considering the parameters of the channel between the user and the data center.

Keywords: optimization, load, cloud computing, distribution, resource, information technology.

Чижов Олександр Вікторович, аспірант кафедри Комп'ютерних Інформаційних Технологій Національного Авіаційного Університету.

Olexander Chizhov, postgraduate student of the Department of Computer Information Technologies of the National Aviation University.
E-mail: alex.definch@gmail.com.
Orcid ID: 0000-0003-2141-9903.

Фесенко Андрій Олексійович, к.т.н., доцент, доцент кафедри Комп'ютерних Інформаційних Технологій Національного Авіаційного Університету.

Andrii Fesenko, PhD in Eng., Associate Professor Department of Computer Information Technologies of the National Aviation University.
E-mail: aafesenko88@gmail.com.
Orcid ID: 0000-0001-5154-5324.

Пустовіт Микола Сергійович, Заступник начальника науково-дослідного центру, Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації.

Mykola Pustovit, Deputy Head of the Research Center, State Research Institute of Cyber Security and Information Protection Technologies.
E-mail: pms09031977@gmail.com.
Orcid ID: 0000-0002-6384-4564.

Німченко Тетяна Василівна, кандидат технічних наук, доцент, доцент кафедри засобів захисту інформації Національного авіаційного університету.

Tetiana Nimchenko, Ph.D., associate professor, associate professor of the Department of information security National Aviation University.
E-mail: zzi.nimchenko@nau.edu.ua.
Orcid ID: 0000-0001-8196-5493.

DOI: 10.18372/2410-7840.25.18227
УДК 65.012.25

ПЛАН УПРАВЛІННЯ БЕЗПЕКОЮ ІНФОРМАЦІЙНИХ АКТИВІВ ОБ'ЄКТІВ АВІАТРАНСПОРТНОГО КОМПЛЕКСУ УКРАЇНИ

Володимир Шульга, Андрій Міщенко, Богдан Моркляник, Сергій Лазаренко, Наталія Ліщиновська

Керівні документи International Civil Aviation Organization (ICAO) визначають систему управління безпекою – як елемент відповідальності корпоративного управління, який визначає політику безпеки компанії та її наміри керувати безпекою як невід'ємною частиною її загального бізнесу. Таким чином, система управління безпекою (Security Management System, SeMS) – це частина загальної системи управління інформаційними активами авіаційного підприємства, що базується на аналізі ризиків і призначена для проектування, реалізації, контролю, супроводження та вдосконалення заходів у галузі забезпечення інформаційної безпеки. Дану систему складають організаційні структури, політика, дії з планування, обов'язки та процедури, процеси і ресурси та багато іншого. Проведено аналіз сучасних заходів управління системою забезпечення інформаційною безпекою об'єктів авіатранспортного комплексу на базі міжнародних стандартів серії ISO. Запропоновано сценарій реалізації плану управління безпекою інформаційних активів об'єктів авіатранспортного комплексу, який засновано на передовому досвіді закордонних країн.

***Ключові слова**: інформаційна безпека, рівень ризику, авіатранспортний комплекс, політики, конфіденційність, доступність, цілісність, технічне завдання, системи безпеки.*

ВСТУП

Зростання злочинів у сфері високих технологій диктує особливі та адаптовані відповідним чином вимоги захисту ресурсів обчислювальних мереж і ставить завдання побудови власної інтегрованої системи забезпечення безпеки. Її рішення передбачає наявність нормативно-правової бази, формування політики та основних концепцій забезпечення безпеки, розробку планів, заходів та процедур щодо безпечної роботи, проектування, реалізації та управління системою забезпечення безпеки в рамках авіаційного підприємства. Ці складові визначають єдину політику системи забезпечення безпеки інформаційних активів об'є-

ктів авіатранспортного комплексу (АТК). Створення ефективних механізмів управління інформаційними ресурсами АТК в сучасних умовах не можливе без наукового обґрунтування та практичної реалізації збалансованої політики інформаційної безпеки, що може бути сформована та реалізована на основі вирішення наступних завдань [2]:

• аналіз процесів інформаційної взаємодії та обміну даних у всіх сферах основної діяльності аеропорту (інформаційних потоків, їх загальної кількості та якості, протиріч з виявленням власників та суперечок);

• розробка якісного та простого кількісного (математичного) опису інформаційної взаємодії;

• запровадження кількісних індикаторів та критеріїв відкритості, безпеки та цілісності інформаційного обміну;

• розробка сценаріїв необхідності та значущості балансу в інформаційній відкритості та конфіденційності;

• визначення ролі та місця політики інформаційної безпеки в управлінні інформаційними ресурсами аеропорту та опрацювання узгоджених принципів і підходів;

• формулювання основних складових політики: цілей, завдань, принципів та ключових напрямів системи забезпечення інформаційної безпеки;

• здійснення та врахування оцінки загроз та ризиків;

• забезпечення регулярної підготовки та перепідготовки фахівців підприємства у сфері системи забезпечення безпеки у відповідності до займаних посад;

• формування позитивної культури безпеки на підприємстві;

• розробка базової методики керування процесом забезпечення політики інформаційної безпеки;

• підготовка проектів нормативно-правових документів;

• здійснення контролю якості за процесами системи забезпечення безпеки.

В інформаційних базах сучасного аеропорту зберігається і обробляється безліч різних даних, пов'язаних із забезпеченням виробничого процесу, персональні дані пасажирів та співробітників, службова, комерційна та інша конфіденційна інформація також інформація, що є державною таємницею.

Згідно з Керівництвом з авіаційної безпеки, експлуатанти авіаційної техніки, включаючи експлуатантів повітряних суден та аеропортів, постачальників обслуговування повітряного руху та інших, повинні визначити програмні та апаратні засоби критичних інформаційних систем, що використовуються ними. До таких засобів можуть належати [3]:

a) системи контролю доступу та охоронна сигналізація;

b) системи контролю вильоту;

c) системи встановлення належності багажу пасажирові;

d) системи виявлення слідів вибухових речовин, що працюють у комплексі чи автономно;

e) бази даних про зареєстрованих агентів та відомих вантажовідправників;

f) системи організації повітряного руху;

g) системи бронювання та реєстрації пасажирів, що використовуються експлуатантами повітряних суден;

h) замкнуті телевізійні системи спостереження;

i) командні, контрольні та диспетчерські системи, що стосуються системи забезпечення безпеки.

Специфіка захисту інформації в авіатранспортній сфері полягає у тому, що інформаційні системи підприємства АТК дуже тісно взаємодіють із аналогічними системами інших підприємств та організацій.

ОСНОВНА ЧАСТИНА

Заходи із забезпечення СУІБ

Особливістю аеропорту, як об'єкта безпеки, є безліч робочих процесів, які пов’язані з інформаційною взаємодією у цілодобовому режимі, що потребує миттєвих комунікацій, як всередині підприємства, так і з іншими об'єктами АТК та просторовою розподіленістю інфраструктури на території підприємства. Сюди можливо віднести і різноманітність джерел фінансування, пов'язаних з авіаційною та не авіаційною діяльністю, наявністю розвиненої структури допоміжних підрозділів та служб (склади ПММ, онлайн реєстрація, електронна система зчитування посадкових талонів для ідентифікації пасажирів, хендлінгова, автотранс-

портна, готельна, експлуатаційно-господарська діяльність тощо), необхідність адаптації до мінливого ринку, відсутність загальноприйнятих ділових процесів, необхідність електронної взаємодії з державними органами та авіакомпаніями [2].

Вказані вище особливості зумовлюють необхідність дотримання наступних вимог:

• комплексного опрацювання завдань системи забезпечення безпеки, починаючи з концепції інформаційної безпеки (ІБ) та закінчуючи супроводом програмно-технічних рішень;

• залучення фахівців, які знають змістовну частину ділових процесів;

• використання модульної структури корпоративних програм, коли кожен модуль покриває взаємопов'язану групу ділових процедур або інформаційних сервісів під час забезпечення єдиних вимог до системи забезпечення безпеки;

• застосування обґрунтованої послідовності етапів у вирішенні завдань інформаційної безпеки;

• документування розробок з урахуванням розумного застосування стандартів, що гарантує створення успішної системи;

• використання надійних та масштабованих апаратно-програмних платформ та технологій різного призначення, що забезпечують необхідний рівень безпеки.

Політика, що формується в галузі системи забезпечення безпеки заснована на міжнародних вимогах, стандартах та рекомендованих практиках передбачає принципи управління ними для всього підприємства в цілому.

Ці основні засади базуються на цілях підприємства, його стратегії розвитку, а також у відповідності до вимог чинного законодавства та стандартів у галузі системи забезпечення інформаційної безпеки

Головний міжнародний стандарт, який представляє можливість бізнесу встановлювати, застосовувати, переглядати, контролювати і підтримувати ефективну систему управління інформаційної безпеки (СУІБ) є серія міжнародних стандартів ISO 27XXX. Вони надають інструмент для розробки, впровадження, супроводу, моніторингу, підтримки та вдосконалення якісно документованої системи управління інформаційною безпекою в контексті розгляду бізнес ризиків.

Стандарт ДСТУ ISO/IEC 27001 гармонізований зі стандартами систем менеджменту якості ДСТУ ISO 9001 і базується на загальних принципах. Більш того, обов'язкові процедури стандарту ДСТУ ISO 9001 потрібні для виконання вимог стандарту ДСТУ ISO/IEC 27001. Структура документації, згідно вимог ДСТУ ISO/IEC 27001, аналогічна структурі за ДСТУ ISO 9001. Значна частина документальних матеріалів, яка потрібна по ДСТУ ISO/IEC 27001, на сьогодні розроблена, і використовується в рамках ДСТУ ISO 9001. Таким чином, якщо організація вже має систему менеджменту, наприклад за ДСТУ ISO 9001, то краще забезпечувати виконання вимог стандарту ДСТУ ISO/IEC 27001 у рамках вже існуючих систем, що передбачає значне зниження внутрішніх витрат підприємства та вартості робіт щодо впровадження та сертифікації [4, 5, 6].

Дотримуючись вимог стандарту ДСТУ ISO 9001, організації АТК повинні вибудовувати поетапний підхід у своїй діяльності, визначати процеси та їх послідовність, взаємодію під час управління ними й зв'язки між даними процесами, при цьому вихідні дані одного процесу являються вхідними даними для наступного.

Процесний підхід, визначений стандартом ДСТУ ISO 9001, під час впровадження та вдосконалення полягає в забезпеченні відповідності вимогам та якості не тільки «виготовленої продукції», але і наданих послуг. Правильне розуміння і планове управління процесами, які взаємопов'язані і створюють систему, мають забезпечити ефективність у досягненні поставлених цілей.

Управління процесом і системою в цілому може бути реалізовано з використанням циклу PDCA (Plan-Do-Check-Act/Плануй-Роби-Перевіряй-Дій) з підходом, заснованим на оцінці ризику, який прагне використовувати в своїх інтересах технічні можливості і запобігати небажаним наслідкам у результаті виявлених загроз.

Стандарт ДСТУ ISO/IEC 27001, також як і стандарт ДСТУ ISO 9001, використовує концепцію циклу PDCA на рівні, що стосується операційних процесів, які реалізуються в рамках системи та зводяться до простої і логічної послідовності дій. Послідовність дій наступна: плануємо діяльність та створюємо критерії до неї, щоб у подальшому можливо було чітко, за встановленими вимогами,

стверджувати те, наскільки успішно були виконані поставлені завдання. Заплановану діяльність потрібно дослідити на відносно невеликих ділянках робіт, де невеликий ризик втрат у разі невдачі, потім потрібно проаналізувати результати та впровадити зміни до вимог, або в робочі процеси. Цикл варто повторювати до тих пір, доки організація не досягне необхідного захисту бізнесу та активів від знищення або витоку. У той же час, заходи з інформаційної безпеки не повинні обмежувати або ускладнювати процеси обміну інформацією, оскільки це може поставити під загрозу розвиток та повноцінну роботу АТК.

Система управління інформаційною безпекою повинна гарантовано забезпечувати досягнення таких цілей як: конфіденційність критичної інформації, неможливість несанкціонованого доступу до критичної інформації, цілісність інформації та пов'язаних з нею процесів (створення, введення, обробки і виведення) і ряду інших процесів та завдань.

Досягнення очікуваних результатів можливо під час планування та у ході вирішення таких основних завдань, як визначення відповідальних за систему забезпечення інформаційної безпеки та розробки наступних вимог: загального плану управління безпекою АТК, плану управління інформаційною безпекою, визначення спектру загроз та ризиків інформаційної безпеки, проведення їх експертних оцінок, розробки політики та правил доступу до інформаційних ресурсів, впровадження системи управління ризиками інформаційної безпеки, (у тому числі методи їх оцінки), а також регулярне здійснення контролю якості інформаційної безпеки на підприємстві. Слід відмітити, що зазначено не повний перелік заходів [1].

Враховуючи вищевикладене доцільно відмітити, що PDCA має великий вплив у впровадженні процесного підходу, адже саме цей механізм відіграє ключову роль для постійного поліпшення роботи організацій АТК на систематичній основі, а безперервне поліпшення - один з принципів процесного підходу.

У загальному вигляді, на етапі планування, організація АТК повинна:

1. Залежно від характеру діяльності організації її місця розташування, ресурсів та технологій, що використовуються, визначити масштаб та межі СУІБ;

2. Визначити, схвалити та затвердити керівництвом політику СУІБ залежно від характеру діяльності організації, її ресурсів та технологій. До таких дій належить:

- визначення інформаційної безпеки, наміри керівництва з системи управління інформаційною безпекою, опис політики безпеки, принципів та стандартів, які мають значення для підприємства;
- визначення загальних та приватних обов'язків з управління системою інформаційної безпеки, а також надання відомостей про інциденти;
- включення посилань на документацію, що може доповнювати опис політики та має більш докладні інструкції для конкретних інформаційних систем або правил із забезпечення безпеки, яких повинен дотримуватись користувач;
- включення схеми визначення цілей і загального напрямку, а також принципів діяльності, що стосуються захисту інформації;
- приймання до уваги ділових та нормативних вимог, а також контрактних зобов'язань, в яких фігурують питання із забезпечення безпеки;
- направлення стратегії управління ризиками організації, в якій планується побудова та підтримка СУІБ;
- встановлення критеріїв, за якими буде проводитись оцінка загроз та ризиків;

3. Визначити:

- методи оцінки ризиків, які відповідають СУІБ, нормативним, діловим, а також іншим вимогам конкретного підприємства;
- критерії для прийняття ризиків та їх допустимі рівні;

4. Для опису ризиків визначити:

- інформаційні ресурси організації та їх власників;
- загрози цим ресурсам;
- вразливості;
- рівень збитку у разі можливого порушення конфіденційності, цілісності або отримання доступу до деяких інформаційних ресурсів;
- вірогідність такого порушення з урахуванням відомих небезпек, вразливостей та застосованих засобів захисту;

5. Проаналізувати та оцінити:

- можливість появи ризиків або ділових невдач організації, що можливо відбулися б через втрату конфіденційності, цілісності або доступності інформаційних ресурсів;

- реальну вірогідність порушення безпеки та збитки організації у випадку реалізації загрози, а також визначити методи контролю якості, що використовуються на даний час;

- чи потребує прийнята оцінка загроз та ризиків застосування додаткових заходів для удосконалення системи захисту;

6. Оцінити методи усунення ризиків, для чого потрібно:

- визначити відповідні методи контролю;

- свідомо і об'єктивно прийняти ризик, що відповідає рівню визначеному політикою безпеки організації;

- визначити шляхи уникнення ризиків.

7. Визначити цілі та методи перевірок результатів усунення ризиків, які повинні відповідати вимогам:

- нормативно-правовим;

- договірним;

- прийнятих ризиків в організації;

8. Узгодити з керівництвом рівні ризиків, що залишились;

9. Отримати повноваження керівництва на впровадження та забезпечення функціонування СУІБ.

Проведений аналіз надає можливість стверджувати, що формалізації процесу планування в циклі PDCA не приділено достатньої уваги. Розглянемо, як приклад, загальні принципи побудови Плану управління системою безпеки на підприємстві (Security Management Plan, SeMP).

Даний План має описувати, як в організації планують забезпечити принципи конфіденційності, цілісності та доступності безпеки відповідних матеріальних та нематеріальних інформаційних активів (класифікованих або некласифікованих) на відповідних його рівнях, включаючи контрагентів організації. Цей План має бути корельований та передбачати обґрунтування запропонованої відповідності вимогам безпеки, які надані в Технічному завданні (Statement of Work, SOW). При складанні цього плану потрібно пройти шлях від простого розуміння, що ризики можуть статися, до чіткого плану дій з управління ризиків.

За змістом План складається з 4 розділів, а саме: загальні положення; документи, що застосовуються та довідкова інформація; принципи та межі діяльності; фізичні елементи системи забезпечення безпеки. Також План включає додатки в яких надані підтвердження виконання Технічного завдання.

У 1 розділі «Загальні положення» відображається предмет документу, напрям та межі застосування, вказується відповідальність сторін, терміни та визначення, крім того приділяється увага еволюції документа.

У 2 розділі «Документи, що застосовуються та довідкова інформація» - надається бібліографія керівних та нормативних документів, які використовуються при складанні Плану та необхідна довідкова інформація.

Розділ 3 «Принципи та межі діяльності» складається з 7 підрозділів. Підрозділ 3.1 надає опис місії, тобто опис основних принципів та засад системи забезпечення безпеки. Підрозділ 3.2 присвячений основним принципам функціонування системи управління безпекою в організації. Метою цього розділу є опис, яким чином буде організована безпека для забезпечення обслуговування та захисту активів. Підрозділ 3.3 має на меті опис процесів та процедур, що забезпечують виконання обов'язків, стандартів, вимог та процедур, пов'язаних із забезпеченням безпеки. У ньому надані посадові інструкції та порядок оповіщення відповідальних осіб таких як: офіцер з безпеки, IT директор та інші. Підрозділ 3.4 «Звітність щодо управління системою безпеки» має на меті опис процесів та процедур, які гарантують, що звітність про систему забезпечення безпеки виконується відповідно до вимог технічного завдання і регулюється внутрішнім контролем якості з оформленням відповідних актів, що є документом суворої звітності. Підрозділ 3.5 визначає заходи та управління системою забезпечення безпеки у разі виникнення інциденту («ПОДІЯ»). Цей підрозділ визначає опис процесів та процедур, які гарантують, що керування заходами системи забезпечення безпеки під час виникнення «ПОДІЇ», виконуються відповідно до вимог технічного завдання і регулюється внутрішнім контролем якості з відповідною фіксацією в акті. Також, надається План реагування на інциденти безпеки, в якому зазначається

опис дій персоналу під час виникнення події: неавторизований доступ; вандалізм; політичні потрясіння та заворушення; терористичні атаки/злочинні дії; втрата, крадіжка, пошкодження або розголошення даних; різновиди мережевих атак, підміни та/або глушіння та інше. Підрозділ 3.6 «Підтримка системи безпеки» надає опис процесу та процедур, які гарантують що буде проводитись технічна підтримка систем забезпечення безпеки. Це обслуговування виконується на відповідному рівні згідно до вимог та стандартів і регулюється внутрішнім контролем якості з відповідним оформленням актів.

У 4 розділі «Фізичні елементи системи забезпечення безпеки» описуються елементи управління фізичною безпекою організації. Цей розділ має 4 підрозділи. Підрозділ 4.1 «Політика системи забезпечення безпеки» крім визначення політики системи забезпечення безпеки, яка реалізована у процесі безперервного вдосконалення безпеки активів (послуг, ресурсів IT та інше) і засобів, що використовуються при наданні послуг організації, також визначаються та ідентифікуються загрози. Підрозділ 4.2 «Опис системи захисту» це один із основних, глобальних розділів Плану в якому визначено середовище системи забезпечення безпеки. Цей розділ спрямований на опис загального середовища фізичної системи забезпечення безпеки, в якому розташоване АТК та всі заходи фізичної безпеки, що застосовуються для захисту її території.

Захист має включати наступні пункти, але не має ними обмежуватись:

- захист від зовнішніх і екологічних загроз;
- засоби безпеки для захисту зовнішніх кордонів (паркан, освітлення, системи відеоспостереження, патрулювання та інше);
- контроль доступу;
- відстеження, моніторинг та виявлення засобами системи забезпечення безпеки (система виявлення вторгнень, відеоспостереження тощо);
- коригувальні засоби контролю безпеки (охоронці, час реакції на подію та інше).

Наступний розділ 4.3 «Захист активів організації (глобальне безпекове середовище)» має на меті опис усіх заходів системи забезпечення безпеки (фізичних і логічних), що впроваджуються для захисту активів підприємства (IT, інформація, ресурси, послуги, частини мережі, що використовується як послуга/з'єднання TWAN, системи контролю доступу тощо), які використовуються для виробничої діяльності. У цьому розділі необхідно детально описати заходи системи забезпечення безпеки, які застосовуються для забезпечення безпеки (доступності, цілісності, конфіденційності) Активів підприємства.

Для наповнення цього розділу застосовують загальний опис елементів системи забезпечення безпеки (включно з найважливішою та корисною інформацією для усвідомлення принципів побудови цієї системи), надаються посилання на внутрішні документи з можливістю їх перевірки на відповідність діючим державним нормативно-правовим актам. Слід зазначити, що внутрішні документи за необхідністю можуть бути наведені у Додатках до цього Плану. Розділ 4.3 також має 2 підрозділи.

Підрозділ 4.3.1 «Опис локального середовища системи безпеки (LSE)». Метою цього підрозділу є опис фізичних заходів системи забезпечення безпеки, які застосовуються для захисту активів підприємства. За допомогою відповідних заходів контролю, гарантується, що лише уповноважений та перевірений персонал має доступ до відповідних зон, включаючи фізичну безпеку для будівлі, офісів, службових приміщень, об'єктів, відповідних зон тощо.

Підрозділ повинен включати наведені пункти, але не може ними обмежуватись. У даному підрозділі може бути зазначена наступна інформація:

- управління системою контролю доступу;
- система виявлення вторгнень;
- система безперервного моніторингу;
- безпека людських ресурсів, включаючи:

- перевірку з попереднього місця роботи;
- причину звільнення з попереднього місця роботи;
- причину нового працевлаштування на дане робоче місце;
- особисте усвідомлення важливості системи забезпечення безпеки;

- управління активами, включаючи:

- управління документацією (особливо документацією, розміщеною в IT-системі підприємства);

• відносини з контрагентами організації, включаючи:

- інформаційну безпеку у відносинах з контрагентами;

- управління і контроль за послугами, що надаються контрагентами.

Підрозділ 4.3.2 «Опис електронного середовища системи безпеки (ESE)». Метою цього підрозділу є опис середовища системи забезпечення безпеки самої IT-системи, яка використовується підприємством та класифікується на заходи:

• логіку системи контролю доступу (беручи до уваги ідентифікацію та аутентифікацію);

• криптографію;

• безпеку операцій, що складаються з:

- процедур та обов'язків;

- захисту від шкідливих програм;

- резервного копіювання;

- ведення журналів, обліку та моніторингу;

- контролю операційного програмного забезпечення;

- моніторингу та управління технічно вразливими місцями;

- координації аудиту інформаційних систем;

• безпеку зв'язку, включаючи:

- управління мережевою безпекою;

- передачу інформації;

• придбання, розвиток та обслуговування системи, включаючи:

- вимоги безпеки інформаційних систем;

- безпеку в процесах розробки та підтримки, даних тестування;

• управління інцидентами інформаційної безпеки, включаючи:

- управління інцидентами інформаційної безпеки та їх парирування;

• аспекти інформаційної безпеки управління безперервністю бізнесу, включаючи:

- безперервність і резервування інформаційної безпеки (з точки зору цілісності та доступності);

• відповідність – відповідність законодавчим і договірним вимогам, аудити та огляди інформаційної безпеки.

Останній розділ 4.4. «Захист активів організації (локальне безпекове середовище)». Очікується, що в цьому розділі буде детальний опис заходів системи безпеки (технічні та організаційні), які застосовуються для забезпечення безпеки (доступності, цілісності, конфіденційності тощо) безпосередньо Активів підприємства. Розділ 4.2 має 2 підрозділи.

Підрозділ 4.4.1 «Опис локального середовища системи забезпечення безпеки (LSE)». Метою цього підрозділу є опис засобів контролю фізичної безпеки, які застосовуються для захисту самих активів за допомогою відповідних засобів контролю, для надання гарантій, що лише уповноважений та перевірений персонал, включаючи фізичну охорону будівлі, даху, офісів, приміщень, складських приміщень, відповідних зон тощо, виконує відповідні функції.

Підрозділ повинен включати наведені пункти, але не може обмежуватись ними. У даному підрозділі може бути зазначена наступна інформація:

• управління системою контролю доступу;

• система виявлення вторгнень;

• система моніторингу;

• безпека людських ресурсів, включаючи:

- перевірку з попереднього місця працевлаштування;

- причину звільнення з попереднього місця роботи;

- обізнаність щодо важливості дотримання вимог системи забезпечення безпеки. Важливо зазначити, що окрім підтем безпеки людських ресурсів, також очікуються пояснення щодо того, як підприємство мотивує свій персонал дотримуватися правил, стандартів та процедур і уникати порушень системи забезпечення безпеки (дисциплінарні процеси та процедури, заохочення, програма/система тощо);

• управління активами, може містити наступні пункти але не обмежується ними:

- ведення документації;

- виявлення слідів втручання;

• взаємовідносини з постачальниками, включаючи:

- інформаційну систему забезпечення безпеки у відносинах з контрагентами (вимоги з безпеки);

- управління з надання послуг контрагентами.

Підрозділ 4.4.2 «Опис середовища електронної системи забезпечення безпеки (ESE)». Метою цього підрозділу є опис середовища системи забезпечення безпеки, що не стосується самих активів.

Удосконалений план УСБ

За результатами проведеного дослідження можливо зазначити, що структура Плану управління системою безпеки на підприємстві не в повній мірі відповідає сучасним викликам, з точки зору забезпечення безпеки.

Враховуючи викладене пропонуємо удосконалений зміст Плану управління системою безпеки на підприємстві (Security Management Plan, SeMP), який засновано на передовому досвіді закордонних країн.

Структура та зміст Плану буде мати наступний вигляд:

План управління системою безпеки підприємства

1. Загальні положення

1.1 Предмет документу та його основна частина;

1.2 Обсяг діяльності;

1.3 Відповідальність сторін;

1.4 Еволюція документа системи забезпечення безпеки;

1.5 Область та межі застосування;

1.6 Терміни та визначення.

2. Документи, що застосовуються та довідкова інформація

2.1 Документи, що використовуються;

2.2 Довідкова інформація.

3. Загальні положення та межі діяльності

3.1 Опис місії;

3.2 Організація функцій системи управління безпекою;

3.3 Права та обов'язки зацікавлених сторін;

3.4 Звітність щодо управління системою безпеки;

3.5 Подія, керування системою безпеки;

3.6 Підтримка системи безпеки;

3.7 Безперервність бізнесу та аварійне відновлення.

4. Фізичні елементи системи забезпечення безпеки

4.1 Політика системи забезпечення безпеки;

4.2 Опис системи захисту

4.3 Захист активів організації (глобальне безпекове середовище)

4.4. Захист активів організації (локальне безпекове середовище)

ДОДАТКИ

ВИСНОВКИ

За результатами проведеного дослідження отримані наступні результати:

1. Система забезпечення безпеки на авіапідприємстві складається з багатьох факторів, ресурсів, вимог, стандартів та рекомендованої практики. Система забезпечення безпеки має бути адаптована до відповідного підприємства та регулюватись чинним державним законодавством і у разі співробітництва з міжнародними організаціями має бути забезпечена відповідно до норм та вимог міжнародного законодавства;

2. Особливості функціонування АТК зумовлюють комплексне опрацювання завдань системи забезпечення безпеки, починаючи з концепції інформаційної безпеки та закінчуючи супроводом програмно-технічних рішень;

3. Проаналізовані заходи із забезпечення безпеки АТК та планування системою безпеки. За результатами аналізу з'ясовано, що формалізації процесу планування в циклі PDCA не приділено достатньої уваги;

4. Запропоновано удосконалену структуру та зміст Плану управління системою безпеки на підприємстві (Security Management Plan, SeMP).

ЛІТЕРАТУРА

[1] Менеджмент у сфері захисту інформації/ Ромака В.А., Корж Р.О., Гарасим Ю.Р// Підручник: Львів: ЗУКЦ, 2013. 462 с.

[2] Міщенко А.В., Козловський В.В., Васянович В.В. Методологія інформаційної безпеки в авіатранспортному комплексу// Вісник Хмельницького національного університету. Серія: технічні науки. 2015. № 2 (223). С. 178-181.

[3] ICAO Aviation Security Manual (Doc 8973 – Restricted).

[4] ДСТУ ISO/IEC 27001:2023. «Information security, cybersecurity and privacy protection. Information security management systems. Requirements».

[5] ДСТУ ISO 9001:2018. «Системи управління якістю. Вимоги».

[6] ДСТУ ISO/IEC 27701:2022. «Методи безпеки. Розширення до ISO/IEC 27001 та ISO/IEC 27002 для керування конфіденційною інформацією. Вимоги та настанови».

SECURITY MANAGEMENT PLAN FOR INFORMATION ASSETS OF OBJECTS OF THE AVIATION TRANSPORT COMPLEX OF UKRAINE

Governing documents International Civil Aviation Organization (ICAO) define a safety management system as an

element of corporate governance responsibility that defines a company's safety policy and its intentions to manage safety as an integral part of its overall business. Thus, the security management system (Security Management System, SeMS) is a part of the overall information asset management system of the aviation enterprise, which is based on risk analysis and is intended for the design, implementation, control, monitoring and improvement of measures in the field of information security. This system consists of organizational structures, policies, planning actions, responsibilities and procedures, processes and resources, and much more. An analysis of modern management measures of the information security system of air transport facilities based on international standards of the ISO series was carried out. A scenario for the implementation of the plan for managing the security of information assets of the air transport complex is proposed, which is based on the best experience of foreign countries.
Keywords: information security, risk level, air transport complex, policies, confidentiality, availability, integrity, terms of reference, security systems.

Шульга Володимир Петрович, доктор історичних наук, в.о. ректора Національного авіаційного університету, професор кафедри безпеки інформаційних технологій Національного авіаційного університету.
Volodymyr Shulha, Acting Rector of National Aviation University, professor of IT-Security Academic Department, National Aviation University.
E-mail: shulga.khnuvs@gmail.com.
Orcid ID: 0000-0003-4356-7288.

Міщенко Андрій Віталійович, доктор технічних наук, професор, професор кафедри засобів захисту інформації Національного авіаційного університету.

Andrii Mishchenko, doctor of technical science, professor, professor of the Department of information security National Aviation University.
E-mail: td@airport.kiev.ua.
Orcid ID: 0000-0001-8376-1777.

Моркляник Богдан Васильович, доктор технічних наук, професор, член Національного агенства кваліфікацій.

Bohdan Morklyanyk, doctor of technical science, professor, Member National Qualifications Agency.
E-mail: kzzi@nau.edu.ua.
Orcid ID: 0009-0000-6564-6804.

Лазаренко Сергій Володимирович, доктор технічних наук, професор, професор кафедри засобів захисту інформації Національного авіаційного університету.

Serhii Lazarenko, doctor of technical science, professor, professor of the Department of information security National Aviation University.
E-mail: zzi.lazarenko@nau.edu.ua.
Orcid ID: 0000-0003-3529-4806.

Ліщиновська Наталія Олександрівна, кандидат технічних наук, асистент кафедри засобів захисту інформації Національного авіаційного університету.

Natalia Lishchynovska, Ph.D., assistant of the Department of information security National Aviation University.
E-mail: natashalil858@ukr.net.
Orcid ID: 0000-0002-1913-8419.

DOI: 10.18372/2410-7840.25.18228
УДК 004.621.5

АНАЛІЗ ПОНЯТТЯ КІБЕРСТІЙКОСТІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Євгенія Іванченко, Олександр Корченко, Олег Зарицький, Сергій Зибін, Наталія Вишневська

У зв'язку зі збільшенням кількості кібератак та інцидентів на об'єкти критичної інфраструктури перед спеціалістами постає проблема підвищення ефективності заходів безпеки, які будуть в змозі забезпечити надійну та безперебійну роботу об'єктів критичної інфраструктури в цілому. Тому поняття кіберстійкість, управління кіберстійкістю, забезпечення кіберстійкості, оцінювання кіберстійкості набувають подальшої актуалізації. До поняття кіберстійкості, крім безпеки, відносять низку завдань і процесів, які стосуються інформаційних технологій (наприклад, резервування та відновлення після збоїв) і захисту бренду. Причому питання стійкості і безперервності сервісів в цьому понятті відносяться як до самої компанії, так і до зовнішніх підрядників, які надають такі послуги. Так, Держспецзв'язку визначили, що передумовою до появи кіберстійкості як напрямку корпоративної кібербезпеки стало прийняття компаніями факту про неминучість кібератаки. В поняття кіберстійкості також включають можливість підготуватися до атаки, забезпечення ефективної діяльності та протидії під час атаки, а також зниження можливих наслідків атаки на компанію. Важливим для підприємств є оцінювання стану кіберстійкості їх критичних інфраструктур для