https://www.sworldjournal.com/index.php/swj/article/view/swj10-01-043
DOI: 10.30888/2663-5712.2021-10-01-043

УДК 004.023

RESEARCH OF PRINCIPLES OF IT SAFETY OF TRANSPORT FLOWS IN THE INTERNATIONAL COMMUNICATION

ДОСЛІДЖЕННЯ ПРИНЦИПІВ ІТ-БЕЗПЕКИ ТРАНСПОРТНИХ ПОТОКІВ В МІЖНАРОДНОМУ СПОЛУЧЕННІ

Mnatsakanian M.S. / Мнацаканян М.С.
c.t .s., as.prof. / к.т.н., доц.
Lyamzin A.O. / Лямзін А.О.
d.t .s ., as.prof. / к.т.н., доц.
Peklova N.M. / Пеклова Н.М.
Student / студент
Pryazovskyi State Technical University, Mariupol, Universytetska st., 7, 87500
Приазовський державний технічний університет,
Маріуполь, вул. Університетська 7, 87500

Анотація. *В роботі розглянуто передумови формування необхідності забезпечення інформаційної та кібербезпеки транспортних потоків в умовах інформатизації та автоматизації транспортних процесів. Сучасна цивілізація сформована постіндустріальними та інформаційними процесами в межах соціально-технічного простору. В просторі, яке досліджується, знання представлені у вигляді інформаційних ресурсів та стають головним надбанням і найважливішим чинником економічного розвитку, а інформаційна індустрія – однією з основних галузей економіки. Процеси інформатизації соціально-технічної діяльності, як у виробничій, так і в невиробничій складовій є настільки масштабними і глибокими, що привело до якісних змін самого суспільства, безмежно розширюючи сферу застосування продуктів і сервісів інформаційної індустрії, неухильно залучаючи у світ обробки інформації все суспільство.*

Ключові слова: *IT-безпека, інформаційна безпека, кібербезпека, інформаційні технології, транспортні потоки.*

Вступ.

IT якісно змінили процеси управління в усіх областях людської діяльності, в тому числі і на транспорті. Електронна торгівля (E - Commerce), інтернет-технології, автоматизоване управління на базі сучасних технічних і програмних засобів відкрили нові можливості підвищення ефективності роботи транспорту і економічності логістичних систем. Цьому значною мірою сприяли сучасні системи телекомунікацій та в першу чергу мобільна система зв'язку на основі стандарту GSM (Global System for Mobile Communication).

Велике значення для автоматизації на всіх видах транспорту має глобальна система визначення місцезнаходження транспортних засобів (GPS) на основі супутникового зв'язку. Значною мірою автоматизації та інформатизації на транспорті сприяли успіхи в області ідентифікації вантажів і носіїв на основі штрихового коду, нові радіочастотні технології ідентифікації із застосуванням транспондерів і ін.

Основний текст.

В якості основного напрямку для оптимізації використання транспорту пропонується застосування автоматизованих навігаційних систем, за допомогою яких визначається оптимальний маршрут руху транспортних засобів. В даний час відомий цілий ряд таких систем з різноманітним

програмним забезпеченням.

Більшість цих систем працює на основі глобальної автоматизованої географічної системи GIS (рисунок 1) з топографічними картами в цифровій формі, яка використовується не тільки на автомобільному, а й на інших видах транспорту для автоматизації управління. Автоматичні транспортні засоби (AVs) є транспортними засобами, в яких, щонайменше, один елемент керування транспортним засобом (наприклад, рульове управління, регулювання швидкості) відбувається без прямої участі водія. Робота AVs організовується шляхом збору інформації з набору датчиків (штучного зору HAVS, CAV і IM) та її обробки обчислювальними ресурсами на борту автомобіля, інтелектуальної інфраструктури і в інших місцях, пов'язаних між собою в практично реальному часі.

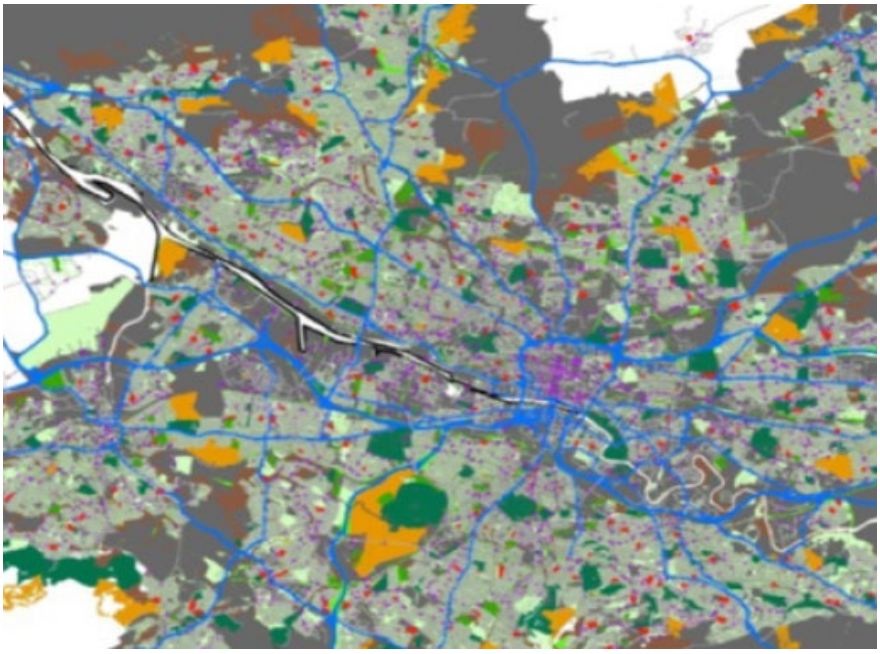

Рисунок 1 - GIS промислового району

Для цього використовуються: відео камери; різноманітні радари; виявлення та ранжування світлових лазерних променів і їх відображень (LiDAR); ультразвукове і інфрачервоне обладнання тощо [1].

На рисунку 2 представлене кратке уявлення типового автоматизованого обладнання і функцій обладнання штучного зору HAVS, CAV і IM.

Інтегрованою частиною AV є навігація і це, по суті, планування маршруту. Більш конкретно, вона створює і перераховує цифрову карту, яка включає інформацію про місця, типи і стан доріг, ландшафтів і прогноз погоди. В даний час транспортні засоби вже повністю планують планування маршруту, використовуючи глобальні системи позиціонування (GPS, Глонас і інші). У повністю автономних автомобілях навігація посилюється шляхом інтеграції транспортних засобів (V2V).

Відбувається безперервний обмін даними між транспортними засобами через системи зв'язку, такі, як бездротові локальні мережі (WLAN). За допомогою V2V-зв'язку, автономна система може розпізнавати критичні і

небезпечні ситуації на ранній стадії, і збирати необхідну інформацію, пов'язану з безпекою. Ситуаційний аналіз контролює навколишнє середовище, через яку транспортний засіб рухається для забезпечення того, щоб автономна система знала про всі відповідні об'єкти і їх рухах.

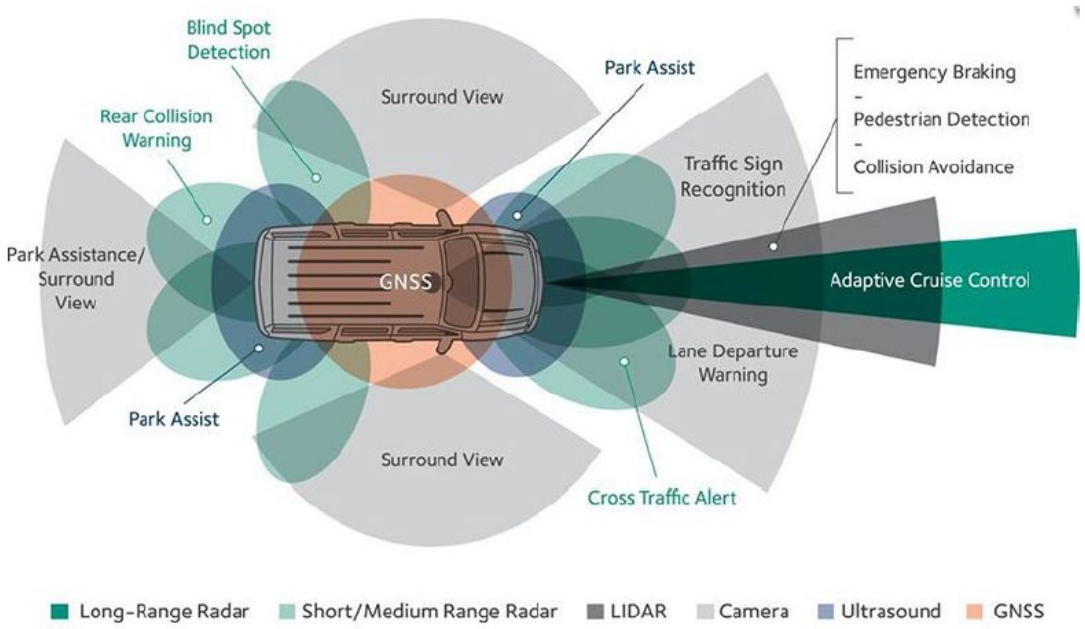

Рисунок 2 - Кратке уявлення типового автоматизованого обладнання та функцій обладнання штучного зору HAVS, CAV та IM

В даний час розвиток будь-якого транспортного підприємства неможливий без забезпечення його інформаційною інфраструктурою. Процес виробництва вимагає не тільки переміщення матеріальних цінностей, а й постійного руху інформаційних потоків. Національне і міжнародне транспортування товарів вимагає безперервного інформаційного покриття і документального забезпечення [2].

ІТ життєво необхідні на транспорті з його швидкоплинними факторами (рисунок 3).

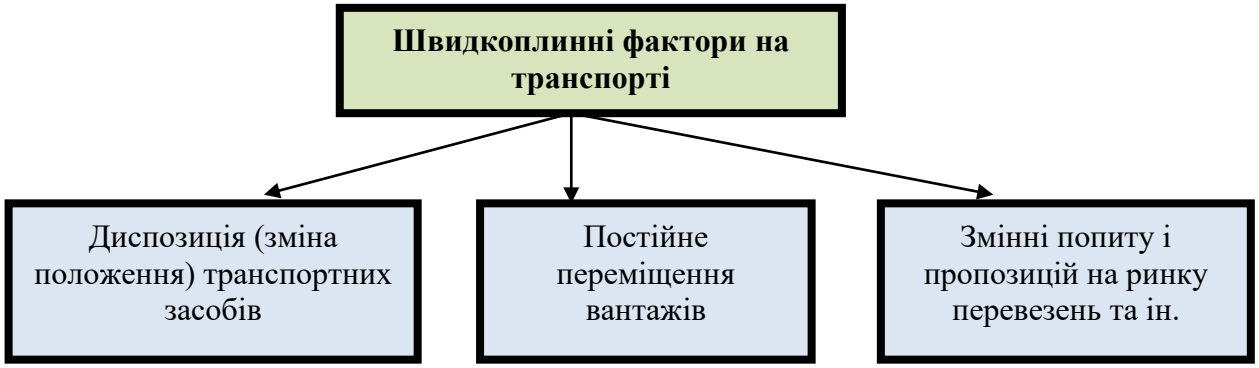

Рисунок 3 - Швидкоплинні фактори на транспорті

На всіх етапах перевезення і перевалки вантажу відбувається постійний обмін даними між учасниками транспортного процесу, висуваючи високі вимоги до точності і швидкості передачі інформації. Від цих показників часто

залежить не тільки чіткість і безперервність процесу, а й виконання умов контракту.

Забезпечити виконання цих вимог можна тільки шляхом впровадження IT-систем управління, що реалізують впорядковане зберігання і швидку передачу інформації, відстеження вантажу і транспорту, узгоджене планування і управління вантажопотоками.

Тому інформаційні технології покликані забезпечувати автоматизацію управлінських операцій, підготовку аналітичної інформації для прийняття рішень і поставляти споживачам будь-які види даних на великі відстані і обсяги.

Фактори і передумови необхідності забезпечення захисту інформаційної інфраструктури транспортних потоків від комп'ютерних атак.

Інформаційна сфера (інформація, інформаційна інфраструктура, інформаційно-комунікаційні технології), інформаційна безпека і кібербезпека починають грати одну з ключових ролей в забезпеченні важливих, перш за все економічних, інтересів транспортного комплексу в рішенні проблем безпеки руху, пасажирських і вантажних перевезень [3].

Основні фактори інформаційної безпеки і кібербезпеки зображені на рисунку 4.

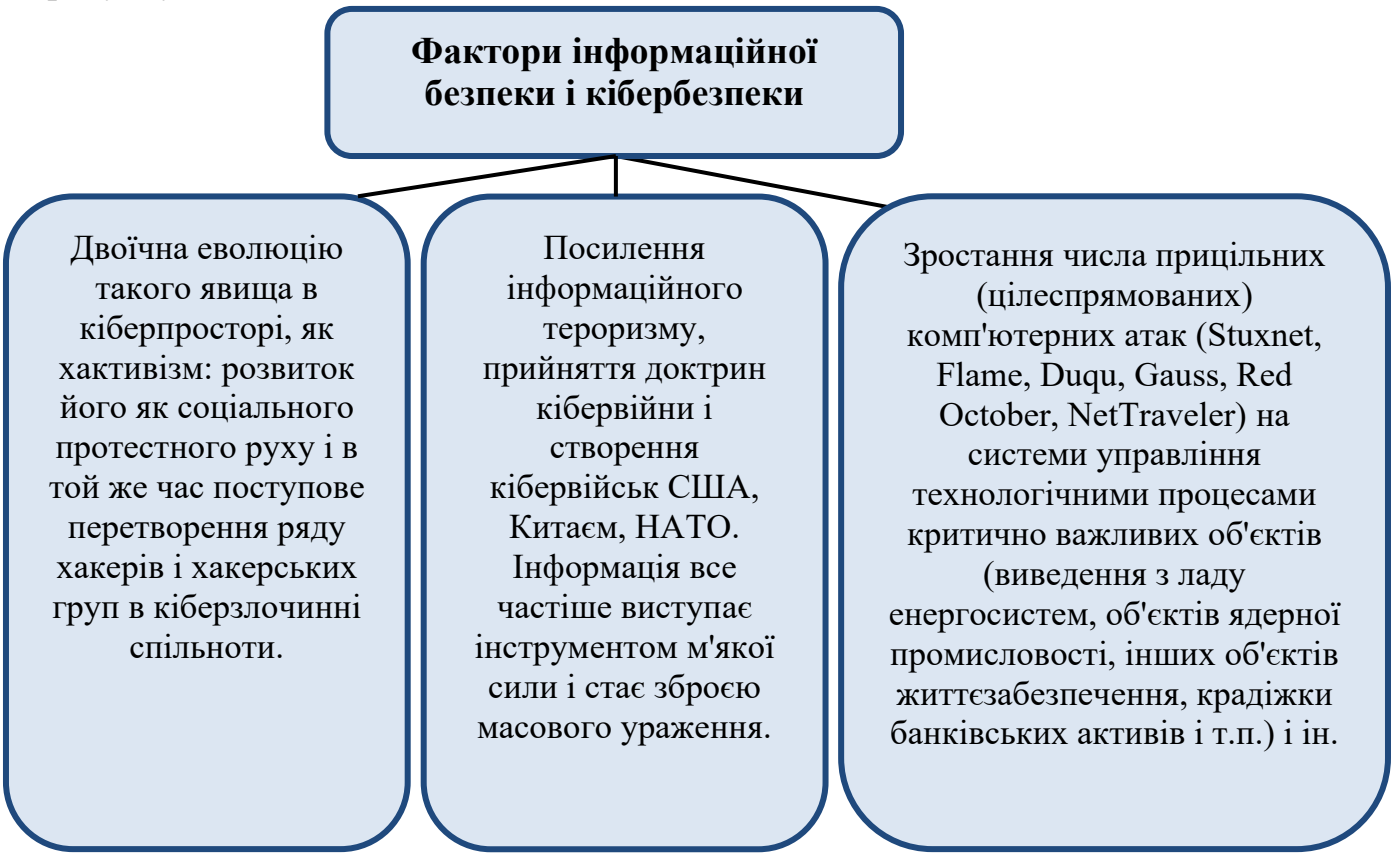

Рисунок 4 - Фактори інформаційної безпеки і кібербезпеки

Фактори інформаційної безпеки і кібербезпеки будуть вирішальними при організації високошвидкісного руху та побудови інтелектуальних центрів і

систем ситуаційного управління, особливо з урахуванням вихідних з кіберпростору загроз і потенційної схильності інформаційної інфраструктури комп'ютерним атакам.

Основними передумовами забезпечення інформаційної безпеки і кібербезпеки транспортних потоків з акцентуванням уваги на захисті її інформаційної інфраструктури від комп'ютерних атак є такі:

1. Інтеграція в єдині комплекси автоматизованих систем, пов'язаних з управлінням руху транспортних засобів, та інших автоматизованих інформаційних і телекомунікаційних систем (АІТС) транспорту.

2. Постійне ускладнення програмного забезпечення і устаткування, використовуваних в інших автоматизованих інформаційних і телекомунікаційних системах транспорту.

3. Практика здійснення розробниками АІТС і постачальниками обладнання моніторингу, технічного обслуговування і віддаленого налаштування АІТС в цілому або їх складових частин, а також серверного та телекомунікаційного обладнання, що входить до складу елементів інформаційної інфраструктури транспорту.

4. Інтенсивне вдосконалення потенційними порушниками засобів і методів використання інформаційних і телекомунікаційних технологій, методів соціальної інженерії для нанесення шкоди, а також почастішали спроби їх застосування в протиправних цілях і конкурентній боротьбі.

5. Ризик приховування спроб або фактів порушення штатного функціонування АІТС транспорту з боку експлуатуючих підрозділів.

6. Тимчасове вимушене залучення при створенні АІТС, в тому числі автоматизованих систем управління технологічними процесами (АСУ ТП), пов'язаних з організацією та управлінням рухом транспорту, представників неконтрольованих фірм-виробників і постачальників програмно-апаратних засобів обробки, зберігання та передачі інформації і застосування неконтрольованих програмно- апаратних рішень.

7. Зростання в світі і країні кількості протиправних дій з використанням інформаційних і телекомунікаційних технологій, в тому числі комп'ютерних атак в транспортних потоках.

Основні принципи заходів щодо забезпечення ІТ-безпеки транспортних потоків в міжнародному сполученні.

Основними принципами заходів щодо забезпечення ІТ-безпеки транспортних потоків в міжнародному сполученні є:

• Принцип законності. Заходи не повинні суперечити вимогам міжнародного законодавства, національних законодавств держав-учасниць, двосторонніх договорів і угод, в тому числі в сфері обміну електронними документами і масивами інформації.

• Принцип превентивності. Організаційно - правові заходи щодо забезпечення ІТ-безпеки транспортних потоків повинні бути спрямовані на попередження порушень вимог ІТ-безпеки при обміні електронними документами і масивами інформації в міжнародному сполученні.

• Принцип економічної доцільності. Витрати на забезпечення IT-безпеки не повинні перевищувати величину можливого збитку, пов'язаного з порушенням

• Принцип адаптивності. Заходи повинні в основі своїй передбачати можливість адаптації до зміни положень міжнародного законодавства, національних законодавств держав-учасниць, а також відповідних договорів і угод, зміни технології, топології, конфігурації, ступеня конфіденційності і цінності електронних документів і масивів інформації, що передаються між транспортними потоками держав-учасниць [4].

• Принцип безперервності і всеохопність. Заходи повинні поширюватися на всі етапи і сторони обміну електронними документами і масивами інформації транспортних потоків між державами-учасницями.

• Принцип гласності. Заходи повинні бути доступні для розуміння і схвалення всіма зацікавленими сторонами.

• Принцип несуперечності. Вимоги заходів не повинні суперечити один одному.

Загрози IT-безпеки транспортних потоків.

У цьому розділі наводиться детальна інформація про загрози і фактори уразливості, які можуть існувати. Загрози, які включені до переліку, відображають сучасний стан техніки на даний момент, але в разі їх використання ці загрози необхідно буде піддавати повторній оцінці на предмет їх повноти. Їх слід використовувати в якості основи для забезпечення належного зниження ризиків. Їх можна також використовувати як підмогу при визначенні рівня вразливості в разі потенційних IT-загроз та в процесі прийняття належних заходів для зниження цих ризиків.

Загрози щодо внутрішніх серверів:

a) Внутрішні сервери, що використовуються в якості засобу кібератаки на транспортний засіб або вилучення даних. Це може бути зловживання привілеями штатними співробітниками. Несанкціонований доступ через Інтернет до сервера (який можливий, наприклад, в результаті обходу системи захисту, не усунених факторів уразливості системи програмного забезпечення, атаки методом використання мови структурованих запитів SQL або іншими способами). Несанкціонований фізичний доступ до сервера (наприклад, за допомогою USB-накопичувачів або інших засобів, що підключаються до сервера).

b) Порушення роботи внутрішніх серверів, яке негативно позначається на експлуатації транспортного засобу. Атака на внутрішній сервер, який припиняє роботу: вона, наприклад, не дає йому можливості взаємодіяти з транспортними засобами і надавати послуги, які потрібні для їх роботи.

c) Дані, що зберігаються на внутрішніх серверах, втрачені або порушені («вразливість» даних). Втрата інформації в хмарі. У разі атаки або аварії, коли дані зберігаються сторонніми провайдерами послуг хмарних технологій, конфіденційні дані можуть бути загублені. Порушення цілісності інформації в результаті ненавмисного обміну даними (наприклад, помилки на рівні адміністрації, зберігання даних на серверах в недопустимому місці).

Загрози щодо транспортних засобів, які стосуються їх каналів передачі даних:

1) Навмисне перекручування повідомлень або даних, отриманих транспортним засобом. Навмисне перекручування повідомлень методом підміни користувача. Атака Сивілли (з метою спотворити повідомлення, одержувані транспортними засобами, і показати, що по дорозі рухається ніби багато транспортних засобів).

2) Канали передачі даних, що використовуються для здійснення несанкціонованих дій, видалення або внесення інших змін до бортової коду / даних транспортного засобу. Канали передачі даних допускають впровадження коду, наприклад, в комунікаційний канал може бути впроваджений підроблений двійковий код програмного забезпечення. Канали передачі даних допускають маніпуляцію з бортовим кодом / даними транспортного засобу. Канали передачі даних допускають накладення інших даних транспортного засобу. Канали передачі даних допускають стирання даних транспортного засобу. Канали передачі даних допускають впровадження даних / коду в систему транспортного засобу (запис даних / коду)

3) Канали передачі даних допускають прийом недостовірних / ненадійних повідомлень або уразливі в разі сеансів зв'язку / атаки з повторним нав'язуванням повідомлення. Прийом інформації з ненадійного або недостовірного джерела. Атака / перехоплення сеансу зв'язку зі зломом. Атака з повторним нав'язуванням повідомлення, наприклад атака на комунікаційний шлюз дозволяє зловмисникові знизити ефективність програмного забезпечення або вбудованих програм шлюзу.

4) Інформацію можна легко розкрити, наприклад шляхом підслуховування повідомлень або несанкціонованого доступу до секретних файлів або папок. Перехоплення інформації / перешкоди в результаті випромінювання / відстеження повідомлень. Отримання несанкціонованого доступу до файлів або даних.

5) Атаки по каналам передачі даних в цілях порушення функцій транспортного засобу у вигляді відмови в обслуговуванні . Передача великої кількості безглуздих даних в інформаційну систему транспортного засобу, в результаті чого нормальне надання послуг неможливо. Атака методом переповнення: з метою порушити передачу даних між транспортними засобами зловмисник може заблокувати передачу повідомлень між транспортними засобами.

6) Користувач з боку може отримати привілейований доступ до систем транспортного засобу.

7) Віруси, занесені в комунікаційне середовище, можуть інфікувати системи транспортного засобу.

8) Повідомлення, отримані транспортним засобом або передані разом з ним, містять шкідливий контент.

Загрози щодо транспортних засобів, що стосуються ненавмисних дій людини:

- Порушення конфігурації обладнання або систем правомірним суб'єктом, наприклад власником або організацією технічного обслуговування.
- Правомірні суб'єкти здатні вживати заходи, які можуть мимоволі полегшити кібератаку. Безневинна жертва (наприклад, власник, оператор чи інженер з технічного обслуговування) вводиться в оману з метою змусити його зробити відповідну дію, для того щоб ненавмисно завантажити шкідливе програмне забезпечення або дати можливість злому.

Загрози щодо транспортних засобів, що стосуються взаємодії з зовнішніми об'єктами і підключення до них:

a) Маніпуляція із засобами взаємодії функцій транспортного засобу відкриває можливість для кібератаки: це може включати засоби телематики; системи, які дають можливість здійснення дистанційних операцій; і системи, що використовують засоби бездротового зв'язку ближнього радіусу дії. Наприклад, маніпуляція з системою вимірювання температури вантажів, що вимагають особливого поводження, дистанційного відкриття дверей вантажного відділення.

b) Розміщення програмного забезпечення третіми особами, наприклад розважальних прикладних програм, що використовуються в якості одного із засобів для атаки систем транспортних засобів .

c) Пристрої, підключені до зовнішніх інтерфейсів, наприклад порти USB або порти OBD, що використовуються в якості одного із засобів для атаки систем транспортних засобів.

Потенційні цілі або мотивування атаки:

- Вилучення даних / коду транспортного засобу.
- Маніпуляція з даними / кодом.
- Стирання даних / коду. Несанкціоноване видалення / маніпуляція з журналами реєстрації системних подій.
- Впровадження шкідливих програм.
- Введення в дію нового програмного забезпечення або затирання існуючого програмного забезпечення.
- Порушення роботи систем або операцій.
- Маніпуляція з параметрами транспортного засобу.

Потенційні фактори уразливості, якими можна скористатися в разі недостатньої захисту або надійності:

a) Криптографічні технології, які можуть бути порушені або які застосовуються неадекватно.

b) Частини або приналежності компонентів, які можуть бути порушені з метою створення можливості для атаки транспортних засобів.

c) Розробка програмного забезпечення або апаратних засобів, яка створює можливість виникнення факторів уразливості.

d) Дизайн мережі, який допускає виникнення факторів уразливості. Надмірне число вільних інтернет-портів, що забезпечує доступ до мережевих систем.

e) Можливість фізичної втрати даних. Збиток, заподіяний третьою

стороною. У разі ДТП або розкрадання конфіденційні дані можуть бути загублені або порушені в результаті нанесення фізичної шкоди.

f) Можливість ненавмисної передачі даних.

g) Фізична маніпуляція з системами, яка може створити можливість для атаки.

Аналіз загроз повинен також враховувати наслідки можливих атак. Вони можуть надати допомогу в з'ясуванні ступеня того чи іншого ризику та виявленні додаткових ризиків. Можливі наслідки атаки можуть включати:

- Порушення безпечної роботи транспортного засобу.
- Відмова деяких функцій транспортного засобу.
- Модифікація програмного забезпечення, зниження ефективності.
- Модифікація програмного забезпечення, але без наслідків для експлуатації.
- Порушення цілісності даних.
- Порушення конфіденційності даних.
- Втрата можливості виведення даних.
- Інші, включаючи злочинні дії.

Висновки.

Останнім часом відзначена зростаюча схильність інформаційної інфраструктури транспорту комп'ютерним атакам і особливо цілеспрямованим кібератакам. Це обумовлено широким впровадженням інформаційно - керуючих і автоматизованих засобів, інформаційних систем та телекомунікаційних мереж.

Було розглянуто основні передумови необхідності забезпечення інформаційної безпеки і кібербезпеки на транспорті в умовах широкої інформатизації та автоматизації транспортних процесів. Це вимагає об'єднання зусиль різних країн з урахуванням інтеграції транспортних систем і забезпечення міжнародної інформаційної безпеки та кібербезпеки на транспорті.

Література:

1. Study of the Potential Energy Consumption Impacts of Connected and Automated Vehicles March 2017 U.S. Energy Information Administration (EIA) U.S. Department of Energy, 15 p.

2. Порицкий, И.А. Оценка полноты информации в едином информационном пространстве / И.А. Порицкий // Вестник РГУПС – 2014. № 1. – С. 705.

3. Nyrkov, A. P., S. S. Sokolov, E. A. Mustakaeva, and V. A. Malcev. “Providing the necessary information security regime assets multiservice network transport industry.” Information security problems. Computer systems. 1 (2014): 51.

4. Makarov, A. D., D. V. Shved, and V. G. Shved. “Innovative approach in the Russian economy – the formal model of information security management.” Actual research directions: from theory to practice: the materials V Intern. scientific and practical. Conf Cheboksary: CNS “Interactive plus”, 2015: 37.

References:

1. Study of the Potential Energy Consumption Impacts of Connected and Automated Vehicles March 2017 U.S. Energy Information Administration (EIA) U.S. Department of Energy, 15 p.
2. Poritsky, I.A. Assessment of the completeness of information in a single information space / I.A. Poritsky // Bulletin of RSTU - 2014. No. 1. - P. 705.
3. Nyrkov, A. P., S. S. Sokolov, E. A. Mustakaeva, and V. A. Malcev. "Providing the necessary information security regime assets multiservice network transport industry." Information security problems. Computer systems. 1 (2014): 51.
4. Makarov, A. D., D. V. Shved, and V. G. Shved. "Innovative approach in the Russian economy – the formal model of information security management." Actual research directions: from theory to practice: the materials V Intern. scientific and practical. Conf Cheboksary: CNS "Interactive plus", 2015: 37.

Annotation. *The paper considers the preconditions for the formation of the need to ensure information and cybersecurity of transport flows in terms of informatization and automation of transport processes. Modern civilization is formed by post-industrial and information processes within the socio-technical space. In the space under study, knowledge is presented in the form of information resources and becomes the main asset and the most important factor in economic development, and the information industry - one of the main sectors of the economy. The processes of informatization of socio-technical activities, both in the production and non-production component are so large and deep that has led to qualitative changes in society itself, infinitely expanding the scope of products and services of the information industry, steadily involving society.*

Key words: *IT security, information security, cybersecurity, information technologies, transport flows.*

Стаття відправлена: 07.10.2021 р.