**УДК 004.056**

**В. Б. Дудикевич, Г. В. Микитин, А. І. Ребець**
Національний університет "Львівська політехніка",
кафедра захисту інформації

# ДО ПРОБЛЕМИ УПРАВЛІННЯ КОМПЛЕКСНОЮ СИСТЕМОЮ БЕЗПЕКИ КІБЕРФІЗИЧНИХ СИСТЕМ



**Проаналізовано моделі управління інформаційною безпекою (ІБ) кіберфізичних систем (КФС) згідно з ISO/IEC TR 13335 та ISO/IEC 27001, що є підґрунтям розвитку методології управління комплексною системою безпеки (КСБ) в рамках моделі управління "плануй – виконуй – перевіряй – дій". Запропоновано структуру управління КСБ КФС на рівні життєвого циклу інформації та багаторівневої моделі "кібернетичний простір – комунікаційне середовище – фізичний простір" на основі концепції "об'єкт – загроза – захист", яка розширює застосування системи управління ІБ.**

**Ключові слова: інформаційна безпека, моделі та методи управління, кіберфізична система, життєвий цикл інформації, комплексна система безпеки, концепція "об'єкт – загроза – захист".**

**Models of information security (IS) management of cyber-physical systems (CPS) were analyzed according to ISO/IEC TR 13335 and ISO/IEC 27001, which are the basis for developing a management methodology of a complex security system (CSS) within the management model "plan – do – check – act". The CSS management structure of CPS was proposed at the level of an information life cycle and the multilevel model "cyberspace – communication environment – physical space" based on the conception "object – threat – protection", which extends an application of the IS management system.**

**Key words: information security, management models and methods, cyber-physical system, life cycle of information, complex system security, conception "object – threat – protection".**

## Вступ

Концепція інформаційної безпеки України у базовому підході спрямована на забезпечення, створення і функціонування системи захисту процесу розвитку інформаційного простору від загроз засобами запобігання, своєчасного виявлення, припинення та нейтралізації реальних і потенційних загроз [1]. Кібернетична безпека є одним із головних сегментів інформаційної безпеки і спрямована на створення підходів і технологій забезпечення безпеки інформаційно-комунікаційних та кіберфізичних систем. Кіберфізичні системи відомі своєю багаторівневістю побудови: кібернетична платформа забезпечує контроль, обробку та управління станом об'єктів; комунікаційна платформа забезпечує передавання/приймання даних; фізична платформа забезпечує відбір інформації від об'єктів через давачі, які є вбудованими в сам об'єкт або у пристрій відбору інформації [2].

У рамках гарантоздатності кіберфізичних систем є актуальними і функціональна, і інформаційна безпека. Багаторівнева структура КФС обумовлює створення багаторівневої ІБ – комплексних систем безпеки кібернетичної, комунікаційної, фізичної платформ. Підґрунтям КСБ є концепція "об'єкт – загроза – захист", яка спрямована на забезпечення інформаційної безпеки: кібернетичної платформи – інформаційні ресурси (ІР), інформаційні системи (ІС), інформаційні процеси (ІП); комунікаційної платформи – інформаційні мережі та канали (ІМ (К)); фізичної платформи – давачі (Д).

У контексті розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та вдосконалення актуальною для кіберфізичних систем є система управління ІБ, як частина загальної системи управління, що враховує ризики ІБ. Відомі стандартизовані моделі управління ІБ інформаційних технологій. Інформаційні технології, зокрема класифікуються за ступенем реалізації в інформаційних системах. У просторі ІС інформаційні технології можуть бути реалізовані, як кіберфізичні системи, які застосовуються у різних предметних сферах з метою вирішення задач управління об'єктами.

***Постановка завдання***: розвиток методології управління інформаційною безпекою КФС у просторі моделі "плануй – виконуй – перевіряй – дій".

***Мета роботи*** – аналітичний огляд моделей управління ІБ та розроблення структури управління комплексною системою безпеки КФС на основі концепції "об'єкт – загроза – захист".

**Розвиток методології управління інформаційною безпекою кіберфізичних систем**

Концепції управління безпекою інформаційних технологій сформовані на основі: принципів безпеки, активів, загроз, вразливостей, впливу, ризику, захисних заходів та обмежень [3–6]. Для ефективного функціонування комплексної системи безпеки КФС фундаментальними є такі високорівневі *принципи безпеки*:

- менеджмент ризику – активи повинні бути захищеними шляхом прийняття відповідних заходів. Вибір і застосування захисних заходів здійснюється на підставі відповідної методології управління ризиками, яка, виходячи з активів організації, загроз, вразливостей і різного впливу загроз, встановлює допустимі ризики і враховує існуючі обмеження;
- зобов'язання – відіграють важливу роль у сфері безпеки КФС та в управлінні ризиками. Для формування зобов'язань необхідно з'ясувати переваги від реалізації безпеки;
- службові обов'язки і відповідальність – керівництво організації несе відповідальність за забезпечення безпеки активів; службові обов'язки і відповідальність, пов'язані з безпекою КФС, мають бути визначені і доведені до відома персоналу;
- цілі, стратегії і політика – мають враховуватися при управлінні ризиками, пов'язаними з безпекою КФС;
- управління життєвим циклом – управління безпекою КФС має бути безперервним впродовж усього їх життєвого циклу.

***Моделі управління інформаційною безпекою*** [3, 4]. *Модель взаємозв'язків елементів безпеки*. Безпека КФС – багатопланова організація процесів захисту, яку можна розглядати з різних точок зору. Взаємозв'язок елементів безпеки показує, як активи можуть підлягати впливу декількох загроз, одна з яких є основною для цієї моделі (рис. 1). Можливі сценарії моделі взаємозв'язків елементів безпеки:

- сценарій 1 – заходи безпеки можуть бути ефективними у зниженні ризиків, пов'язаних із загрозою, здатною використовувати вразливість; загроза може стати ефективною, тільки якщо актив є вразливим до неї;
- сценарій 2 – заходи безпеки можуть бути ефективними у зниженні ризиків, пов'язаних із загрозою використання множинних вразливостей;
- сценарій 3 – декілька заходів безпеки можуть бути ефективними в зниженні ризиків, пов'язаних із численними загрозами, що використовують вразливості; декілька заходів безпеки можуть бути необхідними для зниження ризику до прийнятного рівня залишкового ризику;
- сценарій 4 – ризик вважається прийнятним і ніякі заходи не будуть прийняті, навіть якщо загрози присутні і вразливість існує;
- сценарій 5 – вразливість існує, але немає відомих загроз її використання.

*Модель взаємозв'язків заходів безпеки і ризику*. На практиці часто є необхідність у застосуванні декількох заходів безпеки для зниження ризику до прийнятного рівня. Взаємозв'язок захисних заходів і ризику, який показує ефективність деяких захисних заходів для зменшення ризику, представлений на рис. 2. Якщо ризик вважається прийнятним, реалізація захисних заходів не вимагається.

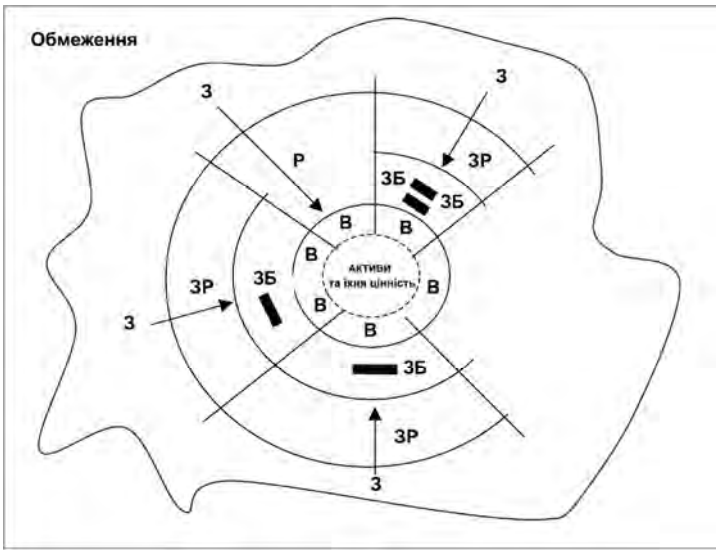


*Рис. 1. Модель взаємозв'язків елементів безпеки: Р – ризик, ЗР – залишковий ризик, З – загроза, ЗБ – заходи безпеки, В – вразливість*

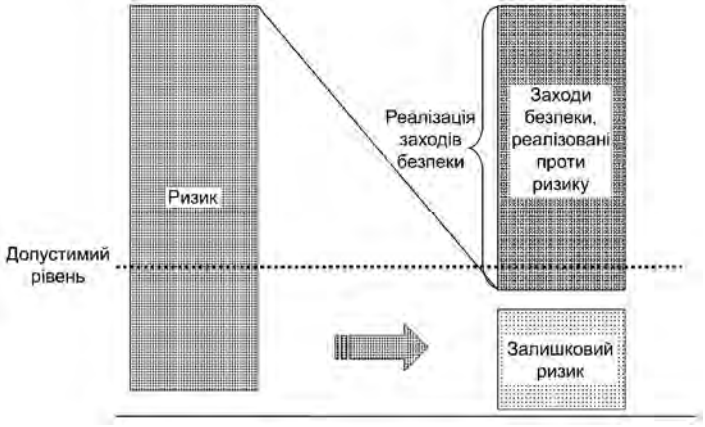


*Рис. 2. Модель взаємозв'язків заходів безпеки і ризику*

На етапі планування модель взаємозв'язків заходів безпеки і ризику передбачає: оцінювання ризиків; розроблення плану безпеки інформаційно-комунікаційних технологій. Після планування наступним етапом є реалізація заходів безпеки. Основні принципи моделі взаємозв'язків заходів безпеки і ризику: з метою зменшення залишкових ризиків до прийнятного рівня можливе одночасне застосування декількох заходів безпеки; для випадку прийнятного рівня залишкового ризику можливе зменшення кількості заходів безпеки.

*Модель ієрархії корпоративних політик безпеки.* Політика безпеки організації може складатися з принципів безпеки і директив організації загалом. У деяких випадках вона може бути включена до складу технічної чи управлінської політики, які разом складають основу політики КФС. Приклад ієрархічних відношень, які можуть виникати між політиками, наведений на рис. 3.

*Основні принципи моделі ієрархії корпоративних політик безпеки:* корпоративна політика безпеки може містити принципи захисту і директиви для організації в цілому; політика ІБ може містити принципи і директиви, які стосуються захисту інформації, яка вразлива до загроз або дуже цінна чи має особливе значення для організації; корпоративна політика безпеки у сфері КФС повинна відображати основні принципи безпеки у сфері КФС і директиви, які належать до корпоративної політики безпеки і політики ІБ та загального використання КФС у рамках організації; політика безпеки КФС повинна відображати принципи безпеки та вказівки, що містяться в корпоративній політиці безпеки у сфері КФС; вона повинна також містити інформацію

про конкретні вимоги і гарантій безпеки, які будуть реалізовані, вказівки правильного використання гарантій для забезпечення належної безпеки.

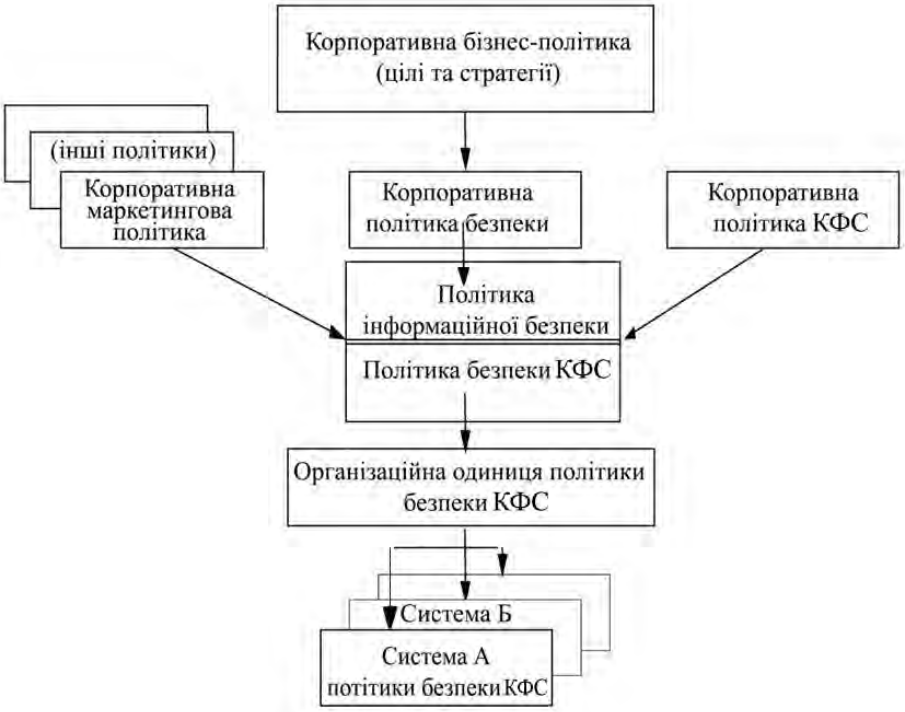


*Рис. 3. Модель ієрархії корпоративних політик безпеки*

*Загальна структура планування й управління безпекою КФС* [7]. Планування і керування захистом КФС – загальний процес встановлення і підтримки програми безпеки КФС в організації. Відмінність типів керування, розмірів і структур організацій спричинює орієнтацію процесу на середовище. На рис. 4. відображено основні положення цього процесу. *Основні принципи загальної структури планування й управління безпекою КФС:*

- корпоративна методика безпеки КФС включає цілі, зобов'язання керівництва та взаємозв'язки методик;
- організаційні аспекти безпеки КФС передбачають використання ради з безпеки КФС та корпоративного контролера безпеки інформаційних технологій;
- загальний огляд керування ризиком функціонує на основі: визначення загальної стратегії керування ризиком згідно з корпоративною методологією; вибір засобів захисту для конкретної КФС згідно з аналізом ризику; розроблення методик захисту КФС, виходячи з рекомендацій безпеки; розроблення проектів безпеки КФС щодо застосування засобів захисту на основі схвалених методик захисту системи ІТ;
- загальний огляд застосування виконує впровадження засобів захисту та покращення загальної компетентності захисту КФС;
- механізм доопрацювання використовують для перевірки узгодженості захисту, контролю робочого оточення, огляду записів журналу та обробки інцидентів для гарантій тривалості процесу забезпечення безпеки КФС.

***Методи управління інформаційною безпекою КФС*** [8]. Важливою частиною процесу управління безпекою КФС є оцінка ризику і комплексне застосування методів управління для зниження його до прийнятного рівня. Для забезпечення цілісного та ефективного захисту активів організації, доцільно застосовувати такі методи управління ІБ:

- формування цілей, стратегії та політики безпеки – полягає у визначенні мети і завдань роботи організації, основних активів та їхньої цінності;

• аналіз ризику організації: *базовий підхід* – передбачає вибір стандартних захисних заходів безпеки; *неформальний підхід* – застосування знань і практичного досвіду конкретних спеціалістів, а не структурних методів; *детальний аналіз ризику* – детальна ідентифікація і оцінка активів, можливих загроз для них, рівня вразливості; *комбінований підхід* – попередній аналіз ризику високого рівня для всіх систем, звертаючи особливу увагу на значимість системи і властивий їй рівень ризику;

• застосування плану безпеки інформаційних технологій: формування плану на основі цілей, стратегії та політики безпеки організації; виконання плану, шляхом дотримання всіх пунктів забезпечення безпеки організації, включаючи навчання;

• підтримання компетентності з питань безпеки – підвищення знань працівників організації до необхідного рівня, коли процеси забезпечення безпеки стають регулярними й усі працівники їх виконують;

• навчання персоналу інформаційній безпеці – проведення спеціальних навчальних заходів, пов'язаних із задачами й обов'язками щодо забезпечення безпеки;

• супровід системи: *перевірка відповідності безпеки* – проведення контролю відповідності КФС вимогам, наведеним політиці безпеки; *моніторинг* – проведення періодичних перевірок системи на відсутність відхилень від політики безпеки; *обробка інцидентів* – збір і аналіз інформації щодо подій порушення безпеки.

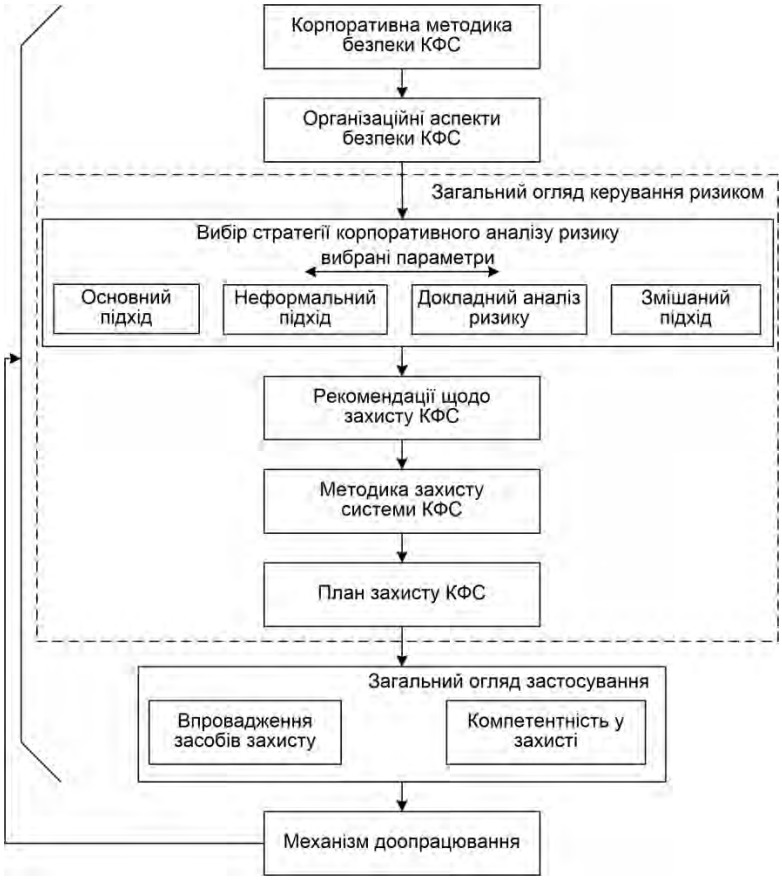


*Рис. 4. Загальна структура планування і управління безпекою КФС*

***Модель "плануй – виконуй – перевіряй – дій"*** [9, 10]. Модель "плануй – виконуй – перевіряй – дій" (рис. 5.) застосовується до усіх процесів системи управління інформаційною безпекою (СУІБ). Вона ілюструє, яким чином СУІБ за допомогою необхідних дій і процесів виробляє вихідні дані інформаційної безпеки, що відповідають вхідним даним – вимогам та очікуванням зацікавлених сторін.

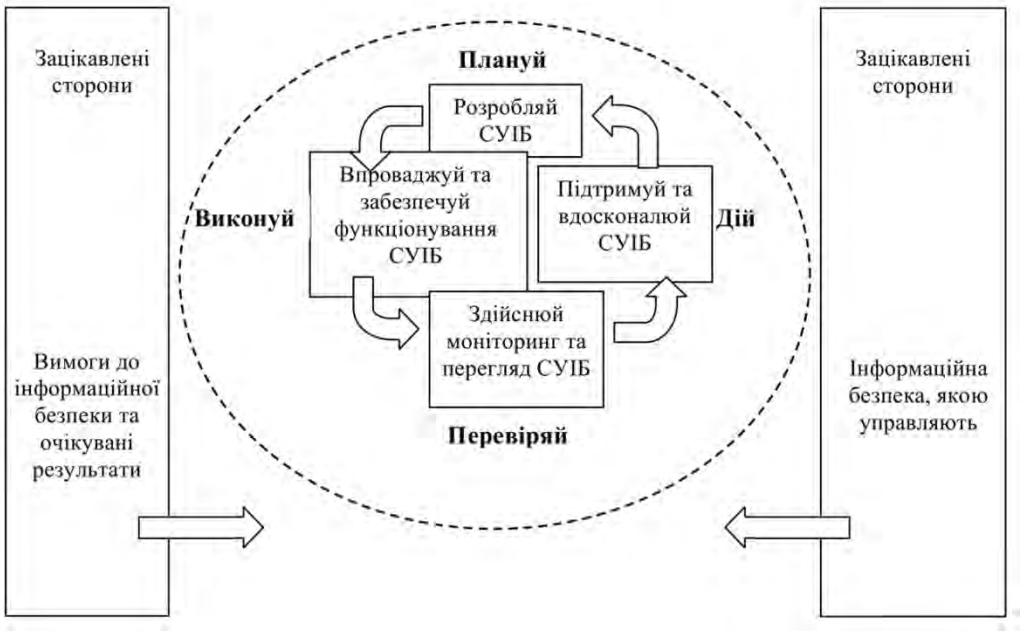


*Рис. 5. Модель "плануй – виконуй – перевіряй – дій", застосована до процесів системи управління інформаційною безпекою*

Зміст етапів управління ІБ КФС відповідно до моделі "плануй – виконуй – перевіряй – дій" наведений у таблиці.

**Етапи управління інформаційною безпекою КФС відповідно до моделі "плануй – виконуй – перевіряй – дій"**

| Етап | Завдання |
|---|---|
| ПЛАНУВАННЯ (розроблення) СУІБ | Розробити політику СУІБ, цілі, процеси та процедури, суттєві для управління ризиком та вдосконалення інформаційної безпеки, щоб одержати результати, які відповідають загальним політикам та цілям організації. |
| ВИКОНАННЯ (впровадження та забезпечення функціонування) СУІБ | Впроваджувати та забезпечувати функціонування політики інформаційної безпеки, контролів, процесів та процедур СУІБ. |
| ПЕРЕВІРКА (здійснення моніторингу та перегляду) СУІБ | Оцінювати і, за можливості, вимірювати продуктивність процесів згідно з політикою, цілями і практичним досвідом СУІБ та звітувати про результати керівництву для перегляду. |
| ДІЯ (підтримка і вдосконалення СУІБ) | Вживати коригувальних та запобіжних заходів на підставі результатів внутрішнього аудиту і перегляду СУІБ з боку керівництва або іншої суттєвої інформації для досягнення постійного вдосконалення СУІБ. |

Проаналізовані моделі управління ІБ є доступними у застосуванні щодо інформаційних технологій. Зокрема, у частині ІС розглянемо структуру управління ІБ кіберфізичних систем.

**Управління КСБ КФС на основі концепції "об'єкт – загроза – захист"**

У контексті моделі "плануй – виконуй – перевіряй – дій" розглянемо структуру управління інформаційною безпекою КФС на рівні життєвого циклу інформації та багаторівневої моделі КФС – кібернетичний простір (ІР, ІС, ІП), комунікаційне середовище (КС), фізичний простір (ФП) на основі концепції "об'єкт – загроза – захист" (рис. 6).

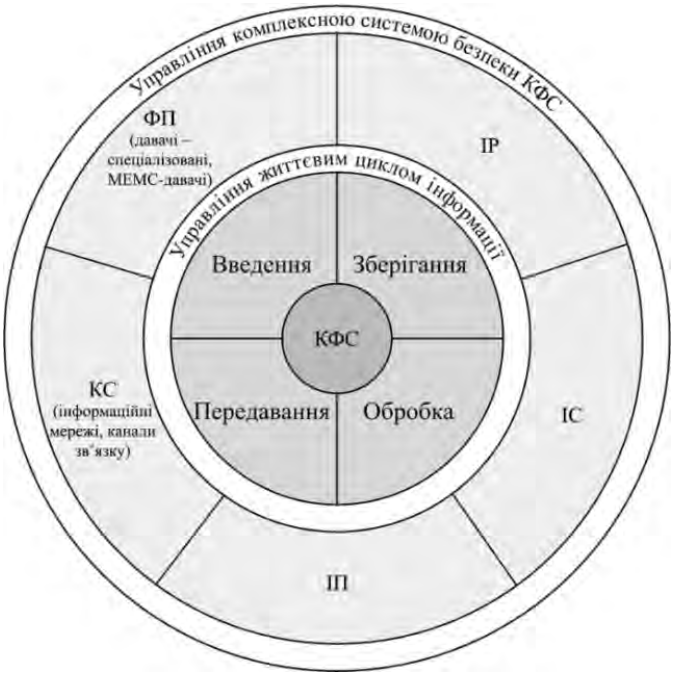


*Рис. 6. Структура управління КСБ КФС*
*на основі концепції "об'єкт – загроза – захист"*

Розглянемо структуру управління життєвим циклом інформації в КФС на основі концепції "об'єкт – загроза – захист" згідно з моделлю "загрози (випадкові/цілеспрямовані) – методи захисту – засоби захисту".

На етапі введення (збору / відбору) даних характерні:

*випадкові загрози /методи захисту/ засоби захисту*

- помилки санкціонованого користувача (адміністратора) / навчання та інструктаж персоналу; ведення журналу дій користувачів / інструкції, розпорядження, укази, нормативні документи;
- помилки, відмови, аварії пристроїв введення даних / функціональний контроль пристроїв введення даних / давачі; централізовані пристрої збору інформації;
- збої програмного забезпечення на етапі введення даних / протоколювання програмних збоїв / модулі реєстрації програмних збоїв;
- випадкове порушення цілісності чи достовірності інформації на етапі її введення / хешування даних; шифрування даних; резервне копіювання даних; обмеження доступу до інформації; метод електронного цифрового підпису / хеш-функції, хеш-таблиці; засоби криптографічного перетворення інформації; засоби реалізації електронного цифрового підпису;

*цілеспрямовані загрози /методи захисту/ засоби захисту*

- виведення з ладу пристроїв введення; зчитування інформації з пристроїв введення / контроль, розмежування доступу до пристроїв введення даних; екранування пристроїв введення даних; забезпечення своєчасного оновлення сигнатур; ідентифікація, аутентифікація, авторизація / системи контролю, розмежування доступу; антишпигунське та антивірусне програмне забезпечення; захисне програмне забезпечення на основі поведінкових аналізаторів; віртуальна клавіатура;
- цілеспрямоване порушення цілісності чи достовірності інформації на етапі її введення / хешування даних; шифрування даних; резервне копіювання даних; обмеження доступу до інформації; метод електронного цифрового підпису / хеш-функції, хеш-таблиці; засоби криптографічного перетворення інформації; засоби реалізації електронного цифрового підпису;
- застосування шкідливого програмного забезпечення / використання сертифікованого ліцензійного програмного забезпечення; обмеження можливості підключення нових зовнішніх пристроїв; обмеження з'єднання з Інтернет / антивірусне програмне забезпечення; міжмережеві екрани.

На етапі введення зберігання даних характерні:

*випадкові загрози /методи захисту/ засоби захисту*

- випадкове видалення – знищення – модифікація – підміна даних або носіїв; помилки, відмови, аварії цифрових носіїв / контроль зберігання даних; ведення журналу дій користувачів; навчання та інструктаж персоналу; функціональний контроль цифрових носіїв / засоби створення та зберігання резервних копій; давачі; централізовані пристрої збору інформації;
- збої програмного забезпечення на етапі зберігання даних / протоколювання програмних збоїв / модулі реєстрації програмних збоїв.

*цілеспрямовані загрози /методи захисту/ засоби захисту*

- викрадення паперових чи цифрових носіїв інформації, несанкціоноване зчитування інформації з них / обмеження доступу до носіїв; шифрування інформації на цифрових носіях; самознищення інформації на цифрових носіях при спробі несанкціонованого доступу; ідентифікація, аутентифікація, авторизація / контрольно-пропускні пункти; ключові, електронні замки; засоби сигналізації; сейфи; засоби криптографічного перетворення інформації;
- цілеспрямоване видалення – знищення – модифікація – підміна даних або носіїв / хешування даних; шифрування даних; обмеження доступу до носіїв інформації; метод електронного цифрового підпису / хеш-функції, хеш-таблиці; засоби криптографічного перетворення інформації; контрольно-пропускні пункти; ключові, електронні замки; засоби сигналізації; сейфи; засоби створення та зберігання резервних копій; засоби реалізації електронного цифрового підпису;
- застосування шкідливого програмного забезпечення та логічних бомб на етапі зберігання / використання сертифікованого ліцензійного програмного забезпечення; обмеження можливості підключення нових зовнішніх пристроїв; обмеження з'єднання з Інтернет / антивірусне програмне забезпечення; засоби створення та зберігання резервних копій.

На етапі обробки даних характерні:

*випадкові загрози /методи захисту/ засоби захисту*

- помилки санкціонованого користувача (адміністратора) на етапі обробки: оновлення – знищення даних / навчання та інструктаж персоналу; ведення журналу дій користувачів / інструкції, розпорядження, укази, нормативні документи;
- помилкове віднесення інформації до категорії, що підлягає знищенню – оновленню / застосування багатоетапної перевірки даних, що підлягають знищенню – оновленню / ідентифікатори;
- помилки, відмови, аварії автоматизованих систем обробки інформації / функціональний контроль автоматизованих систем обробки інформації / давачі; централізовані пристрої збору інформації;
- збої програмного забезпечення на етапі обробки даних / протоколювання програмних збоїв; функціональний контроль програмного забезпечення / модулі реєстрації програмних збоїв.

*цілеспрямовані загрози /методи захисту/ засоби захисту*

- порушення режиму обробки шляхом зміни алгоритму / періодична перевірка алгоритму обробки; обмеження доступу до автоматизованої системи обробки інформації; ідентифікація, аутентифікація, авторизація / ідентифікатори; контрольно-пропускні пункти; ключові, електронні замки; засоби сигналізації;
- несанкціонований доступ до інформації – модифікація – підміна на етапі її обробки / шифрування процесів обробки і даних; обмеження доступу до автоматизованої системи обробки інформації; ідентифікація, аутентифікація, авторизація; хешування даних / засоби криптографічного перетворення інформації; ідентифікатори; контрольно-пропускні пункти; ключові, електронні замки; засоби сигналізації;
- застосування шкідливого програмного забезпечення на етапі обробки / використання сертифікованого ліцензійного програмного забезпечення; обмеження можливості підключення нових зовнішніх пристроїв; обмеження з'єднання з Інтернет / антивірусне програмне забезпечення; засоби створення та зберігання резервних копій;

- зміна ідентифікаторів даних з метою фальсифікації цінності – важливості / хешування даних; шифрування даних; обмеження доступу до автоматизованої системи обробки інформації; метод електронного цифрового підпису / хеш-функції, хеш-таблиці; засоби криптографічного перетворення інформації; засоби реалізації електронного цифрового підпису; контрольно-пропускні пункти; ключові, електронні замки; засоби сигналізації.

На етапі передавання даних характерні:

*випадкові загрози /методи захисту/ засоби захисту*

- помилки користувачів – адміністраторів під час введення адреси отримувача даних / автоматизація вибору адреси отримувача даних / автоматизована система передавання даних;
- вплив сторонніх сигналів на інформативні параметри мовного сигналу в каналі зв'язку; вплив комплексу факторів на корисний сигнал у каналі зв'язку / хешування даних; шифрування даних; завадостійке кодування; модуляція – маніпуляція сигналу / хеш-функції, хеш-таблиці; засоби криптографічного перетворення інформації; кодери – декодери; модулятори – демодулятори.

*цілеспрямовані загрози /методи захисту/ засоби захисту*

- аналіз – перехоплення даних у каналі зв'язку; модифікація – підміна – затримка – знищення даних у каналі зв'язку / шифрування даних; шифрування заголовків пакетів; використання цифрових технологій передавання даних за допомогою пакетів; уникнення передавання конфіденційної інформації незахищеними каналами зв'язку; модуляція – маніпуляція сигналу; хешування даних / засоби криптографічного перетворення інформації; захищені IP-протоколи; модулятори – демодулятори;
- знищення провідних каналів зв'язку / створення резервних провідних каналів зв'язку; обмеження доступу до обладнання передавання даних / пристрої реєстрації несправностей обладнання передавання даних;
- створення перешкод у каналі зв'язку / завадостійке кодування; модуляція – маніпуляція сигналу; хешування даних; шифрування даних; застосування резервних каналів зв'язку – кодери – декодери; модулятори – демодулятори; хеш-функції, хеш-таблиці; засоби криптографічного перетворення інформації.

Розглянемо структуру управління комплексною системою безпеки КФС на основі концепції "об'єкт – загроза – захист" згідно з моделлю "загрози (випадкові/цілеспрямовані) – методи захисту – засоби захисту" на рівні: кібернетичного простору, комунікаційного середовища, фізичного простору.

На рівні інформаційних ресурсів кібернетичного простору характерні:

*випадкові загрози /методи захисту/ засоби захисту*

- втрата та модифікація інформації при відборі, передаванні і обробці / введення додаткових перевірок правильності роботи компонентів; підключення алгоритмів виявлення та корекції помилок; хешування даних; шифрування даних / модулі реєстрації програмних збоїв; хеш-функції, хеш-таблиці; засоби криптографічного перетворення інформації;
- втрата інформації, пов'язана з неправильним зберіганням архівних даних / створення платформи для включення в систему електронного документообігу; організація нових сервісів на базі національних сертифікованих криптомодулів; метод електронного цифрового підпису / засоби криптографічного перетворення інформації; засоби реалізації електронного цифрового підпису;
- помилки санкціонованого користувача (адміністратора) при роботі з IP / навчання та інструктаж персоналу; ведення журналу дій користувачів / інструкції, розпорядження, укази, нормативні документи.

*цілеспрямовані загрози /методи захисту/ засоби захисту*

- несанкціоноване знищення, модифікація, копіювання IP / посилення засобів аутентифікації користувачів і процесів; посилення оперативного реагування на атаки в напрямку інформаційних ресурсів; організація внутрішньо-корпоративного та зовнішнього захищеного документообігу; шифрування даних; ідентифікація – аутентифікація; метод електронного цифрового підпису / засоби криптографічного перетворення інформації; ідентифікатори; засоби реалізації електронного цифрового підпису;
- блокування доступу до IP / застосування резервних каналів доступу до IP; розширення каналу для захисту від атак на відмову; використання захищених топологій мереж / міжмережеві екрани;

- зараження баз даних шкідливим програмним забезпеченням / обмеження доступу до ІР; обмеження з'єднання з Інтернет; використання сертифікованого ліцензійного програмного забезпечення / антивірусне програмне забезпечення; міжмережеві екрани.
- несанкціонована зміна параметрів серверів – носіїв ІР / контроль доступу до серверів – носіїв ІР – засоби реєстрації несанкціонованих змін параметрів серверів – носіїв ІР.

На рівні інформаційних систем кібернетичного простору КФС характерні:

*випадкові загрози /методи захисту/ засоби захисту*

- помилки при конфігуруванні системи / проведення періодичних перевірок конфігурації системи; визначення вимог до фахівців, які конфігурують системи / спеціалізована документація;
- відсутність необхідної кваліфікації персоналу для роботи з системами / підбір кваліфікованих кадрів; проведення курсів підвищення кваліфікації / тренінгів персоналу; ведення журналу дій користувачів / інструкції, розпорядження, укази, нормативні документи;
- збої – відмови – аварії апаратного-програмного забезпечення систем / протоколювання збоїв – відмов – аварій; функціональний контроль апаратно-програмного забезпечення ІС / давачі; централізовані пристрої збору інформації; модулі реєстрації збоїв – відмов – аварій; вплив електромагнітного випромінювання / використання обладнання з низьким рівнем випромінювання / електромагнітні екрани.

*цілеспрямовані загрози /методи захисту/ засоби захисту*

- руйнування – пошкодження апаратури, систем життєзабезпечення; несанкціонований доступ до ІС / контроль, розмежування доступу; забезпечення своєчасного оновлення сигнатур; ідентифікація, аутентифікація, авторизація; шифрування даних / системи контролю, розмежування доступу; ідентифікатори; контрольно-пропускні пункти; ключові, електронні замки; засоби сигналізації; аварійні електрогенератори; блоки безперебійного живлення;
- вимкнення – виведення з ладу систем забезпечення безпеки ІС / моніторинг стану системи забезпечення безпеки ІС; застосування багатоланкових та багаторівневих систем з забезпечення безпеки ІС; обмеження – контроль доступу до пультів управління системами забезпечення безпеки /давачі автоматизованої процедури виявлення атак;
- застосування програмних і апаратних закладок, шкідливого програмного забезпечення в ІС / використання сертифікованого ліцензійного програмного забезпечення; обмеження можливості підключення нових зовнішніх пристроїв; обмеження з'єднання з Інтернет / засоби створення та зберігання резервних копій; антивірусне програмне забезпечення.

На рівні інформаційних процесів кібернетичного простору характерні:

*випадкові загрози /методи захисту/ засоби захисту*

- випадкове порушення цілісності чи достовірності інформації / хешування даних; шифрування даних; резервне копіювання даних; метод електронного цифрового підпису / хеш-функції, хеш-таблиці; засоби криптографічного перетворення інформації; засоби реалізації електронного цифрового підпису;
- збої, відмови, аварії апаратного, програмного забезпечення ІП / протоколювання збоїв, відмов, аварій; функціональний контроль апаратно-програмного забезпечення ІП; проведення періодичних перевірок режимів роботи, конфігурації апаратно-програмного забезпечення ІП / давачі; централізовані пристрої збору інформації; модулі реєстрації збоїв, відмов, аварій;

*цілеспрямовані загрози /методи захисту/ засоби захисту*

- перехоплення інформації на етапах життєвого циклу / шифрування процесів обробки і даних; обмеження доступу до автоматизованої системи обробки інформації; ідентифікація, аутентифікація, авторизація; хешування даних / засоби криптографічного перетворення інформації; ідентифікатори; контрольно-пропускні пункти; ключові, електронні замки; засоби сигналізації;
- застосування шкідливого програмного забезпечення, логічних бомб на етапах життєвого циклу інформації / використання сертифікованого ліцензійного програмного забезпечення; обмеження можливості підключення нових зовнішніх пристроїв; обмеження з'єднання з Інтернетом / засоби створення та зберігання резервних копій; антивірусне програмне забезпечення.

- порушення алгоритмів роботи, конфігурації апаратно-програмного забезпечення ІП / проведення періодичних перевірок режимів роботи, конфігурації апаратно-програмного забезпечення ІП; обмеження доступу до пультів управління / журнал змін конфігурацій, алгоритмів;
- цілеспрямоване порушення цілісності чи достовірності інформації / хешування даних; шифрування даних; резервне копіювання даних; обмеження доступу до інформації; метод електронного цифрового підпису / хеш-функції, хеш-таблиці; засоби криптографічного перетворення інформації; засоби реалізації електронного цифрового підпису; ключові, кодові замки; контрольно-пропускні пункти.

На рівні інформаційних мереж (каналів) комунікаційного середовища характерні:

*випадкові загрози /методи захисту/ засоби захисту*

- помилкове використання ресурсів локальної обчислювальної мережі / розділення наявних ресурсів на часові інтервали; збільшення пропускної здатності мережі / система контролю використання ресурсів мережі;
- помилки при адмініструванні, конфігуруванні мережевого обладнання та програмного забезпечення / проведення періодичних перевірок режимів роботи та конфігурації мережі; встановлення вимог до компетентності фахівців, які адмініструють та конфігурують мережеве обладнання, програмне забезпечення; журнал змін конфігурації мережевого обладнання, програмного забезпечення / журнал змін конфігурації мережевого обладнання / програмного забезпечення;
- збої, відмови, аварії апаратного та програмного забезпечення ІМ (К) / протоколювання збоїв, відмов, аварій; функціональний контроль апаратно-програмного забезпечення ІМ (К); проведення періодичних перевірок режимів роботи, конфігурації апаратно-програмного забезпечення ІМ (К) / давачі; централізовані пристрої збору інформації; модулі реєстрації збоїв, відмов, аварій;

*цілеспрямовані загрози /методи захисту/ засоби захисту*

- аналіз, перехоплення трафіка, циркулюючого в мережі / шифрування даних; шифрування заголовків пакетів; використання цифрових технологій передавання даних за допомогою пакетів; уникнення передавання конфіденційної інформації незахищеними каналами зв'язку; модуляція, маніпуляція сигналу; обмеження доступу до Інтернет; ідентифікація, аутентифікація / засоби криптографічного перетворення інформації; захищені IP-протоколи; модулятори, демодулятори;
- несанкціонована зміна конфігурації, режимів роботи мережі / проведення періодичних перевірок режимів роботи, конфігурації апаратно-програмного забезпечення ІМ (К); обмеження доступу до обладнання, програмного забезпечення мережі; ідентифікація, аутентифікація користувача, параметрів мережі / ідентифікатори; контрольно-пропускні пункти; засоби сигналізації; ключові, кодові замки;
- цілеспрямоване порушення цілісності, достовірності чи доступності інформації в мережі / шифрування даних; хешування даних; резервне копіювання даних; метод електронного цифрового підпису / хеш-функції, хеш-таблиці; засоби криптографічного перетворення інформації; засоби реалізації електронного цифрового підпису;
- підміна санкціонованого користувача (атака "Man in the middle") / ідентифікація, авторизація користувачів, обладнання, даних; періодичне проведення аналізу параметрів мережі; уникнення використання відкритих мереж / цифрові сертифікати обладнання; спеціалізовані захищені IP-протоколи.

На рівні спеціалізованих давачів та МЕМС-давачів фізичного простору у складі КФС, поширених у сферах розумний дім, розумна медицина, розумна енергетика, розумна інфраструктура, характерні:

*випадкові загрози для спеціалізованих давачів, вбудованих в об'єкт або пристрій* – помилки людини як складової системи; структурні, алгоритмічні, програмні помилки; відмови і збої; завади в лініях зв'язку; аварійні ситуації; *цілеспрямовані загрози для спеціалізованих давачів, вбудованих в об'єкт або пристрій* – доступ до терміналів користування; адміністрування, контролю; пасивне/ активне перехоплення;

- побічне електромагнітне випромінювання інформації; *технології захисту* – виявлення і діагностика відмов, збоїв алгоритмів, програм, помилок людини; контроль доступу до терміналів;

контроль доступу до монтажу ліній зв'язку та апаратури; ідентифікація та аутентифікація; захист від побічного випромінювання і наведень інформації.

Для МЕМС-давачів фізичного простору КФС характерні: *загрози* – лінійні навантаження. власні шуми елементів схеми, температурні залежності, зношуваність; *технології захисту* – лінійні стабілізатори, термотривкі елементи, покращення технології виготовлення матеріалів.

**Висновок**

Проаналізовано моделі управління безпекою КФС як сегмента інформаційно-комунікаційних технологій згідно з ISO/IEC TR 13335; розкрито зміст моделі "плануй – виконуй – перевіряй – дій" згідно з ISO/IEC 27001:2010. Створено структуру управління КСБ КФС згідно з концепцією "об'єкт – загроза – захист" на рівні життєвого циклу інформації та багаторівневої моделі "кібернетичний простір – комунікаційне середовище – фізичний простір". Структура управління КСБ дозоляє реалізувати адекватний вибір елементів багаторівневого захисту КФС відповідно до моделей загроз, що забезпечуватиме конфіденційність, цілісність та доступність, відповідно захищений обмін інформації в рамках класичної моделі "плануй – виконуй – перевіряй – дій".

*1. Проект Стратегії кібернетичної безпеки України. [Електронний ресурс]. – Режим доступу: http://www. niss. gov. ua/public/File/2013_nauk_an_rozrobku/kiberstrateg. pdf. 2. Mykytyn G. V. Security of Cyber-Physical Systems from Concept to Complex Information Security System / Dudykevych V., Mykytyn G., Kret T., Rebets A. // Advances in Cyber-Physical Systems. – Vol. 1, No. 2 (2016). – С. 67–75. 3. Інформаційні технології. Настанови з керування безпекою інформаційних технологій (IT). Частина 1. Концепції й моделі безпеки IT (ISO/IEC TR 13335-1: 1996, IDT): ДСТУ ISO/IEC TR 13335-1-2003. – [Чинний від 2004-10-01]. – Київ: Держспоживстандарт України, 2004. – 23 с. 4. Saqib Ali Risk Management for Cyber Physical Systems: An Approach for Smart Grid / Saqib Ali, Amira Al Zadjali, Taisira Al Balushi // 27th IBIMA Conference. – Milan, Italy, 2016. – [Online resource]. – Access at: https://ibima.org/accepted-paper/risk-management-for-cyber-physical-systems-an-approach-for-smart-grid/ 5. Halima Ibrahim Kure An Integrated Cyber Security Risk Management Approach for a Cyber-Physical System / Halima Ibrahim Kure, Shareeful Islam, Mohammad Abdur Razzaque // Applied sciences. – Volume 8, Issue 6, 2018. – [Online resource]. – Access at: https://www.mdpi.com/2076-3417/8/6/898 6. Ibtihaj Ahmad Security Aspects of Cyber Physical Systems / Ibtihaj Ahmad, Muhammad Kaab Zarrar, Takreem Saeed, Saad Rehman // 2018 1st International Conference on Computer Applications & Information Security (ICCAIS). – [Online resource]. – Access at: https://ieeexplore.ieee.org/document/8442009. 7. Інформаційні технології. Настанови з керування безпекою інформаційних технологій (IT). Частина 2. Керування та планування безпеки IT (ISO/IEC TR 13335- 2: 1997, IDT): ДСТУ ISO/IEC TR 13335-2-2003. – [Чинний від 2004-10-01]. – К.: Держспоживстандарт України, 2004. – 20 с. 8. Інформаційні технології. Настанови з керування безпекою інформаційних технологій (IT). Частина 3. Методи керування захистом IT (ISO/IEC TR 13335- 3: 1998, IDT): ДСТУ ISO/IEC TR 13335-3-2003. – [Чинний від 2004-10-01]. – К.: Держспоживстандарт України, 2004. – 48 с. 9. Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Вимоги: ГСТУ СУІБ 1.0 / ISO/IEC 27001: 2010. – [Чинний від 2010-01-01]. – К.: Національний банк України, 2010. – 49 с. 10. Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Звід правил для управління інформаційною безпекою: ГСТУ СУІБ 2.0 / ISO/IEC 27002: 2010. – [Чинний від 2010-01-01]. – К.: Національний банк України, 2010. – 149 с.*