бирає обертів, а значить є сенс вивчати тактику та стратегію супротивника, щоб наносити випереджувальні удари.

Ми повинні визнати, що знаходимося в самому розпалі нової «холодної війни», де інформаційна складова стала ще більш значущою, ніж у попередній.

1. Дубов Д. Инструменты российской пропаганды: старые песни на новый лад. URL: http://www.russkiivopros.com/index.php?pag=one&id= 740&kat=5&csl=83 (дата звернення 12.02.2019).
2. Російська «фабрика тролів»: Колишній працівник розкрив подробиці його роботи. URL: https://24tv.ua/mizhnarodni_novini_tag1121 (дата звернення 13.02.2019).
3. Спеціальний відділ фабрики тролів РФ для підривних пропагандистських операцій в США. URL: https://www.obozrevatel.com/ukr/ my/politics/spetsialnij-viddil-fabriki-troliv-rf-dlya-pidrivnih-propagandistskih-operatsij-v-ssha.htm (дата звернення 16.02.2019).

Вишня Володимир Борисович
професор кафедри,
доктор технічних наук, професор

Гавриш Олег Степанович
викладач кафедри
економічної та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ

БЕЗПЕКА ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ СИСТЕМ НА ЗАЛІЗНИЦЯХ УКРАЇНИ

Однією з інформаційних систем, яку запропоновано до впровадження на залізницях країни, є автоматизована інформаційна система супроводження вантажоперевезень на залізницях [1].

У рамках цієї системи пропонується обладнати на вузлових, стикових і великих залізничних станціях вагоконтрольні пункти (ВКП), які б здійснювали зважування вагонів з високоліквідним вантажем, у русі, без розчеплення вагонів. По цій мережі, у напрямку руху потягу з вантажами, від одного ВКП до іншого повинна передаватися інформація натурного аркуша на потяг, а саме; порядковий номер розміщення вагона з вантажем у складі потягу, вага вагону й вантажу, станції відвантаження й призначення. Результати зважування вантажу на ВКП пересилаються на наступний вагоконтрольний пункт у напрямку руху потягу для подальшого контролю схоронності вантажу, що транспортується

У випадку розбіжності показань вагоконтрольного пристрою на ВКП й супровідної інформації на вантаж фіксується нестача вантажу у вагоні й відповідна інформація про це пересилається до підрозділу поліції й управління залізниці. Тобто маємо приклад оперативного реагування на факт здійснення злочину, що дозволить “гарячими” слідами більш ефективно його розкривати й розслідувати, приймати правильні управлінські й організаційні рішення [2]. Запропонована ідея захищена Патентом України № 8927 «Спосіб контролю схоронності вантажоперевезень на залізниці».

Впровадження такої складної системи контролю і супроводження вантажів, безумовно, потребує її надійності та захищеності від сторонніх втручань. І якщо надійність роботи системи багато в чому залежить від надійності складових системи, то захищеність потребує додаткових теоретичних опрацювань та суттєвих фінансових вкладень.

Взагалі організація забезпечення безпеки інформації повинна мати комплексний характер і спиратися на всебічний аналіз можливих негативних наслідків. При цьому важливо не упустити будь-які суттєві аспекти. Аналіз негативних наслідків припускає обов’язкову ідентифікацію можливих джерел загроз, факторів, сприятливих їх прояву, і, як наслідок, визначення актуальних загроз безпеки інформації.

Виходячи з викладеного, моделювання та класифікацію джерел загроз та їх проявів доцільно проводити на основі аналізу взаємодії такого логічного ланцюга: **джерело загроз – фактор *(уразливість)* – загроза *(дія)* – наслідок *(атака).***

Взагалі загроз безпеки інформації не так вже й багато. Якщо розглядати загрозу як небезпеку нанесення шкоди, то в цьому разі проявляється жорсткий зв’язок технічних проблем з юридичною категорією, якою є шкода.

Виключно для системи, що розглядається, нас цікавить лише шкода, яка нанесена будь-яким суб’єктом і ми маємо у наявності злочин. Інша річ, що дії суб’єкта можуть бути

вчинені з умисною формою вини у вигляді прямого чи евентуального умислу або з необережності, а заподіяна матеріальна шкода є ознакою об'єктивної сторони складу злочину.

Аналізуючи систему електронного супроводження вантажоперевезень і, зокрема, ВКП, можна стверджувати, що основними загрозами безпеці інформації є такі:

- викрадання (копіювання) інформації;
- знищення інформації;
- модифікація (викривлення) інформації;
- порушення присутності (блокування) інформації;
- заперечення дійсності інформації;
- нав'язування хибної інформації.

Носіями загроз безпеки інформації є джерела загроз, які можуть розміщуватися як всередині об'єкта, що захищається (внутрішні джерела), так і за межами його (зовнішні джерела). Такий розподіл джерел загроз є виправданим, бо для однієї і тієї самої загрози методи захисту для внутрішніх і зовнішніх джерел можуть бути різними.

Вище ми зазначали, що будемо враховувати джерела загроз, які обумовлені діями суб'єкта (антропогенні джерела загроз) та технічними засобами (техногенні джерела загроз).

Перша група найбільш численна і представляє певний інтерес, так як дії суб'єкта завжди можна оцінити, спрогнозувати і вжити адекватні заходи. Методи протидії у цьому випадку керовані і прямо залежать від волі організаторів захисту інформації. Антропогенні джерела загроз можуть бути зовнішніми (кримінальні структури, які намагаються приховати місце вчинення відкритого викрадання вантажу; співробітники залізниці і клієнтських організацій, що зацікавлені у приховуванні маскованого викрадання вантажу; потенційні злочинці і хакери; технічний персонал, що надає тематичні послуги; представники силових структур) і внутрішніми (основний персонал (оператор ВКП, розробники обладнання, програмісти); представники служби захисту інформації; допоміжний персонал (прибиральники); технічний персонал, що забезпечує життєдіяльність об'єкта).

Необхідно враховувати, що внутрішні джерела (суб'єкти), як правило, представляють собою висококваліфікованих фахівців в області розробки та експлуатації програмного забезпечення і технічних засобів, знайомих зі специфікою задач, що вирішуються, структурою, основними функціями і принципами роботи програмно-апаратних засобів захисту інформації, мають можливість використання штатного обладнання і технічних засобів мережі.

Окрему групу внутрішніх антропогенних джерел складають спеціально введені особи і завербовані агенти, які можуть належати до основного, допоміжного чи технічного персоналу, а також представників служби захисту інформації. Дана група розглядається у складі наведених вище джерел загроз, але методи протидії загрозам для цієї групи можуть мати свої відмінності.

Техногенні джерела загроз також можуть бути зовнішніми (засоби зв'язку) і внутрішніми (неякісні технічні та програмні засоби обробки інформації; допоміжні засоби охорони, сигналізації, телефонії; інші технічні засоби, які застосовуються).

Надана нами кваліфікація антропогенних та технічних джерел інформації віді важливу роль в оцінці їх впливу і враховується при ранжируванні джерел загроз, яке надає кількісну оцінку міри небезпеки джерела.

Треба розуміти, що можлива небезпека здійснення будь-якої дії, спрямованої проти об'єкта захисту, проявляється не сама по собі, а через уразливості (фактори), що призводять до порушення безпеки інформації на об'єкті. Кожній загрозі можуть бути поставлені у відповідність різні уразливості. Усунення або суттєве ослаблення уразливості впливає на можливість реалізації загроз безпеки інформації.

Уразливості, для зручності аналізу, поділені на класи, групи, підгрупи, і можуть бути: об'єктивними, суб'єктивними та випадковими.

Об'єктивні уразливості залежать від особливостей побудови і технічних характеристик обладнання, що використовується на об'єкті, який захищається. Повне усунення цих уразливостей неможливе, але вони можуть бути суттєво ослаблені технічними та інженерно-технічними методами протидії загрозам безпеки інформації. До об'єктивних належать уразливості: супутні технічним засобам випромінювання (електромагнітні, електричні, звукові), активізовувані (апаратні та програмні закладки), обумовлені особливостями елементів (мікрофони, котушки індуктивності, мікросхеми, магнітні носії та інше), обумовлені особливостями об'єкта, що захищається (організацією каналів обліку інформації, розміщенням об'єкта тощо).

Суб'єктивні уразливості залежать від дій співробітників і переважно усуваються організаційними і програмно-апаратними методами. До них належать помилки (при підготовці і використанні програмного забезпечення, при управлінні складними системами, при експлуатації технічних засобів) та порушення (режиму охорони і захисту, режиму експлуа-

тації технічних засобів, режиму використання інформації, режиму конфіденційності).

Випадкові уразливості залежать від непередбачуваних обставин. Ці фактори, як правило, малоймовірні і їх усунення можливе лише при проведенні комплексу організаційних та інженерно-технічних заходів по протидії загрозам інформаційної безпеки. До випадкових уразливостей належать: збої та відмови (відмови і несправності технічних засобів, старіння и розмагнічування носіїв інформації, збої програмного забезпечення, збої електропостачання) та пошкодження.

При визначенні актуальних загроз експертно-аналітичним методом визначаються об'єкти захисту, піддані впливу тієї чи іншої загрози, характерні джерела цих загроз і уразливості, які сприяють реалізації загрози. При цьому створюється матриця взаємозв'язку джерел загроз і уразливостей, з якої визначаються можливі наслідки реалізації загроз (атаки) і розраховується коефіцієнт небезпечності цих атак. Така матриця створюється для кожної загрози.

На основі викладених положень авторами були розроблені модель загроз (формалізований опис методів і способів здійснення загроз) і модель порушника (формалізовані дії порушення) для об'єктів (ВКП) електронної мережі супроводу вантажоперевезень на залізницях.

Отримані результати дозволять певним чином поліпшити інформаційний захист банку даних мережі та організувати надійну роботу вагоконтрольних пунктів системи.

1. Вишня В.Б. Особливості розкриття крадіжок вантажів на залізничному транспорті. *Науковий вісник Дніпропетровського державного університету внутрішніх справ:* зб. наук. праць. 2015. № 2. С. 315–322.

2. Вишня О.В. Боротьба з викраданням вантажів на залізницях неповнолітніми // Актуальні проблеми боротьби зі злочинністю неповнолітніх: вітчизняний та міжнародний досвід: матеріали Міжнарод. наук.-практ. конф. (м. Дніпропетровськ, 27–28 квітня 2012 р.). Дніпропетровськ, 2012. С. 170–174.

Мокляк Сергій Петрович
професор Воєнно-дипломатичної академії
імені Євгенія Березняка,
кандидат технічних наук, професор

АНАЛІЗ ІСНУЮЧОЇ ПРАКТИКИ ПІДГОТОВКИ ТА ВЕДЕННЯ ІНФОРМАЦІЙНОГО ПРОТИБОРСТВА У СФЕРІ ВІЙСЬКОВО-ТЕХНІЧНОГО СПІВРОБІТНИЦТВА УКРАЇНИ

Активна позиція України на ринку продукції військового призначення виводить сферу ВТС на рівень найбільш прибуткових та найважливіших напрямків зовнішньополітичної та зовнішньоекономічної діяльності нашої держави. В той же час саме експортна спрямованість військово-технічного співробітництва України спричиняє постійну протидію з боку конкурентних країн та транснаціональних корпорацій [1].

Подібні дії створюють пряму загрозу національній безпеці України, оскільки протидія ВТС, як одному з елементів воєнно-економічної безпеки нашої держави, в той же час шкодить і політичному іміджу нашої держави.

Одним з найбільш дієвих засобів протидії успішній реалізації Україною ВТС з іншими країнами є проведення проти неї інформаційних операцій, які здійснюються за класичними методиками та алгоритмами, однак мають певні особливості.

Насамперед, це стосується широкого використання ЗМІ на міжнародному та національному рівні. Специфіка інформаційних матеріалів щодо ВТС надає змогу організаторам інформаційних операцій використовувати ЗМІ «втемну». Це пояснюється тим, що, як правило, журналісти не можуть отримати повну інформацію з цих питань. Більш того, часто вони не володіють усім необхідним масивом інформації і специфічними знаннями в цій сфері. В результаті інформаційна операція може ґрунтуватись на непідтвердженій або повністю сфальсифікованій інформації, однак ЗМІ будуть вимушені користуватися цими даними до отримання коментарів з урядових та експертних джерел.

Також однією зі специфічних рис подібних інформаційних операцій є закритість даних стосовно ВТС. З одного боку, це спрощує завдання організаторам операцій – перевірити їхню інформацію буде важко, оскільки офіційні структури можуть утриматись від коментарів через «грифованість» даних. З іншого боку, реагування представників уряду на інформаційні повідомлення у цій сфері буде завжди затримуватись у зв'язку з існуючою процедурою узгодження та перевірки даних у державних органах.

Виходячи з того, що ВТС з іноземними державами має два аспекти: воєнно-політичний та воєнно-економічний, залежно від мети основні завдання інформаційної про-