УДК 004

С.Коробка, магістр гр. КІ-24М,
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КРИТИЧНИХ РЕСУРСІВ АСУ ТП

У статті розроблено програмне забезпечення, яке призначено для системи забезпечення безпеки критичних ресурсів АСУ ТП. Метою розробки є дослідження та принципи побудови системи забезпечення безпеки критичних ресурсів АСУ ТП. Об'єктом дослідження є процес забезпечення безпеки критичних ресурсів АСУ ТП. Предметом дослідження є методи забезпечення безпеки критичних ресурсів АСУ ТП. Методи дослідження базуються на методах захисту інформації у комп'ютерних мережах, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи забезпечення безпеки критичних ресурсів АСУ ТП. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

забезпечення безпеки, критичні ресурси, АСУ ТП

Постановка проблеми. У наші дні практично в будь-якому виробництві використовуються автоматизовані системи управління технологічними процесами (АСУ ТП). Однак автоматизація без виконання вимог інформаційної безпеки може бути критично небезпечним. Розглянемо, чому захист АСУ ТП сьогодні став особливо важливим, які погрози зараз найбільш реальні, і як захистити промислові інфраструктури від зловмисників. Автоматизована система управління технологічними процесами (АСУ ТП) – це ціла група технічних і програмних засобів, призначених для автоматизації процесів управління технологічним устаткуванням на промислових підприємствах. Сьогодні багато експертів одностайні в тому, що основна погроза – це втручання терористичних, екстремістських і вороже настроєних груп у управління автоматизованими системами критично важливих об'єктів, у тому числі й з метою виводу їх з ладу. Деякі експерти зараз прогнозують, що терористичні організації будуть купувати технічну інформацію компаній для здійснення атак. Тому державам так важливо вчасно убезпечити себе від подібних погроз. Галузі, для яких тема захисту АСУ ТП найбільш критична – ті, де можливий максимальний збиток і може постраждати найбільша кількість людей. У першу чергу, це енергетичні компанії й підприємства ПЕК – отут можливі як економічні наслідки, наприклад, порушення поставок нафти або газу, або перебої в електропостачанні населення, так і екологічні або гуманітарні катастрофи. Крім того, під погрозою перебуває транспорт. Ці галузі мають широку розгалужену мережу по всій країні, і безпека на подібних підприємствах – стратегічно важливе завдання для держави.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні системи забезпечення безпеки критичних ресурсів АСУ ТП.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи забезпечення безпеки критичних ресурсів АСУ ТП.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

- Огляд існуючих систем забезпечення безпеки критичних ресурсів АСУ ТП.
- Дослідження системи забезпечення безпеки критичних ресурсів АСУ ТП.

– Програмна реалізація системи забезпечення безпеки критичних ресурсів АСУ ТП.

Об'єктом дослідження є процес забезпечення безпеки критичних ресурсів АСУ ТП.

Предметом дослідження є методи забезпечення безпеки критичних ресурсів АСУ ТП.

Методи дослідження базуються на методах захисту інформації у комп'ютерних мережах, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Системи безпеки АСУ ТП найбільш актуальні в розвинені з погляду промислової автоматизації галузях – це енергетика, нафтогазова галузь, транспорт, металургія, машинобудування. Безпека всієї промислової мережі й АСУ ТП забезпечується застосуванням комплексного послідовного підходу, що враховує специфіку й особливості промислових систем, і заснованого на вимогах і рекомендаціях як міжнародних стандартів, так і українських нормативних документів з забезпечення інформаційної безпеки промислових систем.

Комплексний підхід означає також проведення регулярного аудита стану захищеності АСУ ТП на основі інтерв'ювання фахівців підприємства, аналізу документації, структури й конфігурації систем, а також проведення інструментального аналізу захищеності з метою пошуку уразливостей. На основі отриманих за підсумками аудита даних виробляється аналіз ризиків, у результаті якого визначаються погрози, що представляють небезпеку функціонуванню об'єкта.

Класифікація рішень для інформаційної безпеки АСУ ТП

Приступаючи до побудови архітектури рішення, у першу чергу, варто підібрати вірний тип базового продукту. Умовно всі рішення ІБ АСУ ТП можна розділити на дві категорії:

– Системи моніторингу активності й виявлення погроз. Вони забезпечують тільки моніторинг, нічого не блокують, але стежать за погрозами й проблемами, виявляють їх і повідомляють служби безпеки.

Системи моніторингу активності також підрозділяються по класах, серед них:

– система виявлення комп'ютерних атак і мережних аномалій;

– система моніторингу подій інформаційної безпеки й бездротових мереж;

– система пасивного аналізу уразливостей;

– система аналізу конфігурацій устаткування, правил доступу мережного встаткування;

– а також система контролю цілісності даних і ПЗ.

Наприклад, перші з них, системи виявлення комп'ютерних атак і мережних аномалій, аналізують мережний трафік і виділяють із нього інформацію про мережні потоки (flow), аналіз якої більше ефективний для виявлення погроз у порівнянні із сигнатурними методами й дозволяє виявити в тому числі й атаки на невідомі (zero day) уразливості й вчасно реагувати на підозрілі інциденти.

– Системи запобігання погроз (або управління доступом).

Ще одна класифікація систем інформаційної безпеки АСУ ТП – це розподіл їх на традиційні й спеціалізовані. Класичні системи ІБ можуть використовуватися на промислових підприємствах для побудови архітектури, управління інформаційними потоками. Друга група рішень – спеціалізовані, підходять для компаній важкої промисловості. Це металургія, енергетика, нафтогаз, де більше агресивне середовище (температура, магнітні випромінювання, пил). Якщо системи безпеки перебувають безпосередньо на промислових об'єктах, отут повинні застосовуватися додаткові умови, ураховуватися специфічні вимоги середовища, застосовуватися спеціальний монтаж промислового встаткування, стійке до агресивних середовищ виконання й т.д. Грубо говорячи, спеціалізовані системи повинні бути «розумними», повинні розбиратися в промисловому трафіку, ураховувати саме програмне забезпечення, трафік промислових систем. Однак це не виходить, що традиційні системи безпеки не застосовуються на промислових підприємствах.

На жаль, сьогодні основна проблема безпеки АСУ ТП – це відсутність уваги до її забезпечення. Через те, що технологічні мережі найчастіше досить статичні, не прийняте що-небудь міняти, устаткування застаріває, використовуються старі версії програмних продуктів і операційних систем з безліччю уразливостей. Відсутність увага до ІБ проявляється й у безконтрольному використанні периферійних пристроїв, флеш-накопичувачів, відсутності політик захисту АСУ ТП і відповідальних осіб.

Також усе реальніше стає ймовірність кібертерроризмау У прогнозі МНС про надзвичайну обстановку на території України відзначається, що в цей час рівень інформаційної безпеки не відповідає рівню погроз у даній сфері, і в 2018 році можливе підвищення хакерських атак з метою створення умов для виникнення техногенних надзвичайних ситуацій. Тому в той час, поки ринок захисту АСУ ТП поки тільки дозріває, важливо нарощувати компетенції для надання ефективної допомоги замовникам у побудові комплексних систем управління й забезпечення інформаційної безпеки.

Сучасним трендом АСУ ТП є впровадження Інтернету речей. Рішення в області Інтернету речей будуються на базі мікропроцесорних систем з використанням різного роду ПЗ, що реалізує, у тому числі, і сучасні технології підключення до зовнішніх мереж зв'язку, які працюють по стандартизованих протоколах. Будь те Wi-fi або Bluetooth. Із цієї позиції різниця між офісною мережею або розумним будинком – невелика. І в того, і в іншого – є можливість підключення до інтернету, наприклад, для віддаленого моніторингу й управління. Але як тільки з'являється підключення до інтернету й програмний рівень, то неминуче виникають і помилки, якими можуть скористатися зловмисники. Тому підходи до забезпечення інформаційної безпеки нових застосувань ІТ повинні бути аналогічні підходам, застосовуваним у класичних випадках забезпечення інформаційної безпеки.

Ринку ще має бути розвиток убік виробництва засобів захисту, які могли б елегантно вбудовуватися в ІТ-контур «розумних» систем, аналогічно тому, як це відбувається із захистом корпоративних систем. Зараз виробники тільки починають вишиковувати в себе життєвий цикл розробки й супроводу компонентів «розумних» систем, що враховує можливість здійснення у відношенні їх несанкціонованих впливів, включаючи тестування на предмет наявності уразливостей.

Все залежить від того, наскільки й із чим інтегровано те, до чого виходить доступ, і хто власник пристрою. Наприклад, якщо говорити про розумний будинок – можна спробувати одержати доступ до конфіденційних даних домовласника, або, також відключивши сигналізацію, проникнути в будинок. У випадку з виробничим підприємством і промисловим Інтернетом речей – також є ризики. Промислові системи, невміло підключені до інтернету, – це дуже небезпечне явище, що може привести не тільки до зупинки технологічного процесу, але й регіональній катастрофі. Тому виробництво змушене балансувати на тонкій грані між безпекою й автоматизацією. Наприклад, відповідно до інформації, на Shodan – ресурсі, що самостійно сканує Всесвітню мережу й надає інформацію про те, які користувальницькі й промислові пристрої підключені до інтернету із вказівкою їхніх протоколів, доступ через інтернет можливий до цілого ряду критичних пристроїв, починаючи від медичних, закінчуючи системами управління будинками, сонячною енергетикою, розумними будинками та ін.

Застосування технологій IoT досить актуально для ЖКГ (за рахунок інтернету речей можна знизити енерго- і теплоспоживання в житлових будинках), для управління міською інфраструктурою (включаючи транспорт, висвітлення й т.д.), у сільському господарстві (для підвищення врожайності ґрунту й відстеження її параметрів), а також для промислового сектора, де збір і аналіз різних даних дозволяє, зокрема, звістці моніторинг стан устаткування й вчасно попереджати його поломку.

При зваженому підході до реалізації захисту з виявленням основних погроз і вбудовуванням в існуючу систему технологій захисту інформації, безумовно, строки впровадження можуть бути трохи збільшені. Однак мінімізація ризиків, що обіцяє рішення питань безпеки, безумовно, цього коштує.

Насправді, напрямок промислового Інтернету речей у нашій країні тільки починає розвиватися. А раз немає публічних проектів, те немає й інформації про відповідні інциденти в області інформаційної безпеки. Але світових випадків злому промислових систем досить багато. Наприклад, кілька інцидентів було в США. А у звіті Центра досліджень ризиків Кембриджського університету США в 2015 році відзначалося, що якщо зловмисники атакують кілька сегментів американської енергомережі, у результаті чого 15 штатів і Вашингтон без електрики, те економічні втрати можуть досягти $1 трлн. доларів.

Інший відомий випадок відбувся в Європі. У грудні 2014 року в Німеччині була зроблена атака на металургійний завод. Хакерам удалося віддалено вивести з ладу доменну піч, що привело до поломки встаткування. Наскільки відомо, атака складалася з декількох проникнень у системи заводу, і в результаті одна з печей перестала бути керованої. Швидше за все, цей напад було цілеспрямованим, а самі зловмисники – підкованими й в області IT, і в області контрольних систем великих промислових підприємств.

Ще приклад – атака із зараженням вірусом Stuxnet декількох ядерних об'єктів Ірану в 2010 році. У результаті було уражено біля третини центрифуг на заводі по збагаченню урану, а також зірвані строки запуску ядерної АЕС. Це, мабуть, найгучніший випадок на сьогодні.

З більше наближених до України випадків – кібератака на українських постачальників електроенергії, «Прикарпатьеобленерго» і «Київенерго», що привела до перебоїв з електрикою. Проте, хоч на об'єктах і було виявлене шкідливе ПЗ BlackEnergy, однак явних доказів тому, що атакуючі скористалися ним для проникнення в технологічну мережу, поки, наскільки я знаю, немає.

З огляду на той факт, що тематика захисту АСУ ТП – автоматизованих систем управління технологічними процесами – зараз набирає популярність. Цей момент також знайшов відбиття в оновленій доктрині інформаційної безпеки, де особлива увага приділяється блоку погроз із боку закордонних країн у плані впливу на критичну інформаційну інфраструктуру України, підприємства оборонно-промислового комплексу та ін. До речі, показово, що й у недавно проведеному опитуванні 18 з 100 опитаних керівників великих українських компаній також бачать погрозу з боку іноземних урядів.

Тому, сподіваюся, що в самому найближчому майбутньому при впровадженні технологій Інтернету речей безпека буде стояти на чолі кута. Адже зовсім точно можна сказати, що витрати на інформаційну безпеку не порівнянні з можливими негативними наслідками. Адже якщо не боротися з виникаючими погрозами, виникають ризики тимчасової зупинки виробництва, повної втрати бізнесу й навіть катастроф.

Багато чого залежить від того, що диктує ринок. Зокрема, мобільні телефони існують досить давно, але користувальницьких засобів захисту дотепер не так вуж багато, а випадки проникнення вірусів або доступу зловмисників до банківських даних через мобільні пристрої трапляються регулярно. Так може бути й у випадку з Інтернетом речей. Однак, чим перспективніше напрямок, чим більше голосних проектів реалізується (у які застосовуються спеціалізовані програмні платформи, використовуються архітектурні підходи IoT, бездротові протоколи й т.п.), тим швидше йде процес створення інструментів по захисту даних.

Моніторинг аномалій мережної активності в промислових системах

У сфері забезпечення ІБ промислових систем важливим завданням є вибір ефективних заходів і засобів захисту, які повинні запобігати несанкціонованому доступу до управління технологічними процесами, але не створювати перешкоди для роботи АСУ. Домагатися цього дозволяють рішення, що забезпечують безперервне пасивне спостереження за активністю в промислових системах і мережах, виявлення потенційних погроз і оперативне повідомлення відповідальних служб про виникаючі проблеми. Серед таких рішень можна виділити системи виявлення аномалій мережної активності (Network Behavior Anomaly Detection), застосування яких у промислових системах активно обговорюється експертним співтовариством.

Основною перевагою систем аналізу аномалій є їхнє пасивне застосування. Компоненти систем, відповідальні за збір мережного трафіку, підключаються до

дзеркалюючих (SPAN) портів мережних комутаторів або безпосередньо до мережі через TAP-пристрої (це дозволяє не створювати мережні навантаження й не породжує затримок у роботі сервісів) і не взаємодіють прямо із промисловим устаткуванням. Такі системи аналізують мережний трафік і виділяють із нього інформацію про мережні потоки (Flow). Аналіз Flow-статистики більше ефективний для виявлення погроз, чим сигнатурні методи, оскільки дає можливість виявляти, у тому числі, атаки на невідомі (zero day) уразливості, сигнатури для яких ще не випущені.

Є й інші переваги. З обліком того, що штатна взаємодія пристроїв у промисловій мережі повинне бути статичним протягом тривалого часу, розгортання систем виявлення аномалій, їх «навчання», запуск в «бойовому» режимі й безперервній експлуатації значно спрощуються, оскільки не потрібні часті зміни профілю нормального поводження. Нарешті, робота систем аналізу аномалій дозволяє оцінити реальний рівень безпеки й виявити проблеми в системі забезпечення ІБ промислової мережі, причому результати аналізу можуть стати основою її вдосконалювання.

Системи класу Network Behavior Anomaly Detection (NBAD) добре зарекомендували себе при захисті офісних мереж і ЦОДів. Серед пропозицій є як комерційні (наприклад, Lancope StealthWatch, Arbor Networks Pravail NSI, McAfee Network Threat Behavior Analysis), так і безкоштовні (FlowMatrix, FlowBAT, Bro) рішення.

Функціонал цих систем містить у собі наступні можливості:

– виявлення підключення мережних пристроїв і побудова карти мережі;

– створення профілю нормальної мережної взаємодії;

– моніторинг мережної активності в режимі 24/7 для виявлення аномального поводження (аномальні з'єднання, пристрої, час і обсяги трафіку й інші показники);

– виявлення зовнішніх і внутрішніх (пов'язаних з навмисними або помилковими діями персоналу) погроз;

– оперативне оповіщення відповідальних служб про проблеми й передача інформації про їх у суміжні системи безпеки;

– ведення історії змін мережного поводження й допомога при розслідуванні інцидентів;

– формування звітів з різними рівнями деталізації.

Експерти затверджують, що своєчасне застосування рішень, що забезпечують моніторинг мережної активності, дозволило б виявити активність шкідливого ПЗ Stuxnet, Havex і BlackEnergy, оскільки в таких випадках мережне поводження виходить за рамки нормальної взаємодії пристроїв у мережі. Наприклад, не залишилися б непоміченими спроби відновлення прошивання контролера по мережі або збору даних. Незважаючи на всю користь і ефективність традиційних NBAD-систем, вони не можуть виявляти аномальний уміст прикладних промислових протоколів. Ріст числа погроз для систем промислової автоматизації привів до того, що на ринку стали з'являтися рішення, адаптовані для роботи саме в промислових мережах. Їхня робота заснована на тім же принципі пасивного збору трафіку, але вони здатні аналізувати промислові протоколи (deep packet inspection) і виявляти в них аномальні дані. У деяких джерелах цей клас рішень одержав назву Industrial Network Anomaly Detection (INAD).

Зараз відомі наступні закордонні рішення: Dragos Security CyberLens, NexDefense Sophia, C4 Security Fides, SCADAfense. Ці рішення перебувають на різних стадіях зрілості. Деякі з них існують уже кілька років (наприклад, NexDefense Sophia), а деякі – тільки анонсовані (зокрема, SCADAfense). У кожному разі помітний інтерес виробників і замовників до рішень цього класу.

Розглянуті системи підтримують як відкриті, так і пропрієтарні промислові протоколи, у тому числі DNP3, ModbusTCP, Profinet, ISO-TSAP, AB-PCCC, BACNet, Ethernet / IP і інші. У різних продуктах підтримувані протоколи й функціональні можливості розрізняються.

У загальному виді системи даного класу дозволяють виявляти наступні види активності:

– нелегітимні команди й мережний трафік, що виводять із ладу системи управління;
– присутність у промисловій мережі шкідливого ПЗ, локалізація вогнищ зараження;
– дії зловмисників у промисловій мережі без використання шкідливого ПЗ;
– керуючі команди, що приводять до порушень технологічного процесу;
– команди на зупинку / перезавантаження / перепрошивання / переконфігурацію контролерів;
– команди, що встановлюють неприпустимі / небажані значення ключових параметрів управління технологічним процесом.

З особливостей застосування таких систем відзначимо наступні. Їм потрібне значний час на первісний збір даних для побудови профілю нормального поводження й завдання базової політики безпеки. Але це – плата за невикористання активного сканування, що може створювати проблеми в роботі промислової мережі. Крім того, для підключення до SPAN-порту мережного комутатора або підключення TAP-пристрою, що необхідно для пасивного збору трафіку, потрібне активна взаємодія з мережним устаткуванням (конфігурація, установка в розрив). Однак імовірність того, що ці дії й подальша робота системи приведуть до проблем, украй мала. Ефективність систем безпеки в цьому випадку незрівнянно вище ризику від їхнього застосування.

Крім систем, орієнтованих на пошук аномалій у мережному трафіку промислових мереж, сталі з'являтися цікаві рішення, націлені на безконтактне виявлення аномалій у роботі промислового встаткування (такий функціонал забезпечує PFP Cybersecurity). Останнє завдання реалізується шляхом спостереження за енергоспоживанням процесора.

Безумовно, вибір конкретного продукту повинен здійснюватися на основі аналізу індивідуальних вимог замовника, особливостей промислових систем і мереж, типу промислового об'єкта. Конче потрібно й ретельне тестування продукту до його введення в експлуатацію. Однак вибір рішень на ринку однозначно є.

Інтеграція бізнес-додатків з виробничими процесами, впровадження рішень класу MES, ERP, розвиток мережних комунікацій між офісними й промисловими сегментами, використання ОС Windows / Linux і IP-протоколів – все це створює потенційну погрозу несанкціонованого доступу до промислових систем з непередбаченим збитком.

Аудит безпеки й аналіз захищеності

Містить у собі аналіз документації, структури й конфігурації систем, проведення інтерв'ю фахівців замовника, а також аналіз захищеності інфраструктури підприємства з визначенням існуючих уразливостей. Підсумковий звіт містить вичерпну інформацію з поточного стану інформаційної безпеки, опис існуючих погроз і рекомендації із протидії їм, методику й опис ходу роботи. У ході аудита перевіряється практична реалізація вимог і рекомендацій IEC 62443, NIST SP 800-82r2, і інших українських і міжнародних стандартів з забезпечення інформаційної безпеки промислових систем.

Побудова системи управління інформаційною безпекою

Розробляється комплексна система управління інформаційною безпекою (СУІБ) підприємства, у тому числі політикові інформаційної безпеки, корпоративні стандарти й нормативна документація, що регулює процеси управління ІБ. Додатково персонал замовника проходить навчання правилам інформаційної безпеки промислових систем.

Побудова системи забезпечення інформаційної безпеки

Система забезпечення ІБ виявляє й блокує спроби несанкціонованого доступу до технологічної інформації й управління промисловими системами. При її створенні враховуються тенденції розвитку сучасних промислових систем при підключенні до Інтернету, організації віддаленого доступу до встаткування Dial-UP, підключенні до корпоративної мережі, використанні бездротових мереж UMTS / HSDPA / ZigBee / WiFi.

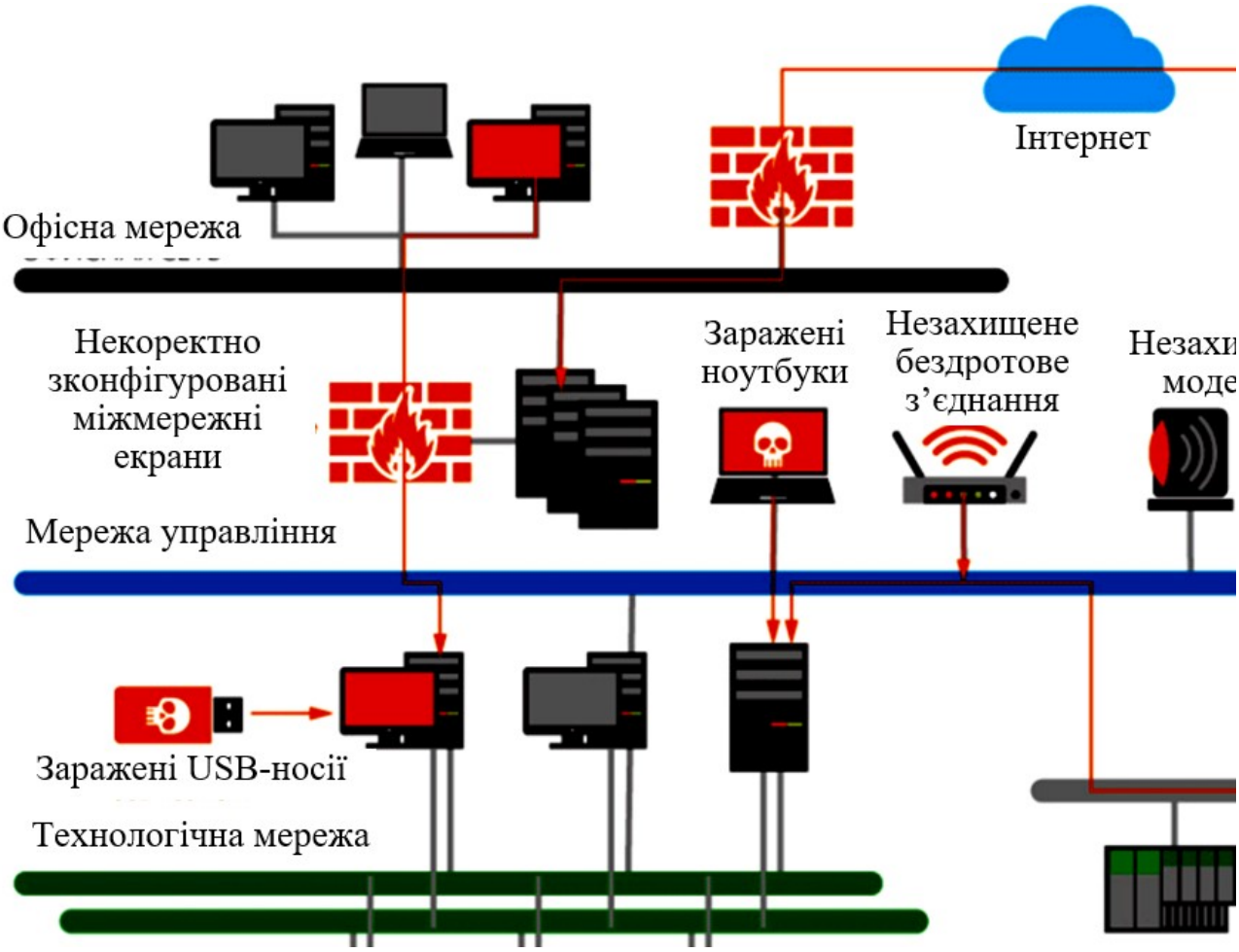

Рисунок 1 – Структурна схема системи

На структурній схемі системи наведена типова мережа промислового підприємства й основні погрози інформаційної безпеки.

Під захист попадають основні компоненти промислових систем: робітники станції операторів і інженерів, сервери SCADA і архіву, програмувальні логічні контролери, інтелектуальні виконавчі пристрої й датчики, промислове мережне встаткування, канали зв'язку, шлюзи віддаленого доступу й інші компоненти. Арсенал використовуваних засобів містить у собі односпрямовані шлюзи, промислові міжмережні екрани, рішення для розвідки кіберзагроз, виявлення мережних атак і аномалій, контролю команд, що відправляються на контролери АСУ ТП, системи контролю запуску додатків на серверах і автоматизованих робочих місцях (АРМ) операторів АСУ ТП, сервіси розвідки кіберзагроз.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів забезпечення безпеки критичних ресурсів АСУ ТП. Рішення даного завдання полягало у вирішенні наступних задач:

– Був проведений огляд існуючих систем забезпечення безпеки критичних ресурсів АСУ ТП.

– Досліджена система забезпечення безпеки критичних ресурсів АСУ ТП.

– На основі отриманих результатів досліджень створена програмна реалізація системи забезпечення безпеки критичних ресурсів АСУ ТП. Розроблені алгоритми дозволяють успішно вирішувати завдання забезпечення безпеки критичних ресурсів АСУ ТП. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Смірнова, Т.В. «Дослідження методів, моделей та сучасних ІТ-рішень для підтримки технологічних процесів у критичній інфраструктурі держави». Кібербезпека: освіта, наука, техніка. 2025. Том 2 № 30. С.195-208, 2025.
2. Kuznetsov, O., Frontoni, E., Kuznetsova, K., Arnesano, M., Smirnov, O. «A secure biometric authentication architecture for blockchain-driven cyber-physical systems». Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications, 2025, pp. 193–224.
3. Kuznetsov, O., Atzeni, G., Arnesano, M., Randieri, C., Smirnov, O. «Secure IoT-based smart wheelchair system: From implementation to security enhancement strategy». Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications, 2025, pp. 225–257.
4. Kuznetsov, O., Smirnov, O., Kuznetsova, T., Shaikhanova, A., Svatowsky, I. «Privacy-utility trade-offs in IoT networks: A comparative analysis of differential privacy mechanisms for sensor data aggregation». Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications, 2025, pp. 589–622.
5. Вінтенко Б., Смірнов О., Миронець І., Смірнова Т., Смірнов С. «Імітаційна модель шляхів вхідних даних комп'ютерної інтелектуальної системи підтримки оператора енергоблоку АЕС». Комбінаторні конфігурації та їхні застосування: Матеріали XXVII Міжнародного науково-практичного семінару, присвяченого 125-річчю Національного університету «Запорізька політехніка» (Запоріжжя-Кропивницький-Київ, 4-6 червня 2025 р.). Запоріжжя: НУ «Запорізька політехніка», 2025. С.82-91.
6. Al-Azzeh, J., Ayyoub, B., Mesleh, A., Smirnova, T., Gnatyuk, S., Drieiev, O., Smirnov, O., Dorenskyi, O. «Cloud-Based Information System for Evaluating Caverns in the Process of Blasting Metal Surfaces of Details». International Review on Modelling and Simulations 18 (1), 2025. pp. 32-42.
7. Вінтенко Б.Ю., Смірнов О.А., Миронець І.В., Смірнова Т.В., Коваленко О.В., Мацуй А.М. «Модель шляхів отримання вхідних даних комп'ютерної інтелектуальної системи підтримки оперативного персоналу АЕС». Центральноукраїнський науковий вісник. Технічні науки. 2025. Вип. 11(42), ч. II. С.52-62.
8. Вінтенко Б.Ю., Смірнов О.А., Миронець І.В., Смірнова Т.В. «Методи забезпечення відмовостійкості інтелектуальних систем підтримки оператора». VIII міжнародна науково-практична конференція "Інформаційна безпека та комп'ютерні технології", м. Кропивницький. 24-25 квітня 2025 р. – Кропивницький: ЦНТУ. – 2025. – С. 44-46.
9. Вінтенко, Б., Миронець, І., Смірнов, О., Коваленко, А., Конопліцька-Слободенюк, О., Смірнова, Т., Константинова, Л. «Дослідження застосування систем підтримки оперативного персоналу об'єкту критичної інфраструктури при керуванні енергоблоком АЕС з реактором типу ВВЕР-1000». Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2024. № 2(26), С. 6-26.
10. Смірнова Т.В., Конопліцька-Слободенюк О.К., Буравченко К.О., Смірнов С.А., Кравчук О.В., Козірова Н.Л., Смірнов О.А. «Дослідження технологій забезпечення кібербезпеки хмарних сервісів IaaS, PaaS та SaaS». Кібербезпека: освіта, наука, техніка. 2024. №4(24), С. 6-27.
11. Вінтенко, Б., Миронець, І., Смірнов, О., Кравчук, О., Козірова, Н., Савеленко, Г., Коваленко, А. «Дослідження вимог та аналіз кібербезпеки програмного забезпечення інформаційно-керуючих систем АЕС, важливих для безпеки». Кібербезпека: освіта, наука, техніка. 2024. №3(23), С. 111-131.
12. Al-Mudhafar Aqeel, A.M., Smirnova, T., Buravchenko, K., Smirnov, O. «The method of assessing and improving the user experience of subscribers in software-configured networks based on the use of machine learning». Advanced Information Systems, 2023, 7(2), pp. 49-56.
13. Kuznetsov, O., Kuznetsova, Y., Smirnov, O., Kostenko, O., Zvieriev, V. «Evaluating Hashing Algorithms in the Age of ASIC Resistance». CEUR Workshop Proceedings, 2023, 3628, pp. 93-105.
14. Smirnov, O., Sydorenko, V., Aleksander, M., Zhyharevych, O., Yenchev, S. «Simulation of the cloud IoT-based monitoring system for critical infrastructures». CEUR Workshop Proceedings, Volume 3530, 2023, pp. 256-265.
15. Smirnov, O., Odarchenko, R., Smirnova, T., Bondar, S., Volosheniuk, D. «Optimal Structure Construction of Private 5G Network for the Needs of Enterprises». Lecture Notes on Data Engineering and Communications Technologies, 2023, 178, pp. 208–223.
16. Вінтенко Б.Ю., Смірнов О.А., Коваленко А.С., Смірнов С.А., Буравченко К.О. «Дослідження вимог міжнародних стандартів IEC60880 та IEC62138 з розробки програмного забезпечення інформаційно-керуючих систем АЕС, важливих для безпеки». Системи управління, навігації та зв'язку, 2023, вип. 3(73), С. 155-166.
17. Аль-Мудхафар Акіл Абдулхуссейн М., Смірнова Т.В., Буравченко К.О., Смірнов О.А. «Метод оцінки та підвищення користувальницького досвіду абонентів в програмно-конфігурованих мережах на основі використання машинного навчання». Сучасні інформаційні системи, 2023, том 7, № 2, С. 49-56.
18. Smirnova, T., Gnatyuk, S., Yudin, O., Sydorenko, V., Polozhentsev, A., «The Model for Calculating the Quantitative Criteria for Assessing the Security Level of Information and Telecommunication Systems». CEUR Workshop Proceedings Volume 3156, 2022, Pages 390-399.
19. Смірнова Т.В., Гнатюк С.О., Сидоренко В.М., Юдін О.Ю., Сидоренко С.Ю., «Модель визначення критичності галузевих інформаційно-телекомунікаційних систем». Проблеми інформатизації та управління, № 2(70). 2022. С. 28-37.

20. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Смірнов С.А., Поліщук Л.І., «Дослідження стійкості до диференціального криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Системи управління, навігації та зв'язку, 2022, № 3(69). С. 93-98.
21. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Поліщук Л.І., Смірнов С.А. «Дослідження статистичної стійкості та швидкісних характеристик запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Вісник Хмельницького національного університету. Серія: «Технічні науки», № 2 (307). С. 46-52. 2022.
22. Смірнов О.А., Смірнова Т.В., Константинова Л.В., Смірнов С.А., Якименко Н.М., «Дослідження стійкості до лінійного криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Системи управління, навігації та зв'язку, 2022, № 1(67). С. 84-89.
23. Smirnova T., Gnatyuk S., Berdibayev R., Avkurova Zh., Iavich M. «Cloud-Based Cyber Incidents Response System and Software Tools». Communications in Computer and Information Science, 2021, vol 1486. Springer, Cham. pp 169-184.
24. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». CEUR Workshop Proceedings. Volume 2740, 2020, Pages 102-114.
25. Smirnov O., Alimseitova Zh., Adranova A., Akhmetov B., Lakhno V., Zhilkishbayeva G. «Models and algorithms for ensuring functional stability and cybersecurity of virtual cloud resources». Journal of theoretical and applied information technology Vol.98. No 21, 2020, P. 3334-3346.
26. Smirnov O., Kuznetsov A., Kiian A., Cherep A., Kanabekova M., Chepurko I. «Testing of code-based pseudorandom number generators for post-quantum application». 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, May 14-18. 2020. P. 172-177.
27. Smirnov O., Kuznetsov A., Pushkar'ov A., Serhiienko R., Babenko V., Kuznetsova T., «Representation of Cascade Codes in the Frequency Domain». In: Radivilova T., Ageyev D., Kryvinska N. (eds) Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies, vol 48. Springer, Cham. 2021. pp 557-587.
28. Smirnov, O., Markovets, O. Vovk, N., Turchyn, Y., «Model of informational support for social network administrators' content creation». CEUR Workshop Proceedings Volume 2616, 2020, Pages 125-136.
29. Smirnov, O., Drieieva, H., Drieiev, O., Polishchuk, Y., Brzhanov, R., Aleksander, M. «Method of fractal traffic generation by a model of generator on the graph». CEUR Workshop Proceedings Volume 2616, 2020, Pages 366-379.
30. Smirnov, O., Drieieva, H., Drieiev, O., Simakhin, V., Bondar, S., Odarchenko, R. «Managing multifractal properties of the binary sequence generated with the Markov chains», CEUR Workshop Proceedings Volume 2608, 2020, Pages 633-645.
31. Smirnov O. Kuznetsov A., Zaicenko Yu., Pastukhov M., Oleshko O., Kuznetsova K., «Formation of Discrete Signals with Special Correlation Properties». International Conference on Information and Telecommunication Technologies and Radio Electronics, UkrMiCo 2019; Odessa; Ukraine; 9-13 September 2019. P.22-28.
32. Smirnov, O., Kuznetsov, A., Kolovanova, I., Kuznetsova, T., «Noise immunity of the algebraic geometric codes». International Journal of Computing; 2019, Volume 18, Issue 4 – Research Institute for Intelligent Computer Systems – 2019. – P. 393-407.
33. Smirnov, O., Kuznetsov, A., Reshetniak, O., Ivko, N., Katkova, T., Kuznetsova, T., «Generators of Pseudorandom Sequence with Multilevel Function of Correlation». 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), Kyiv, Ukraine, 8 – 11 October 2019 . P.517-522.
34. Smirnov, O., Odarchenko, R., Abakumova, A., Usik, P., Kundyz, M., «QoE optimization technique for media delivery in 5G networks». 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), Kyiv, Ukraine, 8 – 11 October 2019. P.597-601.