озвучено прагнення досягти нульового травматизму і повне видалення профзахворювань в гірничодобувному секторі.

Удосконалення умов охорони праці в США займає важливе місце в майбутній політиці держави. Для малого та середнього бізнесу розроблені спеціальні спрощені нормативно-методичні та інформаційні матеріали, які полегшують розуміння правил техніки безпеки, головних обов'язків працівника і роботодавця з управління ризиками.

Література:

1. Р. Б. Бойко (Зовнішторгвидав України) правовий аспект охорони праці: міжнародний досвід для України http://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/vaau_2011_3_13.pdf

2. Управління з охорони праці OSHA https://en.wikipedia.org/wiki/Occupational_Safety_and_Health_Administration

Хілініч І. О.

Науковий керівник: ст. викл. ***Глєбова О. І.,***

Державний університет телекомунікацій, м. Київ

СИСТЕМИ КЕРУВАННЯ У СФЕРІ ЗАПОБІГАННЯ НАДЗВИЧАЙНИМ СИТУАЦІЯМ

У контексті запобігання надзвичайним ситуаціям техногенного, природного, техногенно-природного характеру актуальним є питання створення багаторівневих інтелектуальних систем керування (далі – БІСК), які на основі збору/відбору інформації про стан досліджуваних об’єктів дають підстави для прийняття рішення з керування надзвичайними ситуаціями. Така модель дасть змогу створювати повну інформативну базу знань у сфері запобігання надзвичайним ситуаціям, приймати рішення щодо

керування техногенними і природними об’єктами та коригувати політику інформаційної безпеки держави.

Системи керування (далі – СК) за останні роки зазнали значних змін. На їх основі створюються новітні апаратно-програмні комплекси. СК стають інтелектуальнішими, характеризуються швидкістю та якістю керування, зменшується безпосередня участь людини в цьому процесі. Ці переваги роблять інтелектуальні СК (далі – ІСК) надзвичайно поширеними. Це зумовлено кількістю загроз, яким можуть піддаватися ІСК, та збитками у разі їх некоректного функціонування. Дотримання вимог до системи захисту інформації необхідне на всіх життєвих циклах в ІСК: “проектування – виготовлення – встановлення – експлуатація”. На практиці вимоги до систем технічного захисту упродовж життєвого циклу ІСК не завжди забезпечуються, що призводить до загрози безпеки людини, суспільства та держави загалом.

У загальному випадку об’єкт керування може мати достатньо складну конструкцію, з низкою функціонально підконтрольних систем. Це зумовлює багаторівневу структуру системи керування. Визначення можливих уразливостей в ІСК є ключовим етапом для забезпечення “цілісності–доступності–конфіденційності”. ІСК складаються з різних пристроїв, з’єднаних у єдину мережу. Несанкціонований доступ зловмисника до пристроїв та вузлів ІСК можна реалізувати маніпулюванням функціями керування пристроїв та перехопленням даних, якими обмінюються пристрої у мережі. Доступ до ІСК може здійснюватися віддалено з ноутбуків, смартфонів чи телефонів. Мережеві пристрої можуть обмінюватися даними через радіоканал.

Можна виділити п’ять потенційних уразливостей, що можуть використовуватись для атаки на ІСК, а саме: мережеві, магістральні, комутаційні уразливості мережевих пристроїв та пристроїв керування.

Такі загрози можна зарахувати до двох класів – на рівні мережі та на рівні пристроїв. Для здійснення атаки на мережу противнику необхідно мати фізичний доступ до неї, що легко досягається з використанням радіодіапазону для обміну даними. Таку атаку можна реалізувати через мережевий інтерфейс іншого пристрою. Атаки на пристрій здійснюються через уразливості самого програмного забезпечення, фізичне втручання, збір інформації про роботу пристрою. Оскільки уразливості пристроїв не можна розглядати як такі, що можуть впливати на функціонування усієї ІСК, то на практиці зосереджуються на уразливостях мережі та формуванні підходів до її захисту.

Перепонами різної міцності вважаються: стіни, стеля, підлога, вікна і замок на двері. Наприклад, система контролю відкриття апаратури і система розпізнавання та розмежування доступу, що контролюють доступ до БІСК, утворюють замкнений захисний контур. До захисного контуру на рівні ланок увійдуть: системи контролю доступу в приміщення; засоби захисту від побічного електромагнітного випромінювання і засоби шифрування.

Література:

1. Закон України “Про основи національної безпеки України” від 19.06.2003 р. № 964-IV.

2. Дудикевич В. Б. Аналіз безпеки багаторівневих інтелектуальних систем керування / В. Б. Дудикевич, Т. Б. Крет // Тези доповідей VI міжнародної НПК “Проблеми і перспективи розвитку ІТ-індустрії”. – Харків, 17–18 квітня 2014 р.

3. Юхимчук С. В. Використання інтелектуальних технологій для аналізу небезпечних ситуацій на залізничному транспорті / С. В. Юхимчук, Т. О. Савчук, М. Д. Кацман // Систем. дослідж. та інформ. технології. – 2009.