УДК 004.056.5:629.73(045)

О.О. ЗОЛОТАР, Національний авіаційний університет

ПОПЕРЕДЖЕННЯ ПРАВОПОРУШЕНЬ В ІНФОРМАЦІЙНІЙ СФЕРІ ДІЯЛЬНОСТІ СУБ’ЄКТІВ ЦИВІЛЬНОЇ АВІАЦІЇ

***Анотація**. Щодо загроз діяльності суб’єктів цивільної авіації у зв’язку з функціонуванням телекомунікаційних систем та визначенням напрямів попередження правопорушень в цій сфері.*

Цивільна авіація є сферою, яка постійно зазнає модернізації з метою досягнення максимальної ефективності її функціонування. Сучасні інформаційні технології інтенсивно застосовуються в цивільній авіації, зокрема:

PSTN (Public Switched Telephone Network) – загальнодоступна телефонна мережа, яка комутується;

CSPDN (Circuit Switched Public Data Network) – загальнодоступна цифрова мережа передачі даних, яка комутується;

PSPDN (Packed Switched Public Data Network) – загальнодоступна цифрова мережа передачі даних з комутацією пакетів;

LAN (Local Area Network) – локальна обчислювальна мережа;

ISDN (Integrated Services Digital Network) – цифрова мережа загального обслуговування [1].

Відповідно інтенсивного розвитку вимагає підтримка інформаційної безпеки, яка полягає у застосуванні спеціальних засобів, методів та заходів з метою запобігання завданню шкоди інформації та інформаційним відносинам. Враховуючи те, що інформаційні правопорушення як інформаційні загрози в авіаційній галузі можуть призвести до різних розмірів наслідків – від економічних збитків до зниження безпеки польотів і людських жертв, можна стверджувати, що тема статті є актуальною.

Інформаційна безпека цивільної авіації інтенсивно досліджується з точки зору переважно технічних наук. Однак правовий аспект цього питання на сьогодні залишається не повністю визначений. При написанні цієї статті застосовані окремі результати правових досліджень з питань інформаційної безпеки, зокрема захисту інформації, таких дослідників, як: О. Баранов, В. Брижко, В. Гавловський, Л. Задорожна, Р. Калюжний, А. Кузьменко, В. Цимбалюк, Б. Кормич, М. Швець та інших.

Метою цієї статті є наукове обґрунтування основних напрямів попередження правопорушень в інформаційній сфері діяльності суб’єктів цивільної авіації.

Суспільні відносини в сучасному світі визначаються насиченістю значних обсягів інформації, великою кількістю інформаційних зв’язків. Ця риса сучасності є номінальною ознакою інформаційного суспільства. Кормич Б.А. називає її “всепроникливістю інформації у всі сфери життєдіяльності суспільства” [2].

Створюючи нові можливості, як то прискорення суспільних процесів, доступність взаємозв’язку і співпраці віддалених суб’єктів, вдосконалення функціонування і обслуговування складних систем, інформаційні технології несуть в собі також нові загрози. Інформаційна безпека вимагає комплексного підходу, тобто застосування всіх доступних засобів, методів та ресурсів.

Першим етапом ефективного впливу на будь-яке негативне явище є аналіз його сутності. Зупинимось на принципах побудови сучасних авіаційних телекомунікаційних

систем. Відповідно до керівних матеріалів ІСАО електрозв’язок у цивільній авіації має забезпечувати потреби таких служб: обслуговування повітряного руху, аеронавігаційної інформації, метеорології, пошуку та рятування потерпілих. При цьому мають бути виконані конкретні вимоги щодо надійності і цілісності системи, безперервності обслуговування повідомлень, затримки проходження друкованих та цифрових даних, повідомлень мовного зв’язку.

Поточні потреби обслуговування повітряного руху у більшості регіонів задовольняються за рахунок застосування: ліній передачі та центрів мереж AFTN та CIDIN; ліній передачі та центрів зв’язку європейського метеорологічного оперативного зв'язку (MOTNE); ліній оперативно-мовного зв’язку обслуговування повітряного руху (мережа безпосередньої взаємодії диспетчерських пунктів); ліній передачі обміну даними між ЕОМ обслуговування повітряного руху; радіоканалів зв’язку “Земля – Борт” [1].

Авіаційний електрозв’язок у цивільній авіації має забезпечувати: передавання на борт повітряного корабля різних повідомлень з обслуговування повітряного руху, які спрямовані на безпеку та регулярність польотів; передавання екіпажам повітряного корабля вказівок і розпоряджень та отримання від них донесень і повідомлень на всіх етапах польоту – від злету до посадки включно; передавання та приймання повідомлень про повітряну та метеорологічну обстановку; обмін відповідними повідомленнями з взаємодіючими пунктами керування й органами інших відомств, у тому числі міжнародних; взаємодію між службами та підрозділами авіапідприємств; передавання розпоряджень, вказівок та інших повідомлень від керівних органів цивільної авіації в підлеглі організації і підприємства та отримання від них повідомлень і донесень.

Функції авіаційного електрозв’язку реалізуються рядом центрів комутації, вузлів зв'язку, приймально-передавальних центрів, станцій і кінцевих пристроїв, які з’єднані між собою каналами і лініями передачі в порядку, що відповідає прийнятій системі організації зв’язку.

Авіаційний електрозв’язок має задовольняти високі вимоги щодо оперативності, надійності, достовірності та швидкості передавання повідомлень, необхідної скритості, максимальної економічності організації і функціонування.

Відомчі авіаційні телекомунікаційні системи будуються, як правило, на базі орендованих магістральних ліній передач (телефонних каналів загального користування). Сучасні системи передачі даних – це програмно-технічні комплекси, створені на базі персональних комп’ютерів, високошвидкісних модемів та існуючих каналів зв’язку.

Не заглиблюючись в деталі функціонування згаданих систем, звернемо увагу на канали витоку інформації, тобто дестабілізуючі фактори. До них належать:

1) крадіжки програмно-технічних засобів та (або) документації на них на заводах виробниках, в службах ремонту, під час перевірки сертифікації її у користувача з метою виявлення характеру та структури даних, що передаються;

2) провокування підслуховування розмов осіб, які мають відношення до системи передавання даних та ліній зв’язку, з метою виявлення змісту передавання, параметрів та змісту передавання даних;

3) застосування візуальних засобів (фотоапарати, телекамери, біноклі тощо) з метою отримання інформації про апаратуру та технології обробки інформації, ознаки даних, що передаються;

4) вилучення виробничих відходів (носіїв інформації, документів тощо);

5) перехоплення електромагнітних випромінювань і оптичних сигналів різних видів та джерел як з метою ідентифікації абонентів, так і отримання відповідних даних;

6) копіювання змісту файлів з метою отримання даних, що раніше передавались;

7) перегляд і копіювання експлуатаційних документів та журналів обліку з метою одержання інформації про зміст даних, що передаються, трафік тощо;

8) копіювання сигналів виклику та автовиклику систем передавання даних з метою визначення номера абонента, що викликається;

9) заміна програмно-апаратних засобів апаратури передавання даних з метою наступної переадресації даних зловмиснику;

10) заміна документів, що регламентують трафік;

11) заміна або крадіжка носіїв інформації, які містять дані, що передаються з метою спотворення, знищення або модифікації даних;

12) підключення підслуховуючої апаратури, магнітофонів тощо з метою одержання інформації в наступні періоди про характер даних, трафік, технології передавання;

13) підключення нештатної апаратури до елементів системи передавання даних з метою одержання, спотворення, модифікації або знищення даних, а також з метою переадресації даних зловмиснику;

14) копіювання, спотворення або заміна сигналів автоматичного виклику систем передавання даних з метою визначення і переадресації даних, що передаються;

15) копіювання, спотворення або генерація хибних сигналів з метою копіювання, спотворення або модифікації даних, що передаються, а також з метою знищення даних та інші дестабілізуючі фактори.

Переважна більшість дестабілізуючих факторів у роботі авіаційних систем, телекомунікацій у цивільній авіації є наслідками неправомірного втручання в його функціонування або неправомірного впливу на осіб, що обслуговують відповідні системи.

Окрім несанкціонованого доступу до інформації та інформаційних систем існують також й інші види загроз інформаційній безпеці в цивільній авіації. Інформація може бути втрачена шляхом фізичного знищення її носіїв, пошкодження чи знищення системи передачі даних, втручання в роботу програмного забезпечення.

На основі проведеного аналізу існуючих загроз можна визначити наступні напрями організації попередження інформаційних правопорушень в цивільній авіації:

I. Програмно-технічний.

II. Правовий.

III. Морально-етичний.

Критерієм цієї класифікації є основні засоби впливу на явище з метою підвищення стану його захищеності, тобто підвищення рівня безпеки, і, одночасно, попередження правопорушень у відповідній сфері.

Організація технічного напряму реалізується за допомогою наступних заходів:

- встановлення засобів виявлення та індикації загроз і перевірка працездатності;
- встановлення захищених засобів опрацювання інформації, засобів технічного захисту інформації та перевірка їх працездатності;
- застосування програмних засобів захисту комп’ютерної техніки, автоматизованих систем; здійснення їх тестування на відповідність вимогам захищеності;
- застосування спеціальних інженерно-технічних споруд, засобів (системи) [3].

Вибір засобів організації технічного захисту інформації зумовлюється фрагментарним, ситуативним або комплексним способом. Це забезпечує протидію певній загрозі. Комплексний захист забезпечує одночасну протидію кільком загрозам.

Засоби виявлення та індикації загроз застосовують для сигналізації та оповіщення суб’єкта (користувача, розпорядника) інформації з обмеженим доступом про витік інформації чи порушення її цілісності.

Засоби технічного захисту інформації застосовуються автономно або разом з іншими технічними засобами інформаційної діяльності для пасивного або активного приховування інформації з обмеженим доступом.

Для пасивного приховування застосовують фільтри-обмежувачі, лінійні фільтри, спеціальні абонентські пристрої захисту та електромагнітні екрани.

Для активного приховування застосовують вузькосмугові й широкосмугові генератори лінійного та просторового зашумлення.

Спеціальні інженерно-технічні споруди, засоби та системи застосовуються для оптичного, акустичного, електромагнітного та іншого екранування носіїв інформації. До них належать спеціально обладнані світлопроникні, технологічні та санітарно-технічні отвори, а також спеціальні камери, перекриття, навіси, канали тощо.

Вищезазначене знаходить вираз у юридико-технічних нормативах, які відображаються у державних технічних стандартах та інших нормативних документах. Розміщення, монтування та прокладання спеціальних інженерно-технічних засобів і систем, серед них систем заземлення та електроживлення, здійснюються відповідно до вимог нормативних документів з технічного захисту інформації.

Програмні засоби застосовуються для забезпечення:

- ідентифікації та автентифікації користувачів, персоналу й ресурсів системи обробки даних;
- розмежування доступу користувачів до інформації, засобів обчислювальної техніки й технічних засобів автоматизованих систем;
- цілісності даних та конфігурації автоматизованих систем;
- реєстрації та обліку дій користувачів;
- маскування опрацьованої інформації;
- реагування (сигналізації, відключення, зупинення робіт, відмови у запиті) на спроби несанкціонованих дій [3].

Морально-етичні засоби реалізуються у вигляді різних правил, які склались традиційно в суспільстві, зокрема, що складаються в процесі формування розвитку обчислювальної техніки, телекомунікацій та інформаційних технологій. Комунікативні, інформаційні відносини в суспільстві завжди регулювались переважно в межах інтересів держави. Проте, інформаційна сфера діалектично завжди прагнула до саморегулювання, до самовизначеності людини (що й становить сенс життя), а отже застосовувала практично вироблені **принципи звичаю**, чим намагалась здійснити попередження інформаційних правопорушень. Проте, закріплення цього попереджувального впливу у нормах права завжди було дуже незначним.

Правовий напрям попередження інформаційних правопорушень охоплює множину заходів, які умовно можна класифікувати наступним чином:

I. За змістом:

1) організаційно-технічні;
2) організаційно-технологічні;
3) організаційно-управлінські.

II. За масштабом реалізації:

1) міжнародні чи міждержавні;
2) державні;
3) локальні.

Організаційно-управлінські заходи спрямовані на створення необхідних умов для безпечного обігу використання інформації в соціально-технічних системах. Зокрема, до них можна віднести наступні:

- кадрова політика (підбір, розстановка, виховання, навчання кадрів тощо);
- система режиму доступу до інформації, встановлення порядку обмеженого доступу, реєстрація і облік персоналу, реагування на спроби несанкціонованих дій;
- створення спеціальних структур, які покликані реалізовувати регулятивну і охоронну функції та інші заходи.

Щодо юридичних заходів, то йдеться, насамперед, про створення ефективної системи національного законодавства з урахуванням вимог міжнародно-правових актів, що регламентують правила обробки і поширення інформації, а також встановлюють відповідальність за порушення цих правил.

Висновки.

1. Аналіз чинного законодавства в дослідженій сфері свідчить про його комплексний зміст. Правові норми, які регламентують захист інформації в цивільній авіації, містяться в таких галузях, як конституційне, інформаційне, повітряне, кримінальне, цивільне, міжнародне право. Особливої уваги вимагає значна кількість норм міжнародних актів (вимоги ІСАО), які регулюють зазначену сферу. Це обумовлює необхідність приведення національного законодавства у відповідність до стандартів міжнародного права.

2. Значної уваги потребує ***відповідальність діяльності органів державної влади***, *які відповідають* ***за інформаційну безпеку*** в цивільній авіації.

Конституція України визначає – підтримка інформаційної безпеки, яка є складовою національної безпеки, є однією з найважливіших функцій держави [5].

3. Загальний перелік державних органів, які беруть участь у підтриманні безпеки цивільної авіації, та коло їх повноважень окреслені в Державній програмі авіаційної безпеки цивільної авіації, а також у законах, що регулюють діяльність цих органів. Їх функції є неузгоджені, а повноваження неконкретизовані.

4. Підсумовуючи, зазначимо, що механізм реалізації відповідальності за правопорушення в інформаційній сфері в цивільній авіації потребує вдосконалення. Цим правопорушенням властивий високий ступінь латентності, обумовлений рядом факторів – від недостатнього рівня кваліфікації працівників правоохоронних органів до незацікавленості підприємств цивільної авіації в розголошенні інформації про відповідні правопорушення.

5. Подальші дослідження зазначених і суміжних питань є необхідною умовою створення і функціонування ефективної системи організації попередження правопорушень з метою підтримання безпеки цивільної авіації, в тому числі її інформаційної складової.

Використана література

1. Безпека авіації / [В.П. Бабак, В.П. Харченко, В.Г. Максимов та ін.]. – К. : Техніка, 2004. – 584 с.

2. Кормич Б.А. Інформаційна безпека : організаційно-правові основи : навч. посібник для студентів вищих навчальних закладів / Б.А. Кормич. – К. : Кондор, 2004. – 384с.

3. Домарєв В.В. Організація захисту інформації на об’єктах державної та підприємницької діяльності : навч. посібник / В.В. Домарєв, С.О. Скворцов. – К. : Вид-во Європ. ун-ту, 2006. – 102 с.

4. Організаційно-правові основи захисту інформації з обмеженим доступом : навч. посібник ; за заг. ред. В.С. Сідака. – К. : Вид-во Європ. ун-ту, 2006. – 232 с.

5. Конституція України : Закон України від 28 червня 1996 року // Відомості Верховної Ради (ВВР). – 1996. – № 30. – Ст. 141

6. Державна програма авіаційної безпеки цивільної авіації : Закон України від 20 лютого 2003 року № 545-IV // Відомості Верховної Ради України (ВВР). – 2003. – № 17. – Ст. 140.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~