НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Факультет інформатики та обчислювальної техніки

Кафедра автоматики та управління в технічних системах

«На правах рукопису»
УДК _____

До захисту допущено:

Завідувач кафедри

____

«___»_____20__ р.

Магістерська дисертація

на здобуття ступеня магістра

за освітньо-науковою програмою «Інтегровані інформаційні системи»

зі спеціальності 126 «Інформаційні системи та технології»

на тему: «Метод оптимізації системи захисту інформації на виробництві мінеральних добрив»

Виконав:
студент VI курсу, групи ІА-91мн
Заболотний Владислав Валерійович _____

Керівник:
Професор кафедри АУТС, д.т.н., професор,
Корнієнко Богдан Ярославович _____

Рецензент:
Доцент кафедри технічних та програмних
засобів автоматизації ІХФ, к.т.н., доцент,
Ладієва Леся Ростиславівна _____

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.
Студент _____

Київ – 2021 року

РЕФЕРАТ

Заболотний В.В. Метод оптимізації системи захисту інформації на виробництві мінеральних добрив. КПІ ім. Ігоря Сікорського, 2021.

Робота містить 113 с. тексту, 14 рисунків, 2 таблиці, посилання на 37 літературних джерел та додаток.

Ключові слова: система безпеки, захищеність, оптимізація системи захисту, визначення захищеності, рекомендації з безпеки, хімічне підприємство, підприємство з виробництва хімічних добрив, критерії оптимальності.

Об’єктом дослідження є хімічне підприємство, виробництво мінеральних добрив зокрема.

Метою цієї роботи є компіляція українських та міжнародних досліджень безпеки хімічних підприємств, оптимізація системи захисту критичних інформаційних ресурсів, а також визначення потенційних критеріїв оптимальності оптимізації, враховуючи сектор та потребу у безпеці системи, над якою проводиться дослідження.

У дипломному проекті проведений аналіз структури системи безпеки на хімічному підприємстві, досліджені основні загрози таким системам, виявлені основні способи нанесення їм шкоди. Також з використанням математична моделі впливу загроз на інформаційну систему, розроблені та представлені критерії оцінки оптимальності інформаційної системи захисту інформації.

Отримані результати можуть бути корисними при аналізі та підвищені захищеності систем управління інформаційними об’єктами.

SUMMARY

Zabolotnyi V.V. The optimization method for the information protection system of a mineral fertilizer manufacturing facility. Igor Sikorsky KPI, 2021.

The project contains 113 pages of text, 14 figures, 2 tables, references to 37 literary sources and an annex.

Keywords: security system, protection, security system optimization, determine the protection, security recommendations, chemical facility, mineral fertilizer manufacturing facility, optimality criteria.

The object of the research is a chemical facility, a mineral fertilizer manufacturing facility.

The goal of the research is the compilation of Ukrainian and international research of the chemical facilities' security, the optimization of the protection system of the critical informational resources, keeping in focus the sector and the need of the protection of the researched system.

The graduation project contains an analysis of the structure of the security system of a chemical facility, researches main threats to such systems, discovers the main approaches to break such systems. Also using a mathematical model of the influence of threats on an informational system, the criteria of optimality of the security system of a chemical facility have been developed and presented.

Results of the research could be used to analyze and improve protection of informational object management systems.

ЗМІСТ

ПЕРЕЛІК ВИЗНАЧЕНЬ ТА СКОРОЧЕНЬ

Інтернет речей - концепція мережі, що складається із взаємозв'язаних фізичних пристроїв, які мають вбудовані давачі, а також програмне забезпечення, що дозволяє здійснювати передачу і обмін даними між фізичним світом і комп'ютерними системами в автоматичному режимі

АРСХФ - Антитерористичні стандарти хімічного фонду

РП – Рахункова палата США

ПСУ - Промислова система управління

РСУ - Розподілена система управління

ПЛК - Програмований логічний контролер

ЛМІ - Інтерфейс людини і машини

ІТ – Інформаційні технології

КІКР – Критична інфраструктура та ключові ресурси

СУКБ - Система управління кібербезпекою

СОРРІК - Стратегічна оцінка ризику розвитку інфраструктури країни

ДСНС – Державна служба з надзвичайних ситуацій

SCADA - Програмний пакет, призначений для розробки або забезпечення роботи в реальному часі систем збору, обробки, відображення та архівування інформації про об'єкт моніторингу або управління

NEPIC - Кластер переробної промисловості на північному сході Англії

HSE – Управління з охорони праці у Великій Британії

SABIC - Багатонаціональна компанія з виробництва хімічних речовин у Саудівській Аравії

Tekgem – Британська компанія, яка спеціалізується на кібер-захисті підприємств

Honeywell - Головна американська міжнародна корпорація, що виробляє зброю, космічні системи, автоматичні й контролюючі системи, іженерні послуги, транспортаційні системи

ДМЗ – Демілітаризована зона

Watering hole - Стратегія комп’ютерної атаки, в якій зловмисник здогадується або спостерігає, які веб-сайти організація часто використовує та заражає одну чи декілька з них шкідливим програмним забезпеченням

Triton – Програмне забезпечення, використане для атаки на підприємство у Саудівській Аравії у 2017р

WannaCry — Комп'ютерний вірус, що вражає операційну систему Microsoft Windows шляхом шифрування файлів

COMAH – Британський відділ контролю за масштабними аваріями

MODBUS - Комунікаційний протокол, заснований на технології master-slave

TCP / IP - Набір протоколів мережі Інтернет

NHS - Національної служби охорони здоров’я Великої Британії

Saudi Aramco - Найбільша за видобутком і запасами нафти компанія світу, національна нафтова компанія Саудівської Аравії

ЄС – Європейський союз

NIPP - Національний план захисту інфраструктури у США

ЗЗР - Заходи для зменшення ризиків

СЦЗТ - Серверне цифрове замкнуте телебачення

COVID-19 - Інфекційна хвороба, яку спричиняє новий штам коронавірусу

СМО - системами масового обслуговування

Марковський процес — це випадковий процес, конкретні значення якого для будь-якого заданого часового параметру t+1 залежать від значення у момент часу t, але не залежать від його значень у моменти часу t-1, t-2 і т. д. (дискретний випадок марковського процесу). Іншими словами «майбутнє» процесу залежить лише від «поточного» стану, але не залежить від «минулого» (за умови, коли «поточний» стан процесу відомий).

Рівняння Чепмена-Колмогорова — рівняння, що пов'язує умовні ймовірності для марківського процесу в різні моменти часу.

АХР – американська хімічна рада.

ВСТУП

Хімічний сектор, і виробництво мінеральних добрив як його складова, забезпечує основи сучасного життя. Оскільки сектор стосується багатьох аспектів того, як ми живемо та того, як ведеться бізнес у всьому світі, комунікаційні технології, зв’язок та обмін інформацією є важливими аспектами всіх операцій та процесів компанії в цьому секторі.

Однак ті самі технології, які роблять бізнес-операції та виробничі процеси більш ефективними, можуть створити нові вразливості. Оскільки світ стикається з підвищеними загрозами, хімічний сектор повинен збільшити свою здатність управляти ризиком з боку кібербезпеки та бути захищеним від загрози несанкціонованого доступу до інформації, яка використовується для полегшення або спричинення фізичної атаки або порушення ланцюга поставок.

McMafia - хакер, що отримував доступ до файлів і контролював IT-мережу порту Мумбаї через торговий автомат з поганими захистом. На перший погляд, це може здатися неправдоподібним, але загроза критичній інфраструктурі цілком реальна. У міру підключення більшої кількості пристроїв, здатність компрометувати корпоративну мережу через віддалений пристрій, підключений до Інтернету речей, становить реальну загрозу.

Тисячі хімічних підприємств у всьому світі покладаються на дуже застарілі вказівки з кібербезпеки, роблячи їх вразливими до хакерських атак, які можуть призвести не тільки до економічної шкоди, але й до витоків хімічних речовин або вибухів.

Лише у США, яка є передовою за розвитком країною у світі, 3300 хімічних підприємств знаходяться у групі високого ризику, тобто вони використовують принаймні один з 300 хімікатів, які входять до списку особливо небезпечних [5]. До цього списку входять токсичні та вибухонебезпечні сполуки, такі як хлор та циклопропан, а також хімічні речовини, які не є небезпечними при раптовому випуску, але можуть бути перетворені на зброю в разі викрадення.

Більшість хімічних компаній, включаючи компанії з високим ризиком, мають підключені до Інтернету пристрої як частину своїх систем управління процесами. Це дозволяє, наприклад, виробникам приладів віддалено обслуговувати свої пристрої. Хакери, які беруть під контроль системи, що експлуатують хімічний завод, можуть спричинити катастрофічні наслідки, як показав інцидент на нафтопереробному заводі в Саудівській Аравії [3].

Компанії почали впроваджувати окремі системи контролю безпеки, які безпечно б зупинили хімічний процес у разі атаки чи аварії та які повинні були бути захищені від будь-якого зовнішнього доступу. Але атака у Саудівській Аравії, спрямована саме на ці системи безпеки, довела, що це теж вже не відповідає дійсності.

У США та багатьох країнах світу, хімічні компанії дотримуються вказівок щодо кібербезпеки, опублікованих програмою Антитерористичних стандартів хімічного фонду (АРСХФ) - документу, який не оновлювався більше десяти років. Це означає, що у постійно мінливому середовищі загроз, дуже мало впевненості в тому, що об'єкти насправді захищені, навіть якщо неухильно дотримуються вказівок [2].

У звіті Рахункової палати США (РП) не вперше підкреслюється кібербезпека - або її відсутність. Ще з 2015 року експерти з питань безпеки закликають хімічні заводи оновити свої системи кіберзахисту. Але виробництва можуть не побачити негайної потреби це зробити, аргументуючи, наприклад, що ще ніколи не було теракту на хімічний завод у місті, де знаходиться підприємство, гроші на це витрачати не потрібно.

За даними Міністерства національної безпеки США, кількість інцидентів кібербезпеки на промислових об'єктах зростає: 290 у 2016 році проти 41 у 2010 році.

Часто проблема полягає в тому, що IT-спеціалісти мають гарне уявлення про те, як має працювати система безпеки, але вони зовсім не розуміють, з чим мають справу інженери, які керують заводом.

Передбачається, що до кінця 2020 року буде існувати 20,4 мільярда підключених до мережі Інтернет пристроїв. Очевидно, що кількість пристроїв буде продовжувати збільшуватися, створюючи багато переваг, але також створюючи зростаючий ризик для безпеки. Оскільки мережі стають більш динамічними та

продовжують рости, стає все важче ідентифікувати та керувати всіма підключеними до них пристроями.

Четверта промислова революція представляє надзвичайну можливість для виробництва в цілому, однак за своєю природою вона призводить до підвищеного ризику. У недавньому звіті підкреслюється, що майже 50 відсотків виробників стали жертвами кібер-атак, а чверть зазнала певних фінансових втрат або зривів.

Зараз виробництво є третім за кількістю атак цільовим сектором, після державних та фінансових систем. Постійне оновлення системи безпеки та постійне зберігання даних про роботу підприємства є ключами до високої захищеності.

Об’єктом дослідження є хімічне підприємство, виробництво мінеральних добрив зокрема.

Предметом дослідження є система захисту хімічного підприємства.

Метою цієї роботи є компіляція українських та міжнародних досліджень безпеки хімічних підприємств, оптимізація системи захисту критичних інформаційних ресурсів, а також визначення потенційних критеріїв оптимальності оптимізації, враховуючи сектор та потребу у безпеці системи, над якою проводиться дослідження.

За темою цієї роботи було опубліковано тези на міжнародних конференціях за темами: «Оцінка ризиків в системах захисту інформації критичних ресурсів» («Дні науки», 30 березня – 7 квітня 2021р, м. Шефілд, Велика Британія) та «Контроль доступу до автоматизованої системи управління виробництвом мінеральних добрив» («Наука без кордонів», 22 – 30 березня 2021р, м. Прага, Чеська республіка).

1 ОГЛЯД ХІМІЧНОЇ ПРОМИСЛОВОСТІ

1.1 Огляд промислових систем управління

Промислова система управління (ПСУ) - загальний термін, що охоплює декілька типів систем управління, включаючи системи контролю та збору даних (SCADA), розподілені системи управління (РСУ) та інші конфігурації систем управління, такі як програмовані логічні контролери (ПЛК). у промислових секторах та критичних інфраструктурах. ПСУ складається з комбінацій елементів управління (наприклад, електричних, механічних, гідравлічних, пневматичних), які діють разом для досягнення промислових цілей (наприклад, виготовлення, транспортування речовини або енергії). Частина системи, що в першу чергу займається виробництвом продукції, називається процесом. Керуюча частина системи включає специфікацію бажаного виходу або продуктивності. Контроль може бути повністю автоматизованим або може включати в цикл людину. Системи можуть бути налаштовані на роботу з відкритим, замкненим та ручним режимами. У системах управління з відкритим циклом вихід керується встановленими налаштуваннями. У замкнутих системах управління вихід має вплив на вхід таким чином, щоб підтримувати бажану мету. У ручному режимі системою повністю керує людина. Частина системи, яка в першу чергу стосується підтримання відповідності специфікаціям, називається контролером. Типова ПСУ може містити численні цикли управління, інтерфейси людини і машини (ЛМІ) та засоби віддаленої діагностики та обслуговування, побудовані з використанням масиву мережевих протоколів. Промислові процеси управління ПСУ зазвичай використовуються в електричній, водній, нафти та природного газу, хімічній, транспортній, фармацевтичній, целюлозно-паперовій, харчовій, а також у підприємствах дискретного виробництва (наприклад, у автомобільній, аерокосмічній та довготривалій торгівлі).

ПСУ є критично важливими для роботи критично важливих інфраструктур будь-якої країни, які часто є дуже взаємопов'язаними та взаємозалежними системами. Важливо зазначити, що велика кількість підприємств критичної інфраструктури у розвинених країнах перебуває у приватній власності та експлуатації. Держава також

керує багатьма згаданими вище промисловими процесами, а також має під контролем управління повітряним рухом[3].

Цей розділ надає огляд систем SCADA, РСУ та ПЛК, включаючи типові топології та компоненти. Для полегшення розуміння цих систем представлено кілька діаграм, що зображують топологію мережі, з'єднання, компоненти та протоколи, які зазвичай знаходяться в кожній системі. Ці приклади лише намагаються ідентифікувати поняття топологічної топології. Фактичні реалізації ПСУ можуть бути гібридами, які стирають межу між системами РСУ та SCADA. Зверніть увагу, що схеми в цьому розділі не зосереджені на забезпеченні ПСУ.

1.1.1 Профіль сектору

Хімічна промисловість різноманітна, залучає різноманітні продукти та матеріали та охоплює широкий спектр різних функціональних видів діяльності. Як правило, інфраструктура хімічного сектору класифікується за функціональною сферою в галузевому ланцюжку поставок.

Ланцюг поставок хімічної промисловості охоплює діяльність, пов’язану із заготівлею сировини та проектуванням, виробництвом, збутом, розподілом, транспортуванням, підтримкою споживачів, використанням, переробкою та утилізацією хімічних продуктів. Вивчивши ланцюг поставок та послуги, що його підтримують, інфраструктуру хімічного сектору можна розділити на чотири ключові функціональні галузі:

– виробничі підприємства;
– транспортні системи;
– системи складування та зберігання, включаючи склади та зони постачання;
– кінцеві споживачі хімічних продуктів.

Хоча описи цих ключових функціональних областей в основному зосереджені на їх фізичних характеристиках та діяльності, кожна з чотирьох функціональних областей залежить від кіберсистем для різних цілей, включаючи наступні:

– управління виробничими процесами з використанням автоматизованих систем промислового управління та систем безпеки процесів;

– відстеження запасів, зберігання та переміщення хімічних продуктів;

– зберігання інформації про клієнтів, включаючи товари, які регулярно купуються, та місця, де вони зазвичай надсилаються;

– зберігання інформації про персонал для запобігання крадіжки персональних даних;

– експлуатація периметрів охоронних систем.

Гарантія добросовісності та безпеки персоналу також є важливим аспектом забезпечення кіберсистем на хімічних об'єктах. Багато компаній у цьому секторі зменшили ризик примусу чи інсайдерської загрози використовуючи політики, практики та технології, що захищають зв'язок критично важливих систем заводів із корпоративними мережами. Технологія безпечної автентифікації може використовуватися для обмеження доступу на основі ролей та дозволів, тоді як відповідні політики для припинення дії облікових записів користувачів застосовуються після припинення відносин працівника з компанією. Для останнього та для підготовки працівника для роботи використовуються програми, які, після встановлення на комп’ютер та налаштування, конфігурують обліковий запис, Wi-Fi паролі в офісі, доступ до віддалених серверів, необхідних для роботи та після припинення співпраці автоматично очищують всі дані з комп’ютера, не залишаючи колишньому працівнику можливості впливати на функціонування підприємства.

У результаті важливості кіберсистем у цьому секторі та зосереджених зусиль на кібербезпеці багато компаній намагаються поліпшити зв'язок між безпекою промислових систем управління, безпекою бізнес-систем та фізичною безпекою. Компанії все частіше включають представника з питань захисту інформаційних технологій до команди корпоративного управління кризовими ситуаціями. Інші члени групи з управління кризовими ситуаціями можуть включати представників Управління у справах громадськості, співробітників органів фізичної безпеки та представників бізнесу та фінансів[3].

1.1.2 Мета та профіль сектору

Сотні тисяч об'єктів у будь-якій країні якимось чином використовують, виготовляють, зберігають, транспортують або постачають хімічні речовини, це охоплює все від нафтопереробних заводів до фармацевтичних виробників та будівельних магазинів. Підприємства, що входять до хімічного сектору, зазвичай належать до однієї з чотирьох ключових функціональних сфер:

- виробничі заводи;
- транспортні системи;
- системи складування та зберігання;
- кінцеві споживачі хімічних речовин.

Хоча ключові функціональні сфери в першу чергу описують їх фізичні характеристики та діяльність, кожна з чотирьох функціональних областей залежить від кіберсистем для різних цілей, включаючи діючі виробничі процеси, відстеження запасів та зберігання інформації про клієнтів.

Основною метою є визначення та вжиття заходів для захисту або поліпшення стійкості інфраструктури, визначеної як критично важлива. Як одна з найстаріших галузей промисловості, хімічна промисловість має давню історію стійкості, засновану на здатності сектору адаптуватися, запобігати, готуватися і відновлюватись від усіх небезпек, включаючи стихійні лиха, коливання ринків або зміна регуляторних програм. Щоб зберегти операційну стійкість, успішний бізнес визначає свої критичні залежності та взаємозалежності та розробляє відповідні стратегії для управління зривами в критичних системах у разі їх виникнення[1].

Хімічний сектор також має довгу і добре задокументовану історію законодавства та нормативних актів, що стосуються охорони здоров'я, безпеки, запобігання нещасним випадкам, реагування на надзвичайні ситуації та навколишнього середовища. В останні роки Верховна Рада України надала спеціальні повноваження щодо норм, які зосереджуються на хімічній безпеці[38]. Хоча деякі законодавчі акти зосереджені на забезпеченні хімічних речовин під час транзиту, мабуть, найважливішим для цього сектору є законодавство, яке стосується захисту

найбільш небезпечних хімічних речовин на об'єкті, а саме Наказ про затвердження Положення про порядок підготовки та подання інформації про вантаж для його безпечного морського перевезення (2018р) [39] та Закон про хімічну безпеку (2020р) [40].

1.1.3 Виробничі підприємства

Виробничі підприємства перетворюють сировину (компоненти, що надходять до підприємства) у проміжні та кінцеві продукти (компоненти, що покидають підприємство). Можна розділити процес виробництва хімічної речовини на п’ять стадій, кожна з яких може містити одну або кілька переробних робіт:

– надходження хімічних інгредієнтів;

– тимчасова постановка на зберігання або зберігання хімічних інгредієнтів, що очікують використання у виробництві;

– переробка хімічних інгредієнтів у продукти або напівпродукти;

– тимчасове складування або зберігання хімічних продуктів, що очікують на відвантаження;

– етап доставки хімічної продукції.

Сучасне виробництво хімічних речовин є високо автоматизованим та складним. Проектування, будівництво та експлуатація цих об'єктів вимагає різноманітного досвіду для вирішення проблем безпеки, охорони здоров'я, навколишнього середовища та безпеки. Автоматизація процесів також стала інтегральною. Промислові автоматизовані системи, включаючи системи безпеки технологічних процесів, можуть бути підключені до більшої системи комп'ютерних мереж компанії, яка може мати контрольований віддалений доступ. Безпека цих систем є надзвичайно важливою для забезпечення належного відстеження, обліку та направлення хімічних речовин та продуктів після їх установки та вивезення з приміщень.

1.1.4 Еволюція промислових систем управління

Багато сучасних ПСУ еволюціонували завдяки включенню ІТ-можливостей у існуючі фізичні системи, часто замінюючи або доповнюючи фізичні механізми

управління. Наприклад, вбудовані цифрові елементи управління замінили аналогові механічні елементи керування в обертових машинах і двигунах. Зменшення вартості та покращення продуктивності сприяло еволюції, яка призвела до багатьох сучасних «розумних» технологій, таких як розумна електрична мережа, розумне транспортування, розумні будівлі та розумне виробництво. Хоча це підвищує зв’язок та критичність цих систем, це також створює більшу потребу в їх адаптивності, стійкості, безпеці та безпеці.

Розробка ПСУ продовжує розвиватися з метою надання нових можливостей, зберігаючи типово тривалий життєвий цикл цих систем. Впровадження IT-можливостей у фізичні системи представляє нову поведінку, яка має наслідки для безпеки. Інженерні моделі та аналіз розвиваються для вирішення цих нових вразливостей, включаючи взаємозалежність безпеки, конфіденційності та впливу на навколишнє середовище.

1.1.5 Критичні інфраструктурні взаємозалежності

Критичну інфраструктуру часто називають «системою систем» через взаємозалежність, що існує між різними галузями промисловості, а також взаємозв'язки між діловими партнерами. Критичні інфраструктури дуже взаємопов'язані та взаємозалежні складними способами як фізично, так і за допомогою безлічі інформаційно-комунікаційних технологій. Інцидент в одній інфраструктурі може прямо і опосередковано впливати на інші інфраструктури через каскадні та ескалаційні збої [3].

Обидві галузі передачі та розподілу електроенергії використовують географічно розподілену технологію управління SCADA для роботи високо взаємозв’язаних та динамічних систем, що складаються з тисяч державних та приватних комунальних підприємств та сільських кооперативів для постачання електроенергії кінцевим споживачам. Деякі системи SCADA контролюють розподіл електроенергії, збираючи дані та віддаючи команди географічно віддаленим польовим станціям управління з централізованого місця. Системи SCADA також використовуються для моніторингу та контролю розподілу води, нафти та

природного газу, включаючи трубопроводи, судна, вантажівки та залізничні системи, а також системи збору стічних вод.

Системи SCADA та РСУ часто об'єднані в мережі. Це стосується центрів управління електроенергією та об'єктів з виробництва електроенергії. Незважаючи на те, що функціонування об'єкта з виробництва електроенергії контролюється системою РСУ, система РСУ повинна взаємодіяти із системою SCADA для координації випуску продукції з вимогами до передачі та розподілу.

Електроенергія часто вважається одним із найпоширеніших джерел порушень взаємозалежних критичних інфраструктур. Як приклад, каскадна відмова може бути ініційована порушенням мікрохвильової мережі зв'язку, що використовується для системи передачі електроенергії SCADA. Відсутність можливостей моніторингу та управління може призвести до вимкнення великого енергоблоку в автономному режимі, що призведе до втрати потужності на підстанції передачі. Ця втрата може спричинити серйозний дисбаланс, що спричинить каскадний збій в електромережі. Це може призвести до відключень на великих площах, що потенційно може вплинути на видобуток нафти та природного газу, експлуатацію нафтопереробних заводів, системи очищення води, системи збору стічних вод та трубопровідних транспортних систем, які покладаються на електромережу[3].

1.1.6 Взаємозалежності з іншими секторами

Багато активів, систем та мереж для підтримки функціональності залежать від елементів інших активів, систем та мереж. У деяких випадках відмова в одному секторі матиме значний вплив на здатність іншого сектора виконувати необхідні функції. Опора на інший сектор для функціональності називається залежністю (Рисунок 1.1). Якщо дві частини інфраструктури залежать одна від одної, то вони взаємозалежні. Надзвичайно важливо виявити залежності та взаємозалежності як на рівні сектору, так і на рівні активів, системи чи мережі, щоб повністю зрозуміти наслідки зриву або нападу на частину інфраструктури. Ця інформація також допомагає визначити, яким чином порушення роботи чи атака на іншу інфраструктуру можуть вплинути на взаємозалежний актив, систему чи мережу.

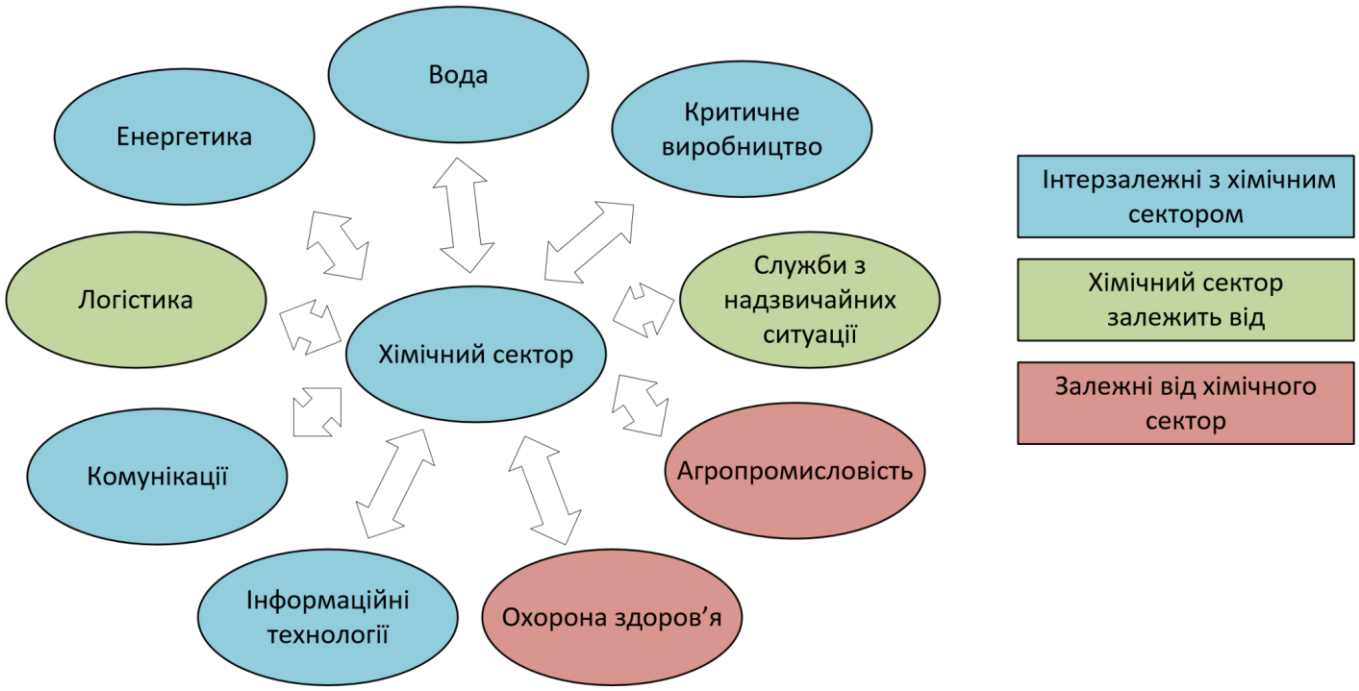

Рисунок 1.1 - Залежності між секторами

Хімічний сектор залежить від багатьох інших секторів, щоб підтримувати повну функціональність. Наприклад, технологічні рішення від секторів інформаційних технологій (IT) та комунікацій відіграють життєво важливу роль у підтримці продуктивності, функціонування та комунікації через усі аспекти ланцюга поставок хімічної промисловості. Цей сектор також сильно залежить від залізничних, автотранспортних та трубопровідних послуг для безпечного транспортування своєї продукції споживачам, які її потребують. І навпаки, багато галузей залежать від хімічного сектору. Наприклад, хлор має вирішальне значення у фармацевтичному виробництві, а також при очищенні питної води, а вибухові речовини мають важливе значення для видобутку вугілля для виробництва енергії. Крім того, пестициди, добрива та консерванти допомагають забезпечити безпечне та рясне продовольче забезпечення[5].

Хімічний сектор також накладається на різні сектори критичної інфраструктури та ключових ресурсів (КІКР) [1]. Наприклад, фармацевтичних виробників можна вважати частиною хімічного сектору, так і сектором охорони здоров'я та охорони здоров'я. Подібним чином нафтохімічні нафтопереробні заводи є частиною як хімічного, так і енергетичного секторів.

1.1.7 Робота та компоненти ПСУ

Типова ПСУ містить численні цикли управління, людські інтерфейси та засоби віддаленої діагностики та обслуговування, побудовані з використанням масиву мережевих протоколів на багатошарових мережевих архітектурах. Контур управління використовує датчики, виконавчі механізми та контролери (наприклад, ПЛК) для маніпулювання деяким контрольованим процесом. Датчик - це пристрій, який виконує вимірювання деяких фізичних властивостей, а потім надсилає цю інформацію як контрольні змінні контролеру. Контролер інтерпретує сигнали та генерує відповідні маніпулятивні сигнали на основі алгоритму управління та цільових заданих значень, які потім передаються виконавчим механізмам. Такі виконавчі механізми, як регулюючі клапани, вимикачі, вимикачі та двигуни, використовуються для безпосереднього керування керованим процесом на основі команд контролера.

Оператори та інженери використовують інтерфейси людини для моніторингу та налаштування заданих значень, алгоритмів управління, а також для налаштування та встановлення параметрів в контролері. Інтерфейс людини також відображає інформацію про стан процесу та історичну інформацію. Службові програми діагностики та обслуговування використовуються для запобігання, виявлення та відновлення після ненормальної роботи або збоїв.

Іноді ці цикли управління є вкладеними та / або каскадними - при цьому задана точка для одного циклу базується на змінній процесу, визначеній іншим циклом. Цикли контрольного рівня та цикли нижчого рівня працюють безперервно протягом усього процесу з часом циклу від кількох мілісекунд до хвилин[2].

1.1.8 Цифрові загрози для хімічного сектору

Інформаційні технології є найважливішим компонентом повсякденної роботи хімічної установки, включаючи бізнес-системи та системи управління процесами. Хоча компанії в хімічному секторі все частіше прагнуть підвищити ефективність, з'єднавши свої системи фізичної безпеки, інформації та управління процесами, зближення між системами є головною проблемою, оскільки створює можливості

отримання доступу до цих систем для потенційних кібер-супротивників. Крім того, системи управління процесами змінюються таким чином, що надаються переваги операторам систем, але також стають більш вразливими до кібератак. Зокрема, власні пристрої в цих системах замінюються більш дешевими та широкодоступними пристроями, які використовують традиційні мережеві протоколи, включаючи ті, що підтримують віддалений доступ. Можливості віддаленого доступу в пристроях можуть полегшити їх обслуговування. Крім того, системи управління процесами розробляються та впроваджуються з використанням традиційних комп'ютерних та операційних систем, що дозволяє їм легше підключатися до корпоративних бізнес-систем, що підтримують продаж, передачу або розподіл хімічних речовин. Наприклад, зловмисні актори національних держав використовували електронні листи зі списовим фішингом для розгортання шкідливого програмного забезпечення на мережах бізнес-інформаційних технологій (IT) під час нападу на українські комунальні підприємства 2015 року [3]. Отримавши початковий доступ до ділових IT-мереж, зловмисники, як повідомляється, використовували різноманітні методи для доступу до мереж промислових систем управління комунальних підприємств.

Існує декілька типів ризиків для інформації про хімічні споруди та систем управління процесами, включаючи неефективний захист кібер-активів, навмисні або ненавмисні загрози:

– неефективний захист кібер-активів може збільшити ймовірність інцидентів безпеки та кібератак, які порушують критичні операції; призвести до неналежного доступу та розкриття, модифікації або знищення конфіденційної інформації; та загрожують національній безпеці, економічному добробуту та охороні здоров'я. Ненавмисні або несуперечливі джерела загроз можуть включати несправності обладнання або програмного забезпечення через старіння; вичерпання ресурсів; та помилки, допущені кінцевими користувачами. Вони також включають стихійні лиха та відмови критичної інфраструктури, від якої залежить організація, але які не підконтрольні організації;

– умисні або ненавмисні загрози можуть включати корумпованих співробітників, злочинні угруповання, терористів та країни, які прагнуть використати

залежність організації від кіберресурсів (тобто інформації в електронній формі, інформаційно-комунікаційних технологій та засобів зв'язку та обробки інформації). Ці супротивники відрізняються за своїми можливостями; готовність діяти; та мотивами, які можуть включати пошук грошової вигоди або досягнення економічної, політичної чи військової вигоди;

– зловмисники можуть використовувати різні техніки, тактики або практики, щоб негативно вплинути на комп’ютери, програмне забезпечення чи мережі організації або перехопити або викрасти цінну або конфіденційну інформацію. Ці вразливості використовуються за допомогою різних каналів, включаючи веб-сайти, електронну пошту, бездротовий та стільниковий зв'язок, Інтернет-протоколи, портативні медіа та соціальні медіа. Крім того, супротивники можуть використовувати загальноприйняті комп'ютерні програми, такі як Adobe Acrobat® та Microsoft Office®, щоб доставити загрозу шляхом вбудовування експлойтів у файли програмного забезпечення, які можна активувати, коли користувач відкриває файл у відповідній програмі[3]. Крім того, супротивники кіберзагроз можуть проникнути в систему управління інформацією та процесами через Інтернет або інший шлях зв'язку, щоб потенційно порушити його діяльність та спричинити розливи, викиди, вибухи або пожежі. Більше того, системи управління процесами, які колись були у своїй більшості ізольовані від Інтернету та систем інформаційних технологій організації, дедалі частіше підключаються до сучасних хімічних установок, що дозволяє кібератакам зароджуватися в бізнес-системах і мігрувати до операційних систем. Рисунок 1.2 показує потенційні кіберзагрози об'єктам, що охоплюються АТСХФ.

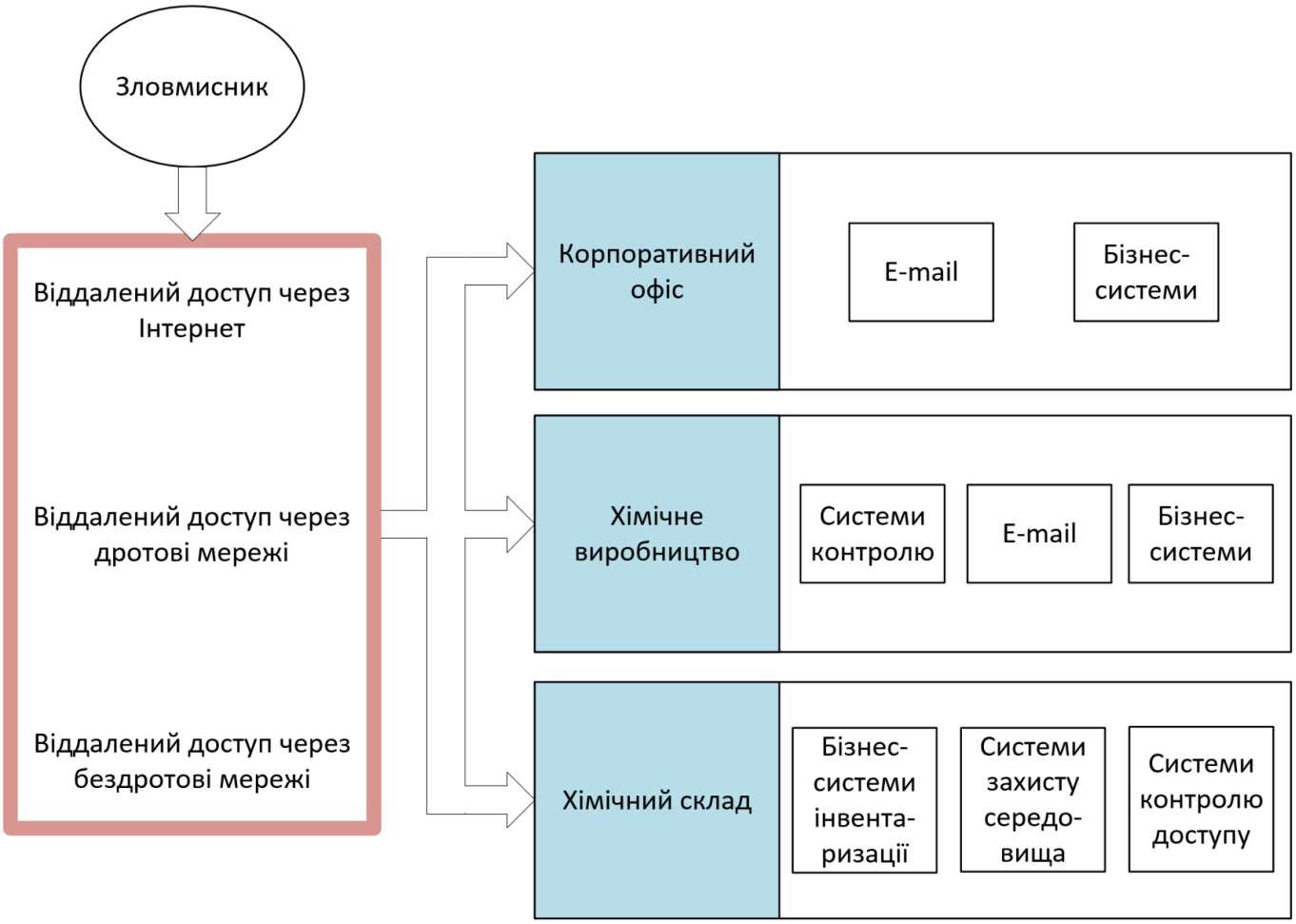

Рисунок 1.2 - Потенційні кіберзагрози

Звіти про відомі та успішно виконані атаки, пов'язані з кібербезпекою, ілюструють наслідки, які можуть мати ці атаки на інформацію та системи управління процесами. У 2018 році зловмисні актори національних держав застосували підводний фішинг та інші подібні підходи проти організацій, щоб отримати доступ до їх мереж та бізнес-систем, проводити розвідку та збирати та маніпулювати інформацією про свою систему промислового контролю [3]. Шкідливий актор, який отримує доступ до інформаційної системи, підключеної до системи управління процесом, потенційно може отримати доступ до системи управління процесом. Завдяки такому доступу актор може спричинити зупинку роботи або фізичне знищення виробництва, змінивши налаштування датчика або маніпулюючи повідомленнями, переданими системі управління процесом, і змусивши контролери вносити невідповідні зміни.

1.1.9 Придатність кібербезпеки у хімічному секторі

Існує безліч ризиків, пов'язаних з традиційною інформацією, IT-активами, системами виробництва та контролю, діловими партнерами, спільними підприємствами. Ризики також пов'язані з низкою інших ділових домовленостей, які дедалі більше переважають у хімічному секторі. Ризики для традиційних IT-активів зосереджуються на конфіденційності, цілісності та доступності інформації. Ризики у виробництві та системах управління різні, оскільки перші більше зосереджуються на безпеці та надійності експлуатації ніж на захисті конфіденційності, цілісності та доступності інформації. Ризики, пов’язані із залученням аутсорсингу, сторонніми підрядниками або іншими партнерами в ланцюжку вироблення продукції хімічного сектору, включають конфіденційну інформацію, що передається, зберігається або обробляється. Інтеграція цих ділових партнерів у діяльність компанії потенційно дозволяє ненавмисний доступ до систем компанії.

Дуже важливо встановити та зрозуміти ціннісну пропозицію, пов’язану з IT-ресурсами та інвестиціями компанії. Створення системи управління кібербезпекою (СУКБ) вимагає розуміння ролі, яку IT відіграють у бізнесі компанії. Ключовим у СУКБ є необхідність визначити толерантність компанії до ризиків та переваги СУКБ, яка визначає потенційні ризики кібербезпеки, наслідки та засоби контролю та встановлює процес для впровадження, експлуатації, моніторингу, перегляду, підтримання та вдосконалення кібербезпеки.

1.2 Управління ризиком

Організації керують ризиками щодня, досягаючи своїх бізнес-цілей. Ці ризики можуть включати фінансовий ризик, ризик виходу з ладу обладнання та ризик безпеки персоналу, якщо назвати лише декілька. Організації повинні розробляти процеси для оцінки ризиків, пов’язаних із їх бізнесом, і вирішувати, як боротися з цими ризиками, виходячи з організаційних пріоритетів та внутрішніх та зовнішніх обмежень. Це управління ризиками проводиться як інтерактивний, постійний процес як частина звичайних операцій. Організації, які використовують ПСУ, історично

управляли ризиками завдяки передовій практиці безпеки та техніки. Оцінки безпеки добре зарекомендували себе в більшості секторів і часто включаються до нормативних вимог. Управління ризиками інформаційної безпеки - це додатковий вимір, який може доповнювати один одного. Процес та рамки управління ризиками, викладені в цьому розділі, можуть застосовуватися для будь-якої оцінки ризику, включаючи як фізичну, так і інформаційну безпеку.

Процес управління ризиками слід застосовувати в організації, використовуючи трирівневий підхід для вирішення ризиків на:

- рівні організації;
- рівень місії / бізнес-процесу;
- рівень інформаційної системи (ІТ та ПСУ).

Процес управління ризиками здійснюється безперебійно на трьох рівнях із загальною метою постійного вдосконалення діяльності організації, пов'язаної з ризиками, та ефективного міжрівневого та внутрішньорівневого спілкування між усіма зацікавленими сторонами, що мають спільний інтерес до успіху організації.

Цей розділ зосереджений насамперед на командах ПСУ на рівні інформаційної системи, однак важливо зазначити, що діяльність з управління ризиками, інформація та артефакти на кожному рівні впливають та інформують інші рівні. Далі будуть представлені концепції контролю та надані спеціальні рекомендації для ПСУ для розширення контролю, будуть висвітлюватися рекомендації для дизайну ПСУ та їх вплив на процес управління ризиками.

1.2.1 Потенційний фізичний вплив аварії

Оцінка потенційного фізичного збитку в результаті кібер-інциденту повинна включати:

- те, як інцидент може маніпулювати роботою датчиків та виконавчих механізмів для впливу на фізичне середовище;
- які надмірні засоби контролю існують в ПСУ для запобігання впливу;
- як може виникнути фізичний інцидент на основі цих умов.

Фізичний вплив аварії може негативно впливати на навколишній світ різними способами, включаючи викид небезпечних матеріалів (наприклад забруднення сирою нафтою), пошкодження внаслідок кінетичного впливу (наприклад вибухи) та впливу збурень джерел енергії (наприклад подавання надвисокої напруги в домашні електричні мережі). Фізичний інцидент може негативно вплинути на ПСУ та допоміжну інфраструктуру, різні процеси, що виконуються ПСУ, або на середовище. Оцінка потенційних фізичних впливів повинна включати всі частини ПСУ, починаючи з оцінки потенційних впливів на набір датчиків та виконавчих механізмів. Кожен із цих доменів буде додатково вивчений далі[6].

Оцінюючи вплив інциденту на фізичне середовище, слід зосередити увагу на потенційному збитку для безпеки людини, природного середовища та інших важливих інфраструктур. Вплив на безпеку людини слід оцінювати, виходячи з того, чи можливі травми, хвороби або смерть від несправності ПСУ. Це повинно включати будь-які попередньо проведені оцінки впливу на безпеку, проведені організацією щодо працівників та широкої громадськості. Можливо, також доведеться розглянути вплив на довкілля. Цей аналіз повинен включати будь-які наявні оцінки впливу на навколишнє середовище, що проводяться організацією, щоб визначити, як інцидент може вплинути на природні ресурси та дику природу протягом короткої або довгострокової перспективи. Крім того, слід зазначити, що ПСУ може не знаходитись в одному контрольованому місці і може розподілятися по широкій фізичній площі та піддаватися неконтрольованому середовищу. Нарешті, вплив на фізичне середовище повинен дослідити, якою мірою інцидент може пошкодити інфраструктури зовнішні до ПСУ (наприклад, виробництво/доставка електроенергії, транспортна інфраструктура та послуги з водопостачання).

1.2.2 Покращення підходів до визначення ризиків

Для проведення оцінки ризиків екзогенних хімічних речовин, для яких також існує ендогенна експозиція, знання хімії та біології обох типів експозиції необхідно інтегрувати у формулювання проблеми та переносити до характеристики ризиків. Це питання оформлено в контексті оцінки ризику, підкреслюючи важливість кількісного

визначення приростів дози з усіх джерел однакових або подібних хімічних речовин, що взаємодіють з біологічними цілями; розуміння впливу ендогенних хімічних концентрацій на ризик захворювання; та оцінки загальної дози до цільових показників при оцінці ризику приросту впливу на навколишнє середовище. Приклади нещодавніх оцінок ілюструють важливість вирішення цього питання. Оцінка даних про концентрацію аміаку, метанолу, формальдегіду, ацетальдегіду та трьох газоподібних сигнальних молекул у крові або органах (сульфід водню, оксид вуглецю та оксид азоту) наводить приклади, коли поточні дані вже інформують про перспективи відносного впливу на організм людини. Для полегшення оцінки ризиків якості екзогенних хімічних речовин з ендогенною експозицією представлено низку конкретних питань, які необхідно розглянути в систематичному огляді для вдосконалення формулювання проблем, вдосконалення розробки цілісних концептуальних моделей та сприяння визначенню пріоритетних потреб у даних для вдосконалення оцінок ризиків.

Протягом останніх двох десятиліть оцінка ризику намагалася вирішити проблему «чорної скриньки» між впливом та наслідками для здоров'я за допомогою вдосконаленої токсикокінетики, розуміння способу дії та застосування системних підходів. Хоча важливість вирішення проблем фонових та хімічних речовин, що виробляються ендогенним шляхом, стає все більш очевидною, оцінка ризиків для екзогенних хімічних речовин з ендогенною експозицією продовжує залишатися проблемою для оцінювачів ризиків, а також для тих, хто приймає рішення щодо управління ризиками[1].

Отже, існує потреба у розробці корисних консенсусних підходів до послідовного роботи в процесі оцінки ризику, щоб заохотити розробку даних та моделей, щоб екзогенний вплив ендогенних або фонових хімічних речовин в контексті став невід’ємною частиною. частину оцінки ризику та систематично переглядати ендогенні або фонові хімікати з екзогенним впливом.

1.2.3 Використання оцінки ризику в секторі

Хімічний сектор має багаторічну історію та великий досвід розробки та застосування різних методологій та інструментів для оцінки ризику підприємства та визначення пріоритетів активів. Такі методології були розроблені різними галузевими партнерами, включаючи професійні галузеві торгові асоціації, національні дослідницькі лабораторії та окремі хімічні компанії. Протягом декількох десятиліть власники об'єктів та оператори зобов'язані проводити оцінку ризиків своїх об'єктів, оскільки вони стосуються питань безпеки, безпеки процесів та екологічних питань. Оцінки необхідні, щоб гарантувати, що базові заходи безпеки та охорони навколишнього середовища застосовуються в місцях, де використовуються костюми хімічного захисту на критичних територіях. Під керівництвом державних агентств та нормативних вимог, приватний сектор використовує різні процеси та термінології для визначення ризику.

Сектор також активно сприяє численним добровільним зусиллям з оцінки вразливості та ризику фізичної та кіберінфраструктури. Ці зусилля включають зусилля, очолювані галузевими асоціаціями, багато з яких підтримують та просувають оцінки вразливості до безпеки як частину своїх вказівок щодо безпеки для компаній-членів. Керівництво з питань безпеки також надає членам асоціації інформацію про найкращі галузеві практики для покращення загальної фізичної безпеки та кібербезпеки.

Зусилля для оцінки ризиків у цьому секторі включають також партнерські відносини між власниками та операторами активів, галузевими асоціаціями та урядом. Одним із таких зусиль є Стратегічна оцінка ризику розвитку інфраструктури країни (СОРРІК) [6]. СОРРІК надає керівникам, які приймають рішення, секторну та міжгалузеву оцінку різних ризиків для національних секторів.

Оцінка - це модель, яка оцінює загрозу від конкретних методів атаки, вразливість до методів атаки та наслідки найбільш імовірної, найгіршої атаки. Оцінюються фізичні та кібератаки, здійснені терористами, національними

державами, зловмисними інсайдерами та нападниками-одиночками, а також стихійні лиха.

Протислужби з хімічної безпеки просять власників та операторів визначити ті сценарії фізичної та кіберзагрози, які найбільше хвилюють хімічний сектор. Партнери сектору надають інформацію про вразливість та наслідки для цих сценаріїв, яка є специфічною для хімічного сектору. Потім ця інформація поєднується з інформацією про загрози з усього розвідувального співтовариства, щоб створити секторний профіль ризику з метою виявлення сценаріїв найвищого ризику для цього сектору.

1.2.4 Оцінка ризику

Кінцевою змінною в рівнянні ризику є загроза. З метою розрахунку ризику загроза навмисної небезпеки, як правило, оцінюється як ймовірність нападу на основі наміру та можливостей супротивника; для інших небезпек загроза, як правило, оцінюється як ймовірність виникнення небезпеки.

Більшість власників активів та операторів повинні покладатися на висновки загроз від Державної служби з надзвичайних ситуацій (ДСНС), щоб точно розрахувати ризик, пов'язаний з конкретним активом. Щоб допомогти у визначенні загрози та ризику, галузеві установи співпрацюють з ДСНС та створюють якнайбільш оновлені та повні списки загроз для якомога більшої кількості галузей виробництва.

На менш небезпечному рівні кібератаки можуть спричинити витік конфіденційних даних або інформації про клієнта або мимовільне порушення стандартів безпеки та довкілля. Хоча і менш шкідливі, подібні атаки все одно можуть означати закриття об'єкта через відсутність довіри споживачів або порушення правил, настільки ж легко, як і вибух або витік.

Дослідження показали, що деякі небезпеки виникають у багатьох об'єктах, що мають суміш старого та нового обладнання, з поступовими модифікаціями, і не завжди з оглядом того, як зміни, внесені в одній області, впливають на інші. Отримати огляд усього обладнання на об'єкті та способу його з'єднання з усім іншим може бути величезною проблемою, якщо це ще ніколи не проводилося комплексно. Якщо програмне забезпечення для управління потенційно знаходиться у висувних ящиках

столів, пожежних сейфах та за межами місця зберігання, а неоднакові системні знання зберігаються різними електронними чи паперовими методами, а то й зовсім відсутні, відповідь на кібератаку належним чином та своєчасно стає майже неможливою[2].

Масштаби проблеми величезні, а хімічна промисловість несе в собі унікальну небезпеку. Наприклад, тільки у США понад 3000 об'єктів вважаються такими, що мають «високий ризик», а це означає, що вони використовують принаймні одну «хімічну речовину, що представляє інтерес», сюди входять токсичні, вибухові та інші сполуки, які можуть перетворитись у зброю[1].

1.2.5 Методологія управління ризиком

Три найбільш важливі частини програми корпоративної безпеки - це люди, процеси та технології (Рисунок 1.3). Якщо ваша програма захисту не враховує всі три частини, вона не вдасться. Відсутність однієї ніжки на 3-ніжному табуреті призведе до його падіння!

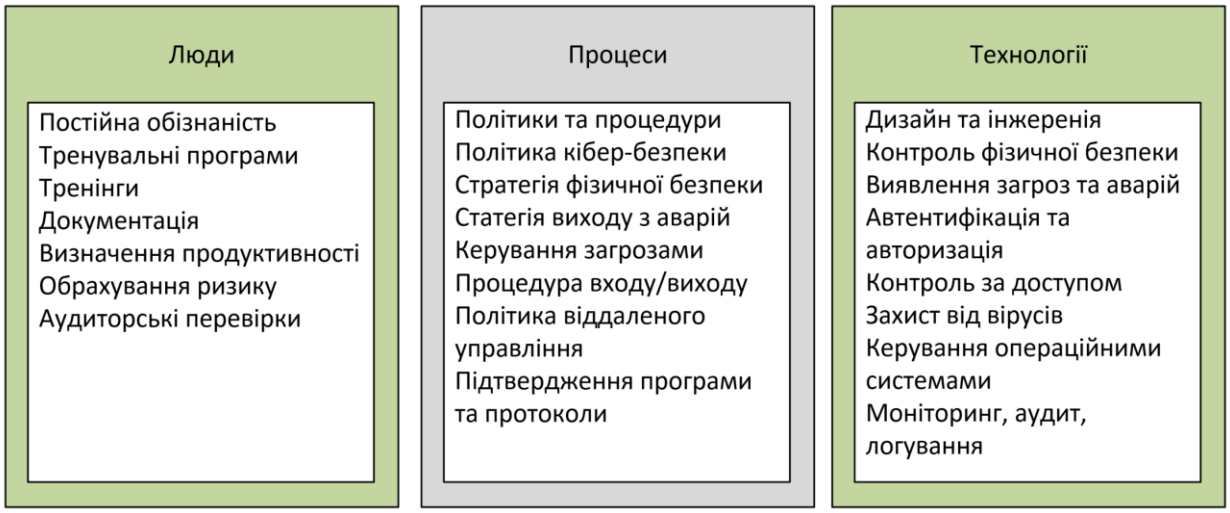

Рисунок 1.3 - Частини програми корпоративної безпеки

Коли більшість людей замислюються про кібербезпеку, відразу на думку спадають такі технології, як брандмауери та антивірусні програми. Поширене непорозуміння, що брандмауер та антивірусне програмне забезпечення захищатимуть системи. Минулий досвід та кілька перевірок виявили, що більшість брандмауерів погано налаштовані та відкриті для багатьох серйозних загроз. Важливо не тільки

правильно встановити брандмауери, але також врахувати інші критичні системи, наприклад резервне копіювання та відновлення. Важливо підготуватися до інциденту та забезпечити швидке відновлення критичних систем. Технологія є основою безпеки, і для цього необхідно встановити відповідні системи. Компанії повинні забезпечити належні брандмауери, антивірус, управління виправленнями, резервне копіювання стрічки, віддалений доступ, автентифікацію та фізичну безпеку. В ході минулого аудиту у великій гірничодобувній організації у Східній Канаді головна американська міжнародна корпорація, що виробляє зброю, космічні системи, автоматичні й контролюючі системи, іженерні послуги, транспортаційні системи Honeywell виявила велику кількість технічних недоліків, які могли б ефективно зупинити їх виробництво [4]. В ході чергового аудиту в компанії з південно-західної гірничодобувної компанії, аудиторська компанія допомогла їм усвідомити ризик безпеки, оскільки їх система управління ділиться з бізнес-мережею.

Коли ми говоримо про людей у контексті безпеки, це стосується працівників, підрядників та будь-якого відвідувача організації. Люди є найбільшим ризиком для безпеки. Для того, щоб програма безпеки була успішною, учасникам та зацікавленим сторонам необхідно мати необхідну обізнаність, навчання, документацію та ролі. Кожен повинен розуміти відповідне використання системи і чому це важливо, а технічні працівники також повинні знати, як визначити та вирішити ризики безпеки. З організаційної точки зору рекомендується мати спеціальну групу безпеки з повноваженнями та підтримкою виконавчої влади для примушення порушень безпеки. Але важливіше мати програму підвищення обізнаності щодо безпеки, щоб співробітники могли поділитися важливістю безпеки та тим, як вони можуть брати участь. Організації повинні зосереджуватися на своїх людях, бо політики безпеки не будуть виконуватись, персонал не розумітиме питань безпеки, а технічний персонал не буде ефективно керувати системами. З досвіду аудиторських перевірок, як правило, часто знаходяться потужні програми корпоративної безпеки, але рідко коли знаходяться організації, які активно включають працівників їхніх виробничих систем у свої навчальні програми та програми підвищення обізнаності щодо кібербезпеки.

Третім аспектом безпеки є процес. Коли обговорюється в контексті безпеки, процес стосується політики, процедур та планів дій. Ефективне планування та процеси мінімізують вплив інциденту. Незалежно від того, наскільки ви стараєтесь, завжди існуватимуть залишкові ризики безпеки та потенційні випадки. Міра готовності та обґрунтованості програми безпеки визначатиме, як добре інцидент буде стриманий і як швидко підприємство від нього оговтається. Необхідно мати на місці такі документи, як відповідна політика використання, політика резервного копіювання та політика бездротового зв'язку, щоб визначити як слід використовувати та розгортати активи компанії. Політика визначає правила користування системою; визначає процедури протидії потенційним ризикам безпеки та будь-які найкращі практики. Процедури - це покрокові вказівки щодо того, як виконати план, не будучи експертом системи. Як хороші програми безпеки, так і політики та процедури необхідні. Процеси або процедури також мають життєво важливе значення для окреслення загальної ментальності безпеки та підходу, який бажає реалізувати організація. У міру розвитку бізнесу змінюватиметься і оточення. Маючи чітко визначені очікування щодо майбутніх програм та додатків, бізнес може розвиватись, зберігаючи при цьому максимально високий рівень безпеки.

Підводячи підсумок, безпека повинна бути зосереджена на людях, процесах та технологіях, щоб бути ефективною. Недолік у будь-якій із цих областей суттєво послабить зусилля компанії, і врешті-решт програма безпеки провалиться. Honeywell створив план управління безпекою, як окреслення найважливіших частин програми безпеки [4]. Це допомагає візуалізувати вимоги промислової безпеки та забезпечити наявність попередньої кадрової роботи.

1.2.6 Програми зменшення ризику

Хімічний сектор відповідає вимогам Програми метрик національного плану захисту інфраструктури у США (NIPP), визначаючи заходи щодо зменшення ризиків ЗЗР та відбираючи ті види діяльності, які є ключовими для зменшення ризиків у цьому секторі. Потім розробляються метрики для вимірювання прогресу визначених ключових ЗЗР. У цьому розділі секторного плану описуються процеси, які сектор

використовує для розробки ЗЗР, які є результатом захисних програм та стратегій стійкості.

ЗЗР, як визначено NIPP, - це програма, інструмент, ініціатива, проект, основне завдання або якесь інше завдання, яке прямо чи опосередковано призводить до зменшення ризику.

У 2009 р. Хімічний сектор посилався на понад 60 ЗЗР у хімічному секторі, представляючи окремі програми, заходи або інструменти. Сектор передбачає, що перелік ЗЗР буде розширюватися з часом, оскільки мережа партнерів та знання існуючих програм у приватному секторі, наукових колах та уряді на державному, місцевому та територіальному рівнях зростатиме[1].

Усі секторні ЗЗР є життєво важливими зусиллями, що підтримують цілі та завдання сектору; У 2009 р. 11 заходів було визначено ключовими. Перелік ключових ЗЗР може змінюватися щороку відповідно до процесу встановлення пріоритетів. Ключові ЗЗР визначаються на основі сфери застосування їх потенційного впливу (кількість об'єктів, що зазнали впливу з точки зору безпеки та/або кількість людей/установ, які можуть зайнятися певною діяльністю) та цілеспрямована увага до зменшення конкретних ризиків, визначених у профілі хімічного сектору. Здатність ЗЗР зменшувати ризик у закладах з високим ризиком, сприяти обміну інформацією в усьому секторі та підвищувати обізнаність щодо питань кібербезпеки також враховується у процесі визначення пріоритетів.

1.3 Фізична безпека промислових об’єктів

Одним з головних пріоритетів будь-якої виробничої операції є безпека - не тільки безпека працівників заводу, а й людей, що живуть в оточуючій громаді. Подібно до того, як практика та обладнання безпеки повинні розвиватися, щоб реагувати на зміни умов праці та правил, світ промислової безпеки змінюється у відповідь на зростаючі глобальні загрози. Сьогодні компанії мають нагальну потребу вдосконалити загальну практику безпеки та системи захисту інтелектуальних та фізичних активів. З фізичної точки зору, користувачам потрібне рішення, яке інтегрує безліч технологій безпеки. Це полегшує автоматизовані процеси, що дають

можливість стримувати, виявляти, затримувати, заперечувати та захищати - і таким чином запобігати та пом'якшувати широкий спектр потенційних небезпек.

Промислові об'єкти будь-якого розміру можуть використовувати потужність автоматизації, щоб відповідати чинним законодавчим вимогам, одночасно підвищуючи рівень безпеки та оптимізуючи свою довгострокову модель безпеки.

1.3.1 Передумови

Промисловий сектор стикається з реальними проблемами, оскільки технології завжди прогресують, досвідчені фахівці виходять на пенсію, а ділове середовище нової світової економіки вимагає все більших конкурентних вимог. У той же час, моральні, нормативні та страхові вимоги повинні виконуватися з точки зору збереження безпечного та надійного робочого місця.

Традиційно промислові фірми орієнтувались на безпеку та продуктивність. Однак нещодавні загрози критичній інфраструктурі спричинили посилення заходів безпеки. Зниження вразливості систем автоматизації заводів та інших важливих активів необхідно для забезпечення безпеки, надійності, цілісності та доступності цих систем.

Небезпеки у світі після 11 вересня стимулювали промислові та державні ініціативи, спрямовані на підвищення безпеки промислових об'єктів у спосіб, що відповідає нетрадиційним сценаріям загрози. Як і у випадку з кібербезпекою, основною концепцією фізичної безпеки є виявлення вразливостей та запобігання вторгненню. Незважаючи на те, що це втручання іншого типу, наслідки ненадання належного захисту можуть бути згубними[1].

Загальні ризики промислової безпеки включають загрози на робочому місці, насильство, крадіжки, підробку, саботаж, терористичні атаки, вторгнення, зриви активістів, вандалізм та забруднення. Багато виробничих потужностей є досить доступними, а рівень обізнаності працівників щодо безпеки часто відсутній або слабкий.

Крадіжка є особливо важливою проблемою під час нових проектів чи розширення підприємств. У звіті Національного бюро з питань злочинності за 2011

рік зазначається, що в США від крадіжки будівельного обладнання та інших цінних матеріалів втрачається від 300 до 1 мільярда доларів на рік [2].

Навіть найжорсткіший захист периметра установи, хоча і важливий, не може забезпечити захист від націленої атаки. Тому компаніям потрібно впроваджувати нові та інноваційні рішення, що охоплюють всю сферу вимог фізичної безпеки.

1.3.2 Важливість та актуальність рішень фізичної безпеки

Виробнича та складська промисловість стикається з підвищеними бізнес-ризиками, які, як правило, потребують ресурсів, з точки зору витрат, обладнання та персоналу. На додаток до забезпечення безпеки працівників, роботодавці повинні захищати дорогий інвентар та обладнання від неправильного використання, крадіжок, небезпеки для навколишнього середовища та контролю якості. Хоча технологія не є єдиним рішенням для зменшення комерційних ризиків, вона є ефективним інструментом в руках досвіду керівників для забезпечення безпеки.

Фізична безпека - це захист персоналу, обладнання та даних від фізичних обставин та подій, які можуть спричинити серйозні втрати або збитки в повсякденній діяльності виробничої та складської промисловості. Це включає захист від пожежі, стихійних лих, крадіжок (внутрішніх та зовнішніх), вандалізму, переслідування та насильства на робочому місці.

Фізичну безпеку часто ігнорують (або її значення недооцінюють) на користь більш високотехнологічних та драматичних питань, таких як хакерство, віруси, троянські програми та шпигунські програми. Однак порушення фізичної безпеки може бути здійснено з незначними або відсутніми технічними знаннями з боку зловмисника. Більше того, аварії та стихійні лиха є частиною повсякденного життя, і в довгостроковій перспективі неминучі.

Складові фізичної безпеки детальніше зображені на Рисунок 1.4 нижче.

Рисунок 1.4 - Складові фізичної безпеки

Є три основні компоненти фізичної безпеки. По-перше, перешкоди на шляху потенційних зловмисників та самі місця виробництва можуть бути укріплені від аварій та екологічних катастроф. Ці перешкоди включають такі системи контролю доступу, як шлюзи, огородження, стіни, протипожежні сейфи та спринклери для води. По-друге, системи спостереження та сповіщення, такі як освітлення, датчики тепла, датчики диму, сповіщувачі вторгнень, сигналізація та відеоспостереження, надають інформацію про події, що допомагає швидше оговтатися від аварій, пожеж чи стихійних лих.

1.3.3 Боротьба з кібер-атаками

Існуючий фізичний захист хімічного об'єкта, огорожі з сітки, двері, які автоматично зачиняються, та камери безпеки можна вважати частиною захисту від кібератаки, оскільки взаємозв'язок між фізичною безпекою та кібербезпекою дуже

взаємопов'язаний. Один захищає інший, і, наприклад, без замку на дверях серверної кімнати найкраща у світі кібербезпека стає ні до чого.

Недостатньо захистити лише одну частину об’єкта, оскільки оборонна стратегія настільки сильна, наскільки найслабша її ланка. Життєво важливо розуміти потенційні ризики, а також як їх запобігти чи контролювати, а також створити політику та процеси, що відповідають вимогам конкретних областей.

Система багаторазового виявлення та попереджувальні заходи із рівнями захисту, які доповнюють один одного, забезпечуючи глибоку оборону, і чіткими планами та непередбачуваними ситуаціями, що підвищує стійкість до кібератак - мета гарного плану кібербезпеки, незалежно від галузі.

Все це може зайняти багато часу та грошей, але є кілька швидких виграшів, таких як отримання, зберігання та регулярне тестування резервних копій як частини плану відновлення після катастрофи.

У будь-якому об'єкті, який використовує мережі та керовану комп'ютером техніку, кібербезпека повинна стати стандартною проблемою на будь-якій зустрічі стратегії управління ризиками.

2 ВИЗНАЧЕННЯ РИЗИКІВ ТА БОРОТЬБА З ЗАГРОЗАМИ

2.1 Спільний підхід

Щоб вирішити цю проблему, Кластер переробної промисловості на північному сході Англії (NEPIC) на початку цього року засідав з компанією британською компанією, яка спеціалізується на кібер-захисті підприємств Tekgem, щоб обговорити, як найкраще навчити тих, хто працює в хіміко-переробній галузі, та допомогти їм вирішити проблеми, пов'язані з кібербезпекою АРСХФ.

У березні 2020р провідні інспектори з питань кібербезпеки Управління з охорони праці у Великій Британії (HSE) обговорили ключові моменти в керівних принципах. HSE, разом із багатонаціональною компанією з виробництва хімічних речовин у Саудівській Аравії SABIC, та Tekgem виступили перед аудиторією, яка варіювалась від інженерів приладів та контролю до техніків технічної підтримки, менеджерів з автоматизації та до інженерних директорів та менеджерів HSE, які в даний час працюють на хімічних заводах.

Подія стала початком подорожі АРСХФ до кібербезпеки для всіх сторін та компаній-учасниць, які чітко дали зрозуміти, що вони бачать реальні вигоди, і погодились з необхідністю відкритого та спільного підходу для ефективного управління постійно зростаючою загрозою кібератаки, незалежно від того, зловмисна вона чи випадкова. Насправді, високий рівень знань, показаний учасниками заходу, є чудовим відображенням справжнього професіоналізму, який існує в галузі.

Повідомляючи про гучні кібератаки з вимогами, гості також усвідомили ризики, спричинені випадковими порушеннями, спричиненими помилками співробітників, або порушеннями мережі, спричиненими сторонніми постачальниками, які становлять основну загрозу для ефективності кібербезпеки АРСХФ в процесах галузі хімічної обробки.

Однак у всіх організаціях, які рухаються вперед, необхідні культурні зміни, щоб, не дивлячись на наслідки кібератаки з перших рук, ми повністю розуміли розмір, масштаби потенційних ризиків і були готові та підзвітні у випадку інциденту відбуваються. Перше запитання, на яке потрібно відповісти, це хто несе

відповідальність. І якщо ви така людина, краще реагувати на ваші загрози кібербезпеки зараз, а не думати, що немислимого не станеться.

HSE запропонували кілька простих кроків для підвищення безпеки систем АРСХФ, а керівні принципи надають більш детальну підтримку. Крім того, досвід надається такими організаціями, як Tekgem, з їх стратегією «Захист у глибину»[1].

2.1.1 Діяльність лідерів

Ще десять років тому, коли більшість систем та бізнес-мереж були ізольовані одна від одної, безпека була відносно простою. Однак з часом обидві мережі стали взаємопов'язаними. Першим методом інтеграції, як правило, був сервер з мережевим інтерфейсом як у діловій, так і у виробничій мережі, який зазвичай називають мостовим. Протягом декількох років це був ефективний спосіб контролювати потік даних з однієї мережі в іншу. Але з недавніми хробаками, які мають можливість заразити один комп’ютер і стати точкою запуску, щоб знайти більше, віруси легко поширюються через мостові мережеві сервери. Використання мостових серверів - це небезпечна обчислювальна практика. Поширеною практикою є встановлення брандмауера між виробничою та діловою мережами, але це все одно дозволяє комп’ютеру у внутрішній мережі бути скомпрометованим та поширювати вірус до критичних систем всередині. На жаль, було кілька компаній, які зазнали операційних збитків через технічні недоліки мостових серверів або погано налаштованих брандмауерів [6].

Найкращий спосіб контролювати безпеку між двома мережами, такими як виробнича та ділова, - це використання декількох брандмауерів та ДМЗ (демілітаризована зона). Це створює мережу середнього рівня, яку можна використовувати для безпечної передачі інформації. Пристрої та програми на ДМЗ стають агентами безпеки або посередниками, щоб гарантувати, що шкідливі загрози локалізуються і їм не дозволяється поширення. Приклад мережі підприємства наведений на Рисунок 2.1 нижче.

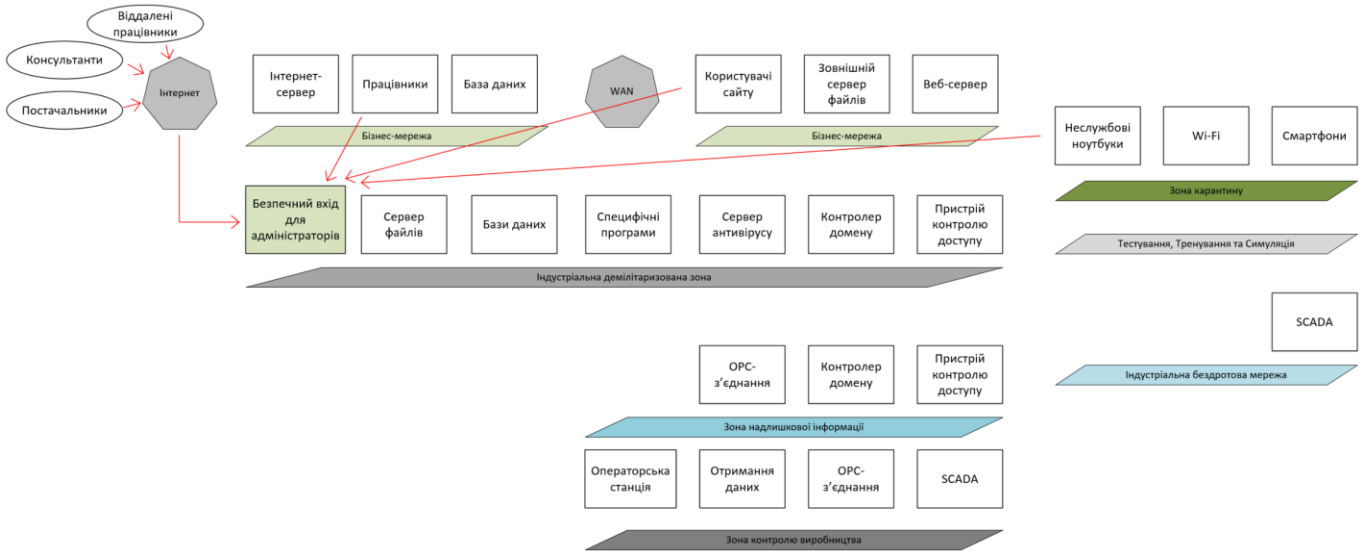

Рисунок 2.1 Приклад мережі підприємства

Рисунок вище демонструє типову архітектуру мережі, яка базується на загальній моделі ДМЗ, але з досвідом Honeywell вона часто вдосконалюється, щоб задовольнити унікальні вимоги сучасної виробничої системи. Мета мережі ДМЗ полягає у забезпеченні структурованого потоку інформація між бізнесом та виробничими мережами при збереженні високого рівня безпеки. Це може включати виробництво, лабораторію, технічне обслуговування, інформацію про перевезення та звіти. Він також дозволяє вхідні з'єднання для адміністраторів, передачу файлів, антивірус та оновлення безпеки. З подібними конструкціями система може працювати безпечно, але також дозволити надходження інформації в бізнес-системи вищого рівня. Якщо в діловій мережі відбувається інцидент безпеки або зміни, критично важливі системи ізолюються від загрози.

Після того, як буде встановлено правильний дизайн мережі, наступним кроком є встановлення допоміжних систем, які допоможуть підтримувати її роботу. З точки зору технічного обслуговування, рекомендується мати активні системи моніторингу, щоб ідентифікувати, чи не вдасться швидко відремонтувати їх. З точки зору безпеки, важливо виявити невідповідне використання та вторгнення, щоб переконатись, що вони зупинені до виникнення інциденту. Важливо реєструвати, перевіряти, відстежувати та ідентифікувати, хто використовує систему, та визначити, хто міг брати участь у зловмисній діяльності. Якщо трапляється інцидент безпеки, хороші

журнали трасування допомагають визначити, як зловмисник потрапив у систему та як вийти із ситуації. Без відповідної інформації про ведення журналу дуже важко правильно визначити проблему безпеки та пом’якшити або вирішити ситуацію. Те, що може виглядати як невдала консоль оператора, може бути наслідком хакера чи вірусу. І у світлі зростаючого тиску та зусиль щодо дотримання вимог, можливості аудиту стають все більш важливими для багатьох організацій[6].

Індикатори промислової безпеки також пишуть, переглядають та застосовують розгорнуту політику та процедури. Кожна організація має політику безпеки, щоб визначити належне використання корпоративних IT-комп’ютерів, але рідко вони враховують унікальні вимоги реального виробничого середовища. Лідери розуміють відмінності та пишуть документи, унікальні для їхніх систем. Наприклад, у них є політика та процедури, що гарантують регулярне резервне копіювання всіх критично важливих систем, а також перевіряють та перевіряють, щоб переконатися, що вони готові швидко відновити систему. Типову IT-інфраструктуру, як резервне копіювання стрічки, не можна використовувати для відновлення всіх виробничих систем. Політика відновлення для живої виробничої системи є унікальною і повинна бути задокументована та регулярно практикуватися. Лідери також мають сувору політику віддаленого доступу, щоб визначити, як постачальники отримують доступ до своїх систем для підтримки та адміністрування як безпечним, так і контрольованим способом.

Щоб забезпечити безперебійну роботу інфраструктури, важливої системи, потрібно оцінити, як вона керується та як проходить навчання персонал. Це просте твердження, але багато систем встановлені і дозволяють працювати без нагляду роками, поки не відбудеться надзвичайна подія. Це найгірша ситуація, оскільки команда підтримки не готова, не практикується і часто не знайома з системою після багатьох років бездіяльності. Це призводить до того, що усунення несправностей та відновлення системи може зайняти кілька днів та з додатковими витратами, коли це може зайняти лише години.

Провідні підприємства з промислової кібербезпеки вже модернізували свої системи та мають на місці широкі політики, процедури, навчальні програми та

команди підтримки. Є багато робочих груп, комітетів, форумів та регуляторних органів, які активно намагаються поліпшити безпеку системи контролю у всіх галузях.

Однією з найважливіших тем, яка присутня в різних інформаційних джерелах, є потреба у підвищенні обізнаності щодо безпеки серед корпорації в цілому. Щоб продовжити будь-яку ініціативу з питань безпеки, необхідно оцінити та зважити всі варіанти, щоб продовжувати будь-які зміни. Для того, щоб ініціатива безпеки була успішною, необхідно визначити дуже тонку межу між захистом даних та доступом до цих даних. Крім того, ще є питання навантаженості користувача. У міру збільшення складності будь-якої системи або доступу до неї неминуче збільшуються завдання та очікування, що покладаються на користувачів цієї системи. Щоб досягти успіху в будь-якому проекті безпеки, у процес прийняття рішень повинна бути включена мультидисциплінарна команда. Ця команда, швидше за все, буде включати когось із операційних служб, IT, інжинірингу, користувачів та команди з виконання проектів. Ця команда може також включати будь-яке адміністративне представництво, яке може вплинути на проект, будь-яку команду з дотримання вимог або присутність на рівні керівника, де це потрібно. Однією з найважливіших функцій мультидисциплінарного підходу є збільшення рівня загальної обізнаності, що досягається лише з командою різнокваліфікованого персоналу постійно представленого на засіданнях. У випадках великих проектів рекомендуються конкретні кампанії з підвищення обізнаності, оскільки ініціатива щодо безпеки буде успішною лише в тому випадку, якщо кінцеві користувачі будуть правильно використовувати нові процедури та системи. Без широкої зацікавленості новими практиками, невдача врешті-решт неминуча[2].

Справжні лідери в області навчання користувачів та кампаній безпеки на рівні всієї компанії мають мультидисциплінарні групи, які перевіряють усі проекти, пов'язані з IT/безпекою, від фази торгів до завершення та тестування. Це слугує різним цілям - від обміну інформацією між командами та підрозділами, залучення підтримки для різних ініціатив та до впорядкування конкретних проектів, коли вони

відхиляються. Найбільше це підвищує обізнаність про будь-який окремий проект у свідомості всієї компанії.

2.1.2 Огляд захисних програм сектору

У сфері захисту критичної інфраструктури комплексна захисна програма - це скоординований план дій щодо зміцнення або забезпечення активу чи групи активів шляхом виявлення, оцінки та реалізації одного або декількох захисних заходів чи дій. Захист критичної інфраструктури в хімічному секторі складається з різноманітних видів діяльності, які застосовуються до аварії, під час інциденту та після інциденту. Ці заходи допомагають запобігти нападу або захистити частину інфраструктури, коли інцидент чи атака триває, а також пом'якшити наслідки та полегшити відновлення після успішно виконаної атаки чи інциденту. У сукупності цей спектр діяльності часто називають «захисним спектром» (Рисунок 2.2).

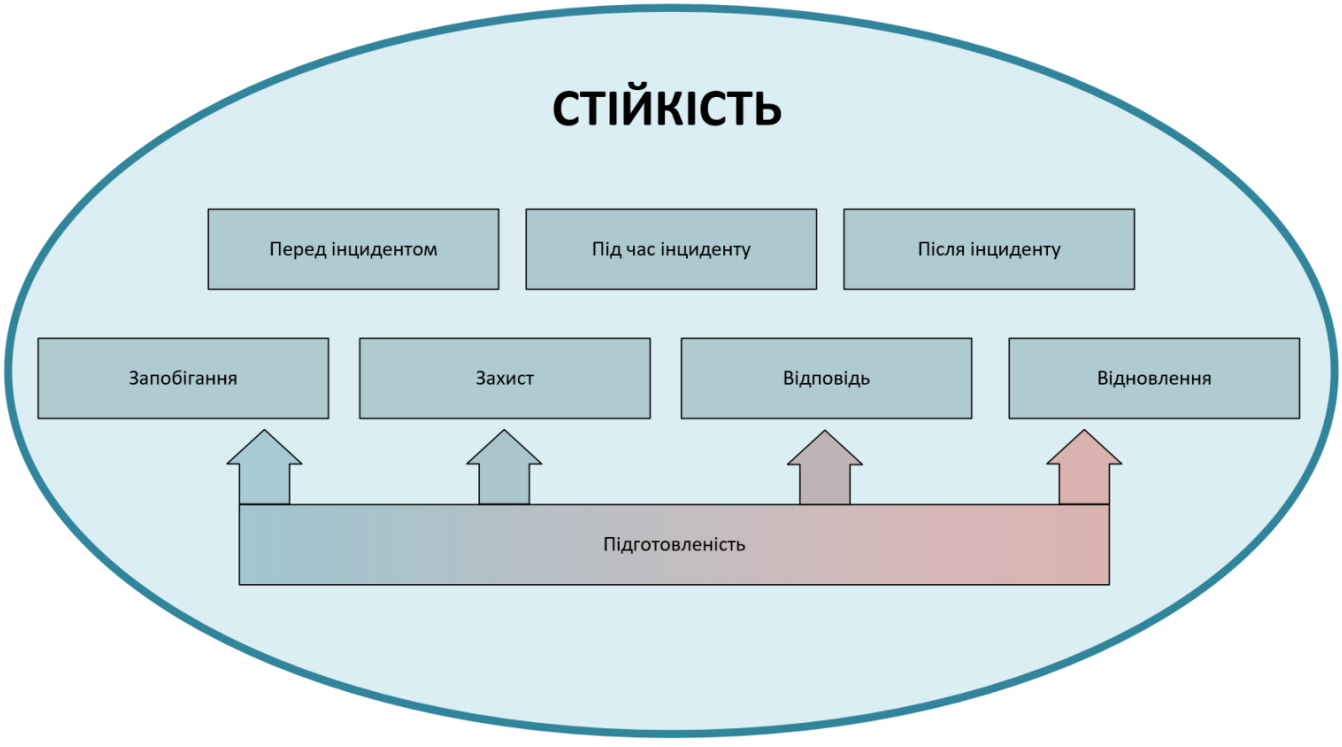

Рисунок 2.2 Захисний спектр

Діяльність захисного спектру, поширена в цьому секторі, включає наступне:

– профілактика. Профілактичні заходи проводяться з метою підвищення ймовірності уникнення інциденту або втручання для припинення інциденту. Ці

заходи спрямовані на стримування та виявлення атак. Приклади включають посилені перевірки, перевірку попереднього досвіду працівників та вдосконалення операцій з нагляду.

– захист. Захисні заходи допомагають зміцнити актив проти потенційних загроз або інцидентів шляхом мінімізації вразливостей або потенційних наслідків нападу чи інциденту. Діяльність, як правило, зосереджена на знеціненні та захисті критично важливих активів, які можуть бути цільовими. Прикладом може бути будівництво огороджень або інших бар'єрів, найм озброєних охоронців, встановлення брандмауерів для захисту кібернетичних активів та розробка резерву та резервних систем.

– реагування. Заходи реагування дозволяють використовувати ресурси під час або відразу після атаки, щоб допомогти зупинити атаку або пом'якшити наслідки атаки. Прикладами можуть бути тактичні плани реагування, плани взаємодопомоги та використання спеціалізованого обладнання для запобігання розливу хімічних речовин.

– відновлення. Відновлення допомагає скоротити час і витрати, необхідні для повернення активу до працездатності та нормального стану після інциденту. Приклади включають розробку планів безперервності роботи та зберігання резервних матеріалів або матеріалів, що замінюють, за межами об'єкта.

– готовність. Заходи щодо готовності доповнюють інші чотири види діяльності, що містяться в Захисному спектрі (Рисунок 2.2). Вони допомагають розробляти елементи (наприклад, плани, процедури, політику, навчання та обладнання), необхідні для максимізації здатності запобігати, захищати, реагувати на ситуації та відновлювати їх після інциденту.

2.1.3 Помітні кібербезпекові тренди

Виходячи за межі інцидентів, пов'язаних із кібербезпекою останніх років, розвідувальні дані про загрози, зібрані з Національного центру кібербезпеки та світових хімічних компаній, разом із висновками та прикладами керівника відділу охорони здоров'я та безпеки Великої Британії (HSE), розкрили ключовий контроль

промисловості та автоматизації. Загрози кібербезпеки систем (АТСХФ), включаючи Watering Hole (стратегія комп’ютерної атаки, в якій зловмисник здогадується або спостерігає, які веб-сайти організація часто використовує та заражає одну чи декілька з них шкідливим програмним забезпеченням); Triton (програмне забезпечення, використане для атаки на підприємство у Саудівській Аравії у 2017р), WannaCry (комп'ютерний вірус, що вражає операційну систему Microsoft Windows шляхом шифрування файлів), напади, що фінансуються національними державами, та причини як людські помилки.

Нещодавній приклад атаки Watering Hole відбувся на сайті британського відділу контролю за масштабними аваріями (COMAH) після повідомлення електронної пошти про «фішинг», надісланого із системи постачальника, і містило шкідливе програмне забезпечення, яке давало зловмисникові команду та контроль над корпоративним настільним ПК. Потім зловмисник поширився побічно по мережі, забезпечивши доступ та отримавши інформацію та знання, необхідні для глибшого проникнення в систему управління. У цьому випадку зловмисник перехопив і модифікував комунікаційний протокол MODBUS через зв'язок TCP / IP і замінив систему приладів безпеки, що призвело до того, що матеріал таємно перекачувався для переповнення пристані.

У 2017 році зловмисна кібератака була здійснена на нафтохімічному заводі в Саудівській Аравії, в результаті чого зловмисники отримали контроль над системою безпеки, що має вирішальне значення для захисту від катастрофічних подій. Шкідливе програмне забезпечення, яке отримало назву Triton, дозволило хакерам маніпулювати пам’яттю пристроїв та запускати несанкціоновані програми в системі, використовуючи раніше невідому помилку.

Ще один приклад у 2017 році, коли WannaCry потрапив у заголовки новин, коли зловмисники тримали Національної служби охорони здоров’я Великої Британії (NHS) на викуп за дані своїх пацієнтів, викликаючи обурення та хаос у рівній мірі. Кібератака WannaCry мала потенційно серйозні наслідки для NHS та її здатності надавати допомогу клієнтам. Це була відносно нехитра атака, яку можна було б запобігти, якби дотримувались найкращих практик IT-безпеки.

В останні роки звинувачення у державних кібератаках відбувалися в регіоні Близького Сходу, причому, мабуть, найбільш відомою була атака найбільша за видобутком і запасами нафти компанію світу, національна нафтову компанію Саудівської Аравії Saudi Aramco. Кібератака Saudi Aramco була здійснена в 2012 році за допомогою вірусу, відомого як Шамун. Вірус порушив роботу комп'ютерів, перезаписавши головний завантажувальний запис, унеможливлюючи їх запуск [3].

Незважаючи на те, що кібер-атаки-вимоги продовжували потрапляти в заголовки новин, випадкові порушення, спричинені помилками співробітників або порушеннями мережі, спричиненими сторонніми постачальниками, продовжують залишатись основною загрозою для ефективності кібербезпеки АРСХФ в хіміко-переробній промисловості.

Одна хімічно-переробна компанія - із сайтами по всьому світу - зіткнулася з серйозною невдачею, яка зачепила 80 серверів та 200 систем баз даних після випадкового інциденту, який стався в той час, коли два її заводи знаходились посеред повороту. Інцидент трипився через постачальника, який встановив непідтримуване обладнання, і хоча постачальник пізніше поставив правильне, були надані неправильні процедури для його встановлення. Це, в свою чергу, спричинило серйозний збій обладнання та пошкодження даних, і хоча було реалізовано аварійне відновлення, проблеми із резервними копіями додатково заважали. Повної втрати функціональних можливостей заводу в основному вдалося уникнути завдяки ефективному зв'язку та відновленню ключових систем, що відбуваються в порядку важливості.

Кібербезпека є невід'ємною частиною загальної безпеки хімічного сектору, і галузь розглядає ризик як загальносекторну ініціативу, щоб мінімізувати потенційний вплив як на безпеку підприємства, громадську безпеку, так і на економіку.

Зниження поточних та майбутніх ризиків кібербезпеки вимагає поєднання передових технологій, прийнятої секторної практики та своєчасного обміну інформацією у всьому секторі. Цей різновид галузевої співпраці для вирішення питань кібербезпеки має багато прецедентів у хімічному секторі.

Хімічний сектор та продукти, які цей сектор виробляє, є важливими для більшості для продуктів сучасної людини та підприємств, що забезпечують більшість аспектів сучасного життя, включаючи безпечне водопостачання, виробництво енергії, виробництво продуктів харчування, житло, охорону здоров'я, комп'ютерні технології та транспорт. Наша національна та економічна безпека, а також сучасний рівень життя залежать від життєздатності хімічного сектору та подальшого виробництва та транспортування хімікатів.

Цей сектор має добре розроблений та успішний підхід кращих практик до управління ризиками стосовно питань безпеки. Після терористичних атак 11 вересня у Нью-Йорку у більшості країн світу почали по-новому дивитись на безпеку підприємств та готовність протидіяти терористичним актам, тому багато хімічних компаній використали новий підхід до управління ризиками до безпеки та застосували його до нової загрози безпеці. Промисловість ініціювала різноманітні добровільні програми безпеки та здійснила значні капіталовкладення для вирішення проблем безпеки. Безліч держав також прийняли закони щодо підвищення безпеки хімічних споруд, що знаходяться під їх юрисдикцією.

Визнаючи зусилля промисловості та штатів щодо захисту хімічних споруд, Федеральний уряд Сполучених Штатів Америки продовжує впроваджувати правила безпеки на об'єктах, які, на його думку, знаходяться під високим ризиком, для забезпечення єдиного підходу до безпеки. Ці стандарти були відразу підхоплені та впроваджені іншими країнами, у тому числі Україною. Крім того, були прийняті норми щодо підвищення безпеки хімічних речовин під час транспортування та розподілу, в тому числі в портових установах країни[3].

Хімічні фірми, як правило, більш консервативні, ніж такі галузі, як фінансові, до впровадження нових інноваційних інформаційних технологій, проте заходи цифрової динамізації набирають сили в цьому секторі продовж останніх років.

Концепція таких заходів, як цифрові близнюки фізичних виробничих фондів та розумні ланцюги поставок, існує, в принципі, вже давно, але збільшення частоти їх використання за останнє десятиліття зробило їх набагато більш доступнішими.

Ці кроки, поряд із збільшенням інтелектуальної власності, що зберігається в хмарі, та використання штучного інтелекту при розробці нових матеріалів, зробили бізнес набагато спритнішим, але зворотним боком цих досягнень є збільшення точок доступності для зловмисних акторів для крадіжки чи фальсифікації активів або крадіжки їх з метою отримання викупу.

На Рисунок 2.3 нижче зображено цікаву тенденцію збільшення об'єму продажу хімічних продуктів у світі.

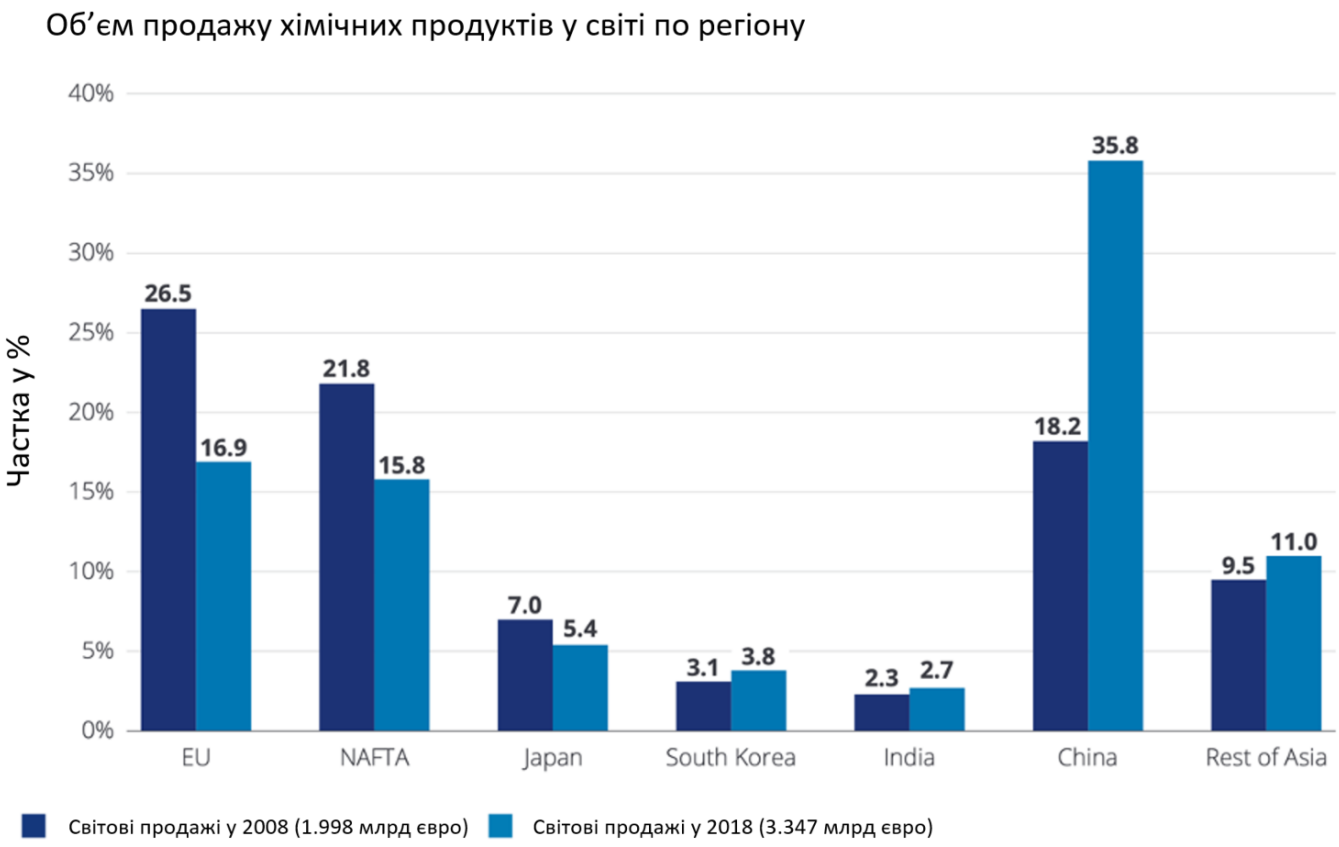

Рисунок 2.3 Об'єм продажу хімічних продуктів

Ці вражаючі цифри та міцний історичний фундамент можуть відвернути увагу від того, що промисловість Європи в майбутньому зіткнеться з низкою викликів. Справа не тільки в тому, що зростання було на рівні менше 1% на рік в останнє десятиліття (CAGR приблизно 0,6% річних з 2008 по 2018 рр.), актуальність внутрішніх ринків Європейського союзу (ЄС) постійно знижувалась (враховуючи обсяги продажів на внутрішньому ринку та експорту всередині ЄС, з -0,4% річних у 2008 р.).

Однак, навіть незважаючи на те, що відсоток експорту до регіонів за межами Європи збільшується на приблизно 4% в рік. у той же час (з 20% до 29% продажів хімікатів у ЄС) є посилення глобальної конкуренції, особливо з боку країн, що розвиваються, таких як Китай та інші азіатські ринки, призвело до різкого зменшення глобальної частки європейських хімікатів у промисловості (спочатку > 25%, а в даний час приблизно 17%)[1].

Додаючи до цього контексту, складне ринкове/конкурентне середовище на внутрішніх ринках ЄС, порушення глобальних ланцюгів поставок, соціально-політичний тиск на стійкість (включаючи намагання перейти до зменшення викидів парникових газів), зміна попиту з боку основних галузей застосування (таких як автомобільна) та несприятлива енергетична та сировинна ситуація (без конкурентних переваг доступу до нафти, наприклад, із Близького Сходу чи сланцевого газу в США) формує структуру, в якій хімічна промисловість Європи повинна конкурувати.

Крім того, Європа є не лише домом багатьох великих хімічних компаній; частка їх продажів, здійснених у Європі, все ще залишається значною і все ще залучає значні інвестиції. В основному це не інвестиції в нові потужності, а в першу чергу, в модернізацію та дешифтування. Капітальні витрати на хімічну промисловість складають > 20 млрд. Євро в європейському регіоні, а отже, майбутнє галузі також має макроекономічне значення.

2.1.4 Анти-терористичні стандарти для хімічних підприємтсв

Тисячі об'єктів, які виробляють, використовують або зберігають небезпечні хімічні речовини, можуть бути націлені або використані терористами, намагаючись завдати масових причинних наслідків, шкоди та страху. Ці хімічні речовини можуть бути випущені з установи, щоб заподіяти шкоду навколишньому населенню, або їх можна вкрасти та використовувати як хімічну зброю або як її складові (інгредієнти для виготовлення хімічної зброї). Крім того, у міру того, як довіра до інформаційних систем продовжує зростати, супротивники захисту від кіберзагроз, такі як терористи, злочинці або держави, можуть зловмисно маніпулювати системами фізичної безпеки, інформацією та управлінням процесами організації для викрадення хімічних речовин

або заподіяння шкоди викидами Наприклад, Національна лабораторія штату Айдахо в США у 2018 році повідомила, що зловмисники працювали над системами промислової безпеки компанії Близького Сходу з метою порушити систему промислового контролю, що дозволило б зловмисникам отримати доступ до систем безпеки та змінити безпекові процеси, які могли бути фізично небезпечними або завдати шкоди людям.

Програма антитерористичних стандартів хімічного фонду (АТСХФ) призначена для забезпечення безпеки хімічної інфраструктури країни. Вона була заснувана для, серед іншого, виявлення хімічних споруд з високим ризиком та оцінки ризику, який створює кожна з них; розміщення об'єктів, визначених у групі високого ризику, в один з чотирьох рівнів, заснованих на оцінці ризику; та для оцінки, затвердження та перевірки заходів безпеки об'єктів для забезпечення відповідності регуляторним вимогам.

Раніше було повідомлено про різні аспекти програми АТСХФ та визначені проблеми, з якими компанії зіткнулись при впровадженні та управлінні програмою. Незважаючи на те, що за останні роки відбулися вдосконалення програми, залишаються питання про прогрес, досягнутий у впровадженні змін до програми та в якій мірі програма АТСХФ забезпечує покращення безпеку у підприємствах з найвищим ризиком.

Крім того що компанії в хімічному секторі все частіше прагнули підвищити ефективність, з'єднавши свої системи фізичної безпеки, інформації та управління процесами. Однак було виявлено, що зближення між цими системами було головним викликом для власників та операторів критичної інфраструктури, включаючи хімічні виробничі потужності, оскільки це створило нові можливості для потенційних кібер-супротивників отримати доступ до цих систем.

Для визначення, якою мірою програма оцінює зусилля з кібербезпеки охоплених хімічних споруд, були вивчені підручники з програм інспекції; керівні матеріали, включаючи Керівництво зі стандартів ефективності на основі ризиків, відоме як керівництво АТСХФ у цій роботі; та стандартні операційні процедури, що використовуються для перевірки стану кібербезпеки охоплених хімічних споруд, щоб

забезпечити їх відповідність стандарту кібербезпеки. Також були отримані окремі звіти про перевірку та затвердження об'єктів АТСХФ, щоб перевірити, як інспектори документують виконання заходів з кібербезпеки об'єкта та будь-які зміни до інформаційні системи та системи управління процесами. Були оцінені зусилля державних служб для оцінки керівних принципів кібербезпеки програми на основі Національного інституту стандартів та технологічних рамок для вдосконалення кібербезпеки критичної інфраструктури та інших керівних принципів кібербезпеки та хімічної промисловості, щоб оцінити ступінь до якого керівництво програмою з кібербезпеки враховувало еволюцію загроз та стратегій пом'якшення наслідків.

Також були вивчені матеріали опитування представників п'яти асоціацій хімічної промисловості та двох хімічних компаній [5], для отримання їхніх перспектив щодо настанов та перевірки програми кібербезпеки АТСХФ, а також інших стандартів, що використовуються для зменшення ризиків на хімічних об'єктах. Були обрані асоціації хімічної промисловості, які були членами Координаційної ради з питань хімічного сектору та відображений цілий ряд типів хімічних споруд, таких як виробники хімічних речовин та вибухових речовин.

Щоб визначити, наскільки правильно програма визначає рівень інспекційного персоналу та спеціальну підготовку, необхідну для оцінки кібербезпеки на охоплених об'єктах, була вивчена документація [2] про роботу та організацію програми, управління ефективністю роботи інспекторів та аналітиків, навчальні матеріали з кібербезпеки та підготовку програми плани та форми оцінки. Були оцінені плани та процеси робочої сили, пов'язані з кібербезпекою програми АТСХФ, з урахуванням ключової практики управління людським капіталом, а також внутрішніх вказівок ДСНС щодо планування робочої сили. Є чотири компоненти процесу навчання та розвитку:

- планування / аналіз інтерфейсу;
- проектування / розробка;
- впровадження;
- оцінка.

Кожен компонент включає безліч питань, які слід враховувати при оцінці кожного з чотирьох компонентів, а також елементи, пов’язані з кожним питанням, наприклад, які заходи агентство використовує для оцінки зусиль щодо навчання та розвитку для досягнення індивідуального майстерності та досягнення цілей. Шкала нижче була використана для оцінки навчальних зусиль програми щодо кібербезпеки ключових практик, які були виділені з кожного з чотирьох компонентів структури:

– Рекомендації дотримані. Навчальні матеріали програми та відповідні документи та інтерв’ю з посадовими особами продемонстрували, що більшість ключових практик відповідають програмі АТСХФ;

– Рекомендації частково дотримані. Навчальні матеріали програми та відповідні документи та інтерв'ю з посадовими особами продемонстрували, що деякі ключові практики відповідають програмі АТСХФ;

– Рекомендації не дотримані. Навчальні матеріали програми та відповідні документи та інтерв'ю з посадовими особами продемонстрували, що ключові практики не відповідають програмі АТСХФ.

2.1.5 Підприємства регульовані АТСХФ

Станом на лютий 2020 р., за оцінками, 3300 об'єктів було визначено об'єктами, що охоплюються АТСХФ, і відповідають нормам АТСХФ. Ці об'єкти містять до 300 хімічних речовин, що входять до списку небезпечних, які потребують спеціальний моніторинг, такі як аміак та хлор, у кількостях, які відповідають або перевищують порогову кількість та концентрацію[3]. Послуги також перетинають багато галузей, включаючи, але не обмежуючись, хімічним виробництвом, зберіганням та розподілом; енергетикою та комунальними послугами; сільським господарством та продовольством; вибуховими речовинами; целюлозно-паперовою індустрією; електронікою; виробництвом пластмаси; університетами та лабораторіями; виробництвом фарби та покриття; охороною здоров'я та фармацевтикою; та виробництвом та обробкою металу. Загрози класифікуються за трьома основними загрозами безпеці:

– вивільнення;

– викрадення чи викрадення;

– саботаж.

Викиди охоплюють будь-які токсичні, легкозаймисті або вибухонебезпечні хімічні речовини або матеріали, які можуть потрапляти на об'єкт та потенційно завдати шкоди навколишньому середовищу та населенню. Викрадення охоплює будь-які хімічні речовини або матеріали, які в разі викрадення або перенаправлення можуть бути перетворені на зброю за допомогою простої хімії, обладнання чи техніки. Саботаж охоплює хімічні речовини або матеріали, які можна змішувати з легкодоступними матеріалами, такими як вода, щоб створити значні несприятливі наслідки для життя або здоров'я людей.

2.2 Визначення ефективності

Показники подаються двома способами - показниками національного координатора та індикаторами прогресу сектору, які описані наступним чином:

– показники прогресу національного координатора описують зусилля інтелектуальної власності для підтримки заходів;

– індикатори прогресу в секторі сукупно описують прогрес, досягнутий кожним сектором, та ефективність різних видів діяльності у секторах.

Показники прогресу національного координатора щороку звітуються у національному щорічному звіті [1]. Показники та метрики, що обговорюються, можуть бути розроблені на основі декількох різних типів даних, зібраних в результаті секторної діяльності, і включають наступне:

– описові дані дають якісну інформацію про прогрес або пояснюють корисну цінність заходів щодо зменшення ризику, досягнутих за звітний період. Приклади включають етапи впровадження, відгуки учасників Саміту з безпеки в хімічному секторі та кількість учасників брифінгу, що проводиться раз на два роки;

– вихідні дані використовуються для оцінки того, чи виконувались конкретні заходи, як планувалось, для відстеження прогресу завдання або для звітування про результати процесу. Вихідні дані показують прогрес у виконанні заходів, необхідних для досягнення цілей захисту КІКР, і вони можуть служити

провідними показниками для вимірювання результатів. Вони також допомагають скласти всебічну картину стану захисту та діяльності КІКР;

– дані про результати - це показники, які вказують на прогрес, цінність чи корисні результати щодо досягнення стратегічної мети та асоційованої цілі, а не рівня активності. Показник високого рівня може продемонструвати національне досягнення щодо зменшення ризику в результаті реалізації певної ініціативи захисту КІКР.

Сектор використовує всі три типи даних та відповідні метрики, які можуть бути розроблені на основі даних, для оцінки прогресу або ефективності секторних ЗЗР. Сектор також працює над отриманням даних про результати та метрик для оцінки прогресу та ефективності ключових ЗЗР. Проте, як очікується, це буде складним процесом через перелічені нижче завдання.

2.2.1 Визначення прогресу сектору

Хімічний сектор стикається з подібними проблемами, як інші сектори КІКР, розробляючи показники результатів. Важко виміряти прогрес до досягнення стратегічної мети, коли цілями є нематеріальні поняття, такі як зменшення ризику або успішна реалізація моделі секторного партнерства. Виміряти стримування за допомогою програми вимірювань, що базується на результатах, також важко, оскільки вона зумовлена сценарієм, який трапляється настільки рідко, що дані історично недоступні і можуть бути недоступними в майбутньому. Тому секторні партнери концентрують свої зусилля на заходах щодо зменшення ймовірності успішності інциденту за допомогою суб’єктивних заходів, таких як успішне проведення оцінки вразливості або тестування планів реагування на надзвичайні ситуації. Секторні партнери вважають, що захисні програми та стратегії стійкості, розроблені сектором, є ефективними та успішними, оскільки програми та стратегії є корисними, своєчасними та якісними. У майбутньому сектор розроблятиме показники результатів із використанням узгоджених цілей програми та суб’єктивних заходів. Хоча деякі показники програм ще не визначені, власникам, операторам та

іншим користувачам галузевих програм буде проведена консультація для визначення найбільш підходящих показників.

2.2.2 Використання метрик для постійного покращення

Показники прогресу хімічного сектору забезпечують механізм, який дозволяє партнерам хімічного сектору визначати ефективність програм захисту та стратегій стійкості, а також надають цінну інформацію для подальшого вдосконалення програми. Метрики переглядаються щороку як частина процесу звітності для оцінки програм на наступне:

– якість та тип інформації, яка передається у кожній програмі. Цей аналіз також може допомогти вказати, чи змінюється середовище загрози для цього сектору і чи потрібно буде розглядати майбутні коригування;

– доцільність пропагандистських та навчальних програм. Результати аналізу допоможуть визначити, чи правильні люди отримують правильну інформацію у придатній для використання формі;

– прогалини в захисних програмах та стратегіях стійкості. Для виявлених прогалин може знадобитися створення нових програм.

Після завершення процесу оцінки результати будуть використані для розподілу ресурсів там, де їх можна буде використовувати найбільш ефективно.

Щорічно звітуючи про показники, сектор може переглядати прогрес та адаптувати програми на основі результатів. Наприклад, дані, зібрані за програмою підготовки фахівців із вибухонебезпечних речовин у хімічному секторі, вказували, що незручні місця проведення подій могли сприяти тому, що рівень участі приватного сектору був нижчим за очікуваний. Як результат, місце проведення тренінгу було змінено, щоб забезпечити більшу участь приватного сектору.

Додатково до підтримки оцінки прогресу програми щодо галузевих пріоритетів, метрики служать механізмом зворотного зв'язку щодо інших частин системи управління ризиками та прогресу до досягнення цілей галузі. Вимірювальний підхід хімічного сектору сприяє постійному вдосконаленню, використовуючи дані,

отримані в результаті вимірювальних заходів, для забезпечення реалізації захисної програми.

2.3 Витрати на безпеку

Через свою важливу роль в економіці, Міністерство національної безпеки США визначило хімічний сектор одним із шістнадцяти «критично важливих секторів інфраструктури» (визначено як «сектори, активи, системи та мережі яких, фізичні чи віртуальні, є вважаються настільки життєво важливими, що їхня недієздатність або знищення матимуть виснажливий вплив на безпеку, національну економічну безпеку, національне громадське здоров'я чи безпеку або будь-яку їх комбінацію.») [2].

Хоча безпека об'єктів довгий час була в центрі уваги хімічної промисловості, події у Нью-Йорку 11 вересня призводять до загострення проблем безпеки у всьому світі.

Керівники підприємств все частіше інвестують в безпеку людей та інформації своїх компаній, а також у технологічні заводи, обладнання, технології, сховища та будівлі. Компанії також повинні враховувати безпеку інших активів, таких як вагони-цистерни та інші транспортні засоби, комунальні послуги (електроенергія, пара, природний газ, вода, каналізація тощо), залізничні лінії та дороги, об'єкти когенерації, об'єкти переробки небезпечних відходів, запаси, інструменти, оргтехніку та навіть особисте майно працівників.

Американська рада з хімії (AXP) збирає дані про витрати на безпеку шляхом щорічного економічного опитування компаній-членів. Деякі компанії витрачають до 2% своїх продажів на забезпечення безпеки своїх ділових операцій. Витрати на охорону включають охорону, сторожових собак, патрульних та інших охоронних служб, інших служб безпеки, електронного спостереження, дистанційного електронного моніторингу охорони та інших охоронних послуг. Витрати на безпеку також включають витрати, які традиційно пов'язані з інформаційною, комп'ютерною, мережевою та пов'язаною з IT-безпекою. Інші витрати, що не містяться на Рисунок 2.4, включають: зусилля з безпеки персоналу, що не охороняється (наприклад, будівельні послуги); витрати на заходи безпеки процесу; більші транспортні витрати;

контроль запасів; додаткові процедури; страхування; та інші супутні витрати. Таким чином, ці витрати представляють не всю вартість безпеки, а лише одну її частину; фактичні загальні витрати на охорону можуть перевищувати цю суму.

Рисунок 2.4 - Безпекові витрати

2.3.1 Сучасні безпекові виклики

Не секрет, що багато видів промислових об'єктів визначені потенційними об'єктами зловмисних атак, включаючи ділянки видобутку нафти та газу, нафтопереробні заводи, газорозподільні майданчики, хімічні заводи, целюлозно-паперові комбінати та електростанції. Таким чином, існує потреба у всебічній стратегії безпеки для цих об'єктів та іншої критичної інфраструктури.

Державні нормативні акти, такі як Антитерористичні стандарти хімічного фонду та Закон про безпеку морських перевезень, також вимагають від компаній вжиття ефективних заходів для захисту від погроз промислової безпеки. Також може виникнути потреба в таких мандатах, як ідентифікаційні дані працівника транспорту.

Щоб захистити матеріальні та людські активи, виробничі підприємства та інші вразливі операції потребують інтегрованої системи безпеки, яка об'єднує безліч технологій безпеки. Ці технології повинні мати можливість комунікації в режимі реального часу, об’єднуючи дані, створюючи нові, більш надійні знання для

швидших, ефективніших дій із меншою кількістю ресурсів. Заходи фізичної безпеки представляють важливі міркування у схемі захисту активів, яка включає кібербезпеку та безпеку інформації. Неможливо повністю відокремити різні аспекти загальної позиції безпеки підприємств. Запобігання зловмисникам отримання доступу до заводу може також заборонити їм доступ до мереж управління критичними процесами.

Поточні вимоги до фізичної безпеки включають:

– виявлення та контроль осіб, які входять і виходять із закладу;

– відстеження рухів мешканців будинків та активів;

– контроль доступу до заборонених місць відстеження та розміщення обладнання, продуктів та інших ресурсів;

– відстеження розташування персоналу на місці у випадку інциденту, інтегруючи системи управління та безпеки для більшої швидкості та ефективності;

– захист мереж та систем автоматизації процесів від потенційного проникнення;

– швидка реакція на тривоги та події.

Міністерство юстиції США визначило, що ефективна система захисту підприємтв виконує три життєво важливі функції: виявлення дії супротивника, затримка (перешкода прогресу супротивника) та реагування персоналу служби безпеки для забезпечення нейтралізації загрози. Приклади традиційних захисних тактик включають посилення патрулювання охорони, зміцнення огороджень, встановлення кращих замків на дверях, переміщення чутливих процесів всередину об'єкта, встановлення систем виявлення зловмисників та сигналізацій, а також проведення перевірок попередньої діяльності працівників[1].

2.3.2 Уніфікований підхід до захисту

Промисловим організаціям завжди доручається захист своїх людей, активів та навколишнього середовища. По суті, фізична безпека допомагає досягти цієї мети, тримаючи неправильних людей ззовні від огорожі, для запобігання вандалізму,

крадіжок і зловмисних дій. Однак сучасне середовище загроз вимагає більш всебічної стратегії вирішення питань безпеки.

Як найкраща галузева практика, багато фірм об'єднують різноманітні аспекти фізичної безпеки підприємств. Цей підхід інтегрує процеси та середовища безпеки для вирішення проблем безпеки від диспетчерської до периметра заводу - і захищає всі активи виробничої операції. Програми безпеки використовують надійні інструменти, такі як відеоспостереження, контроль доступу, виявлення вторгнень по периметру та командні центри, які спільно працюють над ефективним методом захисту промислових об'єктів. Хоча багато інструментів вже деякий час використовуються як самостійні, можливість об’єднати їх в єдину систему додає значну синергію та переваги.

Наявність такого інтегрованого рішення щодо фізичної безпеки дозволяє керівникам та операторам заводів забезпечити виконання своїх головних пріоритетів безпеки, зосереджуючись на інших компонентах безпечної та безпечної експлуатації об'єкта. За допомогою цієї стратегії певні рівні захисту можуть в першу чергу стримувати інциденти, тоді як інші можуть забезпечувати виявлення, попередження та відповідні вказівки. Цей підхід посилює важливі функції безпеки, такі як контроль доступу для збору даних у режимі реального часу під час надзвичайних ситуацій. Заводи більше не стикаються з перевіркою імен з паперового списку, а скоріше використовують такі рішення, як автоматизовані зчитувачі значків, щоб підтвердити, що працівники мають доступ до конкретного приміщення.

Однак для багатьох промислових об'єктів побачити «загальну картину» діяльності може бути важко. Багато джерел даних, проблеми спільної роботи, контекстна обізнаність, безпека становлять складну екосистему, якою важко управляти. Сучасні системи управління відповідають цим викликам, інтегруючи загальнобезпечні ресурси безпеки та роблячи їх доступними за допомогою спільного інтерфейсу людина-машина (ЛМІ). Це рішення зменшує розрив між експлуатаційними елеваторами та об'єднує їх під спільною метою. Користувачі можуть збільшувати та зменшувати наведені дані для отримання детальної

інформації. Крім того, кілька людей у кількох місцях можуть послідовно найкраще реагувати в порядку пріоритетності на ситуацію в безпеці.

Удосконалені інструменти робочого циклу інцидентів направляють персонал заводу на процес прийняття рішень та реагування під час критичних ситуацій. Завдяки безперебійній інтеграції аварійних операцій із системами безпеки вони допомагають зменшити ризик, сприяють безперервності та збільшують продуктивність. Наприклад, уповноважені користувачі можуть виконати ряд дій від одного масового повідомлення до ключових постраждалих людей чи персоналу. Сюди входить автоматичне або ручне керування камерами спостереження, або відмикання та блокування дверей або воріт, щоб дати можливість особам, які швидко реагують, отримати доступ до критичних областей.

Першим кроком у будь-якій ініціативі безпеки на рівні заводу є оцінка вразливості місця для визначення можливих прогалин у захисті. Наріжним каменем визначення потреб об’єкта є розуміння його місця. Організації повинні чітко усвідомлювати не тільки фізичне планування заводу, але й те, як співробітники діють у цьому середовищі. Оцінка додатково вивчить вплив порушення безпеки та його вплив на персонал служби безпеки та операторів процесів. Нарешті, необхідне глибоке розуміння новітніх технологій безпеки, щоб визначити кроки зменшення загрози та способи заповнення виявлених прогалин у безпеці.

Хоча кроки зменшення наслідків унікальні для кожного підприємства, такі практики, як інтеграція систем управління процесами та систем безпеки, можуть посилити ситуаційну обізнаність персоналу процесу та безпеки. Співробітники служби безпеки можуть бути більше поінформовані про випадки, що не стосуються безпеки, а співробітники технологічних процесів - про інциденти, що стосуються безпеки.

2.3.3 Інтегровані технології

Все частіше архітектори систем автоматизації процесів та будівель використовують узгоджену архітектуру системи та додатків. Результатом є уніфіковане рішення для контролю, безпеки та безпеки, завдяки якому

відеоспостереження, контроль доступу та виявлення периметра тісно інтегровані з сигналами тривоги та подіями, що виникають в процесі, та системами безпеки для інтелектуальних, скоординованих реакцій. ЛМІ із загальним зовнішнім виглядом призводить до кращого та швидшого прийняття рішень на пультах диспетчерської та на робочих столах офісів безпеки. Цей підхід також мінімізує складність на всіх етапах впровадження, експлуатації та обслуговування системи.

Якщо на місці коли-небудь трапляється інцидент, усі співробітники служби безпеки та процесу знатимуть про інцидент у режимі реального часу. Керівництво заводу може швидко донести потрібну інформацію до потрібних людей і негайно почати боротьбу з загрозою. Це зменшує ризик і підвищує безпеку.

Відеоспостереження через серверне цифрове замкнуте телебачення (СЦЗТ) є найважливішим компонентом будь-якої інтегрованої програми безпеки. Зазвичай воно використовується для двох цілей: загального спостереження за периметром заводу та критичних внутрішніх місць, а також для моніторингу технологічних процесів, таких як факельні труби або розвантаження залізничних вагонів. Системи відеоспостереження можуть використовувати вибухозахищені камери для небезпечних технологічних середовищ або захищені від фальсифікації камери для районів з великим трафіком.

Інтелектуальні відеосистеми дозволяють відділам управління та безпеки використовувати загальні камери в надзвичайних ситуаціях. Однак оператори переглядають лише ті зображення, які їм потрібно побачити, що стосуються події безпеки або процесу. Ці системи також пропонують можливості «картинка в картинці» для одночасного контролю за безпекою та виробничою діяльністю в різних місцях. У деяких закладах операційна група повинна контролювати охорону та доступ до периметру протягом ночі та в інші періоди мінімальної кількості персоналу.

Централізоване записування, віддалене спостереження за межами майданчика та резервне копіювання відео можуть покращити інтелектуальну відеосистему. Персонал може вказати, коли і які типи записів вони хочуть зробити. Записані зображення можуть включати не тільки інцидент, але й те, що сталося безпосередньо

до і після, забезпечуючи повну картину для покращення процесу розслідування та результатів.

Датчики руху, теплові відеосистеми та інші датчики промислової якості надалі підтримують рішення СЦЗТ. Наприклад, розумні цифрові камери, прив’язані до системи сигналізації заводу, виявляють рух по всій ділянці - якщо виявлено вторгнення людини, спрацьовує сигнал тривоги. Оператори диспетчерської та співробітники служби безпеки отримують повідомлення про тривогу, якщо зловмисник знаходиться поблизу чутливого обладнання технологічного обладнання.

Досвід показав, що цифрове відеоспостереження підвищує безпеку та операційну ефективність; автоматичне виявлення подій покращує реакції оператора, виступаючи наступним поколінням технологічних датчиків. Завдяки загальному відеоспостереженню як для користувачів безпеки, так і для контролю, воно також дозволяє підвищити обізнаність про ситуацію та знизити системні витрати, складність та обладнання.

2.3.4 Переваги цілісного рішення

Застосовуючи цілісне рішення для задоволення потреб як безпеки, так і технологічних операцій, промислові організації можуть значно зменшити ризик, пом'якшити загрози та підвищити загальну готовність до захисту активів. Інтегровані системи виявляють випадки раніше, тому ненормальний час реагування на ситуацію покращується. Використовуючи системи з однаковим зовнішнім виглядом, також знижуються витрати на розробку та навчання.

Покращена фізична безпека також може допомогти захистити корпоративний образ; компанії керують безпекою за меншу кількість інцидентів та покращили безпеку. Дійсно, такий підхід є основою для захисту життя та майна в промислових умовах. Відеоспостереження, викликане подіями та сигналами тривоги, означає кращу реакцію на надзвичайні ситуації, покращену обізнаність та швидше збирання. Наявність історичних даних із цих систем, що відображають події, тривоги та відповідні реакції, допомагає задокументувати належні експлуатаційні процедури та продемонструвати відповідність нормативним актам.

Виробничий завод з більш жорстким рівнем безпеки, який надає доступ лише тим людям, які мають відповідний рівень кваліфікації для певної локації, зменшує ризики відповідальності. Постійний моніторинг активів на всьому об’єкті допомагає зменшити втрати інтелектуальної власності, зменшує орендні та капітальні витрати.

Нарешті, покращена безпека є одночасною з більшою продуктивністю, оскільки захист будівельних майданчиків та місць для забудови за допомогою аналітичного відео-аналізу зменшує ризик крадіжок, що, в свою чергу, допомагає забезпечити швидкі запуски та безперебійне виробництво. А інтегровані рішення означають менші витрати на технічне обслуговування, більшу ефективність та підвищену прибутковість.

Наближення до фізичної безпеки без плану зазвичай призводить до роз’єднаних зусиль. Багато промислових операцій витратили десятки тисяч доларів на огородження та барикади, не визнаючи необхідності більш широкої співпраці між тими сторонами, які повинні визнати та відповісти на загрози безпеці, що впливають на добробут об'єкта.

Комплексний підхід до фізичної безпеки починається з проведення дійсного обстеження вразливості, розуміння вимог об'єкта та використання перевіреної часом концепції стримування, виявлення та затримки. Він також покладається на багаторівневе рішення, яке пов'язує управління процесами з фізичною безпекою на заводі, створюючи видимість на рівні підприємства та лінію зору, необхідну для задоволення нових вимог щодо запобігання загрозам та реагування.

Сучасні технології можуть забезпечити загальне уявлення про вразливі місця для персоналу з управління процесами та охорони, а також забезпечити захист від кімнати управління технологічним процесом до периметра заводу, захищаючи таким чином усі активи виробничої операції.

2.4 Бізнес-проблеми

2.4.1 Використання важкого обладнання

Виробничі компанії використовують важку техніку, але неправильне та невчене використання та нагляд часто призводять до великих ризиків. Безпека робочого місця

є особливо важливим комерційним ризиком у виробничих середовищах. Компенсація робочого часу, час простою та лікарняні часто призводять до дуже високих витрат. На обробну промисловість припадає майже 10 відсотків загальної кількості робочої сили США або 14 мільйонів людей [5]. У 2006 році Бюро статистики праці повідомило, що кількість виробничих травм на виробництві, що не призвело до смертних випадків, становила 859 100. Це становить майже 6,1 відсотка робочої сили, що призводить до мільйонів людських годин відпусток та простоїв, а отже і зниження продуктивності праці. Наглядачі можуть стежити за працівниками за допомогою камер спостереження та втручатися у випадках неправильного використання обладнання для зменшення кількості нещасних випадків та виробничого травматизму, тим самим збільшуючи продуктивність праці та покращуючи операційний прибуток.

Неправильне використання обладнання та вторгнення - це ризики, з якими регулярно стикаються всі виробничі компанії. За останні 2 роки рівень крадіжок міді різко зріс. Ці ризики можна зменшити, стежачи за допомогою датчиків виявлення пожежі, відеоспостереження, контролю доступу та датчиків виявлення вторгнень. Технологія відіграє ключову роль у зменшенні впливу цих викликів і сприяє підвищенню безпеки та безпеки працівників, одночасно зменшуючи втрати майна.

2.4.2 Складський контроль

Склади загрожують загибеллю внаслідок пожежі, пошкодження води та крадіжок. Це призводить до виклику бізнесу прогнозувати та запобігати збиткам, які включають дуже цінні запаси. Убезпечити навколишнє середовище можна за допомогою датчиків навколишнього середовища, таких як виявлення чадного газу, датчиків пожежі та диму, датчиків вологості тощо.

Знизити крадіжки можна за допомогою датчиків виявлення вторгнень та пристроїв контролю доступу, які можуть запобігти потраплянню несанкціонованих людей на склади. Інші ключові функції, пропоновані компаніями з моніторингу, такі як віддалена віртуальна охорона та послуги дистанційного моніторингу, можуть допомогти зменшити вплив цих ризиків.

2.4.3 Продуктивність працівників

На потоки доходів виробників безпосередньо впливає низька продуктивність праці працівників. Існують різні фактори, що знижують продуктивність праці працівників, такі як:

- низька або неповноцінна якість продукції;
- компенсації працівникам;
- лікарняна відпустка;
- простої.

Продуктивність працівників можна покращити за допомогою відеоспостереження, віддаленого моніторингу та віртуальної охорони шляхом постійного спостереження за працівниками, щоб забезпечити обережне дотримання всіх етапів процесу, коли всі працівники прибувають вчасно і працюють відповідно до встановлених правил.

2.4.4 Безперервне виробництво

Виробничі потужності працюють цілодобово з трьома змінами працівників щодня. Змінна робота представляє різні проблеми, що призводять до зниження рівня безпеки працівників. Характер роботи може призвести до високого рівня втомленості працівників та відсутності безпеки на стоянках вночі. Швидка реакція на втомлених працівників може допомогти керівникам підтримувати якість та підвищити безпеку працівників. Співробітники вразливі до атак та аварій на автостоянках у нічний час. Використання відеоспостереження, віддаленого моніторингу та віртуальної охорони може зменшити випадки загроз та захистити працівників.

2.5 Технологічні рішення для проблем бізнесу

Впровадження технологій у бізнесі часто вирішує не тільки своє основне завдання. Нові технології часто є шляхом до покращень в одразу кількох напрямках, навіть якщо це не передбачалось на етапі планування. У Таблиця 2.1 нижче наведені приклади проблем, технологічних рішень та додаткових переваг.

Таблиця 2.1 – Технологічні рішення для проблем бізнесу

Проблеми бізнесу	Технологічні рішення	Сервіси доданої вартості
Важке обладнання	– Відеоспостереження – Контроль доступу – Виявлення несанкціонованого входу – Виявлення пожежі	– Віддалений нагляд – Онлайн моніторинг та контроль
Контроль інвентарю	– Відеоспостереження – Виявлення несанкціонованого входу – Контроль доступу – Сенсори середовища	– Віддалений нагляд – Віртуальна охорона – Онлайн моніторинг та контроль
Продуктивність працівників	– Відеоспостереження – Контроль доступу до мережі	– Віддалений нагляд – Віртуальна охорона
Безперервні операції	– Відеоспостереження – Система масових сповіщень	– Віддалений нагляд – Віртуальна охорона

2.5.1 Контроль доступу

Старомодні ключі та кодові замки мають кілька проблем із безпекою. Працівники неохоче ними користуються, часто підпираючи відчинені двері, оскільки вони трудомісткі та незручні. Крім того, замки та їх комбінації змінюються при звільненні кожного працівника, що впливає на всіх працівників. За допомогою електронної системи контролю доступу затверджений працівник може просто провести пальцем по своїй картці для повторного входу. Якщо картка втрачена або працівник звільнився, вона може бути вимкнена та видана інша. Рішення для

контролю доступу на основі біометрії пропонують ще жорсткіший зовнішній/внутрішній контроль.

2.5.2 Захист навколишнього середовища

Виробничі операції вимагають постійного контролю для захисту працівників та майна від надлишкового рівня води та чадного газу, а також від екстремальних температур та інших пов’язаних з ними умов. Екологічні датчики інтегровані з відеоспостереженням та іншими технологіями безпеки для цілодобового моніторингу багатьох з цих умов, незалежно від того, чи система запущена. Інтегруйте традиційний моніторинг з веб-управлінням та моніторингом для віддаленого сповіщення електронною поштою або стільниковим телефоном[2].

2.5.3 Протипожежний захист

Правила пожежної безпеки та безпеки життєдіяльності стають дедалі складнішими для підприємств. Власники та оператори виробництв та складів можуть скористатися перевагами місцевої, технічної експертизи та продуктів, які допомагають забезпечити безпеку їх бізнесу та працівників та відповідність місцевим, державним та національним вимогам. Системи протипожежного захисту призначені для виявлення тепла та диму цілодобово та без вихідних, навіть коли системи не мають озброєння, а персонал моніторингу може координувати дії з органами надзвичайних ситуацій, щоб надати виробникам якнайшвидшу реакцію у критичних випадках.

2.5.4 Захист від проникнення

Кінцеві користувачі можуть додати систему вторгнення, контролю доступу та відеоспостереження, щоб побудувати повністю інтегровану систему безпеки, яка контролюється спеціально навченими операторами у цілодобовому Центрі безпеки бізнесу. Деяке обладнання, що використовується для виявлення вторгнень, що допомагає захистити співробітників, інвентар та обладнання, включає детектори

руху, фотоелектричні промені, магнітні контакти, датчики удару та тиску, а також детектори розбиття скла.

2.5.5 Система масового сповіщення

Будь то попередження людей про надзвичайні ситуації або просто спосіб зв'язку на об'єкті, інтегрована система домофону допоможе захистити об'єкт і забезпечить керівництво працівниками та клієнтами.

2.5.6 Відеоспостереження

Відеоспостереження може допомогти захистити співробітників та майно. Власники та співробітники служби охорони можуть співпрацювати з продавцями при виборі відповідної внутрішньої/зовнішньої камери та рішення цифрового запису для власності. Користувачі можуть керувати функціями панорамного нахилу окремих камер, вводити команди запису та одночасно переглядати високоякісні живі зображення з одного комп’ютера. Захоплені кадри можуть бути використані як докази для сприяння розслідуванням, розуміння природи загроз у місці чи для навчальних цілей.

2.5.7 Контроль мережевого доступу

Контролюйте та керуйте доступом до об'єкта з будь-якого місця за допомогою підключеного до Інтернету комп'ютера, розширеного мережевими системами контролю доступу. Керівництво може входити в систему, щоб переглядати інформацію про користувача та точки доступу, крім дозволу або заборони доступу в користувачеві, групі, місцезнаходженні тощо. Сповіщення, складання звітів та реєстрація відбитків пальців можуть здійснюватися в Інтернеті.

2.5.8 Віддалений нагляд

Виробничі потужності можна контролювати практично з будь-якого місця, переглядаючи відео в реальному часі з будь-якої підключеної камери на

підключеному до Інтернету комп’ютері. Операторам моніторингу та органам влади може бути забезпечена візуальна перевірка реальних подій тривоги вдома або з усієї країни. Електронні повідомлення з відеозображеннями та до та після активації сигналізації є корисними інструментами для розуміння інцидентів та запобігання в майбутньому.

2.5.9 Дистанційний моніторинг

Незалежно від місця розташування виробничих потужностей, спеціалісти з дистанційного моніторингу можуть проводити віддалені віртуальні екскурсії по приміщеннях з моніторингових центрів. З дозволу кінцевого користувача професіонали можуть отримувати доступ до камер та систем запису та контролювати їх і переглядати ваш бізнес зсередини та зовні, додаючи ще один рівень безпеки до вторгнень, протипожежного захисту та інших датчиків. У випадках, коли на об'єктах присутній персонал служби безпеки, можливість поєднання віртуальної та фізичної охорони - це послуга, яка може допомогти кінцевим споживачам зменшити витрати та підвищити ефективність.

2.5.10 Онлайн-контроль

Служби моніторингу, контролю та сповіщення з підтримкою Інтернету та тексту зазвичай включають:

– сучасний моніторинг центральної станції на предмет вторгнення, пожежі та інших тривожних подій;

– можливість дистанційного запуску та зняття з охорони систем за допомогою телефону або комп’ютера;

– самоконтроль та контроль через захищений веб-інтерфейс на будь-якому підключеному до Інтернету комп’ютері;

– текстові повідомлення та повідомлення електронною поштою про тривожні та нетривожні події (доступ до заборонених номерів, зняття системи з охорони);

– доступний онлайн віддалений моніторинг відео з ініційованими подіями зображеннями, що надсилаються на авторизовані комп’ютери чи мобільні пристрої - Інтернет-доповнює існуюче відеоспостереження, щоб допомогти контролювати та керувати працівниками та іншими внутрішніми ризиками.

2.5.11 Індивідуальні рішення

Провідні постачальники послуг з моніторингу тривоги допомагають розробити та виконати рішення незалежно від того, які технічні характеристики та обладнання для цього потрібні. Якщо в друкованих матеріалах немає інформації, інструктаж консультантів з питань безпеки щодо потреб може допомогти роботодавцям рухатись у правильному напрямку.

2.6 Повернення інвестицій

Хоча системи контролю за вторгненням та пожежею є зрозумілими основними потребами для більшості виробників, ми рекомендуємо компаніям створити прогнозовану рентабельність інвестицій перед впровадженням більш надійної системи фізичної безпеки. Однією з основних цілей рентабельності інвестицій у складській та обробній промисловості є розрахунок безпосереднього впливу систем безпеки на зменшення ризику та підвищення ефективності.

Для того, щоб визначити найкращий набір функцій та функцій, які слід встановити, компаніям слід розраховувати на те, що їхній партнер служби безпеки надасть проформу або прогнозовану рентабельність інвестицій для обґрунтування переваг рекомендованих продуктів та послуг безпеки, постачальників послуг охорони, які готові створити відповідний бізнес-кейс щодо рентабельності інвестицій та уникати тих постачальників, яким бракує навичок або досвіду у проектуванні позитивної віддачі.

Ця прогнозована рентабельність власності на встановлені системи базується на загальній вартості володіння порівняній з очікуваними виграшами в продуктивності та зменшенням втрат або травм:

– продуктивність працівників (контроль якості);

– вплив на страхові тарифи;

– висока вартість запасів;

– зменшує втрати (внутрішні та зовнішні крадіжки);

– скорочення простоїв із травмами зі смертельним наслідком та без летальних наслідків;

– підвищення рівня безпеки працівників;

– знижує штрафи за порушення стандартів безпеки;

– зменшення впливу екологічної шкоди;

– зниження витрат, пов’язаних з вандалізмом та графіті;

– менші витрати на навчання нових співробітників (нижчі показники виснаження).

Зразок інструменту розрахунку рентабельності інвестицій наведено у Таблиця 2.2 нижче.

Таблиця 2.2 - Розрахунку рентабельності інвестицій

	Ціна інвестиції	Покращення від інвестиції
Сума інвестиції	X	
Операційні витрати	X	
Продуктивність працівників (контроль якості)		X
Вплив на ставку страхування		X
Висока ціна інвентаризації		X
Зменшення втрат (внутрішні та зовнішні крадіжки)		X

Продовження Таблиця 2.2.

Зменшення періоду простоювання через травми		X
Покращення безпеки працівників		X
Зменшення штрафів через порушення стандартів		X
Зменшення впливу на забруднення середовища		X
Зменшення ціни тренування нових працівників		X

$$\text{ПІ} = \frac{\text{Прибуток від інвестиції} - \text{Вартість інвестиції}}{\text{Вартість інвестиції}}$$

Розрахунки рентабельності інвестицій базуються на різниці між прибутком від інвестиції та вартістю інвестиції, поділеною на вартість інвестиції. Потенційну рентабельність інвестицій слід розраховувати, виходячи з розумних припущень про вигоди, прибутки та економію протягом певного періоду часу (для більшості обладнання безпеки 4-6 років). В середньому очікується, що прибутковість повинна отримати беззбитковість і почати окуплятися протягом 2-3 років[1]. Ця кількість залежить від ефективного використання встановлених систем безпеки, і компаніям слід очікувати певної мінливості прибутковості залежно від унікальних обставин їхньої ситуації. Використання високотехнологічних та індивідуальних систем безпеки допомагає кінцевим користувачам отримувати більші вигоди та, ймовірно, матиме позитивну рентабельність інвестицій за коротший проміжок часу.

2.7 Зміни у 2020 році

У багатьох країнах хімічна промисловість розглядається як важлива частина національної інфраструктури, рівна за значенням енергетичному, водному та харчовому секторам. Зв'язок між хімічним та фармацевтичним секторами робить захист виробництв ще більш важливим, тоді як світ працює якомога швидше, щоб створити вакцини проти глобальної пандемії коронавірусу.

Практично всі, хто працює, зараз працюють не так, як у 2019 році. Багато співробітників, які раніше працювали в офісі, зараз працюють вдома, створюючи потребу в підвищеному захисті входу в систему, захисті паролем та автентифікації. Багато працівників промисловості все ще повинні працювати на своїх заводах, але додаткова інфраструктура, необхідна для захисту людей від зараження інфекційна хвороба, яку спричиняє новий штам коронавірусу COVID-19, є додатковим тягарем, який необхідно оцінювати, контролювати та управляти ним.

3 ОГЛЯД ВИРОБНИЦТВА МІНЕРАЛЬНИХ ДОБРИВ

Мінеральні добрива - це матеріали, природні чи виготовлені, що містять поживні речовини, необхідні для нормального росту та розвитку рослин. Поживні речовини для рослин - це їжа для рослин, деякі з яких використовуються безпосередньо для харчування людини, інші для годівлі тварин, постачання природних волокон або виробництва деревини. Людина і всі тварини повністю залежать від рослин, щоб жити і розмножуватися. Громадське сприйняття мінеральних добрив часто не враховує цих простих фактів.

Три поживні речовини для рослин застосовуються у великих кількостях - азот, фосфор та калій. Сірка, кальцій і магній також потрібні у значних кількостях. Ці поживні речовини є складовими багатьох рослинних компонентів, таких як білки, нуклеїнові кислоти та хлорофіл, і мають важливе значення для таких процесів, як передача енергії, підтримання внутрішнього тиску та дії ферментів. Сім інших елементів необхідні в малих або мікроелементах і називаються «мікроелементами». Ще п’ять елементів потрібні певним рослинам. Ці елементи виконують різноманітні основні функції в обміні речовин рослин. Метали є складовими ферментів, що контролюють процеси рослин. Дефіцит будь-якої поживної речовини може скомпрометувати розвиток рослини[7].

Мінеральні добрива містять природні елементи, необхідні для життя. Вони дають життя і не є біоцидами. Добрива використовуються для того, щоб:

– доповнити природний запас поживних речовин у ґрунті;

– з метою задоволення попиту на культури з високим потенціалом урожайності та отримання економічно вигідних урожаїв;

– компенсувати поживні речовини, втрачені видаленням рослинних продуктів або вимиванням або втратою газоподібних речовин;

– покращити несприятливий стан або підтримувати хороші ґрунтові умови для посіву.

Існування тісного взаємозв'язку між рівнем споживання добрив та продуктивністю сільського господарства було встановлено без сумніву (Рисунок 3.1).

Серед різноманітних сільськогосподарських ресурсів добрива, можливо поруч із водою, найбільше сприяють збільшенню сільськогосподарського виробництва.

Рисунок 3.1 – Виробництво злакових та споживання мін. добрив

3.1 Як використовуються мінеральні добрива

Використання добрив як звичайна сільськогосподарська практика розпочалось у більшості європейських країн у середині та наприкінці XIX століття, але найбільший приріст споживання у цих країнах відбувся у три десятиліття після Другої світової війни. Їх все більше використання в країнах, що розвиваються, розпочалося в 1960-х.

У 1960 р. 87% світового споживання добрив припадало на розвинені країни, включаючи СРСР та країни Центральної Європи. З 1980 по 1990 р. Споживання, як правило, стабілізувалося в цих регіонах, крім СРСР, де воно зростало до 1988 р. Зростання чисельності населення вирівнювався, майже всі мали достатнє харчування, світовий експорт сільськогосподарської продукції стагнував через економічні проблеми в країнах-імпортерах і далі добре керовані господарства досягли економічного оптимуму наявних сортів [7].

Між 1989 і 1994 рр. Споживання добрив у розвинутих країнах в цілому впало з приблизно 84 млн. т поживних речовин у 1988р. до 52 млн. т поживних речовин у 1994р [7]. Найбільше падіння, на 80%, було в колишніх комуністичних країнах

Центральної Європи та колишнього Радянського Союзу. Виробництво рослинництва в цьому регіоні також впало, хоча і не в такій мірі. Це було пов’язано з тим, що за централізовано запланованою системою добрива використовувались неефективно, а наявні в рослині запаси деяких поживних речовин накопичувались у ґрунті і тепер їх можна видобувати для допомоги в поживі сільськогосподарських культур.

У країнах, що розвиваються, до 1960-х р. добрива застосовували переважно для плантаційних культур, таких як чай, кава, олійний пальм, тютюн і каучук, тоді як внесення в польові культури був або невеликим, або його взагалі не було. Навіть там, де застосовували добрива, норми внесення мали бути малими з огляду на традиційні високорослі сорти злаків, які культивувались на той час. Запровадження високопродуктивних карликових сортів, що реагують на добрива, в середині та кінці шістдесятих років дало значний приріст споживанню добрив, що застосовуються до однорічних польових культур. На жаль, цей розвиток все ще не відбувся у багатьох країнах Африки на південь від Сахари, з економічних та кліматичних причин, а також через відсутність відповідних сортів.

Починаючи з 1960 р. споживання добрив у країнах, що розвиваються, зростало більш-менш безперервно, і сьогодні воно становить близько 60% усього світу, порівняно з 12% у 1960 р., Тенденція, все-ще продовжується. Зважаючи на їх швидко зростаюче населення, багато країн, що розвиваються, змушені надавати сільськогосподарському виробництву та розвитку добрив пріоритет [7].

У період між 1993/94 та 1997/98 рр. Загальне споживання поживних речовин у добривах у світі зросло зі 120 до 136 млн т, середня швидкість приросту склала приблизно 3% в рік. Споживання в Китаї, Південній Азії та Латинській Америці зросло на 10, 5 та 2 млн т відповідно. Але у більшості країн Африки на південь від Сахари кількість добрив, що використовуються, не тільки дуже низька, але й більша частина того, що використовується, застосовується в комерційному секторі плантацій [7].

3.2 Токсичні сполуки

Фосфатні добрива часто містять невелику кількість елементів, які природним чином містяться у фосфатній породі і передаються в процесі виробництва до готового продукту. Коли кінцевим продуктом є відносно цінний матеріал, призначений для використання, наприклад, у харчовій промисловості потенційно шкідливі елементи видаляються, але на сьогодні економічні процеси для економічного видалення цих елементів у виробництві добрив не знайдені. Серед цих елементів найбільша увага приділяється кадмію (Cd).

Є дані про те, що в деяких ґрунтах Cd повільно накопичується. Це викликає занепокоєння, оскільки Cd не є важливим для рослин чи тварин, а при високому рівні може бути токсичним. Джерела включають атмосферне випадання в результаті промислових процесів, мули стічних вод, гній тварин та фосфорні добрива. У багатьох європейських країнах близько 50% загального внесення Cd в сільськогосподарські ґрунти надходить із повітряних джерел. Мули стічних вод містять відносно велику кількість Cd, яка може коливатися від декількох проміле до декількох тисяч на годину. Використання у виробництві фосфатних добрив з фосфатних порід з низьким вмістом кадмію є одним із рішень, але загальна пропозиція обмежена. Це робить акцент на розробці ефективних та життєздатних процесів видалення кадмію, і дослідження з цією метою продовжуються[7].

Зрештою, рішенням може бути поєднання видалення Cd у процесі виробництва та стратегій управління фермами, які мінімізують його потенційний вхід у харчовий ланцюг. На засвоєння Cd рослинами насправді може впливати безліч факторів, таких як pH ґрунту, вміст вологи, різноманітність тощо, які фермер може контролювати.

Азот може втрачатися із сільськогосподарських систем у трьох формах, що може спричинити забруднення; втрати нітратів вимиванням, випаровування аміаку та втрати оксиду азоту під час денітрифікації або нітрифікації. Втрата аміаку в атмосферу та подальше його осадження сприяє евтрофікації природних середовищ існування та морських вод, а також підкисленню ґрунтів та озер, оскільки NH4 перетворюється на NO3. Втрати від денітрифікації нешкідливі, якщо кінцевим

продуктом є газ азоту, але якщо отриманим газом є оксид азоту, це сприяє парниковому ефекту та виснаженню озону у верхніх шарах атмосфери.

Негайної терміновості немає, оскільки, крім кількох місць, сильно забруднених промисловістю, рівень кадмію у грунті, як правило, значно нижчий за критичний. Однак існування середньо- та довгострокової проблеми визнано в галузі виробництва добрив, і дослідження та дослідження з цього питання тривають.

3.3 Правила безпеки

Зберігання та поводження з добривами. Зберігання тепличних добрив містить концентровані поживні речовини, які необхідно зберігати та правильно ними керувати. Добрива можуть завдати шкоди, якщо потрапляють до поверхневих або підземних вод. Надмірна концентрація нітратів у питній воді може спричинити загрозу здоров'ю, особливо у маленьких дітей. Фосфор може транспортуватися до поверхневих вод і спричиняти цвітіння та евтрофікацію водоростей; що призводить до поганої якості води. Зберігання добрив окремо від інших хімічних речовин у сухих умовах може мінімізувати ці ризики. Потрібна особлива обережність щодо концентрації маточних розчинів. Завжди слід використовувати вторинне утримання.

Несвоєчасне внесення добрив призводить до надмірного викиду з виробничої системи у поверхневі та / або підземні води. Потенційні проблеми можна звести до мінімуму за рахунок належної екологічної обізнаності, навчання працівників та готовності до надзвичайних ситуацій. Нижче наведено рекомендації щодо правильного зберігання та обробки тепличних добрив.

Місце зберігання. Території зберігання добрив містять порівняно велику кількість концентрованих хімічних речовин. Ризики в місцях зберігання включають викид через зламану, пошкоджену або негерметичну тару; втрата безпеки, що веде до безвідповідального використання; накопичення застарілих матеріалів, що призводить до надмірної кількості добрив, що надмірно підвищує рівень ризику; спалювання окислювальних сполук у добривах (наприклад, нітратів), спричинене пожежею чи іншою катастрофою.

Найменший ризик передбачає наявність будівлі чи території, призначеної для зберігання добрив, яка відокремлена від офісів, поверхневих вод, сусідніх житлових будинків та водойм; окремо від пестицидів та захищена від сильної спеки та повеней. Зона зберігання повинна мати непроникну підлогу з вторинним резервуаром, подалі від рослинних матеріалів та місць з великою прохідністю. Обладнання для очищення повинно бути легко доступним.

Місця зберігання не повинні містити пестицидів та інших парникових хімікатів; місця зберігання можуть містити загальні тепличні запаси; не повинно бути їжі, напоїв, тютюнових виробів або корму для худоби. Наступні рекомендації повинні бути дотримані у кожного складському приміщенні:

– мають бути забезпечені піддони, щоб тримати великі барабани або сумки окремо від підлоги. Полиці для менших контейнерів повинні мати кришку, щоб контейнери не могли легко зісковзнути. Сталеві полички легше чистити, ніж деревину, якщо трапляється розлив;

– якщо планується зберігання великих насипних цистерн, має бути передбачена зону зберігання, достатня для того, щоб умістити 125 відсотків вмісту найбільшого насипного контейнера;

– будівля чи зона зберігання має триматись зачиненою та чітко позначена як зона зберігання добрив. Запобігання несанкціонованому використанню добрив зменшує ймовірність випадкового розливу або крадіжки. Етикетки на вікнах та дверях будівлі дають пожежникам інформацію про добрива та інші продукти, що зберігаються під час аварійної реакції на пожежу або розлив. Рекомендується вести окремий список хімікатів та їх кількості. Якщо сталась пожежа, подумайте, куди піде вода, яка використовується для боротьби з пожежею, і де вона може збиратися. Наприклад, бордюр навколо підлоги може допомогти обмежити рух забрудненої води.

– має бути забезпечений адекватний доступ до дороги для доставки та використання, а також, роблячи територію зберігання безпечною, також зробіть її доступною, щоб дозволити швидке вивезення добрив та інших хімічних речовин;

– ніколи не зберігайте добрива всередині приміщення для свердловин або приміщення, що містить покинуту криницю.

Якісні контейнери - це ваша перша лінія захисту від розливу або витоку. Якщо контейнер випадково розірваний або збитий з полиці, розлив повинен бути обмежений безпосередньою зоною та негайно очищений. Будівля повинна мати тверду підлогу та, для рідких добрив, бордюр. Об'єм контейнера повинен бути достатньо великим, щоб вмістити вміст найбільшого повного контейнера.

Контейнери. Добрива слід зберігати в оригінальних контейнерах, якщо вони не пошкоджені; етикетки повинні бути видимими та читабельними; контейнери для їжі та напоїв ніколи не слід використовувати для зберігання. Етикетки повинні бути на виду; жодні контейнери не повинні контактувати з підлогою; всі контейнери слід зберігати вгорі; проходи повинні бути досить широкими, щоб зручно розмістити робітників; контейнери не повинні переповнюватися на полицях або піддонах.

Частково використані контейнери. Паперові пакети та коробки слід відкривати ножем або ножицями; відкриті контейнери слід запечатати і повернути на зберігання; всі відкриті паперові пакети повинні бути запечатані всередині іншого, більшого контейнера, та промарковані.

Пошкоджені контейнери. Контейнери слід часто перевіряти на наявність пошкоджень; коли помічені пошкоджені контейнери, вміст слід упаковувати та промаркувати або помістити у відповідний вторинний контейнер, який можна запечатати та промаркувати.

Обмеження. Не повинно бути стоку для підлоги; підлога повинна забезпечувати утримання в разі розливу; повинен бути вторинний резервуар, який зазвичай використовується для більшості відкритих контейнерів; пошкоджені або протікаючі контейнери слід якомога швидше відремонтувати та/або замінити; весь розлитий матеріал слід очистити після виявлення; а матеріали для чищення слід негайно та належним чином утилізувати.

Запобігання та ліквідація пожежі. Повинна бути присутня система пожежної сигналізації та сигналізації; окислювачі та легкозаймисті матеріали слід зберігати

окремо; вогнегасник повинен бути негайно доступний; пожежна служба повинна щонайменше щороку повідомлятися про поточну інвентаризацію.

Інвентаризація та ведення діловодства. Інвентаризація повинна активно вестись у міру додавання або вилучення хімічних речовин зі складу; контейнери повинні бути датовані при придбанні; застарілі матеріали слід регулярно вилучати; інвентаризацію слід контролювати, щоб запобігти накопиченню надлишку матеріалу, який може стати важким у використанні.

Освітлення. Електричне освітлення повинно дозволяти оглянути всі зони та шафи в зоні зберігання.

Моніторинг. Потрібно проводити щомісячну перевірку сховища на предмет:

– ознак корозії контейнерів або інших пошкоджень - контейнери, що протікають або пошкоджені, слід перепаковувати, як слід;

– несправні вентиляційні, електричні та протипожежні системи - проблеми слід повідомляти та виправляти.

Безпека. Кімната для зберігання повинна бути зачинена на замок, а доступ - лише для навченого персоналу.

Вивіски. Повинні бути розміщені вивіски; за потреби слід використовувати попереджувальні знаки; інформація про екстрені контакти повинна бути розміщена.

Контроль температури. Повинен бути активний механічний контроль температури і відсутні прямі джерела тепла (сонячні вікна, паропроводи, печі тощо).

Вентиляція. Система вентиляції повинна працювати.

Зберігання та ведення записів. Резервуари для запасів добрив повинні бути марковані складом та концентрацією добрив; слід вести записи щодо складу добрив, концентрації, дати та місця внесення; слід вести записи про аналіз поживних речовин середовища.

Зберігання концентрованих запасів. Концентрований запас слід зберігати поблизу інжектора в поліетиленових або поліпропіленових контейнерах високої щільності з надміцними стінками; слід забезпечити вторинне стримування.

Утилізація. Слід розробити достатнє планування, щоб виключити необхідність утилізації; порожні контейнери для добрив слід викидати на підставі останньої поради органів охорони навколишнього середовища.

Видалення осаду та залишків. Системи добрив слід очистити. Тверді речовини та розчин для промивання слід компостувати.

Запобігання розливу та готовність. Відкриття контейнерів для добрив, вимірювання кількості та передача добрив до системи доставки включає певний рівень ризику від розливу. Вторинне утримування слід регулярно використовувати для резервуарів для добрив; матеріали для очищення від розливів слід використовувати для рідин (наприклад, абсорбуючих матеріалів), а тверді речовини (наприклад, лопата, сміттєвий посуд, мітла та порожні та / або відра) повинні бути доступні в межах загальної площі.

Система доставки. Обладнання для фертигації слід перевіряти щомісяця на точність; повинні бути перевірені резервуари для запобігання, запобіжники зворотного потоку та будь-яке обладнання, що містить добриво у сухому або рідкому вигляді; резервуари слід оглядати щотижня на предмет пошкоджень та тріщин; слід дотримуватися рекомендацій виробника при калібруванні або роботі на обладнанні інжектора добрив; Резервуари для запасів розчину та місця, що оточують форсунки добрив та концентровані розчини, повинні бути чистими та без сміття.

3.4 Партнери у охороні середовища

Не слід допускати, щоб ідеологічні суперечки щодо використання мінеральних добрив відволікали увагу від головної проблеми, яка полягає в тому, що неефективне використання мінеральних добрив представляє марну трату ресурсів, великі економічні втрати та може спричинити значні екологічні проблеми. Покращення ефективності використання добрив також може зменшити вплив на навколишнє середовище.

У розвинених країнах ефективність використання добрив зростає і повинна продовжувати зростати, але це не так у більшості країн, що розвиваються. Метою має бути оптимізація сільськогосподарського виробництва на одиницю внесеного

добрива, в той час як внесення необхідних кількостей добрив для задоволення світових потреб у сільському господарстві.

Добрива зараз, безперечно, в центрі дискусії про їжу, навколишнє середовище та суспільство. Фермери вносять добрива в поле. Компанії, що виробляють добрива, також впливають на суспільство та навколишнє середовище через виробничий процес. Поміж ними знаходиться весь ланцюг постачання та розподілу з безліччю організацій, інститутів та приватних осіб. Існують також дослідження/розробки та маркетинг.

Промисловість добрив складається з багатьох взаємопов'язаних організацій, виробників, дистриб'юторів, інститутів, програм та асоціацій, а також приватних осіб. Кожна організація певною мірою обмежена тим, що вона може зробити, оскільки частина ланцюга поставок знаходиться поза її контролем. Тим не менше, немає єдиного погляду на те, як можна створити синергію, якщо не існує окреслення корисної ролі для кожної групи, щоб їх внесок доповнив колективний рух у напрямку сталого розвитку.

Координація всередині галузі добрив є роллю таких асоціацій, як Міжнародна організація хімічних добрив, але галузь добрив не може розглядатися окремо. Це важливий, але не єдиний сільськогосподарський матеріал, а метою усіх ресурсів є збільшення виробництва сільськогосподарської продукції. Ринок останніх залежить від попиту споживачів. Отже, як і галузь добрив, споживачі також несуть відповідальність перед суспільством та своїм навколишнім середовищем[7].

Щонайменше дванадцять категорій установ беруть участь у встановленні екологічно стійкого використання добрив:

– асоціації фермерів;

– виробники та розповсюджувачі добрив;

– асоціації добрив, національні та міжнародні;

– інші постачальники сировини та їх асоціації; насіння, засоби захисту рослин тощо;

– сектор сільськогосподарського маркетингу, переробники продуктів харчування, дистрибутори та роздрібні магазини;

– банки та кредитні установи;

– навчальні заклади;

– національні уряди. Міністерства сільського господарства та охорони навколишнього середовища, але й інші міністерства, міністерство охорони здоров'я та праці, відіграють роль регулятора;

– урядові дослідницькі та консультативні служби особливо актуальні для сектора добрив;

– міжурядові організації та ООН, такі як Європейська комісія, ФАО, ОЕСР, ЮНЕП, ЮНІДО, Світовий банк;

– недержавні організації;

– донорські організації - двосторонні та багатосторонні.

– що стосується мінеральних добрив, то існують значні проблеми, пов’язані з їх недостатнім використанням, надмірним використанням та неправильним використанням. У багатьох країнах здійснюється недостатня науково-консультативна діяльність. Ані приватний, ані державний сектор не можуть вирішити ці проблеми. Для сталого розвитку необхідна співпраця та участь усього ланцюжка поставок.

– у деяких сферах застосовується більш глобальне бачення. Наприклад, на міжурядовій конференції 1994 р. У Каїрі щодо світового населення вивчалося рівняння продовольства і населення не простими умовами: багатий-бідний, північ-південь, голодний-перегодований, а як серія складних взаємозв'язків між розвитком для підтримання та підвищення рівня життя зменшення приросту населення та кращий захист навколишнього середовища [7].

4 ОПТИМІЗАЦІЇ СИСТЕМИ ЗАХИСТУ КРИТИЧНИХ РЕСУРСІВ НА ВИРОБНИЦТВІ МІНЕРАЛЬНИХ ДОБРИВ

Дослідження операцій часто приводить до аналізу систем, які називаються системами масового обслуговування (СМО). Такими системами, для прикладу, можуть бути кордон хімічного підприємства або лінія подавання складників для хімічного виробництва. Так, як тривалість обслуговування та потік заявок є випадковими, то, як правило в таких СМО проходить деякий випадковий процес. Для того, щоб визначити та скласти рекомендації та інструкції для оптимальної роботи такої системи, потрібно дослідити випадковий процес, який протікає в системі, створити його математичний опис[8].

Дослідження СМО та розпізнавання деякої залежності між характеристиками потоку заявок, кількістю каналів, їх продуктивністю, правилами роботи СМО та ефективністю (успішністю) роботи було увагою багатьох дослідників. Зокрема, окремі аспекти цього питання аналізувалися в роботах [8-10]. У цих працях увага в основному приділялася процесам, які являють собою марковські випадкові процеси з дискретними станами та неперервним часом. З певним ступенем точності саме такі процеси характерні для пунктів пропуску, а також для систем експлуатації технічних засобів охорони кордону.

Реальний рівень якості роботи СМО сильно залежить від ресурсного забезпечення. Оскільки ця залежність, у більшості випадків, є опосередкованою, а не прямою, то неочевидними видаються ресурсні призначення, які оптимізують ефективність СМО. Саме це зумовлює актуальність задачі оптимізації характеристик СМО.

4.1 Загальні визначення

Вважатимемо, що в досліджуваній системі протікає марковський випадковий процес з дискретними станами та неперервним часом. Він часто характеризуються заданими станами S_i, переходами між ними, густинами ймовірностей переходів λ_{ij},

ефективностями W_i кожного стану та ймовірностями $p_i|_{t=0}$ перебування в заданих станах у початковий момент часу.

Вважатимемо також, що відомими є функціональні залежності значень густин ймовірностей переходів $\lambda_{ij}(x)$ від вартості x їх реалізації.

Крім цього, прийматимемо до уваги і те, що теоретично існує можливість реалізації відсутніх у графі переходів між станами і ця можливість пов'язана з ресурсним забезпеченням.

Робота СМО досліджується для випадку, коли її ефективність не набуває значень менших гранично допустимого рівня.

У залежності від конкретних умов постановка задач оптимізації характеристик систем може мати такі особливості: змінними можуть виступати величини λ_{ij} при заданих переходах; змінними можуть бути самі переходи з відповідними змінними величинами λ_{ij}; змінними можуть бути величини W_i; а також їх можливі комбінації.

При цьому оптимізація може здійснюватися або за вартістю реалізації характеристик системи, або за ефективністю при реалізації характеристик системи, або за узагальненим значенням ефективності $E = \frac{C}{W}$.

Систему, яка розглядається, можна інтерпретувати як систему масового обслуговування, в яку надходять загрози. Для початку розглянемо ситуацію, коли на вхід до системи надходять загрози одного типу, припускаючи, що загроза не може бути реалізована та надходити кілька разів в один і той же період часу. Якщо умови вище виконуються, то система може знаходитись у одному з чотирьох станів:

– загроза не надходила і, відповідно, не була реалізована;
– загроза надійшла, але не була реалізована;
– загроза надійшла та була реалізована;
– загроза надійшла, але була відбита системою захисту[27].

Граф переходів станів системи буде виглядати наступним чином (Рисунок 4.1):

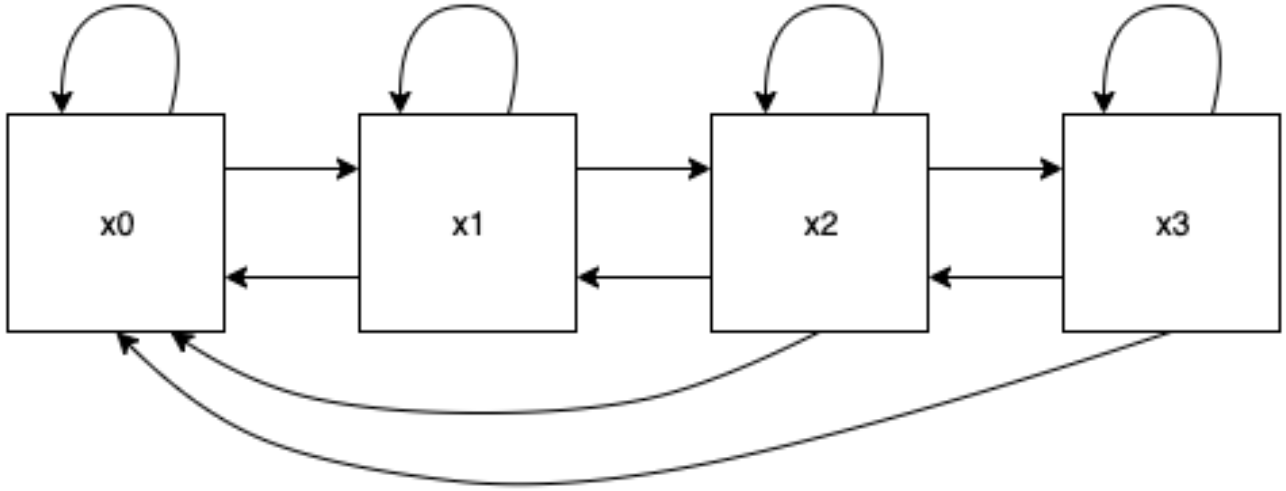

Рисунок 4.1 - Граф станів системи

Система, яка розглядається є системою з відновленням, тобто система може переходити з будь-якого стану в початковий. Будемо розглядати систему з неперервним часом. Перехід зі стану у стан відбувається згідно орієнтованого графу, дивись Рисунок 4.1. Для опису процесу переходу зі стану у стан, побудуємо матрицю інтенсивностей переходу:

$$p_{ij} = \begin{vmatrix} \lambda_{11} & \lambda_{12} & \lambda_{13} & 0 \\ \lambda_{21} & \lambda_{22} & \lambda_{23} & \lambda_{24} \\ \lambda_{31} & \lambda_{32} & \lambda_{33} & \lambda_{34} \\ \lambda_{41} & \lambda_{42} & \lambda_{43} & \lambda_{44} \end{vmatrix} \quad (4.1)$$

Елементи матриці інтенсивностей можуть бути обраховані за допомогою імітаційної моделі, запропонованої в [10]. У цій роботі опишемо імовірнісно-аналітичний спосіб їх визначення.

З попередніх погоджень випливає, що елементи цієї матриці мають такі властивості:

$$\begin{aligned}
\lambda_{11} &= -\lambda_{12} - \lambda_{13} \\
\lambda_{22} &= -\lambda_{21} - \lambda_{23} - \lambda_{24} \\
\lambda_{33} &= -\lambda_{31} - \lambda_{32} - \lambda_{34} \\
\lambda_{44} &= -\lambda_{41} - \lambda_{42} - \lambda_{43}
\end{aligned} \tag{4.2}$$

Надійність обладнання системи зумовлює тривалість виконання системою своїх функцій. Розрахунок параметрів функціонування системи з урахуванням надійності обладнання є актуальним науково-виробничим завданням. Знання характеру технічних відмов обладнання дозволяє досить ефективно організувати роботу служб ремонту і матеріально-технічного забезпечення.

Зі стану в стан систему переводять потоки подій, наприклад, подача сировини на обробку, ремонт обладнання системи і т.д. Кількісною характеристикою потоку подій є його інтенсивність, тобто число подій в одиницю часу.

На підставі графа станів системи будується математична модель її роботи у вигляді диференціальних рівнянь Чепмена-Колмогорова. Система диференціальних рівнянь зміни ймовірностей станів у часі виглядає наступним чином[17]:

$$\begin{cases}
\dfrac{dp_0(t)}{dt} = p_0(t)\lambda_{11} + p_1(t)\lambda_{21} + p_2(t)\lambda_{31} + p_3(t)\lambda_{41} \\
\dfrac{dp_1(t)}{dt} = p_0(t)\lambda_{12} + p_1(t)\lambda_{22} + p_2(t)\lambda_{32} + p_3(t)\lambda_{42} \\
\dfrac{dp_2(t)}{dt} = p_0(t)\lambda_{13} + p_1(t)\lambda_{23} + p_2(t)\lambda_{33} + p_3(t)\lambda_{43} \\
\dfrac{dp_3(t)}{dt} = p_1(t)\lambda_{24} + p_2(t)\lambda_{34} + p_3(t)\lambda_{44}
\end{cases} \tag{4.3}$$

При розрахунку треба брати до уваги наступні обмеження: сума коефіцієнтів λ_{ij} в одному рядку повинна дорівнювати нулю.

Найпоширенішим способом задання інформації про інтенсивність потоків загроз і ймовірностей зломів - це отримання значень на основі наявної статистики загроз безпеки інформаційних систем, які використовують системи захисту. Найкращий випадок трапляється коли наявна статистика для такої ж або

аналогічної інформаційної системи. Тоді задавати вихідні параметри для оцінки захищеності можна на її основі. При рекомендовано, щоб обрана інформаційна система експлуатувалася на виробництвах з подібною специфікою діяльності.

Але реалізація такого підходу вразлива до наступних складнощів. По-перше потрібен значна кількість інформації про події в цій області. По-друге цей підхід далеко не завжди виправданий. Якщо інформаційна система, яка розглядається, є досить великою (містить багато структурних елементів, розташована на великій території), є не зовсім сучасною, то такий підхід, за відсутності інших проблем, можна використати. Але якщо система відносно невелика і використовує нові структурні елементи та технології (для яких поки-що немає достовірної статистики), оцінки загроз можуть виявитися неповними та недостовірними.

Важливо пам'ятати, що статистика загроз час від часу публікується багатьма авторитетними виданнями. Це означає, що завжди існують вихідні дані для використання даного підходу для більшості систем та засобів захисту інформації. Якщо така статистика існує, то вона часто доступна в Інтернеті на сайтах організацій, які працюють у цій сфері.

Матриця коефіцієнтів інтенсивностей переходу індивідуальна для кожної окремої системи, так як визначає стан та умови її роботи. З цього виходить, що неможливо побудувати одну матрицю, яка буде справедливою для всіх систем.

Для розрахунків у наступних розділах візьмемо таку матрицю коефіцієнтів інтенсивностей:

$$\begin{vmatrix} -0.040 & 0.015 & 0.025 & 0 \\ 0.225 & -0.250 & -0.025 & 0.050 \\ 0.625 & -0.160 & -0.855 & 0.390 \\ 0 & 0.075 & 0.200 & -0.275 \end{vmatrix} \quad (4.4)$$

Матриця відповідає вимогам, описаним вище, тому може використовуватись як обмеження у методі розрахунку критеріїв оптимальності описаному в наступному розділі.

4.2 Розрахунок критеріїв оптимальності

4.2.1 Квадратичне програмування

Завданням квадратичного програмування (КП) називається задача оптимізації з квадратичною цільовою функцією і лінійними обмеженнями. Завдання КП, в якій цільова функція підлягає мінімізації, має вигляд:

$$f(x) = \sum_{j=1}^{n} c_j x_j + \sum_{j=1}^{n}\sum_{k=1}^{n} d_{jk} x_j x_k \to min,$$
$$\sum_{j=1}^{n} a_{ij} x_j \le b_i, \quad i = \overline{1,m}, \tag{4.5}$$
$$x_j \ge 0, \quad j = \overline{1,n}.$$

Допустима множина X є опуклою, матриця $D = [d_{jk}]$ передбачається симетричною невід'ємно визначеною. При цьому $f(x)$ опуклою на X і завдання є окремим випадком завдання опуклого програмування.

Для вирішення завдання КП використовуються необхідні умови Куна - Таккера, які в силу опуклості завдання КП виявляються також достатніми для встановлення наявності рішення[15].

Попередньо складається функція Лагранжа:

$$L(x, \lambda) = f(x) + \sum_{i=1}^{m} \gamma_i g_i(x), \tag{4.6}$$

де $g_i(x) \equiv \sum_{j=1}^{n} a_{ij} x_j - b_i$.

Умови Куна - Таккера мають такий вигляд:

$$\begin{gathered}
\frac{\partial L(x,\gamma)}{\partial x_j} \geq 0, \;\; j = \overline{1,n}; \\
x_j \geq 0, \;\; j = \overline{1,n}; \\
x_j \frac{\partial L(x,\gamma)}{\partial x_j} = 0, \;\; j = \overline{1,n}; \\
\frac{\partial L(x,\gamma)}{\partial \gamma_j} \leq 0, \;\; i = \overline{1,m}; \\
\gamma_i \geq 0, \;\; i = \overline{1,m}; \\
\lambda_j \frac{\partial L(x,\gamma)}{\partial \gamma_j} = 0, \;\; i = \overline{1,m};
\end{gathered} \tag{4.7}$$

Співвідношення вище визначають умови нежорсткості.

Безпосереднє рішення даної системи дуже громіздке. Тому використовується наступний прийом. Нерівності вище перетворюють в рівності, вводячи відповідно дві групи додаткових змінних $v_j, j = \overline{1,n}$, і $w_i, i = \overline{1,m}$, що задовольняють вимогам невід'ємності.

В результаті переходять до наступної системи:

$$\begin{gathered}
\frac{\partial L(x,\gamma)}{\partial x_j} - v_j = 0, \;\; j = \overline{1,n}; \\
x_j \geq 0, \;\; v_j \geq 0, \;\; j = \overline{1,n}; \\
x_j v_j = 0, \;\; j = \overline{1,n}; \\
\frac{\partial L(x,\gamma)}{\partial \gamma_j} + w_i = 0, \;\; i = \overline{1,m}; \\
\gamma_i \geq 0, \;\; w_i \geq 0, \;\; i = \overline{1,m}; \\
\gamma_i w_i = 0, \;\; i = \overline{1,m};
\end{gathered} \tag{4.8}$$

Система рівнянь вище має $(m+n)$ лінійних рівнянь з $2(m+n)$ невідомими. Таким чином, вихідна задача еквівалентна задачі знаходження допустимого, тобто

задовольняє вимогам невід'ємності, базисного рішення системи лінійних рівнянь, що задовольняє також умовам доповнює нежорсткості. Так як завдання КП є опуклою завданням оптимізації, то допустиме рішення, яке задовольняє всім цим умовам, є оптимальним.

Для знаходження допустимого базисного рішення системи лінійних рівнянь може бути застосований метод штучних змінних, який використовується в лінійному програмуванні (ЛП) для визначення початкового базису. При цьому у рівняння системи, у яких знаки додаткових змінних v_j або w_i збігаються з класами вільних членів, вводяться невід'ємні штучні змінні $z_l, l = \overline{1, l_{max}}$, $l_{max} \leq m + n$, знаки яких не збігаються зі знаками відповідних вільних членів[14].

Потім вирішується допоміжна завдання ЛП:

$$F(z) = \sum_{l} z_l \rightarrow min \tag{4.9}$$

при обмеженнях з введеними невід'ємними штучними змінними. Для вирішення цього завдання використовується симплекс-метод. У процесі рішення необхідно враховувати умови доповнює нежорсткості. Виконання цих умов означає, що x_j і v_j, γ_i і w_i не можуть бути позитивними одночасно, тобто змінну x_j не можна зробити базисної, якщо v_j є базисної і приймає позитивне значення, також і γ_i з w_i.

У результаті рішення допоміжної задачі можуть бути два випадки.

1. $\min\limits_{z} F(z) = 0$, тобто всі штучні змінні виведені з базису. Отримане оптимальне допустиме базисне рішення допоміжної задачі ЛП є допустимим базисним рішенням системи і, отже, рішенням завдання КП.

2. $\min\limits_{z} F(z) > 0$, тобто серед базисних залишилися штучні змінні. Це означає, що система не має допустимого базисного рішення і, отже, завдання КП не має рішення.

Для розв’язання рівнянь такого типу та полегшення розуміння та розрахунків було розроблено скрипт у середовищі Matlab (Додаток А).

Так, як у роботі розглядається метод оптимізації, то він не може бути справедливий без визначення критеріїв, за якими його можна визначити.

Використовуючи скрипт з Додатку А, побудуємо графік оптимізації імовірностей знаходження системи у кожному з 4-х станів (Рисунок 4.2).

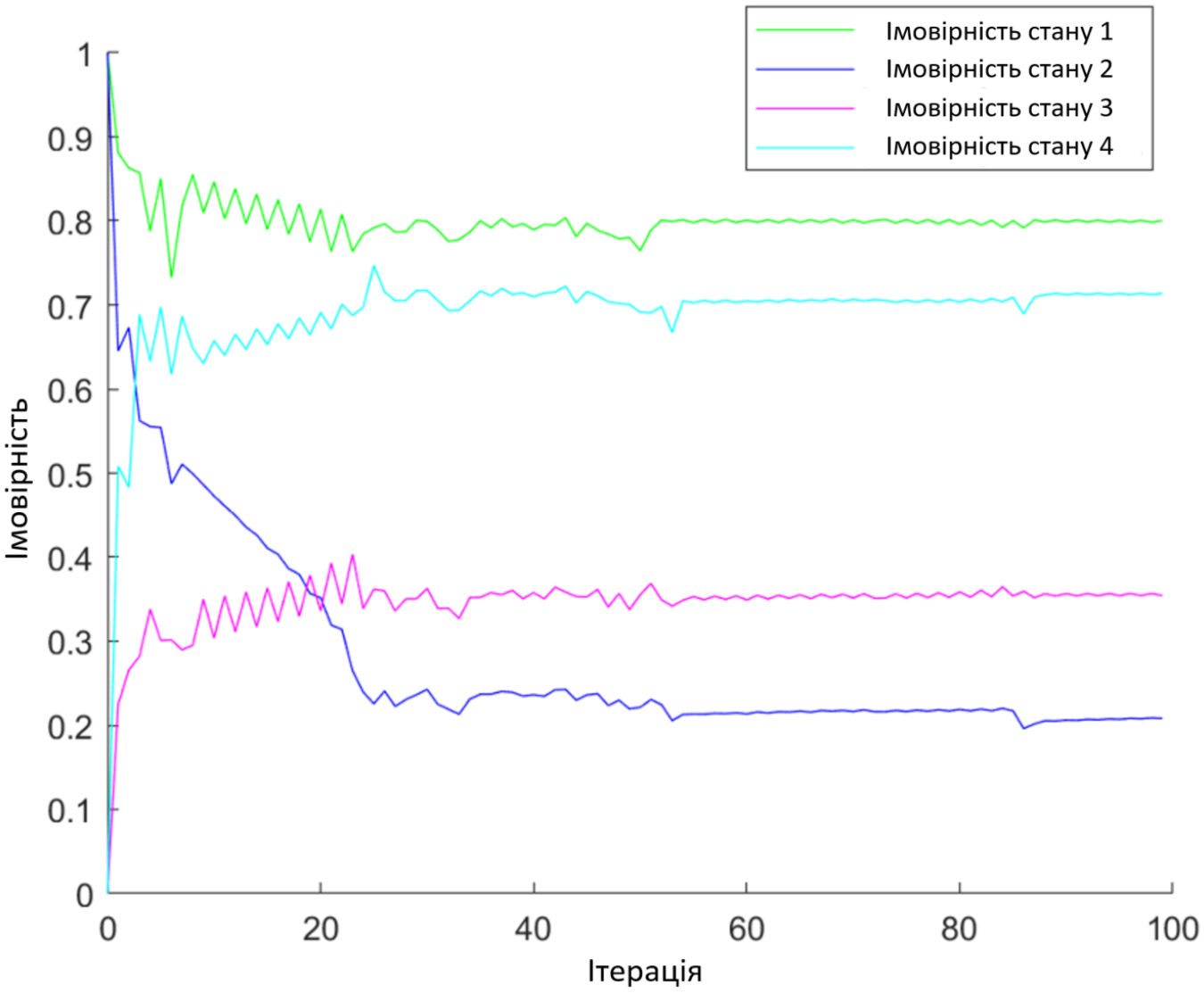

Рисунок 4.2 - Графік імовірностей

4.2.2 Загальний критерій оптимальності

Проведена оцінка ефективності системи за параметром захищеності, як основним показником, що характеризує рівень забезпечення захисту системи захисту інформації, а на інші характеристики вводяться обмеження. Будемо оцінювати

захищеність системи (Z) кількісно залежно від вартості інформації, що захищається, ймовірності злому, вартості самої системи захисту, продуктивності системи:

$$Z = f(C_{\text{інф}}, p_{\text{зл}}, B_{\text{сзі}}, \text{П}) \tag{4.10}$$

де $C_{\text{інф}}$ - вартість інформації, що захищається; $p_{\text{зл}}$ - ймовірність злому; $B_{\text{сзі}}$ - вартість системи захисту інформації; П - продуктивність системи.

З урахуванням введеного поняття захищеності системи оптимізаційна задачі полягає в забезпеченні максимального рівня захищеності (як функції вартості інформації, що захищається і ймовірності злому) при обмеженнях вартості системи захисту і впливу на продуктивність системи:

$$Z^{opt} = \max Z\left(C_{\text{інф}}, p_{\text{зл}}, B_{\text{сзі}}, \text{П}\right) \tag{4.11}$$

Таким чином, всі окремі критерії, крім одного, перетворюється на обмеження, додатково звужують область допустимих рішень X. Тоді вихідна багатокритеріальна задача (1) перетворюється в однокритеріальну виду:

$$k_i(x) \geq (\leq) k_i^B(x), \;\; i = 1, n-1, \tag{4.12}$$

де $k^*(x)$ - оптимізаційний скалярний критерій; $k_i^B(x)$ - найгірші допустимі значення окремих критеріїв-обмежень; знак «>» використовується для критеріїв, які необхідно максимізувати, а знак «<» - мінімізувати[14].

Виведення головного (оптимізаційного) критерію і рівнів обмежень для $k_i^B(x)$ всіх інших критеріїв є суб'єктивною операцією, здійснюваною експертами. Слід зазначити, що можна розглянути декілька різних варіантів і порівняти результати.

Розглянемо захищеність системи з точки зору ризику. Зауважимо, що використання теорії ризиків для оцінки рівня захищеності на сьогоднішній день є

підходом, який найбільш часто використовується на практиці. Ризик R - це потенційні втрати від загроз захищеності:

$$R(p) = C_{\text{інф}} \times p_{\text{зл}}, \tag{4.13}$$

По суті, параметр ризику тут вводиться як мультиплікативна згортка двох основних параметрів захищеності.

З іншого боку, можна розглядати ризик як втрати в одиницю часу:

$$R(\lambda) = C_{\text{інф}} \times \lambda_{\text{зл}}, \tag{4.14}$$

де $\lambda_{\text{зл}}$ - інтенсивність потоку зломів (під зломом будемо розуміти вдалу спробу реалізації загрози інформації).

Ці дві формули пов’язані наступним співвідношенням:

$$p_{\text{зл}} = \frac{\lambda_{\text{зл}}}{\Lambda}, \tag{4.15}$$

де Λ - загальна інтенсивність потоку несанкціонованих спроб порушення основних властивостей інформації зловмисниками.

В якості основного критерію захищеності будемо використовувати коефіцієнт захищеності *(D)*, що показує відносне зменшення ризику в захищеній системі в порівнянні з незахищеною системою:

$$D = \left(1 - \frac{R_{\text{зах}}}{R_{\text{нез}}}\right) \times 100\%, \tag{4.16}$$

де $R_{\text{зах}}$ - ризик в захищеній системі;

$R_{\text{нез}}$ - ризик в незахищеною системі.

Для вирішення цієї задачі зведемо її до однокритеріальної за допомогою введення обмежень. У результаті отримаємо:

$$\begin{cases} D\left(C_{\text{інф}}, p_{\text{зл}}\right) \to max; \\ B_{\text{сзі}} < B_{\text{зад}}; \\ \Pi_{\text{сзі}} \geq \Pi_{\text{зад}}. \end{cases} \quad (4.17)$$

де $B_{\text{зад}}$ і $\Pi_{\text{зад}}$ - задані обмеження на вартість системи захисту і продуктивність системи.

Цільова функція обрана виходячи з того, що саме вона відображає основне функціональне призначення системи захисту - забезпечення безпеки інформації [9].

Тепер виразимо коефіцієнт захищеності через параметри загроз. У загальному випадку в системі присутня безліч видів загроз. У цих умовах задамо такі величини: W - кількість видів загроз, що впливають на систему; $C_i(i = 1, w)$ - вартість втрати від злому і-того виду; $\lambda_i(i = 1, w)$ - інтенсивність потоку зломів і-того виду, відповідно; $Q_i(i = 1, w)$ - ймовірність появи загроз і-того виду в загальному потоці спроб реалізації загроз, причому $Q_i = \frac{\lambda_i}{\Lambda}$, $p_i(i = 1, w)$ - ймовірність відбиття загроз і-того виду системою захисту. Відповідно, для коефіцієнта втрат від зломів системи захисту маємо:

$$R(p) = \sum R_i(p) = \sum C_i \times p_{\text{зл}_\text{і}}; \quad (4.18)$$

де $R_i(p)$ - коефіцієнт втрат від злому і-того типу; показує, які в середньому втрати припадають на один злом і-того типу.

Для незахищеної системи $P_{\text{загр\_}i} = Q_i$, для захищеної системи:

$$P_{\text{загр\_}i} = Q_i \times (1 - p_i). \quad (4.20)$$

Відповідно, для коефіцієнта втрат від зломів системи захисту в одиницю часу маємо:

$$R(\lambda) = \sum_{1}^{w} R_i(\lambda) = \sum_{1}^{w} C_i \times \lambda_{\text{загр\_}i}, \tag{4.21}$$

де $R_i(\lambda)$- коефіцієнт втрат від зломів і-того типу в одиницю часу.

Для незахищеної системи $\lambda_{\text{загр\_}i} = \lambda$, для захищеної системи $\lambda_{\text{загр\_}i} = \lambda(1 - p_i)$. Відповідно, маємо:

$$D = 1 - \frac{\sum_1^w C_i \times Q_i \times (1 - p_i)}{\sum_1^w C_i \times Q_i} = 1 - \frac{\sum_1^w C_i \times \lambda_i \times (1 - p_i)}{\sum_1^w C_i \times \lambda_i}. \tag{4.22}$$

Для оптимізації використовуються кінцеві усталені значення p_i.

Використовуючи Matlab алгоритм з додатку А, розрахуємо значення критерію оптимальності (Рисунок 4.3).

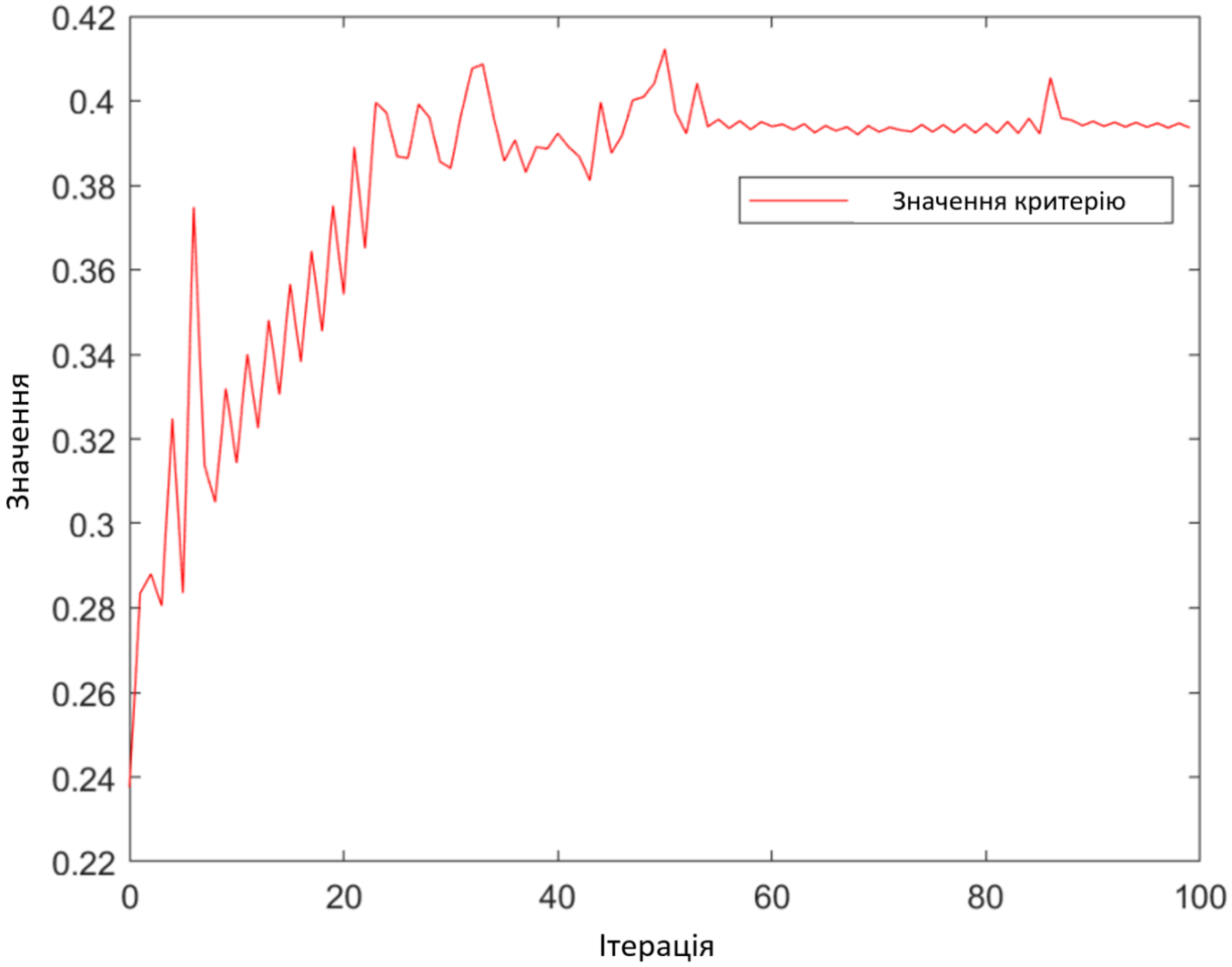

Рисунок 4.3 - Графік значення критерію

Кінцеві значення імовірностей:

– 0.7883
– 0.2211
– 0.3365
– 0.7141

Кінцеве значення критерію:

– 0.3971

4.2.3 Метод статистичної оцінки

Основним способом завдання інтенсивностей потоків загроз λ_i (ймовірностей загроз Q_i) і ймовірностей зломів p_i це використання вже існуючої статистики загроз

безпеки інформаційних систем, які використовують системи захисту, для отримання значень. Найкращим випадком буде той, коли вже існує статистика для дуже схожої або аналогічної інформаційної системи. Тоді вихідні параметри для оцінки захищеності можуть бути задані вже на її основі. Але рекомендовано, щоб такі інформаційні системи використовувались на виробництвах з такою ж або подібною специфікою діяльності.

Але практично реалізуючи такий підхід, спеціалісти можуть зіштовхнутись з наступними складнощами. Для початку має бути скомпільований досить великий матеріал про безпекові події в цій області. По-друге цей підхід далеко не завжди є потрібним та виправданим. Якщо інформаційна система, яка розглядається, є досить великою у розмірі (складається з багатьох елементів, розташована на великій території), є не новою, то такий підхід можна застосовувати. Але якщо система порівняно невелика і використовує лише нові елементи та технології, оцінки загроз швидше за все виявляться неправильними через відсутність достатньої кількості історичної інформації.

Якщо статистика по загрозах безпеки відсутня для системи, яка розглядається, то потрібно використати один з інших підходів, які описаних далі.

Першим способом є спосіб однакових інтенсивностей $\forall\lambda_i = \alpha, \alpha = const$. При цьому способі для розрахунку захищеності константа α може бути обрана будь-якою. У формулі вона буде винесена за дужки і в кінцевому підсумку скоротиться, так що захищеність в даному випадку буде залежати тільки від втрат:

$$\begin{aligned} D &= 1 - \frac{\sum_i^w C_i \times \lambda_i \times (1 - p_i)}{\sum_i^w C_i \times \lambda_i} = \\ &= 1 - \frac{\sum_i^w C_i \times \alpha \times (1 - p_i)}{\sum_i^w C_i \times \alpha} = \\ &= 1 - \frac{\alpha \sum_i^w C_i \times (1 - p_i)}{\alpha \sum_i^w C_i} = \\ &= 1 - \frac{\sum_i^w C_i \times (1 - p_i)}{\sum_i^w C_i}. \end{aligned} \tag{4.23}$$

Використовуючи Matlab алгоритм з додатку А, розрахуємо значення критерію оптимальності (Рисунок 4.4).

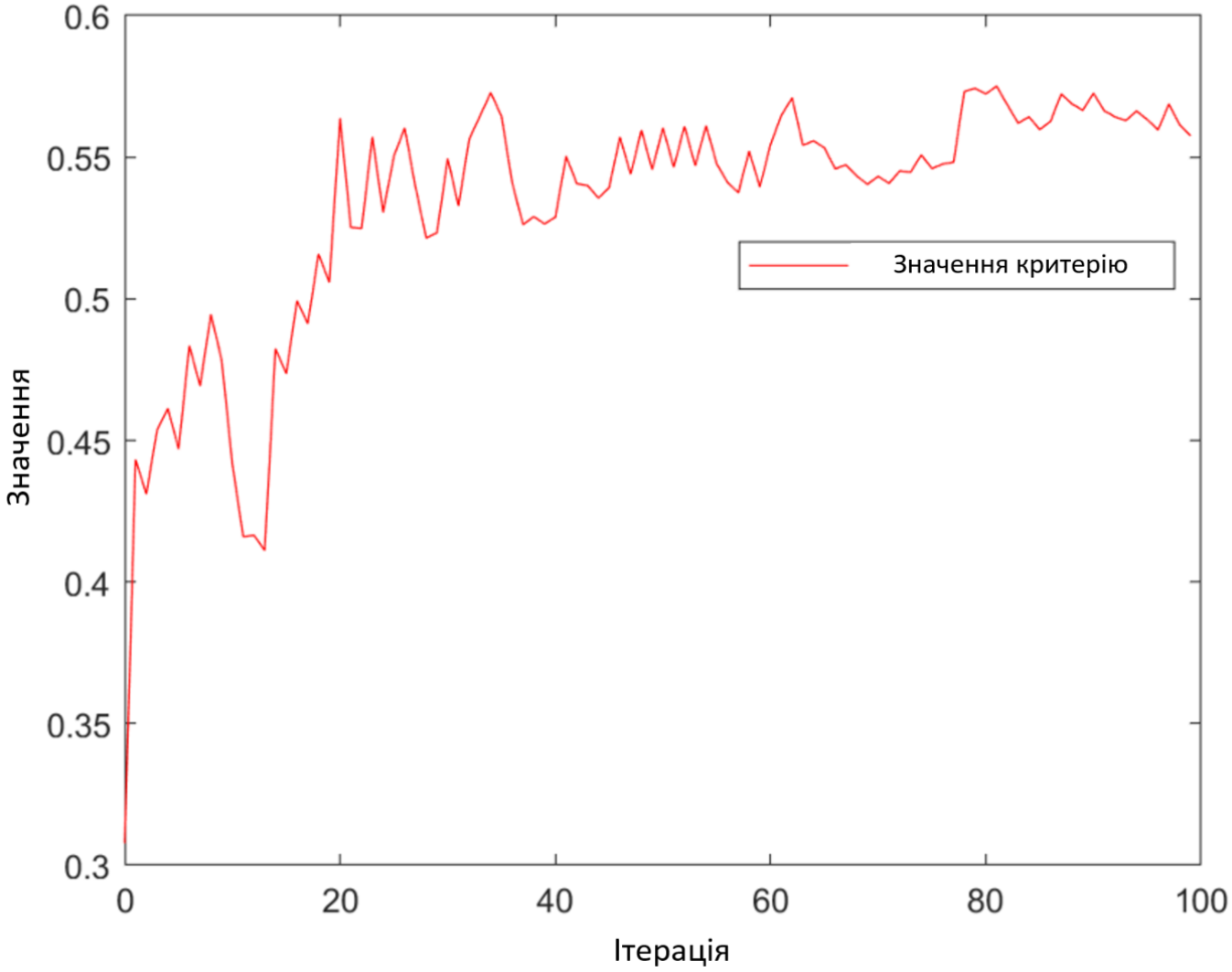

Рисунок 4.4 - Графік значення критерію

Кінцеві значення імовірностей:

– 0.7880
– 0.2216
– 0.3500
– 0.7150

Кінцеве значення критерію:

– 0.5675

Ще один спосіб - це спосіб пропорційності втратам $\lambda_i = \alpha * C_i, \alpha = const.$

У цьому способі передбачається, що чим більші втрати від злому, тим частіше здійснюються спроби несанкціонованого доступу до цієї інформації. Тобто інтенсивності потоків загроз прямо пропорційні втрат. В цьому випадку захищеність буде залежати від квадрата втрат:

$$\begin{aligned} D &= 1 - \frac{\sum_i^w C_i \times \lambda_i \times (1 - p_i)}{\sum_i^w C_i \times \lambda_i} = \\ &= 1 - \frac{\sum_i^w C_i \times \alpha \times C_i \times (1 - p_i)}{\sum_i^w C_i \times \alpha \times C_i} = \\ &= 1 - \frac{\alpha \sum_i^w C_i^2 \times (1 - p_i)}{\alpha \sum_i^w C_i^2} = \\ &= 1 - \frac{\sum_i^w C_i^2 \times (1 - p_i)}{\sum_i^w C_i^2}. \end{aligned} \tag{4.24}$$

Використовуючи Matlab алгоритм з додатку А, розрахуємо значення імовірностей та критерію оптимальності (Рисунок 4.5).

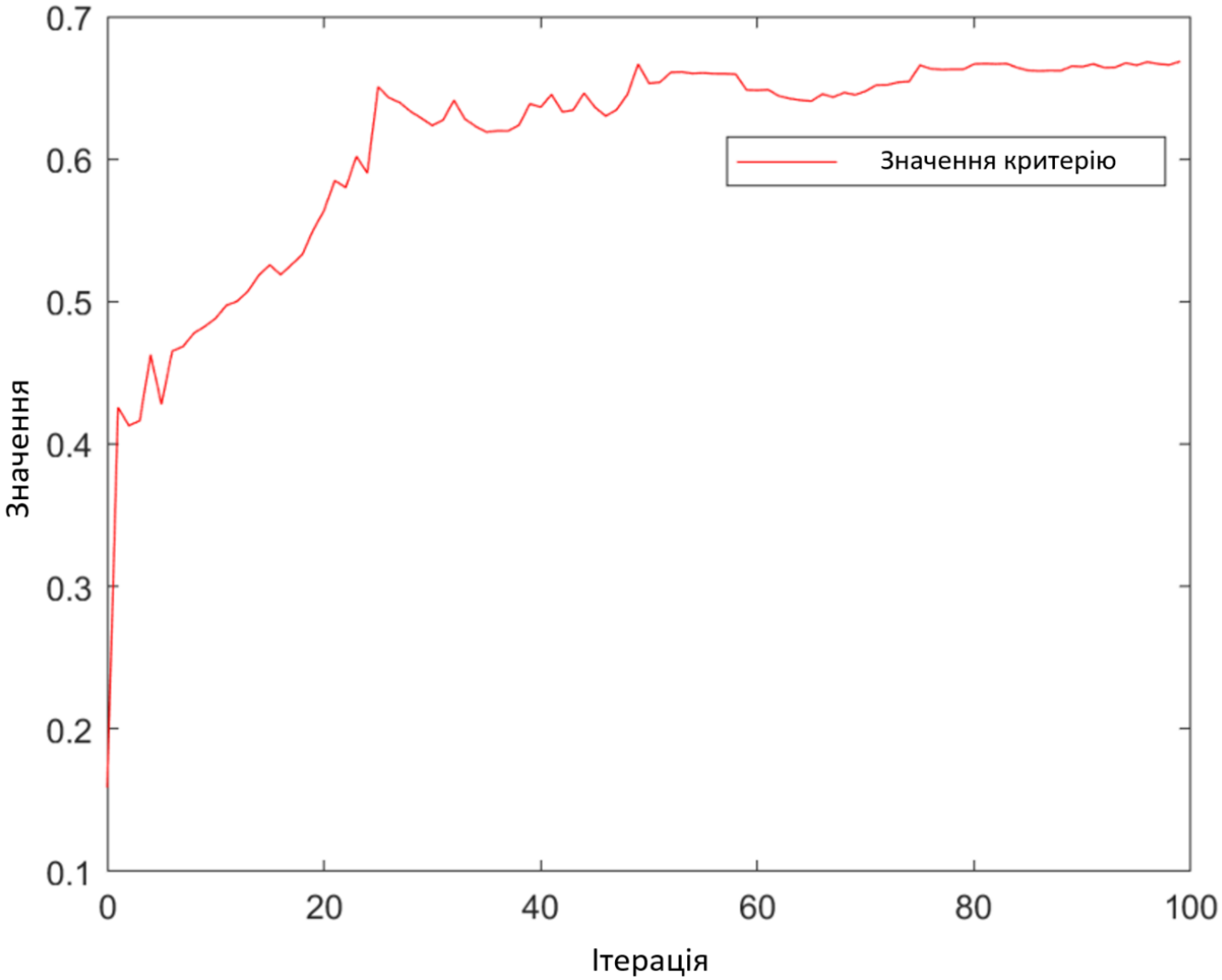

Рисунок 4.5 - Графік значення критерію

Кінцеві значення імовірностей:

– 0.7857
– 0.2245
– 0.3582
– 0.7099

Кінцеве значення критерію:

– 0.6684

ВИСНОВКИ

У роботі було наведено та розглянуто основні та другорядні способи захисту хімічного підприємства та його працівників від загроз з боку зловмисників. Особливий наголос відбувався на інформаційних засобах безпеки тому, що світ все з більшими темпами переходить на електронний зв'язок у всіх сферах, що, з одного боку збільшує швидкість та якість процесів, які відбуваються навколо нас, а з іншого боку відкриває нові «двері» для зловмисників та опонентів, через які можна нанести шкоду підприємству чи його працівникам.

Сектор виробництва мінеральних добрив є суттєвою частиною хімічного сектору, будучи інтегральною частиною життя сучасної людини. Виробництво добрив часто пов'язане з роботою з токсичними та вибухонебезпечними матеріалами, помилка в експлуатації чи зберігання яких може призвести до масштабних аварій, як це показав вибух у порту Бейрута у 2020р.

Але потрібно пам'ятати, що зловмисники завжди шукають найпростіший спосіб завдання шкоди, тому підприємство, маючи комплексний та повний захист від інформаційних загроз все-ще є незахищеним, якщо відсутній фізичний захист. Інформаційний захист не має сенсу без фізичного, якому також були приділено увагу у цій роботі.

Проблема захищеності підприємства створює значну кількість бізнес-проблем та викликів, на які часто не вистачає грошей, часу або ресурсів, але це має бути центральною частиною впровадження та модернізації кожного стратегічного підприємства.

Але бізнес-проблеми не можуть бути вирішені лише за допомогою технологій безпеки. Підготовка та підвищення морального духу співробітників - це інші способи підвищення продуктивності праці та збільшення результатів. Окрім зменшення втрат, відеоспостереження можна використовувати для навчання працівників найкращим практикам, вдосконалення послуг та підвищення рівня задоволеності споживачів. Системи контролю доступу та виявлення вторгнень допомагають забезпечити безпечне середовище для роботи та відпочинку, що призводить до підвищення

продуктивності праці співробітників та підвищена задоволеність споживачів. Як і в будь-якій індустрії сфери послуг, високий рівень безпеки та безпеки дозволяє співробітникам зосередитись на наданні якісних послуг споживачам.

Компанії, що займаються спостереженням за сигналізацією, надають апаратне та програмне забезпечення, щоб допомогти компаніям, що виробляють та складають товари, підвищити рівень безпеки. Послуги варіюються від якісного апаратного та програмного забезпечення з послугами з доданою вартістю, які включають віддалений моніторинг, віртуальну охорону та доступ до моніторингу через Інтернет. Ключовими критеріями, які слід взяти до уваги, є можливість встановлення обладнання, що забезпечує незменшену продуктивність протягом його життєвого циклу, послуги з доданою вартістю для підвищення безпеки та неперевершене обслуговування клієнтів.

Просто встановлення обладнання не допоможе компаніям запобігти втратам, загрозам безпеці життя та продуктивності праці працівників, про які йдеться в цій роботі. Щоб отримати бажані результати, компаніям слід взаємодіяти з постачальниками послуг, які пропонують такі можливості;

– охоронні компанії, що мають досвід у виробничій та складській промисловості;

– перевірений досвід демонстраційних тематичних досліджень та відгуків клієнтів;

– охоронні компанії, які застосовують консультативний підхід, охочі вийти на роботу та провести всебічний аналіз ризиків, а потім запропонувати рішення, розроблене для задоволення конкретних потреб кінцевих споживачів;

– постачальник послуг безпеки, який слухає та розуміє виклики кінцевого користувача та пропонує перевірені рішення.

Кінцеві користувачі повинні уникати спілкування з постачальниками послуг безпеки, які не розуміють проблемних точок для кінцевих споживачів, і керувати розмовами про товари та послуги, які пропонує компанія.

Виробнича та складська промисловість є важливою складовою економіки. Сучасні економічні умови підсилюють важливість захисних технологій для

зменшення збитків та підвищення прибутковості. Незважаючи на те, що важко розрахувати точну рентабельність інвестицій у безпеку, важливо використовувати технологію для вирішення деяких бізнес-питань, що впливають на обробну промисловість, а саме використання важкого обладнання, контроль запасів, підвищення продуктивності праці та змінні роботи. Збільшення доступності індивідуальних рішень для вирішення кожної з цих бізнес-проблем допомогло виробничим компаніям використовувати технології, щоб покращити свої результати.

Процес оцінки ризику продовжує розвиватися. Концепція експозоми підкреслила необхідність розгляду окремих експозицій у ширшому контексті впродовж усього життя ендогенних та екзогенних експозицій. Одним із напрямків, що явно потребує додаткової уваги, є підхід до оцінки ризику від дії ендогенних хімічних речовин з екзогенною експозицією. Поточна практика, як правило, не в змозі адекватно розглянути або вирішити цю проблему. Недостатньо вказівок для допомоги оцінювачам ризиків у вирішенні складності цього завдання, хоча певний прогрес досягнуто. Нещодавні приклади таких оцінок ризику можуть бути корисними при розробці відповідним чином розробленого формулювання проблеми для таких оцінок, щоб гарантувати, що необхідна інформація: розробляється у разі потреби; розглядається в систематичних оглядах; включається в оцінки ризиків; і представляється менеджерам ризику, які можуть краще оцінити свої варіанти управління ризиками для таких ситуацій. Набір питань, отриманих із цих прикладів та запропонованих до використання і, за необхідності, розробка конкретної інформації, доступної для їх вирішення, пропонує відправну точку для подальших удосконалень у процесі вирішення цієї проблеми оцінки ризику.

Враховуючи важливість інформаційних систем захисту паралельно з фізичними, за результатами проведеного дослідження в роботі здійснена постановка задач оптимізації характеристик систем, запропоновано алгоритм, який може застосовуватись для їх розв’язування, а також на основі аналізу математичних методів, які реалізують окремі кроки алгоритму, обґрунтовано висновок про доцільність створення спеціалізованої інформаційної системи, що дозволяла б здійснювати оптимізацію характеристик систем.

Розроблено метод оптимізації системи захисту критичних інформаційних ресурсів. Запропоновано перехід від багатокритеріальної задачі оптимізації, до однокритеріальної. При сформульованому понятті захищеності системи оптимізаційна задача полягає в забезпеченні максимального рівня захищеності (як функції вартості інформації, що захищається і ймовірності злому) при обмеженнях вартості системи захисту і впливу на продуктивність системи.

Також було запропоновано три варіанти критеріїв оптимальності оптимізації. Для їх обчислення було написано Matlab-скрипт. Використовуючи написаний скрипт, були отримані графіки оптимізації та визначення імовірностей та значення критеріїв, результати наведені у відповідних розділах. Проаналізувавши результати, можна пройти до висновку значення імовірностей з використанням усіх критеріїв солідарні, що стверджує про правильність розрахунків. а 3-й критерій (спосіб пропорційності втратам) виявився найвищим.

ПЕРЕЛІК ПОСИЛАНЬ

1. US Department of Homeland security. Chemical sector-specific plan – M., 2010.
2. CIDX. Guidance for addressing cybersecurity in the chemical sector – M., 2004.
3. US Government Accountability Office. Critical infrastructure protection – M., 2020.
4. Honeywell. Chemical Processing – M., 2013.
5. American Chemistry Council. Guide to the Business of Chemistry – M., 2019.
6. US Department of Commerce. Guide to industrial control systems security – M., 2015.
7. International fertilizer industry association, United Nations Environment programme. Mineral Fertilizer Use and the Environment – M., 2000.
8. Гнеденко Б.В., Коваленко И.Н. Введение в теорию массового обслуживания. – М., 1987.
9. Кениг Д., Штойян Д. Методы теории массового обслуживания: Пер. с нем. / Под. ред. Г.П. Климова. – М., 1981.
10. Вентцель Е.С. Исследование операций. – М.: Советское радио, 1972. – 552 с.
11. Боровик О. В., Боровик Л. В. Дослідження операцій в оперативно- службовій діяльності органів охорони державного кордону: Підручник. – Хмельницький: Видавництво Національної академії Державної прикордонної сужби України імені Б. Хмельницького, 2009. – 444 с.
12. Купрієнко Д. А., Боровик О. В. Структурний синтез динамічних систем із квазілінійним і часовим розподіленням компонентів: Монографія. – Хмельницький: Видавництво НАДПСУ, 2015. – 348 с.
13. Аттетков А.В., Галкин С.В., Зарубин В.С. Методы оптимизации: Учеб. для студ. втузов. − М.: Изд-во МГТУ, 2001.
14. Банди Б. Методы оптимизации. Вводный курс. – М.: Радио и связь, 1988.
15. Карманов В.Г. Математическое программирование. − М.: Физматлит, 2000.
16. Корбут А.А., Финкельштейн Ю.Ю. Дискретное программирование. – М.: Наука, 1969.
17. Лесин В.В., Лисовец Ю.П. Основы методов оптимизации: Учеб. пособие для втузов. − М.: Изд-во МАИ, 1995.

18. Корнієнко Б.Я. Дослідження імітаційного полігону захисту критичних інформаційних ресурсів методом IRISK. Моделювання та інформаційні технології. 2018. Вип. 83. С. 34-41.
19. Корнієнко Б.Я. Побудова та тестування імітаційного полігону захисту критичних інформаційних ресурсів. Наукоємні технології. 2017. № 4 (36). С. 316 - 322.
20. Korniyenko B., Yudin A., Galata L. Risk estimation of information system.Wschodnioeuropejskie Czasopismo Naukowe. 2016. № 5. P. 35 - 40.
21. Корнієнко Б.Я., Юдін О.К., Снігур О.С.Безпека аутентифікації у web-ресурсах. Захист інформації. 2012. № 1 (54). С. 20 -25. DOI: 10.18372/2410-7840.14.2056 (ukr).
22. Корнієнко Б.Я., Максімов Ю.О., Марутовська Н.М. Прикладні програми управління інформаційними ризиками. Захист інформації. 2012. № 4 (57). С. 60 – 64. DOI: 10.18372/2410-7840.14.3493 (ukr).
23. Galata, L., Korniyenko, B., Yudin, A.: Research of the simulation polygon for the protection of critical information resources. In: CEUR Workshop Proceedings, Information Technologies and Security, Selected Papers of the XVII International Scientific and Practical Conference on Information Technologies and Security (ITS 2017), 30 Nov 2017, Kyiv, Ukraine. vol. 2067. pp. 23–31., urn:nbn:de:0074-2067-8.
24. Корнієнко Б.Я. Безпека інформаційно-комунікаційних систем та мереж. Навчальний посібник для студентів спеціальності 125 «Кібербезпека». – К.:НАУ, 2018. – 226 с.
25. Корнієнко Б.Я., Галата Л.П. Оптимізація системи захисту інформації корпоративної мережі. Математичне та комп'ютерне моделювання. Серія: Технічні науки, Випуск 19, 2019. - С. 56-62.
26. Korniyenko B., Galata L. Implementation of the information resources protection based on the CentOS operating system. Conference Proceedings of 2019 IEEE 2nd Ukraine Conference on Electrical and Computer Engineering (UKRCON -2019) July 2 – 6, 2019, Lviv, Ukraine. - pp. 1007-1011.

27. Галата Л.П., Корнієнко Б.Я., Заболотний В.В. Математична модель протидії загрозам у системі захисту критичних інформаційних ресурсів. Наукоємні технології, Том 43, № 3, 2019. – С. 300 – 306.
28. Корнієнко Б.Я. Modeling of information security system in computer network. Безпека інформаційних систем і технологій, Том №1 (1), 2019. – С.36-41.
29. Korniyenko B., Galata L., Ladieva L. Research of Information Protection System of Corporate Network Based on GNS3. Conference Proceedings of 2019 IEEE Inernational Conference on Advanced Trends in Information Theory (IEEE ATIT -2019) Dezember 18 – 20, 2019, Kyiv, Ukraine. - pp. 244-248.
30. Korniyenko B., Galata L., Ladieva L. Mathematical model of threats resistance in the critical information resources protection system. CEUR Workshop Proceedings, Selected Papers of the XIX International Scientific and Practical Conference «Information Technologies and Security» (ITS 2019) Kyiv, Ukraine, November 28, 2019. Vol-2577. P.281-291.
31. Корниенко Б.Я. Кибернетическая безопасность – операционные системы и протоколы. ISBN 978-3-330-08397-4, LAMBERT Academic Publishing, Saarbrucken, Deutschland. − 2017. – 122 с.
32. Korniyenko B.Y., Galata L.P. Design and research of mathematical model for information security system in computer network. Науковий журнал «Наукоємні технології». – 2017, № 2 (34), С. 114 - 118.
33. Корниенко Б.Я. Информационная безопасность и технологии компьютерных сетей : монография. ISBN 978-3-330-02028-3, LAMBERT Academic Publishing, Saarbrucken, Deutschland. − 2016. – 102 с.
34. Korniyenko B., Galata L., Kozuberda O. Modeling of security and risk assessment in information and communication system. Sciences of Europe. – 2016. – V. 2. – No 2 (2). – P. 61 -63.
35. Korniyenko B. The classification of information technologies and control systems. International scientific journal. – 2016. –№ 2. – P. 78 - 81.
36. Корнієнко Б.Я. Інформаційні технології оптимального управління виробництвом мінеральних добрив :монографія. – К.: Вид-во Аграр Медіа Груп, 2014. – 288 с.

37. Korniyenko B., Galata L., Ladieva L. Security Estimation of the Simulation Polygon for the Protection of Critical Information Resources / B. Korniyenko, //CEUR Workshop Proceedings, Selected Papers of the XVIII International Scientific and Practical Conference «Information Technologies and Security» (ITS 2018) Kyiv, Ukraine, November 27, 2018, Vol-2318, - P. 176-187, urn:nbn:de:0074-2318-4

ДОДАТОК А

Matlab-скрипт для розрахунку критеріїв оптимальності

```
function [] = thesis_script()
    % Lower bounds
    lb = [];
    % Upper bounds
    ub = [];
    % Start point
    x0 = [1; 1; 0; 0];

    iterValues = [];
    funValues = [];
    x1Values = [];
    x2Values = [];
    x3Values = [];
    x4Values = [];

    % Optimization options parameters
    options = optimset('LargeScale', 'off', 'Display', 'iter', 'OutputFcn', @OutFcn, 'TolCon', 0.001, 'MaxFunEvals', 500);
%'MaxFunEvals', 100
    % Optimization function call
    [x, fval, exitflag, output] = fmincon(@objfun2, x0, [], [], [], [], lb, ub, @confun, options);
    x % minimum point
    fval % function value in minimum point
    % constraints
    [c, ceq] = confun(x)

    %figure;
    plot(iterValues, funValues, 'r');
    xlabel('Iteration');
    ylabel('Value');
    set(gcf,'color','w');
    legend('criterion              value');

    figure;

    hold on;

    plot(iterValues, x1Values, 'g');
    plot(iterValues, x2Values, 'b');
```

```
plot(iterValues, x3Values, 'm');
plot(iterValues, x4Values, 'c');

xlabel('Iteration');
ylabel('Probability');
set(gcf,'color','w');

hold off;

legend('probability 1', 'probability 2', 'probability 3', 'probability 4');

% criterion 1
function f = objfun(x)
    x1 = x(1); x2 = x(2); x3 = x(3); x4 = x(4);
    c1 = 0.2; c2 = 0.7; c3 = 0.1; c4 = 0.3;
    l1 = 20; l2 = 3; l3 = 4; l4 = 5;
    % target function
    f = (c1 * l1 * (1 - x1) + c2 * l2 * (1 - x2) + c3 * l3 * (1 - x3) + c4 * l4 * (1 - x4)) / (c1 * l1 + c2 * l2 + c3 * l3 + c4 * l4);
end

% criterion 2
function f = objfun1(x)
    x1 = x(1); x2 = x(2); x3 = x(3); x4 = x(4);
    c1 = 0.2; c2 = 0.7; c3 = 0.1; c4 = 0.3;
    % target function
    f = (c1  * (1 - x1) + c2  * (1 - x2) + c3 * (1 - x3) + c4 * (1 - x4)) / (c1 + c2 + c3 + c4);
end

% criterion 3
function f = objfun2(x)
    x1 = x(1); x2 = x(2); x3 = x(3); x4 = x(4);
    c1 = 0.2; c2 = 0.7; c3 = 0.1; c4 = 0.3;
    % target function
    f = (c1.^2  * (1 - x1) + c2.^2  * (1 - x2) + c3.^2 * (1 - x3) + c4.^2 * (1 - x4)) / (c1.^2 + c2.^2 + c3.^2 + c4.^2);
end

function [c, ceq] = confun(x)
   x1 = x(1); x2 = x(2); x3 = x(3); x4 = x(4);
   % Non-equality constraints, <= 0
   c = [-x1, x1 - 0.3, -x2 + 0.4, x2 - 0.6, -x3 + 0.6, x3 - 0.5, -x4 + 0.9, x4 - 0.6];
   % Equality constraints
   ceq = [-0.040 * x1 + 0.015 * x2 + 0.025 * x3 + 0 * x4 - 1,
```

```
        0.225 * x1 - 0.250 * x2 - 0.025 * x3 + 0.050 * x4 - 1,
        0.625 * x1 - 0.160 * x2 - 0.855 * x3 + 0.390 * x4 - 1,
        -0.00 * x1 + 0.075 * x2 + 0.200 * x3 - 0.275 * x4 - 1];
    end

    function stop = OutFcn(x, optimvalues, state)
      stop = false;
      PlotIter(x, optimvalues);
    end

    function PlotIter(x, optimvalues)
      x1 = x(1); x2 = x(2); x3 = x(3); x4 = x(4);

      iterValues(end + 1) = optimvalues.iteration;
      funValues(end + 1) = optimvalues.fval;
      x1Values(end + 1) = x1;
      x2Values(end + 1) = x2;
      x3Values(end + 1) = x3;
      x4Values(end + 1) = x4;
    end

end
```