КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (23), 2024
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2024.23.110130
УДК 004.4

Вінтенко Борис Юрійович
аспірант кафедри інформаційної безпеки та комп'ютерної інженерії
Черкаський державний технологічний університет, Черкаси, Україна
ORCID 0009-0008-3748-0374
boris.vintenko@gmail.com

Миронець Ірина Валеріївна
кандидат технічних наук, доцент, доцент кафедри інформаційної безпеки та комп'ютерної інженерії
Черкаський державний технологічний університет, Черкаси, Україна
ORCID 0000-0003-2007-9943
i.myronets@chdtu.edu.ua

Смірнов Олексій Анатолійович
доктор технічних наук, професор, завідувач кафедри кібербезпеки та програмного забезпечення
Центральноукраїнський національний технічний університет, Кропивницький, Україна
ORCID 0000-0001-9543-874X
dr.smirnovoa@gmail.com

Кравчук Оксана Вікторівна
інспектор відділу кадрів
Центральноукраїнський національний технічний університет, Кропивницький, Україна
ORCID 0009-0008-8453-0557
vov-14@i.ua

Козірова Наталія Леонідівна
асистент кафедри кібербезпеки та програмного забезпечення
Центральноукраїнський національний технічний університет, Кропивницький, Україна
ORCID 0009-0005-8753-5132
natalidonchenko23@gmail.com

Савеленко Григорій Володимирович
кандидат технічних наук, доцент кафедри економіки, підприємництва та готельно-ресторанної справи
Центральноукраїнський національний технічний університет, Кропивницький, Україна
ORCID 0000-0001-9310-6223
grigoriy.savelenko@gmail.com

Коваленко Анна Степанівна
кандидат технічних наук, доцент, доцент кафедри кібербезпеки та програмного забезпечення
Центральноукраїнський національний технічний університет, Кропивницький, Україна
ORCID 0000-0003-3610-9465
annasun911@gmail.com

ДОСЛІДЖЕННЯ ВИМОГ ТА АНАЛІЗ КІБЕРБЕЗПЕКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНО-КЕРУЮЧИХ СИСТЕМ АЕС, ВАЖЛИВИХ ДЛЯ БЕЗПЕКИ

Анотація. Для забезпечення протидії криптоатакам на елементи критичної інфраструктури, зокрема на комп'ютерні системи управління атомних електростанцій, у даній роботі досягнута мета, яка складається у проведенні аналізу вимог до комп'ютерної безпеки (кібербезпеки) програмного забезпечення даної системи, що мають відношення до етапу його проектування, розробки та експлуатації, також запропоновані критерії та методика розрахунку якості дотримання даних вимог. Для досягнення поставленої мети в першому розділі статті наведена інформація про стандарти та виявлені вимоги до кібербезпеки програмного забезпечення. В другому розділі проведений аналіз вимог та описаний підхід до розробки програмного забезпечення з урахуванням даних вимог та аналізу їх врахування. В

третьому розділі запропонований підхід до розрахунку показника виконання вимог кібербезпеки програмного забезпечення. В четвертому розділі наводиться приклад застосування даного підходу для існуючої комп'ютерної системи управління АЕС для оцінки відповідності вимог кібербезпеки. В статті розглянуто вимоги міжнародного стандарту IEC62645 та галузевого стандарту України «НП 306.2.237-2022», що мають відношення до розробки програмного забезпечення комп'ютерної системи управління АЕС. Забезпечення кіберзахисту програмного забезпечення комп'ютерної системи управління АЕС є комплексною задачею, що містить адміністративно-правові, технічні, культурні, організаційні складові. З точки зору розробки та експлуатації програмного забезпечення основні заходи щодо кіберзахисту включають в себе заходи з верифікації коду програмного забезпечення, забезпечення відсутності прихованих функцій, реалізацію фізичного захисту обладнання, захищеність складових частин програмного забезпечення, автентифікацію, безпеку під час обміну даними. Для визначення відповідності програмного забезпечення вимогам кіберзахисту необхідно визначити вимоги, що є застосовними до кожного компоненту програмного забезпечення, та провести аналіз їх виконання. Дана дія має відбуватися постійно під час розробки нового програмного забезпечення та оцінюванні програмного забезпечення існуючих комп'ютерної системи управління. Після проведення аналізу застосовності та виконання вимог може бути проведений розрахунок коефіцієнту виконання вимог. Відмічено, що кіберзахист є лише складовою частиною якості програмного забезпечення комп'ютерної системи управління АЕС, що є важливим для виконання функцій безпеки. Аналіз вимог та розрахунок коефіцієнту їх виконання може бути складовою частиною комплексної моделі процесу розробки програмного забезпечення комп'ютерної системи управління АЕС.

Ключові слова: кібербезпека; програмне забезпечення; інформаційно-керуючі системи; атомні електростанції; енергетика.

ВСТУП

Постановка завдання дослідження. Сучасний світ характеризується досить великою кількістю систем критичної інфраструктури. Серед такого роду систем можливо виділити енергетичну інфраструктуру, у складі якої є атомні електростанції. Атомною електростанцією (АЕС) називається промислове підприємство, де атомну енергію перетворюють на електричну [1]. В Україні на даний момент діє 4 атомних електростанції [2], одна з яких (Запорізька) окупована російськими військовими [3]. Назагал у світі експлуатується 191 атомна електростанція [4]. Одним з важливих елементів АЕС є Комп'ютерна Система Управління (КСУ). І, як будь яка комп'ютерна система, вона вимагає підвищених вимог щодо забезпечення кібербезпеки та захисту інформації, яка в ній циркулює.

Постановка проблеми. Останні роки характеризуються кібератаками на різні об'єкти критичної інфраструктури. Особливо їх кількість збільшилася за час агресії росії проти України, починаючи з 2014 року. До найбільш відомих криптоатак на системи критичної інфраструктури можливо віднести наступні: 23.12.2015 року з використанням троянської програми BlackEnergy3, у застосуванні якої були раніше помічені російські хакери, було відключено близько 30 підстанцій Прикарпаттяобленерго, що призвело до того, що більш ніж 200 тисяч жителів Івано-Франківської області залишалися без електроенергії терміном від однієї до п'яти годин. Тоді ж відбулися атаки на Київобленерго і Чернівціобленерго [5], [6], 17.12.2016 року кібератака на підстанцію Північної компанії Укренерго привела до збою в автоматиці управління, що призвело до того, що більше години знеструмленими залишалися райони північній частині правобережного Києва і прилеглі райони області [5], [6], 27.06.2017 року відбулася масштабна хакерська атака за допомогою вірусної програми Petya.A, яка порушила

роботу численних українських державних і приватних підприємств, зокрема аеропорту Бориспіль, Укртелекому, ЧАЕС, Укрзалізниці та інших, а також Кабінету міністрів і ряду ЗМІ. СБУ заявила про причетність до атаки російських спецслужб [5], [6]. 12.12.2023 року була проведена одна з наймасштабніших кібератак у вітчизняній історії проти телеком-оператору України — «Київстар». Внаслідок кібератаки, виник збій у системах оператора, що привело до того, що без зв'язку залишилося понад 20 мільйонів абонентів по всій країні [7], [8]. Крім того, треба відмітити, що з початку повномасштабного вторгнення до сьогодні Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA, яка діє при Держспецзв'язку, в ручному режимі опрацювала та дослідила понад 3000 кіберінцидентів і кібератак [9]. Якщо взяти світові тенденції, то кількість криптоатак на критичну інфраструктуру у тому числі й у сфері енергетики, також постійно зростає [10]. Таким чином існує проблема протидії криптоатакам на складові критичної інфраструктури, у тому числі й на КСУ АЕС, використовуючи серед інших підходів й підхід до розробки безпечного, з точки зору кібербезпеки, програмного забезпечення відповідної системи.

Аналіз останніх досліджень і публікацій. Наведена стаття продовжує цикл огляду аспектів розробки Програмного Забезпечення (ПЗ) КСУ АЕС. У попередніх статтях [11], [12] були проаналізовані міжнародні стандарти та галузеві нормативні документи, що мають відношення до розробки ПЗ КСУ АЕС, а також наведений детальний огляд вимог міжнародних стандартів IEC60880 [13] та IEC62138 [14] до розробки даного ПЗ.

Мета статті. Проведення аналізу вимог до комп'ютерної безпеки (кібербезпеки) програмного забезпечення, що мають відношення до етапу його проектування, розробки та експлуатації, та запропонувати критерії та методику розрахунку якості дотримання даних вимог.

Для досягнення поставленої мети в першому розділі статті наведена інформація про стандарти та виявлені вимоги до кібербезпеки ПЗ. В другому розділі проведений аналіз вимог та описаний підхід до розробки ПЗ з урахуванням даних вимог та аналізу їх врахування. В третьому розділі запропонований підхід до розрахунку показника виконання вимог кібербезпеки ПЗ. В четвертому розділі наводиться приклад застосування даного підходу для існуючої КСУ АЕС для оцінки відповідності вимог кібербезпеки.

Дослідження, виконані в даній статті, можуть бути використані як під час розробки нового ПЗ КСУ АЕС для підвищення його рівня кібербезпеки, так і для проведення оцінювання ПЗ існуючих КСУ АЕС з метою виявлення компонентів, які мають бути вдосконалені з точки зору кібербезпеки.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Дослідження вимог до кібербезпеки КСУ АЕС

На сучасному етапі розвитку КСУ АЕС процеси з забезпечення кібербезпеки КСУ АЕС є надзвичайно актуальними та є складними і комплексними. У статті [15] розглядаються процеси впровадження та підтримки політики, програми та плану кібербезпеки на АЕС. «*Історично склалося так, що комп'ютерній безпеці на атомних електростанціях не приділялося належної уваги, оскільки передбачалося, що апаратні або аналогові системи невразливі до кібератак через їх жорстку реалізацію, ізоляцію та сегрегацію, а також майже повну відсутність зв'язку із зовнішніми мережами або*

системами… зараз відбувається повсюдний перехід на цифрові АСУ ТП під час модернізації існуючих АЕС та будівництва нових. Однак використання цифрових технологій в АСУ ТП зробило їх уразливими для кібератак».

Забезпечення кіберзахисту КСУ критичного застосування є комплексною задачею, яка передбачає поєднання законодавчих, культурних, технологічних, адміністративних заходів. В дослідженні [16] розроблено модель керування кібербезпекою (*Cyber Security Management Model*), в якій виділяються шість головних сфер, що є критичними для кібербезпеки:

- правове регулювання (Legal Regulation), яке визначає закони, інструкції та стандарти;
- розуміння керівництвом (Good Governance) важливості забезпечення кібербезпеки та мінімізації наслідків кіберінцидентів;
- керування ризиками (Risk Management), що вимагає не тільки зменшення ризиків виникнення інцидентів, а і вивчення даних ризиків та підготовку контрзаходів при виникненні нестандартних ситуацій;
- культура безпеки (Security Culture), що включає в себе розуміння персоналом необхідності забезпечення кібербезпеки, вивчення та дотримання ним вимог інструкцій, іншими словами — «людський фактор»;
- керування технологіями (Technology Management), що включає в себе розуміння рівня загроз, що виходять від кожного компонента КСУ, для скорочення часу відновлення працездатності КСУ після виникнення кіберінциденту;
- керування інцидентами (Incident Management), що включає в себе створення чітких планів реагування на кіберінциденту з метою якнайшвидшого усунення наслідків інциденту та відновлення нормальної роботи.

Схематичне зображення розробленої авторами моделі приведене на рис. 1.

Рис. 1. Модель керування кібербезпекою

Аналогічні сфери кібербезпеки КСУ критичного застосування відображаються в міжнародних стандартах та нормативних документах різних країн. Зокрема, вимоги до комп'ютерної безпеки (кібербезпеки) КСУ АЕС містяться в міжнародному стандарті IEC62645 [17] та галузевому стандарті України «НП 306.2.237-2022» [18].

Стандарти, що розглядаються, вводять класифікацію рівнів кіберзахисту КСУ, їх компонентів та ПЗ для визначення вимог до кібербезпеки (розділ 5.2.3.1 стандарту IEC62645, розділ II стандарту НП 306.2.237-2022). Ці рівні визначаються категоріями виконуваних функцій, важливих для безпеки (категорії «А», «В», «С» визначені у [19]). Визначаються три рівні: «S1» («К1») (виконання функцій категорії «А»), «S2» («К2») (виконання функцій категорії «В» та робота в реальному часі) та «S3» («К3») (виконання функцій категорії «С», а також допоміжних та обслуговуючих функцій). Зазначається, що визначення рівня не є жорстко регламентованим, і виконується на основі аналізу функцій КСУ.

Згідно дослідження вимог стандартів (розділ 5.1 стандарту IEC62645, розділ III-IV стандарту НП 306.2.237-2022), **основні загальні принципи забезпечення кіберзахисту** є наступними:

- наявність політики кіберзахисту, що охоплює всі етапи ЖЦ КСУ як з точки зору підприємства-розробника, так і з точки зору АЕС-експлуатуючої організації;
- глибокоешелонований кіберзахист, що реалізує послідовність бар'єрів для захисту КСУ;
- диференційований підхід, що забезпечує пропорційність застосування заходів захисту відповідно до потенційно можливих наслідків кіберінцидентів, та логічне об'єднання КСУ з однаковими рівнями в зони кіберзахисту. При об'єднанні КСУ в зони кіберзахисту вводяться вимоги щодо передачі даних між зонами;
- заходи щодо попередження шкідливих дій, виявлення та реагування на шкідливі дії, пом'якшення їх наслідків та відновлення;
- заходи щодо попередження внесення несанкціонованих змін, надлишкових функцій, некоректних даних тощо;
- заходи щодо культури кіберзахисту;
- заходи щодо мінімізації впливу кіберзахисту на якість виконання основних функцій КСУ;
- заходи щодо оцінювання та переоцінювання кіберзахисту КСУ, що знаходяться в експлуатації.

Згідно дослідження вимог стандартів щодо **забезпечення кіберзахисту на етапі розробки та експлуатації** (розділ 5.2.3.2.3 – 5.2.3.2.7, 6.4 «IEC62645», розділ V-VII — «НП 306.2.237-2022») ПЗ КСУ необхідно врахування основних нижченаведених аспектів.

Процес та засоби розробки. Розробка ПЗ та інструментальних засобів власного використання має вестися в захищеному середовищі, що виключає несанкціоноване внесення змін до ПЗ та створення непередбачуваних функцій. Засоби розробки ПЗ мають бути ліцензовані та/або петрифіковані.

Контроль за наявністю прихованих функцій. Метою даного контролю є відсутність в ПЗ прихованих функцій, що дозволяють несанкціоновано обійти захист і можуть бути використані при атаках.

Мінімізація впливу засобів кіберзахисту на виконання функцій. Метою даної мінімізації є відсутність негативного впливу засобів кіберзахисту на швидкість, точність, зручність користування ПЗ КСУ даної системи та ПЗ КСУ інших систем.

Напрямок передачі інформації. Вимоги з кіберзахисту встановлюють обмеження на обмін інформацією між системами. Під час проектування має враховуватися, що зв'язок має здійснюватися в односторонньому напрямку від систем з вищим рівнем

кіберзахисту до систем з нижчим рівнем кіберзахисту (наприклад, від «К1» до «К2»). Зворотній напрямок обміну можливий лише за запитом системи з вищим рівнем з контролюванням змісту потоку даних.

Контроль потоку даних. Для забезпечення кібербезпеки при прийомі даних від будь-якого джерела або системи прийняті пакети даних мають контролюватися.

Автентифікація та авторизація. Згідно вимог до кіберзахисту, ПЗ КСУ АЕС повинно забезпечувати доступ до своїх функцій тільки авторизованим користувачам. Через це специфікація вимог до ПЗ має містити пункт про обов'язкову автентифікацію користувачів та надання доступу за принципом найменших привілеїв. Будь-які спроби неавторизованого доступу повинні відображатися в журналах роботи програми, сигналізації тощо. Для систем, що виконують функції категорії «К1» та «К2» може бути необхідним використання автентифікація (наприклад, пароль і електронний ключ);

- ***фізичний захист компонентів КСУ.*** Стандартами кібербезпеки передбачене забезпечення контролю та сигналізації фізичного доступу до КСУ та ПЗ;
- ***захист від несанкціонованого доступу.*** Стандартами кібербезпеки передбачене обмеження доступу до носіїв інформації, файлів ПЗ та даних, конфігурації обладнання тощо.

Висновок. Дослідження стандартів кібербезпеки КСУ АЕС показують, що виконання вимог кібербезпеки є обов'язковим на всіх етапах життєвого циклу продукту. Необхідною умовою реалізації заходів кібербезпеки ПЗ є визначення його компонентів, які можуть бути об'єктами кібератак та містять вразливості, що можуть бути причиною відмов при виконанні функцій КСУ. Після визначення цих компонентів ПЗ в них має бути програмно реалізовані функції для забезпечення розглянутих аспектів кібербезпеки та проведене тестування цих функцій. У наступній частині статті описується підхід до проведення аналізу ПЗ КСУ АЕС для забезпечення кібербезпеки.

Аналіз кібербезпеки ПЗ КСУ АЕС

Метою даного розділу статті є деталізація заходів для забезпечення досліджених аспектів кібербезпеки, а також опис послідовності дій, які пропонуються для забезпечення кібербезпеки нового ПЗ КСУ під час розробки та оцінювання відповідності ПЗ існуючих КСУ вимогам кібербезпеки .

Виходячи з досліджених вимог стандартів з кібербезпеки, можуть бути виділені критерії, які доцільно враховувати під час проектування та оцінки захищеності ПЗ КСУ:

1) фізичний захист технічних засобів;
2) управління конфігурацією ПЗ;
3) контроль за відсутністю прихованих функцій в ПЗ;
4) захищеність доступу до ПЗ;
5) автентифікація при доступі до функцій ПЗ;
6) напрямки прийому та/або передачі даних;
7) захищеність від некоректності прийнятих даних;
8) контроль параметрів, що вводяться оператором.

Нижче наводиться опис дослідження ПЗ за даними критеріями.

Для дослідження базових критеріїв необхідним етапом є складання переліку технічних засобів КСУ та ПЗ, що входить до його складу. На цьому етапі можливий розгляд ПЗ з точки зору наступних критеріїв:

- фізичний захист технічних засобів;
- управління конфігурацією ПЗ;
- контроль за відсутністю прихованих функцій в ПЗ;

- захищеність доступу до ПЗ;
- автентифікація для доступу до функцій ПЗ.

Базові фактори впливу на кібербезпеку. Для будь-якого ПЗ проводяться наступні дотримання та перевірки:

- **фізична захищеність.** Даний критерій є визначальним для забезпечення кібербезпеки будь-якого компонента, що містить ПЗ. За відсутності контролю над фізичним доступом до носіїв інформації, модулів, серверів, робочих станцій, комутаторів існує загроза несанкціонованого копіювання, знищення, підміни ПЗ та підключення додаткових, не передбачених проектом пристроїв та програм;
- **контроль конфігурації.** Для забезпечення вимог кібербезпеки важливим є дотримання керування конфігурацією кожного компонента ПЗ. Зокрема, під час проектування має бути передбачена ідентифікація версії ПЗ, дати компіляції, контрольної суми програмного коду, цифрові підписи файлів тощо. Під час компіляції ця інформація повинна автоматично оновлюватися в коді та бути доступною для аналізу та перегляду. Це надає можливість під час планових заходів з перевірки кібербезпеки пересвідчитися у відсутності підміни ПЗ або даних. Необхідним є забезпечення відповідності версій ПЗ та документації;
- **відсутність прихованих функцій.** Приховані функції, що містяться в програмному забезпеченні, можуть містити засоби для несанкціонованого обходу засобів захисту і є значною загрозою для кібербезпеки. Забезпечити відсутність прихованих функцій в ПЗ може проведення верифікації вихідного коду. Згідно вимог стандарту розробки ПЗ, що виконує функції безпеки категорії «А», верифікація має проводитися незалежною від розробників організацією. Для ПЗ інших категорій можливі інші заходи за принципом двох осіб, наприклад парне програмування або Code Review.

На всіх етапах Життєвого Циклу (ЖЦ) ПЗ, від розробки до інтеграції та встановлення, необхідне використання ліцензованих та верифікованих інструментів, бібліотек мов програмування. Це унеможливлює внесення прихованого коду або функцій під час редагування коду розробником або компіляції.

Доступ до ПЗ як фактор, що впливає на кібербезпеку. При забезпеченні кібербезпеки КСУ АЕС доступ до ПЗ може розглядатися в двох аспектах: доступ до функцій ПЗ та доступ до складових частин ПЗ. Доступ до функцій ПЗ відбувається через інтерфейс користувача ПЗ та необхідний оперативному персоналу під час регламентних операцій, корекції параметрів, отримання інформації, перевірок та технічного обслуговування КСУ. Під доступом до складових частин ПЗ мається на увазі доступ до файлів програм ПЗ, файлів конфігурації, баз даних, змісту енергонезалежної пам’яті тощо, а також доступ до конфігурації середовища функціонування ПЗ, наприклад IP-адреси мережевих карт або портів введення-виведення.

З точки зору доступу до функцій в ПЗ мають забезпечуватися наступні засоби кібербезпеки:

- обов’язкова авторизація для доступу до можливостей ПЗ, що мають вплив на виконання КСУ керуючих функцій. Парольний захист має передбачати заборону на використання порожніх паролів, надійне зберігання даних автентифікації;

– ведення архіву дій користувача, з зазначенням часу, логіну та виконаних операцій.

З точки зору доступу до складових частин ПЗ повинна унеможливлюватися несанкціонована зміна файлів програм, баз даних, конфігурації, налаштувань. Для цього можуть використовуватися засоби обмеження доступу, що входять до складу ОС, на якій виконується ПЗ — облікові записи користувачів з обмеженими правами, вірне встановлення прав доступу до файлів, налаштувань, використання блокування робочого столу тощо.

Обмін інформацією як фактор, що впливає на кібербезпеку. Більшість компонентів ПЗ КСУ виконує функції обміну інформацією з іншими компонентами КСУ або зовнішніми системами. Відповідно до цього, інформація, яка приймається компонентами ПЗ, потенційно може бути спотвореною, некоректною або підробленою, що створить загрозу для виконання ПЗ своїх функцій. Під час розробки нового або дослідженні існуючого ПЗ необхідно вжити заходи щодо мінімізації даної вразливості.

Для аналізу факторів передачі даних може бути складена схема напрямків передачі даних між ПЗ:

– напрямок прийому та/або передачі даних;
– залежність ПЗ від зовнішніх даних (наявність прийому).

Схема являє собою орієнтований граф, вузли котрого є функціональними модулями або окремими програмами, а ребра — каналами передачі даних. Вершини даного графа мають бути згруповані за зонами, що мають однаковий рівень кібербезпеки. Ця схема може бути використана для визначення того програмного забезпечення, в якому необхідна реалізація вимог різного рівня кібербезпеки при прийомі інформації та віддалених підключеннях.

Перед визначенням заходів захисту ПЗ під час обміну інформацією необхідно виконати аналіз створеної схеми передачі даних та визначити необхідні напрямки потоків даних. Згідно з ними необхідно виділити компоненти ПЗ, які мають тільки передавати дані та компоненти, які мають також приймати дані. Крім того, необхідно визначити компоненти ПЗ, які приймають інформацію від інших зон безпеки (нижчих, вищих або однорангових).

Якщо ПЗ тільки передає інформацію, для реалізації вимог кібербезпеки мають використовуватися наступні основні підходи у проектуванні обміну:

– при передачі інформації в пакеті даних має міститися інформація для перевірки його достовірності з боку приймача: версія, розмір, контрольна сума тощо;
– при передачі за межі довірених зон, інформація, що передається, при необхідності може бути зашифрована;
– при передачі інформації від вищої в нижчу зону безпеки мають використовуватися протоколи даних, що можуть працювати лише в односторонньому порядку, без відповідей з боку приймача. Прикладами таких протоколів є UDP (надсилання пакетів без зворотного прийому) або передача даних послідовним інтерфейсом з використанням однієї лінії Tx.

Якщо ПЗ також (або тільки) приймає інформацію, для нього мають використовуватися наступні підходи у проектуванні обміну:

– контроль цілісності прийнятих пакетів за форматом, контрольною сумою тощо;

- ігнорування пакетів даних, що прийняті від невідомих джерел (наприклад, непередбачених IP-адрес) при прийомі від ПЗ зони нижчого рівня кіберзахисту;
- ігнорування пакетів даних, що мають невірний формат;
- перевірка коректності параметрів, що прийняті, з технологічної точки зору (наприклад, перевірка входження введеного керуючого параметра до допустимого діапазону).

У випадку, якщо ПЗ, що приймає дані та ПЗ, що передає дані, знаходяться в одній зоні безпеки, до якої немає зовнішнього доступу (локального або віддаленого) та використовує виділену відокремлену лінію зв'язку, можлива відсутність додаткових перевірок, наприклад на прийом даних від невідомих джерел. Проте контроль цілісності пакетів та коректності параметрів є обов'язковим.

Висновок: проведені основні рекомендації з реалізації вимог кібербезпеки в ПЗ. Необхідно зазначити, що для контролю виконання даних вимог зручно створити кількісний показник. Для розв'язання даної задачі може бути складений звіт, в якому для кожного компонента ПЗ КСУ зазначається застосовність певних вимог кібербезпеки та відповідність даним вимогам. Інформація з даного звіту може бути використана для розрахунку числового показника кібербезпеки ПЗ.

Проведення розрахунку ступеню кібербезпеки ПЗ

Для проведення розрахунку числового показника кібербезпеки ПЗ КСУ АЕС проводяться наступні дії.

Кожний вид ПЗ позначається змінною S0..Si

Кожний фактор кібербезпеки позначається змінною Rq0..Rqi

На основі аналізу властивостей ПЗ складається матриця застосовності вимог (Matrix of Requirements Acceptance), рядками якої є ПЗ (змінні S), а стовпцями — фактори кібербезпеки (змінні R).

Елементи матриці являють собою числа 0 та 1, де 1 означає, що певний фактор кібербезпеки може бути застосований до певного виду ПЗ, а 0 у протилежному випадку.

$$Mra = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \quad (1)$$

Після цього складається матриця виконання вимог (Matrix of Requirements Implementation), рядками якої є ПЗ (змінні S), а стовпцями — фактори кібербезпеки (змінні R).

Елементи матриці являють собою числа в діапазоні від 0 в 1, які вказують на повноту виконання певної вимоги певним ПЗ.

$$Mri = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0.4 & 1 & 1 & 0 \\ 1 & 1 & 0.8 & 0.8 & 0 & 0.8 \\ 1 & 1 & 1 & 0 & 1 & 0 \end{bmatrix} \quad (2)$$

Після складання матриці проводиться розрахунок за наступною формулою:

$$\mathrm{k} = \frac{\sum_{i=1\ j=1}^{iMax,jMax}(Mri[i,j])}{\sum_{i=1\ j=1}^{iMax,jMax}(Mra[i,j])} \quad (3)$$

Показник k являє собою число від 0 до 1, де 0 — мінімум, 1 — максимум виконання вимог.

Висновок. Запропонований підхід дозволяє обчислити числовий показник виконання вимог кібербезпеки до ПЗ КСУ АЕС. В наступному розділі буде наведено приклад використання даного підходу для існуючої КСУ.

Приклад проведення аналізу вимог до кібербезпеки КСУ АЕС

Метою даного розділу статті є дослідження складу та структури програмного забезпечення КСУ АЕС, що використовується для виконання функцій Аварійного та Попереджувального Захисту (АЗ-ПЗ) виробництва ПАТ НВП «Радій».

Структура, особливості та типовий перелік обладнання, модулів та функцій програмного забезпечення КСУ наведений у монографії [20].

Згідно з приведеними особливостями, в модулях КСУ використовуються Програмовані Логічні Інтегральні Схеми (ПЛІС) високого ступеню інтеграції. При створенні проектів ПЛІС використовуються три основні технології: розробка графічних схем технологічних алгоритмів, написання коду мовою опису цифрових схем (наприклад, VHDL), а також написання програмного коду мовами високого рівня (С та С++), що виконується емулятором мікропроцесора, для виконання функцій обробки сигналів, діагностування, обміну інформацією тощо. У верхньому рівні КСУ використовується ПЗ, написане мовою програмування С++, що виконується під керуванням ОС Windows.

Відповідно до даних особливостей є очевидним, що кожний компонент, який містить ПЗ, може містити потенційні вразливості, і через те потребує дотримання вимог під час розробки ПЗ та експлуатації КСУ.

Типова структура КСУ АЗ-ПЗ. Як зазначається в роботі, програмно-апаратна платформа для побудови КСУ поділяється на верхній та нижній рівень.

До складу верхнього рівня входять робочі станції, що виконують наступні функції:

- прийом технологічної та діагностичної інформації від верхнього рівня;
- відображення технологічної інформації про виконання функцій безпеки, стан вхідних та вихідних параметрів, роботу алгоритмів;
- відображення діагностичної інформації про стан технічних засобів;
- архівування прийнятої інформації;
- передача реєстраційної інформації до Інформаційно-Обчислювальної Системи енергоблоку (ІОС).

До складу нижнього рівня входять шафи з типовими функціональними модулями. Найважливіші функції, які виконують дані модулі, наступні:

- прийом значень аналогових або дискретних сигналів (модулі БВА, БВД);
- виконання логіки технологічних алгоритмів формування захисту (модулі БФЗ);
- видача керуючих аналогових та дискретних сигналів (модулі БОС, БДС);
- діагностування апаратних засобів (модулі БДН);
- корекція параметрів роботи алгоритмів, що можуть змінюватися оператором (модуль МКУ).

КСУ КЗ-ПЗ складається з двох комплектів, кожен з яких складається з трьох незалежних каналів захисту (шафи ШФС), що взаємно резервують один одного. До складу кожного каналу входить кросова вихідна шафа (КШВ), що об’єднує вихідні сигнали каналів за мажоритарною схемою «2 з 3». Також до складу КСУ входять комп’ютерні шафи (основна та резервна) та інженерні робочі станції. Обмін інформацією між ПЗ КСУ відбувається за допомогою оптичних ліній зв’язку.

Загальна структурна схема КСУ АЗ-ПЗ наведена на рис. 2.

ISSN 2663 - 4023

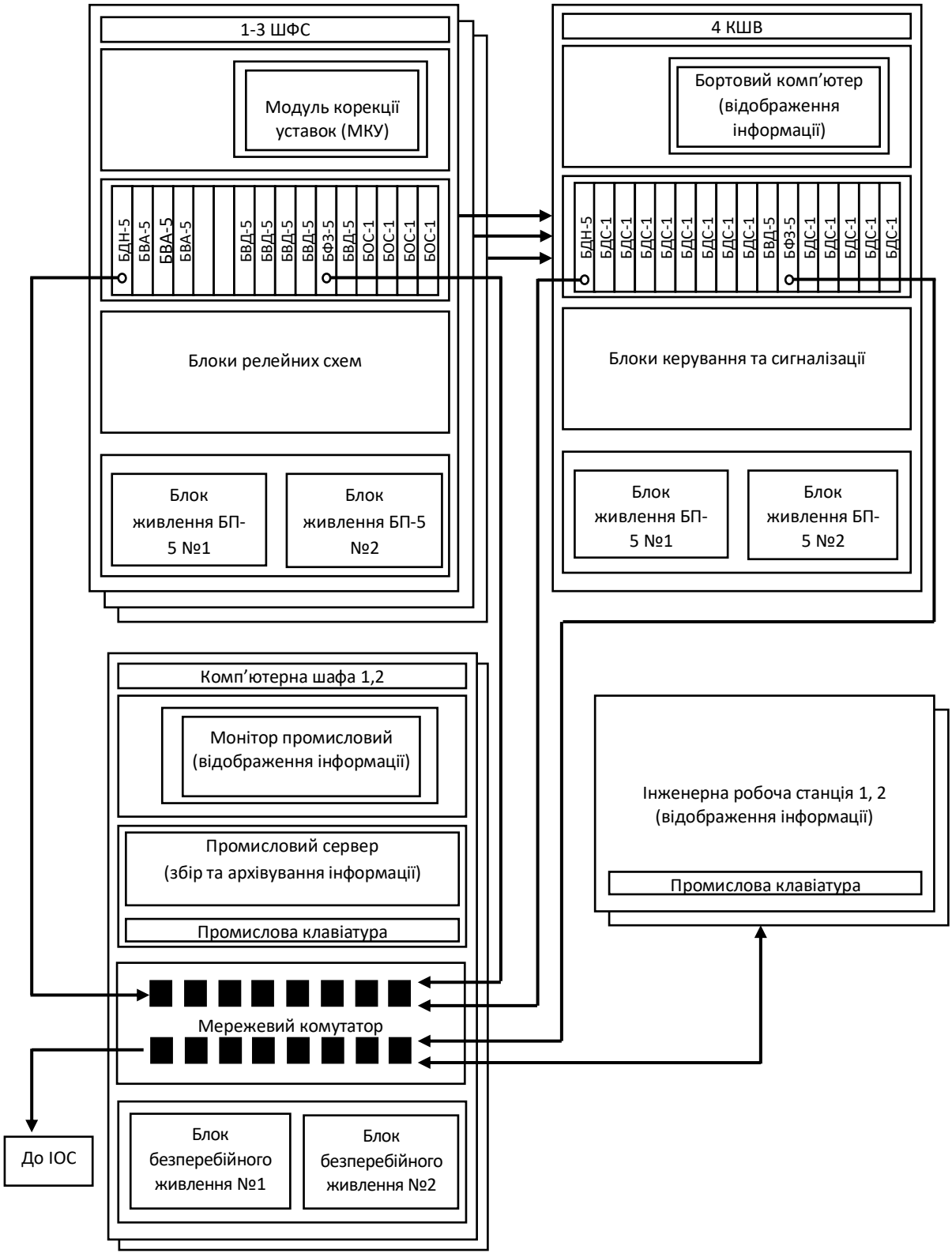

Рис. 2. Структурна схема КСУ АЗ-ПЗ

Перелік компонентів ПЗ. Згідно з описаним підходом до дотримання вимог кібербезпеки, спираючись на наведену інформацію про структуру КСУ, складені таблиці з переліком компонентами КСУ, його програмним забезпеченням, а також властивостями, що впливають на вразливості.

Перелік назв модулів нижнього рівня КСУ та застосовність вимог до основних властивостей його ПЗ приведений в табл. **Error! Reference source not found.**.

Таблиця 1

Застосовність вимог до ПЗ нижнього рівня

Назва модуля	Фізичний захист	Управління конфігурацією	Приховані функції	Доступ до ПЗ	Автентифікація
БДН	1	1	1	0	0
БВА	1	1	1	0	0
БВД	1	1	1	0	0
БФЗ	1	1	1	0	0
БОС	1	1	1	0	0
БДС	1	1	1	0	0
Модуль корекції уставок (МКУ)	1	1	1	1	1

Перелік ПЗ верхнього рівня КСУ та застосовність вимог до його основних властивостей приведений в табл. 1.

Таблиця 1

Застосовність вимог до ПЗ верхнього рівня

Назва модуля	Фізичний захист	Управління конфігурацією	Приховані функції	Доступ до ПЗ	Автентифікація
Сервер реєстрації (InfoServer)	1	1	1	1	1
Сервер діагностики (DiagInfoServer)	1	1	1	1	1
Monitor	1	1	1	1	1
Diagnostics	1	1	1	1	1

Після визначення застосовності вимог до ПЗ проведено аналіз їх реалізації в КСУ на основі ([20], ст. 311, 317–318).

Фізичний захист. Згідно опису захисту системи від несанкціонованого доступу, всі компоненти нижнього рівня знаходяться під фізичним захистом в шафах, що обладнані сигналізацією. Зміна конфігурації ПЗ та в ПЛІС неможлива іншими способами, крім через переносні інструментальні ЕОМ, що підключаються для кожного модулю окремо при фізичному доступі до КСУ. Компоненти верхнього рівня знаходяться на серверах, що також знаходяться під фізичним захистом у шафах, що унеможливлює підключення непередбачених комунікацій, зовнішніх носіїв тощо. *Таким чином, вимоги фізичного захисту виконуються.*

Управління конфігурацією. Під час всього процесу роботи проводиться технічне діагностування стану КСУ, що включає в себе перевірку працездатності всіх частин, наявності живлення, температури, достовірності параметрів тощо. Зокрема, також в системі діагностики передбачені технічні та програмні засоби перевірки адекватності

експлуатованого ПЗ поставленому (версії, контрольні суми виконуваних файлів та файлів конфігурації, а також відображення та перевірка цих даних на відповідність еталонам). Відповідно, може бути проконтрольована версія всього експлуатованого ПЗ та зроблений висновок щодо вірності його конфігурації. ПЗ КСУ поставляється на АЕС на компакт-диску виробником, на якому записані потрібні файли та вказані їх конфігураційні дані. При модифікаціях дана інформація оновлюється виробником. *Таким чином, вимоги управління конфігурацією виконуються.*

Приховані функції. ПЗ КСУ поставляється виробником у вигляді виконуваних модулів, що не можуть бути перетворені у вихідний код з подальшим внесенням непередбачуваних змін. Згідно стандартів забезпечення якості підприємства-виробника ([20], ст. 311, 317–318), розробник гарантує високий рівень якості та надійності ПЗ, його верифікацію, відсутність непередбачуваних функцій. Контроль якості ПЗ за допомогою методів Code review (перегляд коду), парне програмування, верифікація коду. Як зазначалося вище, наявність управління конфігурацією дозволяє пересвідчитись в адекватності експлуатованого ПЗ поставленому. *Таким чином, вимоги щодо відсутності та неможливості внесення непередбачуваних функцій до ПЗ виконуються.*

Доступ до ПЗ та автентифікація. ПЗ нижнього рівня входить до складу модулів (плат) БВА, БВД, БФЗ, БОС, БДС, БДН. По-перше, як зазначалося при аналізі аспектів фізичного захисту ПЗ, користувач системи ні віддалено, ні локально не може мати доступ до нього без фізичного доступу до модуля та засобів перепрограмування. По-друге, користувач системи напряму не працює з даним ПЗ, оскільки воно не має інтерфейсу. Отже, вимоги контролю доступу та автентифікації доступу не можуть бути застосовані до даного виду ПЗ.

ПЗ верхнього рівня, виконується на промислових комп’ютерах, виконує інформаційно-діагностувальні функції, що не впливають на виконання функцій безпеки. Через це оперативний персонал має мати доступ до його інтерфейсів користувача. Згідно вимог стандартів кібербезпеки, по-перше, має бути виключена можливість несанкціонованої зміни ПЗ, що знаходиться на носіях інформації, що забезпечується засобами ОС шляхом встановлення прав доступу до файлів ПЗ та даних різними обліковими записами користувачів (адміністратори, оперативний, ремонтний персонал). По-друге, засоби кібербезпеки мають передбачати автентифікацію для доступу до функцій ПЗ, що також забезпечується засобами ОС шляхом блокування робочого столу інтерфейсу ОС, виходу з облікового запису ОС тощо. Реалізація даної вимоги залежить переважно від адміністративних заходів та культури безпеки на АЕС, що має виконуватися. Для прикладу, під час ПЗ КСУ АЕС змодельована ситуація, що на деякій робочій станції, де виконується ПЗ «Монітор», може бути виявлений порожній пароль для розблокування робочого столу, тому виконання вимог даного пункту може бути оцінене на 50% за наявності двох інженерних робочих станцій (конкретне значення може встановлюватися в залежності від кількості екземплярів ПЗ, серверів тощо).

До складу ПЗ верхнього рівня може входити панельний комп’ютер, що містить особливе ПЗ, яке вносить корективи до виконання технологічних алгоритмів, наприклад Модуль Корекції Уставок (МКУ). Оскільки дана функція впливає на виконання КСУ функцій захисту, для даного ПЗ застосовуються всі наявні критерії кіберзахисту: фізичне розташування в шафі з замком доступу, захист ПЗ при доступі персоналу від несанкціонованих змін засобами ПЗ та ОС, обов’язкова автентифікація. Цим забезпечується вимога стандарту з кібербезпеки щодо двофакторної авторизації. *Таким чином, вимоги щодо контролю доступу до ПЗ та авторизації ПЗ виконуються, (для прикладу, для ПЗ «Монітор» — на 50%).*

Аналіз ПЗ з точки зору обміну даними. Схема обміну даними КСУ АЗ-ПЗ буде приведена на рис. 3.

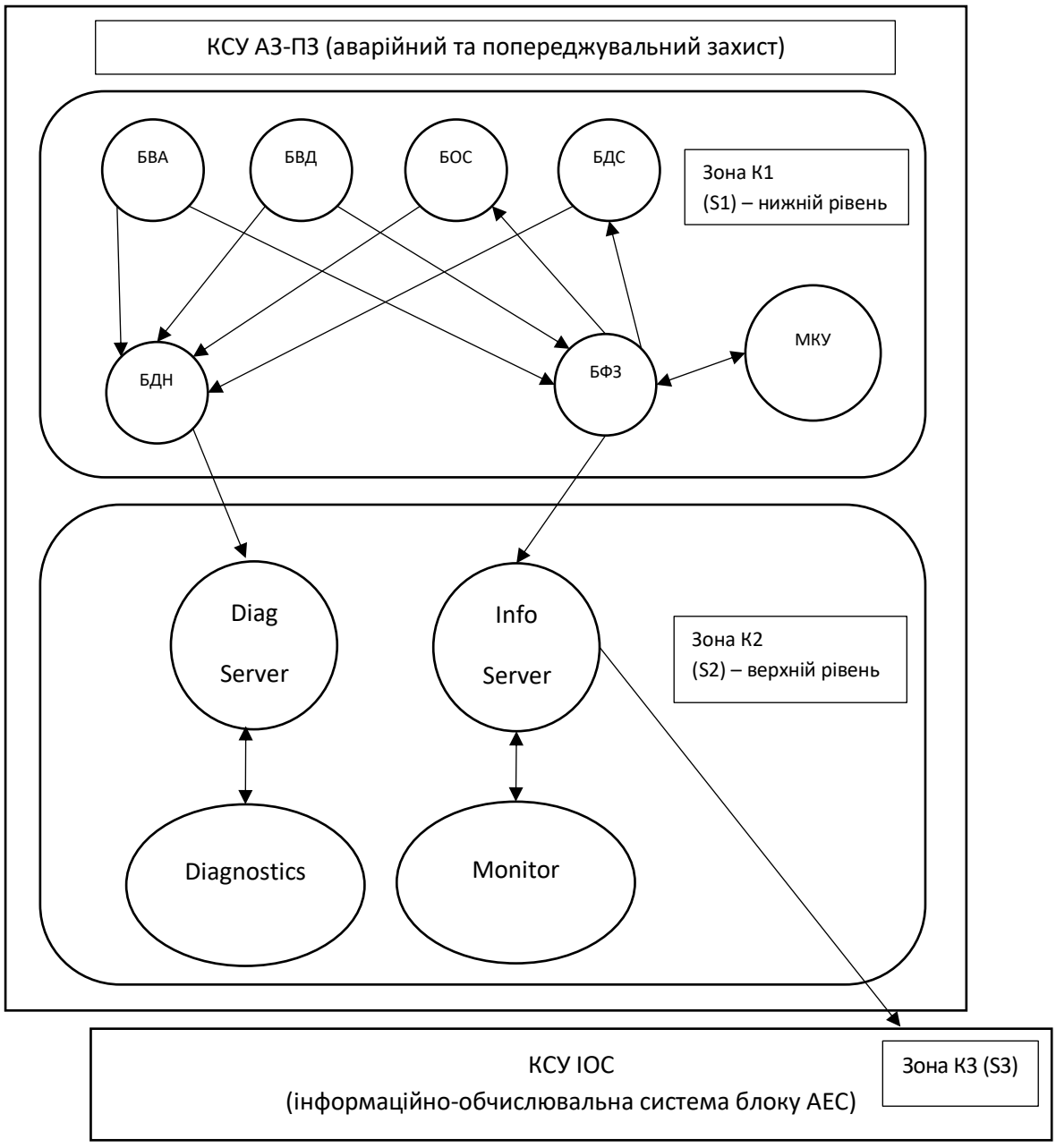

Рис. 3. Схема обміну даними ПЗ КСУ АЗ-ПЗ

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Аналіз створеного графу обміну інформації дозволяє зробити наступні висновки:

- до складу ПЗ, що передає передає інформацію, входять всі компоненти;
- до складу ПЗ, що передає передає інформацію в односторонньому напрямку хоча б одним каналом, входять компоненти БВА, БВД, БОС, БДС, БФЗ, БДН, InfoServer;

ISSN 2663 - 4023

– до складу ПЗ, що приймає інформацію, входять компоненти БДН, БФЗ, БОС, БДС, МКУ, DiagServer, InfoServer, Monitor, Diagnostics;
– ПЗ, що приймає інформацію від ПЗ зони нижчого рівня: відсутнє, тому немає необхідності в додаткових перевірках.

Таким чином, з точки зору напрямків передачі інформації та її контролю ПЗ має оцінюватися наступним чином:

– для всіх компонентів ПЗ — передача з додаванням інформації для перевірки її достовірності з боку приймача: версія, розмір, контрольна сума тощо;
– для компонентів ПЗ БВА, БВД, БОС, БДС, БДН, БФЗ, InfoServer — використання для окремих каналів протоколів даних, що можуть працювати лише в односторонньому порядку, без відповідей з боку приймача;
– для компонентів ПЗ БФЗ, БОС, БДС, МКУ, DiagServer, InfoServer, Monitor, Diagnostics — контроль цілісності прийнятих пакетів, ігнорування пакетів невірного формату;
– для компонентів ПЗ БФЗ, МКУ — перевірка коректності параметрів, що прийняті, з технологічної точки зору (перевірка входження значення уставки до допустимого діапазону).

В прикладі, що наводиться, передбачається повне виконання всіх необхідних вимог щодо обміну інформацією.

Застосовність вимог щодо обміну інформацією ПЗ приведена в табл. 2.

Таблиця 2

Застосовність вимог до ПЗ нижнього рівня

Назва модуля	Передача інформації для перевірки даних	Використання одно-направлених протоколів	Контроль цілісності прийнятих даних	Прийом від нижчої зони безпеки	Перевірка коректності введених параметрів
БДН	1	1	1	0	0
БВА	1	1	0	0	0
БВД	1	1	0	0	0
БФЗ	1	1	1	0	1
БОС	1	1	1	0	0
БДС	1	1	1	0	0
Модуль корекції уставок (МКУ)	1	0	1	0	1
Сервер реєстрації (InfoServer)	1	1	1	0	0
Сервер діагностики (DiagServer)	1	0	1	0	0
Monitor	1	0	1	0	0
Diagnostics	1	0	1	0	0

ISSN 2663 - 4023

Для розрахунку показника виконання вимог кібербезпеки складемо табл. 3 змінних ПЗ S.

Таблиця 3

Змінні ПЗ

Змінна	ПЗ
S0	БДН
S1	БВА
S2	БВД
S3	БФЗ
S4	БОС
S5	БДС
S6	МКУ
S7	DiagServer
S8	InfoServer
S9	Monitor
S10	Diagnostics

Також складемо табл. 4 змінних вимог Rq.

Таблиця 4

Змінні вимог

Змінна	ПЗ
Rq0	Фізичний захист
Rq1	Управління конфігурацією
Rq2	Захист від прихованих функцій
Rq3	Захищеність доступу до ПЗ
Rq4	Реалізація автентифікації
Rq5	Передача інформації для перевірки достовірності пакету
Rq6	Однонаправлена передача даних
Rq7	Контроль достовірності прийнятих пакетів Ігнорування пакетів даних невірного формату
Rq8	Ігнорування пакетів даних з невідомих джерел від нижчого рівня
Rq9	Перевірка коректності параметрів, що прийняті

Матриця застосовності вимог виглядатиме наступним чином:

$$Mra(azpz) = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \end{bmatrix} \quad (4)$$

Матриця виконання вимог виглядатиме наступним чином:

$$Mri(azpz) = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0.5 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \end{bmatrix} \quad (5)$$

Виконавши розрахунок показників виконання вимог кібербезпеки за формулою (3), отримаємо:

$$k = \frac{71.5}{72} = 0.993 \quad (6)$$

Наведений результат інтерпретується як виконання 99.3% вимог до кібербезпеки КСУ АЗ-ПЗ.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У даній роботі було розглянуто вимоги міжнародного стандарту IEC62645 та галузевого стандарту України «НП 306.2.237-2022», що мають відношення до розробки ПЗ КСУ АЕС. Забезпечення кіберзахисту ПЗ КСУ АЕС є комплексною задачею, що містить адміністративно-правові, технічні, культурні, організаційні складові.

З точки зору розробки та експлуатації ПЗ основні заходи щодо кіберзахисту включають в себе заходи з верифікації коду ПЗ, забезпечення відсутності прихованих функцій, реалізацію фізичного захисту обладнання, захищеність складових частин ПЗ, автентифікацію, безпеку під час обміну даними.

Для визначення відповідності ПЗ вимогам кіберзахисту необхідно визначити вимоги, що є застосовними до кожного компоненту ПЗ, та провести аналіз їх виконання. Дана дія має відбуватися постійно під час розробки нового ПЗ та оцінюванні ПЗ існуючих КСУ. Після проведення аналізу застосовності та виконання вимог може бути проведений розрахунок коефіцієнту виконання вимог.

Необхідно відмітити, що кіберзахист є лише складовою частиною якості ПЗ КСУ АЕС, що є важливим для виконання функцій безпеки. Аналіз вимог та розрахунок коефіцієнту їх виконання може бути складовою частиною комплексної моделі процесу розробки ПЗ КСУ АЕС.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Атомна електростанція.* (2019). ВУЕ. https://vue.gov.ua/Атомна_електростанція
2. *Діючі АЕС України.* (б.д.). Uatom.org. https://www.uatom.org/zagalni-vidomosti
3. *Війна та атомна енергія: як працює Запорізька АЕС під окупацією.* (б. д.). Суспільне|Новини. https://suspilne.media/254222-vijna-ta-atomna-energia-ak-pracue-zaporizka-aes-pid-okupacieu/
4. *These countries have the most nuclear reactors.* (2019). Weforum. https://www.weforum.org/agenda/2019/11/countries-that-have-the-most-nuclear-power-alternative-energy-electricity-climate-change/?DAG=3&gad_source=1&gclid=CjwKCAiAyp-

sBhBSEiwAWWzTnlkktfFh8DZ27khXqhSO76F18heFwSfVPxqo1oN07YwKaMUU_SjOMBoCpe0QAvD_BwE

5. *Кібератаки російської федерації. Хронологія*. (2018). Міністерство оборони України. https://www.mil.gov.ua/ukbs/kiberataki-rosijskoi-federaczii-hronologiya.html
6. *Найбільші кібератаки проти України з 2014 року. Інфографіка.* (б.д.). Новини України та Світу. Головні і останні новини - NV. https://nv.ua/ukr/ukraine/events/najbilshi-kiberataki-proti-ukrajini-z-2014-roku-infografika-1438924.html
7. Українська правда. (2023). *Кібератака на «Київстар»: як хакерам вдалося «покласти» зв'язок і чи можливі такі атаки у майбутньому?* https://www.pravda.com.ua/podcasts/63bff58767d28/2023/12/21/7434067/
8. *СБУ допомагає «Київстару» відновити роботу мережі.* (б.д.). https://ssu.gov.ua/novyny/sbu-dopomahaie-kyivstaru-vidnovyty-robotu-merezhi
9. *The state of cybersecurity in 2023 - Just Food | Issue 52 | June 2023.* (б. д.). Home | Slimmer pickings? - Just Food | Issue 55 | March 2024. https://just-food.nridigital.com/just_food_jun23/cybersecurity-trends-market-forecast-2023
10. *Ворожі хакери атакують критичну інфраструктуру України: працювати над посиленням захисту треба постійно.* (2023). Державна служба спеціального зв'язку та захисту інформації України. https://cip.gov.ua/ua/news/vorozhi-khakeri-atakuyut-kritichnu-infrastrukturu-ukrayini-pracyuvati-nad-posilennyam-zakhistu-treba-postiino
11. Вінтенко, Б., Смірнов, О., Коваленко, О., Смірнов, С., & Коваленко, А. (2023). Дослідження нормативних документів та галузевих стандартів розробки програмного забезпечення комп'ютерних систем управління АЕС, важливих для безпеки. *Системи управління, навігації та зв'язку, 2(72)*, 170–178. https://doi.org/10.26906/SUNZ.2023.2.170
12. Вінтенко, Б., Смірнов, О., Коваленко, О., Смірнов, С., & Буравченко, К. (2023). Дослідження вимог міжнародних стандартів IEC60880 та IEC62138 з розробки програмного забезпечення інформаційно-керуючих систем АЕС, важливих для безпеки. *Системи управління, навігації та зв'язку, 3(73)*, 155–166. https://doi.org/10.26906/SUNZ.2023.3.155
13. *Nuclear power plants - Instrumentation and control systems important to safety - Software aspects for computer-based systems performing category A functions* (IEC 60880:2006). (2006). International Electrotechnical Committee.
14. *Nuclear power plants - Instrumentation and control systems important for safety – Software aspects for computer-based systems performing category B or C functions.* (IEC62138-2004). (2004). International Electrotechnical Commission.
15. Сімонов, А., Клевцов, О., Трубчанінов, С., & Лазуренко, О. (2019). Комп'ютерна безпека інформаційних та керуючих систем АЕС: документи, що обґрунтовують комп'ютерну безпеку. *Ядерна та радіаційна безпека, 4(84),* 73–81. https://doi.org/10.32918/nrs.2019.4(84).09
16. Limba, T., Plėta, T., Agafonov, K., & Damkus, M. (2017). Cyber security management model for critical infrastructure. *Entrepreneurship and Sustainability Issues, 4(4)*, 559–573. https://doi.org/10.9770/jesi.2017.4.4(12)
17. *Nuclear power plants - Instrumentation and control systems – Requirements for security programmes for computer-based systems.* (IEC62645-2014). (2014). International Electrotechnical Commission.
18. *Вимоги до кіберзахисту інформаційних та керуючих систем атомних станцій для забезпечення ядерної та радіаційної безпеки.* (НП 306.2.237-2022). (2022). Держатомрегулювання України.
19. *Nuclear power plants - Instrumentation and control important to safety – Classification of instrumentation and control functions.* (IEC61226-2009). (2009). International Electrotechnical Commission.
20. Бахмач, Є., Герасименко, О., Головір, В., Сіора, О., Скляр, В., Токарєв, В., & Харченко, В. (2008). Стійкі до відмов інформаційно-керуючі системи на програмованій логіці. *НАУ «ХАІ», НВП «Радій».*

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (23), 2024
ISSN 2663 - 4023

Borys Vintenko
PhD graduate student of the department of information security and computer engineering
Cherkasy State Technological University, Cherkasy, Ukraine
ORCID 0009-0008-3748-0374
boris.vintenko@gmail.com

Iryna Myronets
candidate of technical sciences, associate professor, associate professor of the department of information security and computer engineering
Cherkasy State Technological University, Cherkasy, Ukraine
ORCID 0000-0003-2007-9943
i.myronets@chdtu.edu.ua

Oleksii Smirnov
Doctor of technical sciences, professor, head of Cybersecurity & Software Academic Department
Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine
ORCID 0000-0001-9543-874X
dr.smirnovoa@gmail.com

Oksana Kravchuk
HR department inspector,
Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine
ORCID 0009-0008-8453-0557
vov-14@i.ua

Nataliia Kozirova
assistant of Cybersecurity & Software Academic Department
Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine
ORCID 0009-0005-8753-5132
natalidonchenko23@gmail.com

Hryhorii Savelenko
candidate of technical sciences, associate professor of the department of economics, entrepreneurship and hotel and restaurant business
Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine
ORCID 0000-0001-9310-6223
grigoriy.savelenko@gmail.com

Anna Kovalenko
candidate of technical sciences, associate professor, associate professor of Cybersecurity & Software Academic Department
Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine
ORCID 0000-0003-3610-9465
annasun911@gmail.com

STUDY OF REQUIREMENTS AND CYBER SECURITY ANALYSIS OF THE SOFTWARE OF INFORMATION AND CONTROL SYSTEMS OF NPP, IMPORTANT FOR SECURITY

Abstract. In order to counter cryptoattacks on elements of critical infrastructure, in particular on computer control systems of nuclear power plants, the goal achieved in this work is to analyze the requirements for computer security (cyber security) of the software of this system, which are relevant to the stage of its design, development and operation, as well as proposed criteria and methodology for calculating the quality of compliance with these requirements. To achieve the goal, the first section of the article provides information on standards and identified requirements for software cyber security. In the second section, an analysis of the requirements is carried out and an approach to software development is described, taking into account these requirements and analyzing their consideration. In the third section, an approach to calculating the performance

indicator of software cyber security requirements is proposed. The fourth chapter provides an example of the application of this approach to the existing computerized NPP management system to assess compliance with cyber security requirements. The article discusses the requirements of the international standard IEC62645 and the industry standard of Ukraine "NP 306.2.237-2022", which are related to the development of software for the computer control system of nuclear power plants. Ensuring cyber protection of the software of the NPP computer management system is a complex task that includes administrative, legal, technical, cultural, and organizational components. From the point of view of software development and operation, the main cyber security measures include software code verification, ensuring the absence of hidden functions, implementing physical equipment protection, security of software components, authentication, security during data exchange. To determine the compliance of the software with the requirements of cyber protection, it is necessary to determine the requirements applicable to each component of the software and conduct an analysis of their implementation. This action should occur continuously during the development of new software and software evaluation of existing computer control systems. After the analysis of the applicability and fulfillment of the requirements, the calculation of the coefficient of the fulfillment of the requirements can be carried out. It was noted that cyber protection is only a component of the quality of the software of the NPP computer control system, which is important for the performance of security functions. The analysis of requirements and the calculation of the coefficient of their fulfillment can be an integral part of the complex model of the software development process of the computer system of NPP management.

Keywords: cyber security; software; information and control systems; nuclear power plants; energy.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. *Nuclear power plant.* (2019). VUE. https://vue.gov.ua/Атомна_електростанція
2. *Operating NPPs of Ukraine.* (n.d.). Uatom.org. https://www.uatom.org/zagalni-vidomosti
3. *War and atomic energy: how Zaporizhia NPP works under occupation.* (n.d.). Suspilne|News. https://suspilne.media/254222-vijna-ta-atomna-energia-ak-pracue-zaporizka-aes-pid-okupacieu/
4. *These countries have the most nuclear reactors.* (2019). Weforum. https://www.weforum.org/agenda/2019/11/countries-that-have-the-most-nuclear-power-alternative-energy-electricity-climate-change/?DAG=3&gad_source=1&gclid=CjwKCAiAyp-sBhBSEiwAWWzTnlkktfFh8DZ27khXqhSO76F18heFwSfVPxqo1oN07YwKaMUU_SjOMBoCpe0QAvD_BwE
5. *Cyber attacks of the Russian Federation. Chronology.* (2018). Ministry of Defence Ukraine. https://www.mil.gov.ua/ukbs/kiberataki-rosijskoi-federaczii-hronologiya.html.
6. *The biggest cyber attacks against Ukraine since 2014. Infographics.* (n.d.). news of Ukraine and the world. main and latest news – NV. https://nv.ua/ukr/ukraine/events/najbilshi-kiberataki-proti-ukrajini-z-2014-roku-infografika-1438924.html
7. Ukrainian Pravda. (2023). *Cyber attack on "Kyivstar": how hackers managed to "make" a connection and whether such attacks are possible in the future?* https://www.pravda.com.ua/podcasts/63bff58767d28/2023/12/21/7434067/
8. *The SSU is helping Kyivstar restore the network.* (n.d.). https://ssu.gov.ua/novyny/sbu-dopomahaie-kyivstaru-vidnovyty-robotu-merezhi
9. *The state of cybersecurity in 2023 - Just Food | Issue 52 | June 2023.* (б. д.). Home | Slimmer pickings? - Just Food | Issue 55 | March 2024. https://just-food.nridigital.com/just_food_jun23/cybersecurity-trends-market-forecast-2023
10. *Enemy hackers are attacking the critical infrastructure of Ukraine: it is necessary to constantly work on strengthening protection.* (2023). State Service of Special Communications and Information Protection of Ukraine. https://cip.gov.ua/ua/news/vorozhi-khakeri-atakuyut-kritichnu-infrastrukturu-ukrayini-pracyuvati-nad-posilennyam-zakhistu-treba-postiino
11. Vintenko, B., et al. (2023). Study of regulatory documents and industry standards for the development of software for NPP computer control systems important for safety. *Control, navigation and communication systems, 2(72),* 170–178. https://doi.org/10.26906/SUNZ.2023.2.170
12. Vintenko, B., et al. (2023). Study of the requirements of international standards IEC60880 and IEC62138 for the development of software for information and control systems of nuclear power plants important for

safety. *Control, navigation and communication systems, 3(73),* 155–166. https://doi.org/10.26906/SUNZ.2023.3.155

13. *Nuclear power plants - Instrumentation and control systems important to safety - Software aspects for computer-based systems performing category A functions* (IEC 60880:2006). (2006). International Electrotechnical Committee.
14. *Nuclear power plants - Instrumentation and control systems important for safety – Software aspects for computer-based systems performing category B or C functions.* (IEC62138-2004). (2004). International Electrotechnical Commission.
15. Simonov, A., et al. (2019). Computer security of NPP information and control systems: documents justifying computer security. *Nuclear and radiation safety, 4(84),* 73–81. https://doi.org/10.32918/nrs.2019.4(84).09
16. Limba, T., et al. (2017). Cyber security management model for critical infrastructure. *Entrepreneurship and Sustainability Issues, 4(4),* 559–573. https://doi.org/10.9770/jesi.2017.4.4(12)
17. *Nuclear power plants - Instrumentation and control systems – Requirements for security programmes for computer-based systems.* (IEC62645-2014). (2014). International Electrotechnical Commission.
18. *Requirements for cyber protection of information and control systems of nuclear plants to ensure nuclear and radiation safety.* (NP 306.2.237-2022). (2022). State Nuclear Regulatory Commission of Ukraine.
19. *Nuclear power plants - Instrumentation and control important to safety – Classification of instrumentation and control functions.* (IEC61226-2009). (2009). International Electrotechnical Commission.
20. Bakhmach, Y., et al. (2008).Failure-resistant information and control systems on programmable logic. “KHAI” NAU, “Radio” R&PE.