УДК 004.413.7

І.Д. ГОРБЕНКО, д-р техн. наук, О.А. ЗАМУЛА, д-р техн. наук,
С.Г. ВДОВЕНКО, В.І. ЧЕРНИШ

МЕТОД ОЦІНКИ ЗРІЛОСТІ СИСТЕМИ УПРАВЛІННЯ БЕЗПЕКОЮ ПРИ ОРГАНІЗАЦІЇ ПОВІТРЯНОГО РУХУ

Вступ та постановка проблеми дослідження

Безпека на повітряному транспорті – це комплексна властивість авіаційної транспортної системи виконувати свої функції без нанесення шкоди самій системі або населенню. Питання забезпечення захисту інфраструктури системи організації повітряного руху (ОрПР) провайдера аеронавігаційного обслуговування (АНО) здійснюється шляхом забезпечення безпеки інформаційно-телекомунікаційних систем (ІТС), фізичної безпеки, кадрової безпеки та забезпечення безперервності надання послуг з АНО. Аеронавігаційне обслуговування – це обслуговування, яке здійснюється провайдерами АНО на всіх етапах польоту повітряних суден, що включає організацію повітряного руху, зв'язок, навігацію, спостереження (радіотехнічне забезпечення), пошук і рятування, метеорологічне обслуговування та надання аеронавігаційної інформації [1]. Провайдер АНО – це суб'єкт авіаційної діяльності, який надає послуги з елементів (напрямів) аеронавігаційного обслуговування повітряних суден [1]. Система організації повітряного руху (ОрПР) – це частина аеронавігаційної системи, яка складається з наземних та повітряних компонентів організації повітряного руху [1]. Система ОрПР включає також людські ресурси, процедури та обладнання (технічні засоби та програмне забезпечення), що використовуються для реалізації завдань з ОрПР, а також передбачає наявність систем зв’язку, навігації та спостереження (ЗНС).

Забезпечення інформаційної безпеки (ІБ) при ОрПР являє собою комплексну проблему, яка включає:

- правове регулювання застосування інформаційних технологій (ІТ);
- вдосконалення технологій розробки ІТ і захисту інформації в інформаційно-телекомунікаційних системах (ІТС);
- розвиток системи сертифікації; забезпечення відповідних організаційно-технічних умов експлуатації ІТС.

Недопущення авіаційних подій та інцидентів, пов'язаних з операційними діями при наданні послуг з аеронавігаційного обслуговування є бажаним результатом діяльності галузі та провайдерів АНО. Захист інфраструктури в частині, що стосується забезпечення ІБ провайдера АНО, необхідно для того, щоб в умовах виникнення загроз в розумній мірі забезпечувалась безпека при ОрПР. Забезпечення безпеки системи організації повітряного руху являє собою захист системи ОрПР провайдера АНО від загроз безпеки, захист вразливих місць, а також внесок системи ОрПР в забезпечення безпеки цивільної авіації, національної безпеки і оборони та охорони правопорядку [2].

1. Аналіз процесу забезпечення безпеки системи організації повітряного руху провайдера аеронавігаційного обслуговування

Інфраструктура системи ОрПР охоплює персонал, процедури, інформацію, ресурси, засоби і служби, у тому числі центри управління, аеропорти і обладнання, включаючи системи ЗНС та інформаційно-телекомунікаційні системи (ІТС). Захист інфраструктури системи ОрПР реалізується за допомогою забезпечення безпеки інформаційно-телекомунікаційних систем $InfSEC$, фізичної безпеки $PhSEC$ і безпеки персоналу $HrSEC$.

Забезпечення безпеки ІТС провайдера АНО передбачає застосування заходів захисту інформації та даних, які обробляються, зберігаються або передаються в ІТС, від випадкової або навмисної втрати цілісності, конфіденційності та доступності, а також захисту самих систем від

втрати цілісності або доступності. Заходи щодо забезпечення безпеки ІТС включають в себе захист:

- робочих місць персоналу провайдера АНО;
- автоматизованих систем керування повітряним рухом (АС КПР);
- систем передачі інформації і даних.

Відповідні заходи також передбачають ідентифікацію загроз інформаційної безпеки (ІБ) інфраструктури провайдера АНО, складання документальної бази стосовно протидії загрозам ІБ.

При розробці програми забезпечення безпеки ІТС провайдера АНО повинні застосовувати підхід до управління ризиком.

Фізична безпека $PhSEC$ – складовачастина діяльності з забезпечення безпеки системи ОрПР, що передбачає прийняття фізичних заходів для захисту персоналу, запобігання несанкціонованого доступу до обладнання, засобів, матеріалів і документів та забезпечення гарантій того, що система захисту не буде зруйнована. Фізична безпека передбачає вжиття заходів, покликаних виключити можливість доступу до будівель, ресурсів або інформації, що зберігається, з боку персоналу, який не має на те відповідного дозволу. Фізична безпека може забезпечуватися простим замиканням дверей або застосуванням складного багаторівневого підходу з використанням заходів стримування, виявлення і захисту. Заходи безпеки повинні застосовуватися таким чином, щоб при цьому забезпечувалася ефективність використання наявних ресурсів. Іншими словами, по відношенню до передбачуваних загроз заходи безпеки повинні бути економічно ефективними і відповідати ступеню критичності об'єктів.

Безпека персоналу $HrSEC$ є складовою частиною діяльності по забезпеченню безпеки системи ОрПР провайдера АНО, що передбачає використання процедур, які дозволяють оцінити можливість надання будь-якій особі, враховуючи при цьому його лояльність, ступінь довіри до нього і надійність, початкового та постійного доступу до конфіденційної інформації і доступу в контрольовані зони об’єктів провайдера АНО без створення неприйнятного ризику безпеки системи ОрПР.

2. Загальна модель управління ризиками безпеки інфраструктури системи організації повітряного руху

Повністю виключити ризик неможливо, тому управління ризиком безпеки при ОрПР провайдер АНО повинен здійснювати на основі підходу, що передбачає використання наявної інформації стосовно потенційного ризику .

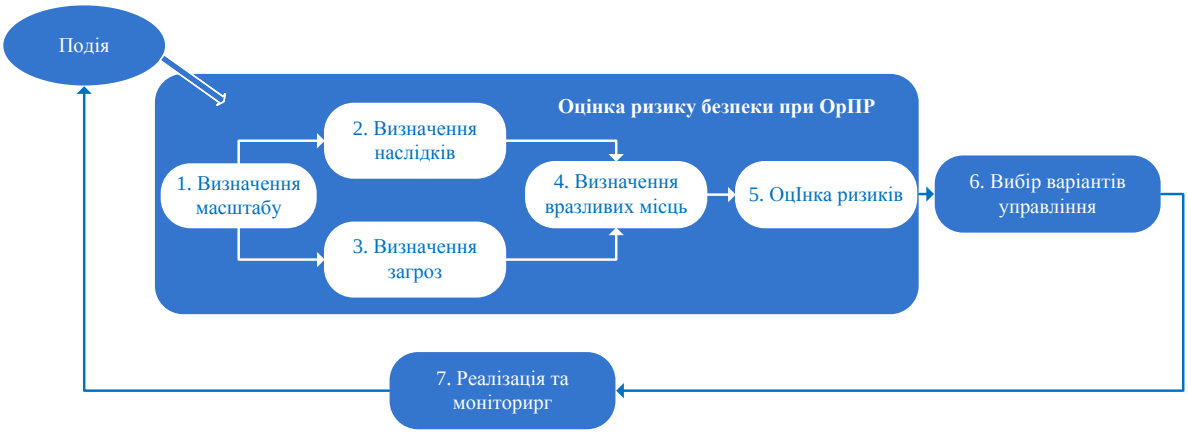
Процес управління ризиками $R(ATM)$ забезпечує можливість використання провайдером АНО структурованого підходу до прийняття обґрунтованих рішень щодо ризику безпеки персоналу $HrSEC$, фізичної безпеки $(PhSEC)$ та інформаційної безпеки (безпеки ІТС – $InfSEC$) і визначається правилом [2]:

$$R(ATM) = R\ (HrSEC), R\ (PhSEC), R\ (InfSEC). \quad (1)$$

Процес управління ризиком безпеки охоплює ряд взаємопов'язаних елементів і являє собою безперервно здійснювану діяльність циклічного характеру. Рисунок ілюструє цей процес, який може використовуватися провайдером АНО для систематичного виявлення ризику безпеки і визначення варіантів попередження наслідків [2].

Модель управління ризиком безпеки при ОрПР, що представлена в [2], має ряд недоліків, а саме:

- не враховує процеси управління фактором ризику для безпеки польотів;
- відсутність деталізації процедури управління ризиками, пов’язаними з безпекою персоналу $HrSEC$, інформаційною $InfSEC$ і фізичною безпекою $PhSEC$ відповідно;
- відсутність кількісної шкали оцінки визначення наслідків від реалізації загрози $T(ATM)$;
- відсутність кількісної шкали оцінки критичності активів провайдера АНО.



Процес управління ризиком безпеки при ОрПР

Одним із проблемних місць при розробці системи управління безпекою при ОрПР провайдером АНО є відсутність єдиного підходу до класифікації процесів управління безпекою ІТС. Для ефективного управління ризиком провайдер АНО визначає ініційовану подію, що забезпечить можливість постійного корегування процесу управління безпекою системи ОрПР (HrSEC, InfSEC, PhSEC). Оцінку ризику безпеки провайдер АНО може проводити на регулярній основі або у зв'язку зі зміною основних факторів, які здійснюють вплив на ступінь загрози системи ОрПР, при цьому характерними ініціюючими подіями є:

- зміна характеру загрози (типів загроз або частоти їх виникнення);
- інцидент, що пов'язаний з порушенням безпеки;
- зміна політики в сфері безпеки, яка може привести до зміни пріоритетів в сфері ризику або параметрів прийнятного ризику;
- впровадження змін у систему ОрПР.

3. Оцінка зрілості системи управління безпекою при ОрПР

Безпека в системі організації повітряного руху характеризується комплексом заходів протидії загрозам (у тому числі, загрозам інформаційної безпеки), які направлені на систему організації повітряного руху провайдера аеронавігаційного обслуговування. Такими загрозами можуть бути спроби атаки на активи провайдера АНО (органи обслуговування повітряного руху (ОПР), об’єкти радіотехнічного забезпечення (зв’язку, навігації, спостереження), персонал, тощо).

Основним напрямом забезпечення безпеки при ОрПР є захист інфраструктури провайдера АНО. Одним з найактуальніших на сьогодні питань в рамках забезпечення безпеки при ОрПР є оцінка ефективності системи управління безпекою при ОрПР, що розроблюється провайдером АНО. Управління безпекою при ОрПР, що включає захист інфраструктури системи ОрПР, спрямовано на підвищення якості управління провайдера АНО взагалі, тому показники ефективності їх формування та використання мають бути інтегрованими в систему управління провайдера АНО на всіх рівнях прийняття рішень, що викликає необхідність розробки методів оцінки ефективності [2].

На теперішній час відсутність кількісної оцінки щодо зрілості процесів забезпечення безпеки інфраструктури ускладнює створення відповідної системи управління провайдерами АНО.

Рівні зрілості бізнес-процесу –це розвиток провайдера АНО відповідно до стандартизованих моделей оцінки рівня зрілості управління, що визначаються різними характеристиками, такими як місія, стратегія, організаційна структура, безпека польотів, безпека при ОрПР та ін. Переходи з рівня на рівень роблять провайдера АНО більш конкурентоспроможним, підвищують рівень безпеки польотів та експлуатаційну ефективність системи ОрПР.

Більшість підприємств застосовують універсальну модель оцінки рівня зрілості управління – Capability Maturity Model Integration (CMMI) [3]. Набір моделей (методологій) дозволяє вдосконалити бізнес-процеси в організаціях різних розмірів і видів діяльності та може використову-

ватись для покращення процесу як на рівні проекту чи відділу, так і на рівні цілої організації. CMMI дозволяє інтегрувати традиційно відокремлені організаційні функції, ставити цілі та пріоритети покращення процесів, забезпечує інструкцією по створенню якісних процесів і дає контрольну точку для оцінки поточних процесів [CMMI]. Відповідно до [3 – 5] існує 5 рівнів зрілості, кожен з яких вказує на зрілість (з точки зору управління процесами безпеки) організації.

У сфері інформаційних технологій рівень зрілості визначається за допомогою моделі зрілості можливостей (модель повноти потенціалу) створення програмного забезпечення (ПЗ) – Capability Maturity Model (CMM) та ДСТУ ISO / IEC 15504 [4].

Вищезазначені методології не описують процедуру оцінки зрілості безпеки при ОрПР. Для визначення кількісного показника рівня розвитку системи управління безпекою при ОрПР провайдера АНО авторами розроблена та запропонована шкала еволюції, що заснована на п'яти загальних рівнях зрілості від A до E:

Ідентифікатор рівня	Якісний показник	Кількісний показник	Відповідність встановленим вимогам, %
A	Відсутній	0	(0 – 20]
B	Початковий	1	(20 – 40]
C	Середній	2	(40 – 60]
D	Високий	3	(60 – 80]
E	Оптимізований	4	(80 – 100]

Показником, що характеризує організаційну ефективність процесу забезпечення безпеки при ОрПР, формування і використання заходів з безпеки інфраструктури системи ОрПРв умовах стратегічного управління, є загальний рівень зрілості системи управління безпекою при ОрПР, який визначається на основі часткових рівнів зрілості для напрямків:

- безпека персоналу $HrSEC$;
- безпеку інформаційно-телекомунікаційних систем $InfSEC$;
- фізичної безпеки $PhSEC$;
- підтримки національних інтересів S, з ваговим коефіцієнтом часткового рівня 0,25 (або 25 %) та визначається виразом

$$M(SAS) = \left((M(HrSEC) \cdot 0{,}25) + (M(InfSEC) \cdot 0{,}25) + (M(PhSEC) \cdot 0{,}25) + (M(S) \cdot 0{,}25)\right) \cdot 100\%. \quad (2)$$

Відповідний підхід дозволяє охарактеризувати основні процеси забезпечення безпеки об'єктів АНО, зв'язку, навігації, спостереження (ЗНС) та інших структурних підрозділів провайдера АНО. Оцінка зрілості безпеки при ОрПР є основною складовою такого бізнес-процесу підприємства як якість надання послуг з АНО користувачам повітряного простору.

Авторами запропоновано при визначенні часткових рівнів зрілості системи безпеки при ОрПР використовувати опитувальник, у якому аудитор визначає відповідність провайдера АНО встановленим вимогам за напрямками $HrSEC, InfSEC, PhSEC, S$.

Частковий показник рівня зрілості за кожним запитанням відповідного напрямку опитувальника може бути обчислено відповідно до виразу

$$R\ (Q_i) = A_i\ \cdot W_i, \quad (3)$$

де: Q_i – і – та вимога відповідного напрямку; A_i – виконання Q_i-ї вимоги відповідного напрямку (кількісний показник знаходиться у діапазоні $0 < A_i \leq 2$), де 0 – вимога не виконується; 1 – вимога виконується частково; 2 – вимога виконується у повному обсязі; W_i – ваговий коефіцієнт Q_i-ї вимоги (встановлюється аудитором при розробленні листу відповідності, кількісний показник знаходиться у діапазоні $0 < Q_i \leq 4$).

Часткові показники для напрямків можуть бути розраховані відповідно до виразів:

$$RM(InfSEC) = \frac{R_{cur}(Q_1(InfSEC)) + R_{cur}(Q_i(InfSEC))}{R_{max}(Q_1(InfSEC)) + R_{max}(Q_i(InfSEC))} \cdot 100\%, \quad (4)$$

де $R_{cur}(Q_1(InfSEC)) + R_{cur}(Q_i(InfSEC))$ – підсумкова сума відповідей з урахуванням вагового коефіцієнту W_i для напрямку «безпека ІТС» (інформаційна безпека); $R_{max}(Q_1(InfSEC)) + R_{max}(Q_i(InfSEC))$ – підсумкова сума максимального значення відповідей (виконання вимог) з урахуванням вагового коефіцієнту W_i для напрямку «безпека ІТС» (інформаційна безпека);

$$RM(HrSEC) = \frac{R_{cur}(Q_1(HrSEC)) + R_{cur}(Q_i(HrSEC))}{R_{max}(Q_1(HrSEC)) + R_{max}(Q_i(HrSEC))} \cdot 100\% \quad , \quad (5)$$

де $R_{cur}(Q_1(HrSEC)) + R_{cur}(Q_i(HrSEC))$ – підсумкова сума відповідей з урахуванням вагового коефіцієнту W_i для напрямку безпека персоналу; $R_{max}(Q_1(HrSEC)) + R_{max}(Q_i(HrSEC))$ – підсумкова сума максимального значення відповідей (виконання вимог) з урахуванням вагового коефіцієнту W_i для напрямку безпека персоналу;

$$RM(PhSEC) = \frac{R_{cur}(Q_1(PhSEC)) + R_{cur}(Q_i(PhSEC))}{R_{max}(Q_1(PhSEC)) + R_{max}(Q_i(PhSEC))} \cdot 100\% \quad , \quad (6)$$

де $R_{cur}(Q_1(PhSEC)) + R_{cur}(Q_i(PhSEC))$ – підсумкова сума відповідей з урахуванням вагового коефіцієнту W_i для напрямку фізична безпека; $R_{max}(Q_1(PhSEC)) + R_{max}(Q_i(PhSEC))$ – підсумкова сума максимального значення відповідей (виконання вимог) з урахуванням вагового коефіцієнту W_i для напрямку фізична безпека;

$$RM(S) = \frac{R_{cur}(Q_1(S)) + R_{cur}(Q_i(S))}{R_{max}(Q_1(S)) + R_{max}(Q_i(S))} \cdot 100\% \quad , \quad (7)$$

де $R_{cur}(Q_1(S)) + R_{cur}(Q_i(S))$ – підсумкова сума відповідей з урахуванням вагового коефіцієнту W_i для напрямку підтримка національних інтересів; $R_{max}(Q_1(S)) + R_{max}(Q_i(S))$ – підсумкова сума максимального значення відповідей (виконання вимог) з урахуванням вагового коефіцієнту W_i для напрямку підтримка національних інтересів.

Висновки

Провайдери АНО повинні забезпечити облік заходів безпеки при проектуванні, впровадженні та експлуатації нових ІТС. Крім того, провайдери АНО повинні визначити програмні і апаратні засоби ІТС як елементи інфраструктури системи ОрПР які, зокрема, можуть включати в себе:

- ресурси і компоненти системи ОрПР;
- контролюючі системи диспетчеризації, які мають відношення до забезпечення безпеки;
- системи контролю доступу та охоронної сигналізації органів обслуговування повітряного руху;
- системи спостереження;
- електронні пристрої, що використовуються для обробки, зберігання і передачі критично важливої інформації провайдера АНО.

Захист критичних ІТС провайдера АНО повинен передбачати процедури оцінки ризику. Це може досягатися шляхом охоплення критичних елементів інфраструктури системи ОрПР, оцінками ймовірності загроз (атак), вразливостей і впливу або наслідків відмови ІТС.

Провайдери АНО повинні розробляти заходи зниження ризику потенційних атак на інфраструктури системи ОрПР і перевіряти реалізацію цих заходів, використовуючи механізм регулярного контролю за виконанням вимог, наприклад шляхом проведення аудитів та інспекторських перевірок.

Авторами вперше запропоновано метод оцінки зрілості системи управління безпекою при організації повітряного руху провайдера аеронавігаційного обслуговування. Зазначений метод дозволяє визначити фактичний та прогнозований рівні відповідності системи управління безпекою при організації повітряного руху чинним вимогам нормативно-правових актів, міжнародних стандартів та з урахуванням вагових коефіцієнтів.

Список літератури:

1.Повітряний кодекс України від 19.05. 2011. – № 3393-VI.

2. Керівництво з безпеки системи організації повітряного руху, DOC ICAO 9985.

3. Денис М. Ахен, Арон Клауз, Ричард Тернер CMMI: Комплексный подход к совершенствованию процессов. Практическое введение в модель. – Москва : МФК, 2005. – 300 с.

4. ДСТУ ISO/IEC TR 15504-4:2002 Інформаційні технології. Оцінювання процесів життєвого циклу програмних засобів. Ч. 4. Настанови з виконання оцінювання (ISO/IEC TR 15504-4:1998, IDT).

5. Проверка и оценка деятельности по управлению информационной безопасностью : учеб. пособие для вузов / П.Г. Милославская, М.Ю. Сенаторов, А Н. Толстой. – Москва : Горячая Линия-Телеком, 2014. – 166 с.

Харківський національний
університет імені В.Н. Каразіна

Надійшла до редколегії 05.10.2018