УДК 621.039:004.9 Doi: https://doi.org/10.32918/nrs.2020.4(88).09

Комп'ютерна безпека інформаційних та керуючих систем АЕС: оцінювання комп'ютерної безпеки

■ **Клевцов Олександр Леонідович**
Державне підприємство «Державний науково-технічний центр з ядерної та радіаційної безпеки», м. Харків, Україна
ORCID: https://orcid.org/0000-0001-5665-5039

■ **Симонов Артем Андрійович**
Державне підприємство «Державний науково-технічний центр з ядерної та радіаційної безпеки», м. Харків, Україна
ORCID: https://orcid.org/0000-0001-6971-523X

■ **Трубчанінов Сергій Олександрович**
Державне підприємство «Державний науково-технічний центр з ядерної та радіаційної безпеки», м. Харків, Україна
ORCID: https://orcid.org/0000-0003-4256-5192

Стаття присвячена питанням оцінювання комп'ютерної безпеки інформаційних та керуючих систем (ІКС) АЕС. Визначено основні напрями оцінювання комп'ютерної безпеки ІКС АЕС, зокрема: оцінювання кібернетичних загроз, оцінювання вразливостей комп'ютерної безпеки ІКС, оцінювання достатності застосованих заходів забезпечення комп'ютерної безпеки ІКС, оцінювання ризиків комп'ютерної безпеки ІКС, а також періодичне переоцінювання комп'ютерної безпеки ІКС. У статті детально розглядаються оцінювання вразливостей комп'ютерної безпеки ІКС та достатності застосованих заходів забезпечення комп'ютерної безпеки ІКС (оцінювання кібернетичних загроз та ризиків комп'ютерної безпеки ІКС докладно розглядаються в інших публікаціях із циклу статей «Комп'ютерна безпека інформаційних та керуючих систем АЕС»).

Розглянуті підходи до оцінювання вразливостей комп'ютерної безпеки ІКС та програмного забезпечення (ПЗ) на кожному етапі життєвого циклу ІКС. Надано рекомендації щодо оцінювання вразливостей стосовно технічного та програмного захисту від несанкціонованого доступу або під'єднання до ІКС, захисту локальних мереж, реалізації організаційних заходів та процедур забезпечення комп'ютерної безпеки.

У статті описано обсяг і порядок первинного оцінювання та періодичного переоцінювання комп'ютерної безпеки ІКС АЕС. Надані рекомендації щодо формування відповідної команди оцінювання. Детально розглянуті методи оцінювання комп'ютерної безпеки ІКС, зокрема: аналіз документації (політики, програми, плану, звітів з комп'ютерної безпеки тощо), опитування персоналу (адміністративного, оперативного, обслуговуючого та фахівців з комп'ютерної безпеки), безпосередній огляд ІКС, їх компонентів та локальних мереж. Визначені етапи оцінювання (збір інформації, детальний аналіз, звітування) та описаний обсяг робіт на кожному етапі.

Надана загальна інформація щодо можливості та необхідності оцінювання ризиків комп'ютерної безпеки ІКС у разі застосування ризик-інформованих підходів.

Окремо зазначена необхідність документування результатів оцінювання та надані конкретні пропозиції щодо порядку підготовки відповідних звітів.

Ключові слова: інформаційна та керуюча система, комп'ютерна безпека, оцінювання вразливостей, оцінювання комп'ютерної безпеки, оцінювання ризиків.

Ця стаття продовжує цикл публікацій [1] – [5] з комп'ютерної безпеки ІКС АЕС у журналі «Ядерна та радіаційна безпека». Аналіз потенційних кібернетичних загроз на стадіях розробки та експлуатації ІКС АЕС надано в [1]. У [2] наведено огляд нормативних документів Міжнародного агентства з атомної енергії (МАГАТЕ), Комісії ядерного регулювання США та Міжнародної електротехнічної комісії з комп'ютерної безпеки ядерних установок (ЯУ). Вимоги, встановлені в цих документах, залежать від прийнятої категоризації систем з комп'ютерної безпеки, яка детально розглянута в [3]. У [4] проаналізовані основні принципи та методи захисту від комп'ютерних загроз та запропоновані відповідні заходи захисту від комп'ютерних загроз залежно від рівня комп'ютерної безпеки. У [5] розглянуті підходи до створення та керування документами, що обґрунтовують комп'ютерну безпеку, такими як: політика, програма та план комп'ютерної безпеки, план реагування на комп'ютерні інциденти, звітні документи з комп'ютерної безпеки.

Проблема забезпечення інформаційної та комп'ютерної безпеки ЯУ (зокрема АЕС) стає все більш актуальною. Оцінювання комп'ютерної безпеки є одним з найважливіших етапів забезпечення комп'ютерної безпеки, який сприяє здійсненню необхідних практичних заходів із захисту ІКС АЕС від кіберзагроз.

Оцінювання комп'ютерної безпеки дозволяє виявити можливі вектори кібератак та наявні вразливості в захисті ІКС АЕС від кіберзагроз. На основі результатів цього оцінювання реалізуються відповідні заходи комп'ютерної безпеки для підвищення захищеності ІКС АЕС та для зменшення ймовірності успішних кібератак з небезпечними наслідками для безпеки АЕС.

Мета цієї статті – розгляд основних складових оцінювання комп'ютерної безпеки ІКС АЕС:

оцінювання вразливостей комп'ютерної безпеки ІКС АЕС;

оцінювання достатності заходів забезпечення комп'ютерної безпеки ІКС АЕС;

оцінювання ризиків комп'ютерної безпеки ІКС АЕС (якщо застосовуються ризик-інформовані підходи).

Комп'ютерна безпека ІКС АЕС є складною багатокомпонентною задачею, рішення якої вимагає комплексного підходу та реалізації заходів у кількох напрямах:

розвиток законодавчої та нормативної бази з комп'ютерної безпеки;

дотримання загальних принципів забезпечення комп'ютерної безпеки (наприклад, глибокоешелонований захист, диференційований підхід, політика комп'ютерної безпеки, культура комп'ютерної безпеки тощо);

створення команд комп'ютерної безпеки на підприємствах та АЕС, які займаються розробкою та впровадженням заходів і засобів кіберзахисту ІКС АЕС;

оцінювання комп'ютерної безпеки;

реалізація заходів з комп'ютерної безпеки (включно з проєктними заходами) під час розробки, виробництва, впровадження, експлуатації та виведення з експлуатації ІКС АЕС;

розробка процедур та навчання персоналу для реагування на інциденти комп'ютерної безпеки;

звітування та розслідування інцидентів комп'ютерної безпеки з метою реалізації відповідних заходів та ухвалення галузевих рішень для запобігання поширенню таких інцидентів на інші АЕС та їх повторному виникненню в майбутньому.

Оцінювання комп'ютерної безпеки є важливим етапом, який передує розробці та впровадженню конкретних заходів забезпечення комп'ютерної безпеки ІКС АЕС. Оцінювання також дозволяє визначити достатність реалізованих заходів захисту від кіберзагроз.

Багато міжнародних та національних документів містять вимоги та опис процедур оцінювання комп'ютерної безпеки. Вимоги до оцінювання комп'ютерної безпеки містяться в документі [6], згідно з яким таке оцінювання потрібно проводити для кожного етапу життєвого циклу ІКС для виявлення потенціальних загроз, а також вразливостей. Кожна організація, яка відповідає за розробку, впровадження, експлуатацію, технічне обслуговування або зняття з експлуатації ІКС або їх компонентів, повинна проводити періодичне переоцінювання та аудит комп'ютерної безпеки.

Документ [7] надає детальний опис процедур, обсягу та змісту оцінювання комп'ютерної безпеки ЯУ, охоплюючи оцінювання вразливостей.

Документ [8] заборонений для публічного доступу, однак, згідно з назвою, він містить положення для самооцінювання комп'ютерної безпеки, рекомендовані для АЕС США.

Документ [9] не застосовується безпосередньо до ІКС АЕС, однак є одним з найбільш детальних посібників, що містять загальні рекомендації з оцінювання комп'ютерної безпеки. Документ містить опис методів аналізу, ідентифікації цілей кібератак, ідентифікації вразливостей, планування та проведення оцінювання комп'ютерної безпеки (включно з тестуванням).

Певний інтерес викликає дослідження, опубліковане в доповіді [10], де описані сценарії кібернетичних ризиків та розглянуто моделювання загроз для АЕС.

Загалом можна виділити чотири основні напрями оцінювання комп'ютерної безпеки ІКС АЕС:

оцінювання можливих кіберзагроз;

оцінювання вразливостей комп'ютерної безпеки ІКС;

оцінювання достатності застосованих заходів забезпечення комп'ютерної безпеки ІКС;

SSTC NRS ДЕРЖАВНЕ ПІДПРИЄМСТВО ДЕРЖАВНИЙ НАУКОВО-ТЕХНІЧНИЙ ЦЕНТР З ЯДЕРНОЇ ТА РАДІАЦІЙНОЇ БЕЗПЕКИ

оцінювання ризиків комп'ютерної безпеки ІКС.

Кібернетичні загрози ІКС АЕС були детально проаналізовані в [1]. Інші напрями розглядаються нижче.

Оцінювання вразливостей комп'ютерної безпеки ІКС АЕС

Надзвичайно важливо проаналізувати вразливості комп'ютерної безпеки ІКС, її компонентів та ПЗ на кожному етапі життєвого циклу ІКС.

Насамперед, необхідно оцінити вразливості та заходи захисту від несанкціонованого фізичного доступу до ІКС (наприклад, наявність або відсутність замків та пломб на дверях шаф, сигналізація відкривання дверей шафи тощо). Це важливо, оскільки за наявності таких вразливостей інсайдери можуть отримати несанкціонований доступ до технічних засобів ІКС та вчинити шкідливі дії щодо ІКС.

Також необхідно оцінювати можливі вразливості щодо несанкціонованого доступу до ІКС, її компонентів та ПЗ через інтерфейс людина-машина, зокрема оцінювання порядку та засобів програмного моніторингу доступу користувачів до ІКС. Проведення такого оцінювання має підтвердити, що в ІКС:

впроваджена автентифікація користувачів (зокрема, зчитування конфігураційних файлів, що містять деталі облікових записів користувачів) та не допускається анонімний доступ до ІКС;

доступ надається лише до обмеженого набору функцій, даних і компонентів ІКС, які необхідні та доступні певному користувачу або групі користувачів (згідно з принципом найменших привілеїв);

заборонено віддалений доступ до компонентів та ПЗ ІКС з-за меж АЕС та із загальностанційних мереж, забезпечено запобігання несанкціонованому віддаленому доступу (віддалений доступ дозволений лише для автентифікованих та авторизованих користувачів);

відсутні обхідні облікові записи з правами адміністратора для забезпечення доступу;

реалізується блокування користувача у разі декількох невдалих спроб отримати доступ до облікового запису ІКС та забезпечується інформування відповідального персоналу про несанкціонований доступ або спробу несанкціонованого доступу до ІКС;

примусово забезпечуються необхідні довжина, надійність, складність та періодичність зміни паролів;

регламентовані та документовані процедури створення, зміни, блокування та видалення облікових записів користувачів ІКС.

Мають бути оцінені вразливості та заходи захисту від будь-якого несанкціонованого під'єднання (зокрема з використанням бездротового зв'язку) до ІКС будь-яких зовнішніх пристроїв, охоплюючи сервісне та випробувальне обладнання, ноутбуки, мобільні пристрої, зовнішні носії даних (наприклад, диски, флешки, карти пам'яті, портативні жорсткі диски тощо).

Вразливості та захист локальних мереж потрібно оцінювати з урахуванням потенційних негативних наслідків впливу на ІКС АЕС через ці мережі. Для цього проводяться перевірки:

правильного визначення периметра безпеки;

правильного конфігурування мережевого обладнання;

забезпечення безпеки портів на мережевому обладнанні та обмеження доступу до конкретних портів технічних засобів ІКС;

наявності або відсутності відповідної сегментації мереж (наприклад, використання некерованого трафіку в мережі управління, доступність або недоступність ІКС у загальній локальній мережі АЕС, розміщення сервісів мережі управління безпосередньо в цій мережі тощо);

використання міжмережевих екранів для розділення локальних мереж та наявності чи відсутності підключень в обхід міжмережевих екранів та наявність належних заходів адміністративного контролю;

наявності або відсутності демілітаризованих зон;

фільтрації вхідних пакетів даних;

обмеження доступу.

Розробник має оцінювати наявність та достатність організаційних заходів і процедур забезпечення комп'ютерної безпеки середовища розроблення ІКС та їх компонентів. Під час такого оцінювання виконується перевірка наявності або відсутності:

осіб, відповідальних за комп'ютерну безпеку в організаційній структурі підприємства;

документації з комп'ютерної безпеки;

локальної мережі середовища розроблення, відокремленої від інших локальних та зовнішніх мереж підприємства;

заходів захисту від несанкціонованого доступу;

порядку зберігання конфіденційної інформації та документації;

обмежень на використання зовнішніх носіїв даних, портативних та мобільних пристроїв;

порядку авторизації та автентифікації співробітників, які беруть участь у розробленні програмно-технічних комплексів, технічних засобів автоматизації, ПЗ;

аудитів або оцінок безпеки;

порядку реєстрації та реагування на кіберінциденти.

Експлуатуюча організація має оцінювати організаційні заходи та процедури із забезпечення комп'ютерної безпеки, зокрема наявність або відсутність:

осіб, відповідальних за комп'ютерну безпеку в організаційній структурі АЕС;

документації з комп'ютерної безпеки;

задокументованих процедур резервного копіювання та відновлення;

аудитів або оцінок безпеки;

порядку авторизації та автентифікації користувачів;

максимально спрощеної та задокументованої мережевої архітектури;

контролю вхідних та вихідних потоків даних;

моніторингу кіберінцидентів.

Результати оцінювання загроз та вразливостей ІКС мають бути задокументовані у відповідному звіті, які потрібно враховувати під час розробки конкретних заходів захисту в плані комп'ютерної безпеки ІКС (вимоги та підходи до створення плану розглянуті в [5]). Якщо аналіз показав, що заходів комп'ютерної безпеки на рівні ІКС недостатньо, то мають бути реалізовані додаткові компенсаційні заходи.

Оцінювання достатності застосованих заходів забезпечення комп'ютерної безпеки ІКС

Оцінювання комп'ютерної безпеки під час модифікації або впровадження нової ІКС проводиться спеціально сформованою командою оцінювання, що складається з представників експлуатуючої організації, розробника ІКС та інших організацій (за потреби).

Команда оцінювання повинна містити фахівців з експлуатації, технічного обслуговування, ядерної та радіаційної безпеки ІКС та фахівців з комп'ютерної безпеки. Зазвичай члени групи оцінювання підписують договір про нерозголошення конфіденційної інформації, оскільки зловмисники можуть використовувати розкриття конфіденційної інформації для виявлення вразливостей та розробки можливих сценаріїв атаки.

Оцінювання комп'ютерної безпеки діючих ІКС, які були впроваджені раніше і вже експлуатуються на АЕС, проводиться в межах аналогічної окремої процедури. Водночас потрібно враховувати, що проєкт діючих ІКС АЕС міг не мати належних захисних заходів проти кіберзагроз.

Оцінювання комп'ютерної безпеки конфігурації та параметрів ІКС на місці експлуатації виконується з метою підтвердження реалізації відповідних заходів захисту від потенційних кіберзагроз. Якщо результати оцінки показують, що реалізовані заходи є недостатніми, то визначаються вимоги до додаткових заходів захисту.

Оцінювання комп'ютерної безпеки ІКС потрібно проводити за допомогою таких методів отримання необхідної інформації:

Аналіз документації (наприклад, політика, програма та план комп'ютерної безпеки, звіти з оцінювання комп'ютерної безпеки, навчальні матеріали з комп'ютерної безпеки, технічна документація на ІКС, інвентарні списки технічних засобів ІКС, списки контролю доступу, архітектура локальної мережі, операційні журнали, звіти про інциденти комп'ютерної безпеки, звіти з оцінювання ризиків тощо). Під час аналізу документації проводиться оцінювання відповідності існуючих заходів комп'ютерної безпеки вимогам норм, правил і стандартів, політики, програми та плану комп'ютерної безпеки. Крім того, оцінюється відповідність поточного стану захищеності від існуючих кіберзагроз.

Опитування персоналу (зокрема адміністративного, оперативного та обслуговуючого персоналу, фахівців з комп'ютерної безпеки). Опитування персоналу спрямоване на оцінювання обізнаності персоналу та розуміння політики, програми та плану комп'ютерної безпеки, ефективності підготовки персоналу щодо комп'ютерної безпеки, розуміння персоналом кібернетичних загроз та ризиків, готовності до реагування на інциденти, визначення обов'язків та розподілу відповідальності, ефективності культури комп'ютерної безпеки, заходів забезпечення конфіденційності.

Безпосередній огляд ІКС, їх компонентів та локальних мереж. Безпосередній огляд необхідний для оцінювання заходів комп'ютерної безпеки (з урахуванням рівнів комп'ютерної безпеки ІКС, які розглянуті в [3]), впровадження зон комп'ютерної безпеки, контролю доступу до ІКС та їх компонентів (зокрема до запасних частин), фактичної архітектури локальних мереж, порядку та результатів тестування і обслуговування ІКС, управління конфігурацією, моніторингу та реєстрації інцидентів комп'ютерної безпеки.

Існує три основні етапи оцінювання комп'ютерної безпеки ІКС.

Етап 1: Збір інформації. На цьому етапі група оцінювання проводить попередній збір інформації, необхідної для подальшого детального аналізу, під час якого оцінюється:

політика, програма і план комп'ютерної безпеки та звіти з їх реалізації;

порядок, обсяг і результати аналізу кіберзагроз та їх можливих наслідків;

застосування диференційованого підходу до комп'ютерної безпеки, визначення рівнів комп'ютерної безпеки;

впровадження глибокоешелонованого захисту в ІКС та АЕС загалом;

наявність оцінки ризиків та відповідних заходів комп'ютерної безпеки.

Етап 2: Детальний аналіз. На цьому етапі група оцінювання на основі раніше зібраної інформації проводить детальний аналіз таких факторів забезпечення комп'ютерної безпеки:

SSTC NRS ДЕРЖАВНЕ ПІДПРИЄМСТВО ДЕРЖАВНИЙ НАУКОВО-ТЕХНІЧНИЙ ЦЕНТР З ЯДЕРНОЇ ТА РАДІАЦІЙНОЇ БЕЗПЕКИ

поінформованість персоналу щодо політики комп'ютерної безпеки, спеціалізоване навчання з питань комп'ютерної безпеки та наявність на АЕС відповідальних за комп'ютерну безпеку;

розподіл обов'язків і порядку доступу до ІКС персоналу, підрядників та сторонніх організацій;

наявність в інвентарному списку ІКС, їх компонентів, мережевого обладнання, ПЗ, запасних частин, їх класифікації з комп'ютерної безпеки, переліку їх фізичного розташування, функціональних схем ІКС та схем зональної моделі (водночас оцінюється відповідність зональної моделі фізичному розміщенню ІКС і відсутність віднесення обладнання одночасно до декількох зон);

впровадження адміністративних, технічних і програмних засобів захисту та моніторингу несанкціонованого доступу до ІКС, їх компонентів, мережевого обладнання, ПЗ, запасних частин;

фізичне відокремлення ІКС, їх компонентів та мереж з різним рівнем комп'ютерної безпеки;

порядок використання випробувального, налагоджувального обладнання, портативних пристроїв та зовнішніх носіїв даних у місцях розміщення ІКС;

порядок утилізації непрацездатних або замінених технічних засобів та носіїв даних;

обмеження доступу користувачів і ПЗ лише до інформації та ресурсів, які є мінімально необхідними для успішного виконання необхідних функцій;

неможливість несанкціонованого доступу до ІКС, їх компонентів, ПЗ та даних через мережі, модеми, точки дротового або бездротового підключення, порти, незаблоковані технічні засоби або робочі станції, сполучені ІКС тощо;

реалізація виявлення вразливостей за допомогою відповідного аналізу та тестування;

достатність заходів комп'ютерної безпеки, реалізованих в ІКС та їх компонентах, відповідно до плану комп'ютерної безпеки;

реалізація додаткових компенсуючих заходів, якщо в межах конкретної ІКС неможливо застосувати необхідні заходи комп'ютерної безпеки;

процедури впровадження або модифікації ІКС та їх компонентів, модифікації або встановлення нового ПЗ і оцінювання впливу цих змін на комп'ютерну безпеку;

впровадження заходів комп'ютерної безпеки в розробників, виробників та постачальників ІКС, їх компонентів, ПЗ та елементної бази;

заходи комп'ютерної безпеки під час монтажу ІКС та їх компонентів;

програми і методики та результати випробувань комп'ютерної безпеки на підприємстві після виготовлення ІКС, їх компонентів і на АЕС після монтажу ІКС та їх компонентів;

заходи комп'ютерної безпеки під час технічного обслуговування, яке виконується сторонніми організаціями на АЕС;

наявність документально підтверджених процедур реагування (тобто, дії персоналу, інформування, контрзаходи, відновлення, розслідування та коригувальні дії) на інциденти комп'ютерної безпеки, враховуючи зовнішні та внутрішні (інсайдерські) кіберзагрози.

Етап 3: Звітування. На цьому етапі команда оцінювання складає відповідний звіт, який відображає детальні результати аналізу, вказує на потенційні загрози, виявлені вразливості, рекомендації щодо усунення виявлених недоліків, поліпшення комп'ютерної безпеки, проєктні заходи комп'ютерної безпеки ІКС, впровадження компенсаційних заходів комп'ютерної безпеки (за необхідності).

Періодичне переоцінювання комп'ютерної безпеки

Кожна організація, відповідальна за розробку, впровадження, тестування, експлуатацію, обслуговування ІКС, її компонентів та/або ПЗ проводить періодичне переоцінювання комп'ютерної безпеки.

Рекомендується проводити періодичне переоцінювання комп'ютерної безпеки не рідше одного разу на два роки.

Додаткове переоцінювання комп'ютерної безпеки ІКС також має бути виконано у випадку:

модифікації ІКС, їх компонентів та ПЗ;

виникнення інциденту комп'ютерної безпеки;

ідентифікації нових вразливостей ІКС.

Результати періодичного переоцінювання комп'ютерної безпеки відображаються у відповідному звіті.

Зазначимо, що під час оцінювання або періодичного переоцінювання та підготовки відповідного звіту має бути забезпечено належний рівень захисту конфіденційної інформації, зокрема, належне маркування, зберігання, передача та знищення всіх документів, підготовчих матеріалів, технічних записів, проєктів звіту і підсумкового звіту. Під час підготовки звіту застосовуються відповідні обмеження щодо використання електронних пристроїв та носіїв даних.

Оцінювання ризиків комп'ютерної безпеки

У разі використання ризик-інформованих підходів щодо комп'ютерної безпеки ІКС проводиться оцінювання ризику для виявлення вразливостей до кібернетичних атак, що впливають на цю ІКС, та визначення потенційних наслідків успішного використання зловмисниками цих вразливостей. Відповідні заходи комп'ютерної безпеки ґрунтуються на результатах такого аналізу ризику.

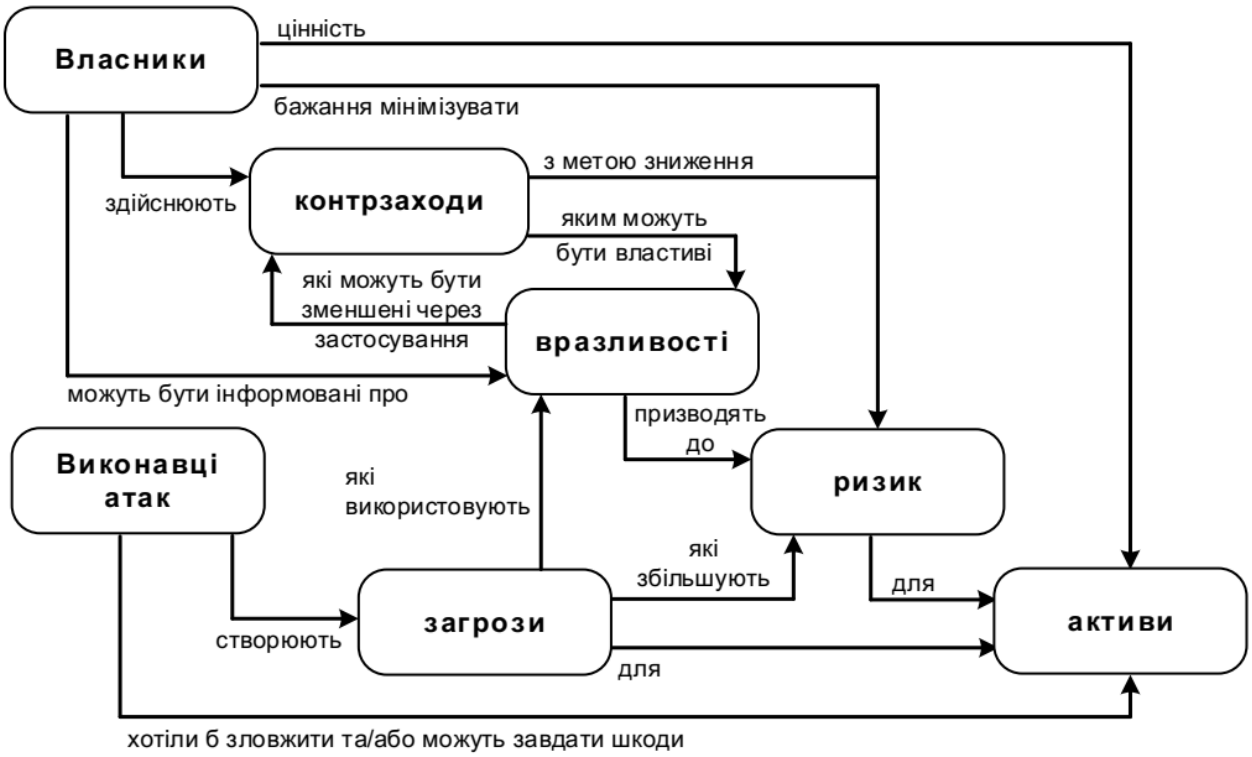

Рисунок 1 – Взаємозв'язки комп'ютерної безпеки

Ризик у контексті комп'ютерної безпеки ІКС – це потенційна можливість того, що задана кіберзагроза використовує вразливість ІКС та/або їх компонентів і тим самим може завдати шкоди безпеці АЕС. Ризик вимірюється як комбінація ймовірності події та важкості її наслідків. Відповідно до [11] у документі МАГАТЕ [12] сформована діаграма взаємозв'язків між загрозами, вразливостями та ризиком (Рисунок 1).

Під час оцінювання ризику необхідно визначити та задокументувати конкретні поєднання загроз, вразливостей і наслідків. Після цього мають бути розроблені (якщо це необхідно) відповідні доповнення до вимог комп'ютерної безпеки та заходи для запобігання або пом'якшення потенційних наслідків кібернетичних атак на ІКС. Тобто, здійснюються відповідні дії для зменшення ризику.

Оцінювання ризиків комп'ютерної безпеки ІКС буде докладно розглянуто в окремій публікації.

Висновки

Забезпечення комп'ютерної безпеки ІКС АЕС є актуальним питанням для багатьох країн світу, зокрема для України. Першочерговим кроком забезпечення комп'ютерної безпеки ІКС АЕС є всебічне оцінювання різних аспектів комп'ютерної безпеки.

Оцінювання комп'ютерної безпеки охоплює:

Вивчення можливих кіберзагроз. Аналіз, наведений в [1], показав, що забезпечення комп'ютерної безпеки є складним завданням, під час вирішення якого потрібно враховувати різні типи кіберзагроз на етапах розробки та експлуатації ІКС.

Оцінювання вразливих місць ІКС. Оцінювання вразливостей в ІКС та конфіденційності відповідної документації (наприклад, політики, програми та плану комп'ютерної безпеки) необхідні для виявлення слабких сторін в ІКС та можливі шляхи кібератак.

Оцінювання адекватності та повноти застосованих заходів комп'ютерної безпеки. Виявлення кіберзагроз, вразливостей ІКС та можливих слабких місць щодо конфіденційності документації дозволяють розробити відповідні заходи з захисту ІКС від кібератак. Адекватні захисні заходи повинні охоплювати всі стадії життєвого циклу ІКС АЕС. Первинне оцінювання та подальші періодичні переоцінювання адекватності та повноти застосованих заходів комп'ютерної безпеки є важливими етапами оцінювання комп'ютерної безпеки ІКС, що дозволяє підтримувати заходи захисту на належному рівні.

SSTC NRS ДЕРЖАВНЕ ПІДПРИЄМСТВО ДЕРЖАВНИЙ НАУКОВО-ТЕХНІЧНИЙ ЦЕНТР З ЯДЕРНОЇ ТА РАДІАЦІЙНОЇ БЕЗПЕКИ

Оцінювання ризиків комп'ютерної безпеки (у разі використання ризик-інформованого підходу). Оцінювання комп'ютерної безпеки ІКС є обов'язковою та важливою складовою комплексу заходів із забезпечення комп'ютерної безпеки ІКС АЕС, тому компетентне оцінювання комп'ютерної безпеки є основним підґрунтям для подальшого ефективного забезпечення комп'ютерної безпеки ІКС.

Список використаної літератури

1. Клевцов А. Л., Трубчанинов С. А. Компьютерная безопасность информационных и управляющих систем АЭС: кибернетические угрозы. *Ядерна та радіаційна безпека.* 2015. № 1 (65). С. 54 – 58.

2. Клевцов А. Л., Ястребенецкий М. А., Трубчанинов С. А. Компьютерная безопасность информационных и управляющих систем АЭС: нормативная база. *Ядерна та радіаційна безпека*. 2015. № 4 (68). С. 51 – 57.

3. Клевцов А. Л., Симонов А. А., Трубчанинов С. А. Компьютерная безопасность информационных и управляющих систем АЭС: категоризация. *Ядерна та радіаційна безпека*. 2016. № 4 (72). С. 65 – 70. doi: 10.32918/nrs.2016.4(72).10.

4. Симонов А. А., Клевцов А. Л., Трубчанинов С. А. Компьютерная безопасность информационных и управляющих систем АЭС: меры защиты от компьютерных угроз. *Ядерна та радіаційна безпека*. 2017. № 2 (74). С. 46 – 50. doi: 10.32918/nrs.2017.2(74).09.

5. Симонов А. А., Клевцов А. Л., Трубчанинов С. А. Лазуренко О. П. Компьютерная безопасность информационных и управляющих систем АЭС: документи, що обґрунтовують комп'ютерну безпеку. *Ядерна та радіаційна безпека*. 2019. № 4 (84). С. 73 – 81. doi: 10.32918/nrs.2019.4(84).09.

6. Computer security of instrumentation and control systems at nuclear facilities: technical guidance. Vienna : International Atomic Energy Agency, 2018. (IAEA nuclear security series, ISSN 1816-9317; No. 33-T). ISBN 978-92-0-103117-4.

7. Conducting Computer Security Assessment at Nuclear Facilities. Vienna : International Atomic Energy Agency, 2016. (IAEA-TDL-006). ISBN 978-92-0-104616-1.

8. NUREG/CR-6847; PNNL-14766. Cyber Security Self-Assessment Method for U.S. Nuclear Power Plants. Richland, WA : Pacific Northwest National Laboratory. Washington, DC : U.S. Nuclear Regulatory Commission, October 2004.

9. Technical Guide to Information Security Testing and Assessment. Recommendations of the National Institute of Standards and Technology. Gaithersburg, MD : National Institute of Standards and Technology, September 2008. (NIST Special Publication 800-115).

10. Masood, R. Assessment of Cyber Security Challenges in Nuclear Power Plants. Security Incidents, Threats, and Initiatives. Report GW-CSPRI-2016-03. The George Washington University, Washington, DC, August 15, 2016. 43 p.

11. ISO/IEC 13335-1:2004. Information Technology – Security Techniques – Management of Information and Communications Technology Security – Part 1: Concepts and Models for Information and Communications Technology Security Management. Geneva : International Electrotechnical Commission, 2004. Withdrawn. 28 p.

12.Computer security at nuclear facilities : reference manual : technical guidance. Vienna : International Atomic Energy Agency, 2011. (IAEA nuclear security series, ISSN 1816-9317; No. 17). ISBN 978-92-0-120110-2.

References

1. Klevtsov, A., Trubchaninov, S. (2015). Computer security of NPP instrumentation and control systems: cyber threats. *Nuclear and Radiation Safety*, 1(65), 54–58.

2. Klevtsov, A., Yastrebenetsky, M., Trubchaninov, S. (2015). Computer security of NPP instrumentation and control systems: regulatory framework. *Nuclear and Radiation Safety*, 4(68), 51–57.

3. Klevtsov, A., Symonov, A., Trubchaninov, S. (2016). Computer security of NPP instrumentation and control systems: categorization, *Nuclear and Radiation Safety*, 4(72), 65–70. doi: 10.32918/nrs.2016.4(72).10.

4. Symonov, A., Klevtsov, A., Trubchaninov, S. (2017). Computer security of NPP instrumentation and control systems: protection from computer threats. *Nuclear and Radiation Safety*, 2(74), 46–50. doi: 10.32918/nrs.2017.2(74).09.

5. Symonov, A., Klevtsov, A., Trubchaninov, S., Lazurenko O. (2019). Computer security of NPP instrumentation and control systems: documents, which substantiate the computer security. *Nuclear and Radiation Safety,* 4(84), 73–81. doi: 10.32918/nrs.2019.4(84).09.

6. Computer security of instrumentation and control systems at nuclear facilities: technical guidance. Vienna, International Atomic Energy Agency, 2018. (IAEA nuclear security series, ISSN 1816-9317; No. 33-T). ISBN 978-92-0-103117-4.

7. Conducting computer security assessment at nuclear facilities. Vienna, International Atomic Energy Agency, 2016. (IAEA-TDL-006). ISBN 978-92-0-104616-1.

8. Cyber security self-assessment method for U.S. nuclear power plants. Richland, WA, Pacific Northwest National Laboratory, Washington, DC, U.S. Nuclear Regulatory Commission, October 2004. (NUREG/CR-6847; PNNL-14766).

9. Technical guide to information security testing and assessment. Gaithersburg, MD, National Institute of Standards and Technology, September 2008. (NIST Special Publication 800-115).

10. Masood, R. (2016). Assessment of cyber security challenges in nuclear power plants. Security Incidents, Threats, and Initiatives. Report GW-CSPRI-2016-03, The George Washington University, Washington, DC, 43.

11. Information technology – security techniques – management of information and communications technology security. Part 1 Concepts and models for information and communications technology security management. Geneva, International Electrotechnical Commission, 2004. (ISO/IEC 13335-1:2004).

12. Computer security at nuclear facilities, reference manual, technical guidance. Vienna, International Atomic Energy Agency, 2011. (IAEA nuclear security series, ISSN 1816-9317; No. 17). ISBN 978-92-0-120110-2.

Computer Security of NPP Instrumentation and Control Systems: Computer Security Assessment

Klevtsov O., Symonov A., Trubchaninov S.

State enterprise «State Scientific and Technical Center for Nuclear and Radiation safety», Kharkiv, Ukraine

The paper is devoted to the issues of computer security assessment of instrumentation and control systems (I&C systems) of nuclear power plants (NPPs). The authors specified the main areas of assessing the computer security of NPP I&C systems, especially the assessment of cyber threats, vulnerabilities of I&C computer security, sufficiency of applied measures for ensuring I&C systems computer security, risks of I&C system computer security as well as periodic reassessment of I&C computer security. The paper considers the assessment of I&C computer security vulnerabilities, sufficiency of applied measures for ensuring I&C computer security (assessment of cyber threats and the risks of I&C computer security are discussed in detail in other publications from the series "Computer Security of NPP Instrumentation and Control Systems").

Approaches to assessing the computer security vulnerabilities of I&C systems and software at each stage of I&C life cycle are considered. The recommendations for assessing vulnerabilities regarding technical and software protection against unauthorized access or connection to I&C, protection of local networks, implementation of organizational measures and procedures for computer security are provided.

The paper describes the scope and procedures for the initial assessment and periodic reassessment of NPP I&C computer security. Recommendations for the formation of an appropriate evaluation team are provided. Methods of assessing I&C computer security are considered, namely: analysis of documents (computer security policy, program, plan, reports, etc.), survey of staff (administrative, operational, service and computer security experts), direct review of I&C systems, their components and local networks. The evaluation stages (collection of information, detailed analysis, reporting) and the scope of work at each stage are described.

General information about the possibility and necessity of assessing the computer security risks of I&C systems in the case of using risk-informed approaches is provided.

The need to document the results of the assessment is noted separately and specific proposals about the procedure for developing relevant reports are made.

Keywords: computer security, instrumentation and control system, computer security assessment, vulnerability assessment, risk assessment.

Отримано 21.09.2020.