, репутації, фінансових збитків.

Третє, це комп'ютерні віруси, категорія електронних методів впливу та інші шкідливі програми. Це реальна небезпека для всіх сучасних інформаційних систем, що часто використовують комп'ютерні мережі, електронну пошту та інтернет. Проникнення вірусу на вузли корпоративної мережі призводить до цілковитого порушення їх функціонування, значної втрати робочого часу, повної втрати наявних даних, зникнення усіх особистих даних, що були в комп'ютерній мережі та навіть фінансових засобів підприємства. Вірусна програма, яка потрапила в будь-яку корпоративну мережу підприємства, може дати злочинцям частковий або повний контроль над діяльністю організації [7, 10].

Четверте, це спам, що за кілька років перетворився на значну загрозу безпеці. Електронна пошта стала одним із головних каналів поширення різних шкідливих програм. Багато часу витрачається на перегляд різного роду спаму та його подальше видалення, що викликає у співробітників підприємства почуття типічного психологічного дискомфорту. Приватні особи й організації стають основними жертвами шахрайських схем. Разом зі спамом можливо нерідко видалення важливої кореспонденції, що призводить до втрати всієї корисної інформації. Небезпека втрати будь-якої кореспонденції збільшується при використанні різноманітних простих та складних методів для фільтрації спаму.

П'яте, це так звані «побутові» загрози. Можливий вплив на інформаційну безпеку вагоноремонтних підприємств різноманітних зовнішніх факторів таких, як: неправильна експлуатація або зберігання, що може стати причиною втрати даних; крадіжка як комп'ютерів, так і потрібних носіїв інформації; типові та не типові форс-мажорні обставини (затоплення, коротке замикання, механічне пошкодження) тощо.

Наявність різноманітної системи інформаційної безпеки підприємства є найважливішою умовою високої конкурентоспроможності та ефективної працеспроможності.

Всесвітня інформаційна мережа (павутина) зростає великими кроками, і як показує статистика, користувачів з плином часу стає тільки більше. Доступна інформація у всесвітній мережі займає всі сторони життєдіяльності як людини, так і нашого суспільства. Користувачі мережі довіряють цій формі своє особисте життя і свою трудову діяльність.

Фахівці галузі звертають увагу на те, що головна причина несанкціонованого проникнення в комп'ютерні мережі підприємства – це елементарна непідготовленість користувачів і їх порівняно невеликий досвід у сфері інформаційних технологій. Це зумовлено стрімким розвитком мережі інтернет та мережевих технологій.

Слід зазначити, що близько дев'яноста відсотків від всіх проникнень у комп'ютери шкідливих програм, припадає на інтернет (через електронну пошту та постійний перегляд Web-сторінок). Особливо серед таких програм виділяється цілий клас паразитів, таких як інтернет-черв'яки [6]. Вони можуть поширюватися автономно від механізму роботи комп'ютера й виконувати свої основні завдання щодо зміни програмних налаштувань комп'ютера-жертви, знищують адресну книгу або іншу цінну інформацію, дезорієнтують самого користувача, запускають розсилку з робочого комп'ютера за адресами, які були взяті із адресної книжки, можуть зробити комп'ютер підприємства стороннім ресурсом або навіть забирати значну частину робочих ресурсів для своїх цілей, а також самоліквідуватися, знищуючи при цьому на дисках всі файли.

Усі викладені проблеми, потрібно вирішувати за допомогою опрацьованого на вагоноремонтному підприємстві документа, що повністю відображає політику інформаційної безпеки. В цьому документі мають бути чітко виписані такі положення: як організована робота з інформацією вагоноремонтного підприємства; хто до неї має вільний доступ; як проходить копіювання і зберігання даних; який режим роботи на персональних комп’ютерах; наявність реєстраційних документів на обладнання персональних комп’ютерів та їх програмне забезпечення; вимоги до приміщення, де розташовується персональні комп’ютери і робочі місця користувачів; наявність робочих інструкцій і їх технічної документації.

Необхідно обов’язково відслідковувати новинки в технічних та інформаційних системах, які публікуються у фахових виданнях, і стежити за подіями, що обговорюються на відповідних семінарах та в соціальних мережах.

За нагальної потреби підключення інформаційних систем, інформаційно-телекомунікаційних мереж та всіх засобів обчислювальної техніки підприємств вагонного господарства до інформаційно-телекомунікаційних мереж міжнародного інформаційного обміну може проводиться тільки з використанням спеціальних, сертифікованих засобів захисту інформації, в тому числі шифрувальних (криптографічних) засобів, які пройшли порядок сертифікації, установлений законодавством.

Забезпечення інформаційної безпеки підприємств вагонного господарства повинно вирішуватися системно. Мають застосовуватися різні засоби захисту. Це фізичні, апаратні, програмні, організаційні та інші. Вони можуть застосовуватися як одночасно, так і під централізованим управлінням. Але при цьому всі компоненти системи мають взаємодіяти між собою і забезпечувати захист від зовнішніх та внутрішніх загроз.

У даний час ми маємо великий вибір методів забезпечення інформаційної безпеки підприємства це: засоби ідентифікації і автентифікації користувачів комп'ютерів; засоби шифрування інформації, що зберігається в комп'ютерах; міжмережеві екрани комп'ютерів; віртуальні приватні мережі; засоби тематичної фільтрації; інструменти перевірки цілісності вмісту дисків комп'ютерів; засоби антивірусного захисту програм; системи виявлення слабких місць мереж і аналізатори мережевих атак.

Всі перелічені засоби можуть бути використані самостійно, а також разом з іншими, що робить можливим створення систем інформаційного захисту в мережі різної складності і конфігурації, незалежно від платформ, які використовуються.

Основними елементами безпеки інформації називають авторизацію та ідентифікацію. Функція ідентифікації при доступу до інформаційних активів дисків комп'ютерів відповідає на запитання: «хто ви є?», «де ви є?», «ви користувач мережі?». А функція авторизації дозволяє доступ до ресурсів конкретного користувача. Роль функції адміністрування є в наданні користувачеві певних ідентифікаційних особливостей у межах мережі, розгляду та наданні кількості дій, допустимих для нього.

Шифрування даних дає змогу значно зменшити втрати при доступу стороннього користувача до даних, що зберігаються на стаціонарному носії, а також зчитування інформації, яка пересилається електронною поштою. Даний засіб ефективно забезпечує

захист конфіденційності наявної інформації. Високий показник криптостійкості і законне використання – основні вимоги до систем шифрування.

Принцип, на якому побудована дія міжмережевих екранів, ґрунтується на перевірці кожного масиву даних на ідентичність, вихідної та вхідної IP-адреси, дозволених наявних баз адресатів. Як наслідок значно розширюються можливості міжмережевих екранів інформаційних мереж за контролем переміщення даних.

Аналізуючи криптографію та діючі міжмережеві екрани, звертаємо увагу на інші захищені мережі приватних власників таких, як віртуальна приватна мережа (Virtual Private Network – VPN). При їх використанні вирішуються всі проблеми цілісності й конфіденційності даних при пересилці відкритими або напіввідкритими комунікаційними каналами. Впровадження VPN зводиться до наступних завдань, що можна розділити: на захист усіх інформаційних потоків у структурі підприємства вагонного господарства (шифрування всієї інформації на виході з внутрішньої мережі); повністю захищений доступ користувачів мережі до наявних інформаційних масивів підприємства, що використовує інтернет; захист наявних інформаційних потоків всередині корпоративної мережі підприємства.

Фільтрація кількості вхідної та вихідної інформації через електронну пошту – один із найефективних способів захисту конфіденційної інформації від її втрати. Постійна перевірка всіх поштових повідомлень і включень у них на основі правил, які встановлені на підприємстві, забезпечує ефективний захист підприємства вагонного господарства від відповідальності по судовим позовам і дає можливість захистити своїх співробітників від наявного спаму. Функція тематичної фільтрації може переглядати і перевіряти файли всіх наявних форматів, включаючи стислі і графічні. Під час цієї операції пропускна спроможність робочої мережі не змінюється.

Усі наявні зміни на працюючому сервері відслідковуються адміністратором цієї мережі або авторизованим виконавцем, використовуючи елементи технології перевірки незмінності вмісту на жорсткому диску. В результаті це допомагає виявляти різні дії з файлами, такі як зміна, видалення, відкриття, та ефективно ідентифікувати появу вірусів, виявити несанкціонований доступ до мережі або крадіжку даних користувачами, що мали до нього доступ.

Новітні антивірусні технології виявляють майже всі відомі користувачам вірусні програми, використовуючи порівняння наявного коду підозрілого робочого файлу із зразками, що знаходяться в антивірусній базі комп'ютера. Розроблено свіжі моделюючі програми технології поведінки, які ефективно виявляють нові вірусні програми.

Щоб протидіяти техногенним і природним загрозам інформаційній безпеці на підприємстві вагонного господарства, повинен бути спроєктований і впроваджений цілий набір різних процедур для протидії надзвичайним ситуаціям. Це може бути фізичний захист усієї робочої апаратури від пожежі та її наслідків, що може мінімізувати збитки, якщо виникне така ситуація. Один із надійних методів захисту інформації від втрати даних – постійне резервне копіювання матеріалу при чіткому виконанні встановлених правил.

На підприємствах вагонного господарства на сьогоднішній день конструкторська, службова, робоча, технологічна документація відпрацьовується на комп'ютерній техніці. Вся робоча інформація обробляється, архівується виключно на електронних носіях інформації. На підприємствах існує можливість для скритого, не дозволеного копіювання, передачі, видалення, зміни, знищення електронних даних на носіях інформації. Безпечне, надійне, безперервне функціонування баз даних в інформаційних комп'ютерних системах підприємства, є основою його стабільної роботи.

Причини, які можуть викликати зміну або знищення інформації, що знаходиться в комп'ютерах автоматизованих робочих місць, мають наступне походження, а саме ненавмисна помилка працівників, свідоме завдання шкоди зловмисниками, шкідливим програмним продуктом, неполадками в самому комп'ютері, схованими елементами недоробленого програмного забезпечення, виведення з ладу технічних пристроїв автоматизованих робочих місць, аваріями на електричних та інженерних мережах, стихійними лихами.

Статистика показує, що від п’ятдесяти до вісімдесяти відсотків випадків втрат даних комп'ютера становлять помилкові або не зовсім професійні дії працюючого персоналу. Втрата даних з технічних причин – від п'ятнадцяти до двадцяти п'яти відсотків.

Помилки в діях працівників можна пояснити низьким рівнем дисципліни, слабкою професійною підготовкою, безвідповідальністю, недостатніми знаннями програмного забезпечення і самої комп'ютерної техніки. Незважаючи на причини втручання чи втрати будь-якої із необхідних інформацій для підприємства, од-

нозначно буде завдана шкода бізнесовому іміджу підприємства та його фінансовій репутації.

При розробці проєкту автоматизованих робочих місць на підприємствах вагонного господарства необхідно в обов'язковому порядку враховувати ці загрози і розробляти заходи по мінімізації її наслідків. Комплекс заходів для досягнення позитивних цілей включає в себе організаційні, програмні, інженерно-технічні методи захисту інформації та її збереження.

Найвідоміші методи захисту комп'ютерної інформації – захист за допомогою спеціальних програм або програмні методи захисту, що являє собою комплекс програм різного призначення, алгоритмів для забезпечення безперебійної роботи комп'ютерної техніки. Вони виконують контроль та розмежування доступу до наявної інформації з видаленням непідконтрольних дій по відношенню до неї. Програмні методи захисту передбачають простоту, реалізацію, універсальність, гнучкість, пристосованість, варіативність у налаштуванні.

Щоб захистити комп'ютерну інформацію спеціалісти використовують антивірусні програми разом із профілактикою і постійною діагностикою, це ускладнює проникнення комп'ютерного вірусу в інформаційну систему, очищає уже заражені робочі файли та диски і не допускає нового зараження.

Ідеальних антивірусних програм, які вчасно виявляли б і знищували будь-який вірус, спеціалісти ще не зробили. Найбільш надійний антивірусний захист має багаторівнева система, що має наступні складові: використання тільки ліцензійного програмного продукту, періодичне резервне копіювання інформаційних матеріалів і програм, постійна перевірка уже отриманих даних на наявність вірусних програм, використання нових антивірусних продуктів під час перевірки своїх носіїв інформації при перенесенні на них інших масивів інформації, а також при переформатуванні.

Існує думка, що найефективнішим способом захисту інформації під час передачі її через комп'ютерні лінії є шифрування. Його називають криптографічним методом захисту інформації.

Технічний захисту інформації – це пристрої та способи, що попереджають і убезпечують від крадіжок, нецільового використання, приведення в непридатний стан мережевого устаткування та автоматизованих робочих місць. Для цього встановлюють на вікна та двері металеві решітки, огорожі, турнікети, кодові замки на двері, різні системи відеоспостереження і сигналізації. Також всі робочі підрозділи забезпечуються системами зв'язку, управління

контролю доступом, телекомукаційними, пожежними, охоронними системами та іншими інженерними пристроями [8].

Важливим для інформаційної безпеки є досягнення стану її захищеності, тобто створення і підтримка відповідних інженерно-технічних потужностей та інформаційної організації, що відповідають реальним і потенційним загрозам [9].

Організаційні методи засоби захисту інформації включають у себе регламентацію виробничої праці та на нормативно-правовій базі взаємовідносини між виконавцями, що приводить до зменшення чи суттєво ускладнення незаконного привласнення інформації конфіденційного характеру. Вони ще організовують роботу з персоналом, документацією, синхронізацією різних технічних засобів, а також проведення аналізу різних загроз інформаційній безпеці підприємства, організовують режим охорони.

Для забезпечення захисту зберігання та обробки інформації в автоматизованих робочих місцях при проникненні в їх робочу структуру розділяють доступ до об'єктів усіх суб'єктів.

Організаційні методи захисту інформації включають в себе аналітичну роботу з кадрами, вибірковий режим доступу, цілісність документообігу, постійне використання технічних засобів забезпечення безпеки, аналітичний аналіз по недопущенню зовнішніх та внутрішніх загроз інформаційній безпеці, призначення відповідальних за наявне обладнання, проведення періодичних та цільових інструктажів працюючого персоналу.

Організаційні методи захисту інформації мають три складові: контроль доступу персоналу, обмеження доступу персоналу, розмежування доступу персоналу.

Обмеження доступу персоналу до комп'ютерних машин – такий принцип роботи, щоб виключити будь-який доступ до цієї системи сторонніх осіб. Один із варіантів, це розмістити автоматизовані робочі місця в штучно ізольованому приміщенні. При тривалому простої системний блок користувача і всі носії інформації рекомендується розміщати в сейфі.

Розмежування доступу персоналу полягає в розподілі всієї інформації на якісні частини й дозволу доступу до неї згідно із затвердженими функціональними та посадовими інструкціями персоналу. Суть завдання розмежування доступу – це захист інформації від зловмисника, що має допуск до роботи в даній комп'ютерній мережі.

Розділення інформації може проходить відповідно до наступних критеріїв, таких як: функціональне призначення, ступінь важ-

ливості та інші. При проведенні розмежування доступу виконують наступні правила: технічне обслуговування всього обладнання під час експлуатації повинне проводитись спеціалістами, які не мають доступу до захищеної інформації; будь-яку заміну програмного забезпечення комп'ютерної мережі покладають на спеціально, призначеного для цієї цілі, спеціаліста.

Контроль доступу – впізнання автентичності особи та цілковита фіксація моменту початку роботи. При цьому, на початку усім, хто допускається до закритої інформації, надається унікальний образ, число, ім'я – ідентифікацію. Процес перевірки або впізнання дійсності особи, чи дійсно особа є та за кого себе подає називається автентифікацією [11].

Суб'єктами автентифікації та ідентифікації в комп'ютерній мережі можуть бути технічний засіб, документ, працівник тощо. Працівником може виступати оператор комп'ютерної мережі, користувач, адміністратор.

Автентифікація може проходити відносно технічних засобів, персоналу, документів. Найвідоміший метод – надання паролю та запиту при новому вході в комп'ютерну мережу. Приклад автентифікації технічних засобів – поставити автентифікаційний термінал для входу в комп'ютерну мережу працівника. Описана процедура також проходить за допомогою паролю.

Висновки та пропозиції. Проведений аналіз методів забезпечення інформаційної безпеки підприємств вагонного господарства дає чітке розуміння в необхідності системного та комплексного підходу до зазначеної проблеми. Одним з необхідних кроків до забезпечення інформаційної безпеки відносяться організаційні заходи захисту інформації, що являють собою сукупність заходів щодо підбору, перевірки и навчання персоналу, який бере участь у всіх стадіях інформаційного процесу підприємств вагонного господарства. Також на вищезазначених підприємствах необхідно дотримуватися постійного контролю за джерелами виникнення потенційних загроз та у відповідь сучасним викликам здійснювати пошук й застосовувати найкращі рішення у здійсненні захисту інформації різними формами та способами. Форми і способи забезпечення інформаційної безпеки утворюють власне інструмент, за допомогою якого засоби інформаційної безпеки вирішують весь комплекс завдань із захисту життєво важливих інтересів підприємств вагонного господарства.

ЛІТЕРАТУРА

1. Юдін О. К., Богуш В. М. Інформаційна безпека держави: навч. посіб. Харків: Консум. 576 с.

2. Черняк Г. Ю., Щербина Ю. В. Розробка моделі пасажирського вагона для досліджень динаміки в програмному комплексі «Универсальный механизм». *Збірник наукових праць Київського університету економіки і технологій транспорту. Серія «Транспортні системи і технології»*. Київ, 2007. Т 12. С. 75–82.

3. Черняк Г. Ю., Щербина Ю. В. Базова комп'ютерна модель просторової динаміки пасажирського вагона для швидкісного руху. *Залізничний транспорт України*. 2012. № 6. С. 55–58.

4. Обуховський В. В., Іщенко В. М., Щербина Ю. В. Аналіз автоматизованих систем керування вагонів метрополітену (пасажирських поїздів). *The 3 rd International scientific and practical conference «Topical aspects of modern scientific research»(November 23–25, 2023)*. CPN Publishing Group, Tokyo, Japan. 2023. 725 p.

5. Краснобрижий І. В. Види та методики реалізації dos та ddos атак на державні автоматизовані системи, а також можливі шляхи боротьби з ними. *Економічна та інформаційна безпека: проблеми та перспективи:* матеріали Всеукр. наук.-практ. конф., м. Дніпро, 14 квіт. 2017 р. Дніпро, 2017. С. 89-94.

6. Авраменко В. С., Авраменко А. С. Основи операційних систем : навч. посіб. Черкаси, 2018. 524 с.

7. Буров Є. В. Комп'ютерні мережі : підручник. Львів: «Магнолія 2006», 2010. 262 с.

8. Нормативний документ системи технічного захисту інформації. Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці НД ТЗІ 1.6-005-2013 : наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 15.04.2013 № 215.

9. Крюков О. І. Інформаційна безпека держави в умовах глобалізації. *Державне будівництво*. 2007. № 2.

10. Петрик В. М., Галамба М. В. Інформаційна безпека України: поняття, сутність та загрози. *Юридичний журнал*. 2006. № 11. С. 49–52.

11. Критерії оцінювання захищеності інформації в комп'ютерних системах від несанкціонованого доступу : нормативний документ НД ТЗІ 2.5-004-99 від 28 квіт. 1999 р. № 22.

REFERENCES

1. Yudin O. K., Bohush V. M. Informatsiina bezpeka derzhavy: navch. posib. Kharkiv: Konsum. 576 s.

2. Cherniak H. Yu., Shcherbyna Yu. V. Rozrobka modeli pasazhyrskoho vahona dlia doslidzhen dynamiky v prohramnomu kompleksi «Unyversalnыi mekhanyzm». Zbirnyk naukovykh prats Kyivskoho universytetu ekonomiky i tekhnolohii transportu. Seriia «Transportni systemy i tekhnolohii». Kyiv, 2007. T 12. S. 75–82.

3. Cherniak H. Yu., Shcherbyna Yu. V. Bazova kompiuterna model prostorovoi dynamiky pasazhyrskoho vahona dlia shvydkisnoho rukhu. Zaliznychnyi transport Ukrainy. 2012. № 6. S. 55–58.

4. Obukhovskyi V. V., Ishchenko V. M., Shcherbyna Yu. V. Analiz avtomatyzovanykh system keruvannia vahoniv metropolitenu (pasazhyrskykh poizdiv). The 3 rd International scientific and practical conference "Topical aspects of modern scientific research"(November 23–25, 2023). CPN Publishing Group, Tokyo, Japan. 2023. 725 p.

5. Krasnobryzhyi I. V. Vydy ta metodyky realizatsii dos ta ddos atak na derzhavni avtomatyzovani systemy, a takozh mozhlyvi shliakhy borotby z nymy. Ekonomichna ta informatsiina bezpeka: problemy ta perspektyvy: materialy Vseukr. nauk.-prakt. konf., m. Dnipro, 14 kvit. 2017 r. Dnipro, 2017. S. 89 94.

6. Avramenko V. S., Avramenko A. S. Osnovy operatsiinykh system : navch. posib. Cherkasy, 2018. 524 s.

7. Burov Ye. V. Kompiuterni merezhi : pidruchnyk. Lviv: «Mahnoliia 2006», 2010. 262 s.

8. Normatyvnyi dokument systemy tekhnichnoho zakhystu informatsii. Zakhyst informatsii na obiektakh informatsiinoi diialnosti. Polozhennia pro katehoriiuvannia obiektiv, de tsyrkuliuie informatsiia z obmezhenym dostupom, shcho ne stanovyt derzhavnoi taiemnytsi ND TZI 1.6-005-2013 : nakaz Administratsii Derzhavnoi sluzhby spetsialnoho zviazku ta zakhystu informatsii Ukrainy vid 15.04.2013 № 215.

9. Kriukov O. I. Informatsiina bezpeka derzhavy v umovakh hlobalizatsii. Derzhavne budivnytstvo. 2007. № 2.

10. Petryk V. M., Halamba M. V. Informatsiina bezpeka Ukrainy: poniattia, sutnist ta zahrozy. Yurydychnyi zhurnal. 2006. № 11. S. 49–52.

11. Kryterii otsiniuvannia zakhyshchenosti informatsii v kompiuternykh systemakh vid nesanktsionovanoho dostupu : normatyvnyi dokument ND TZI 2.5-004-99 vid 28 kvit. 1999 r. № 22.

СТАТТЯ НАДІЙШЛА ДО РЕДАКЦІЇ 02.12.2023