Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню бакалавра

студента *Черненка Єгора Юрійовича*

академічної групи *125-17-2*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему ***Система захисту інформації виробничої дільниці ЧПУ ООО «Техноком»***

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	доц.Горєв В.М.			
розділів:				
спеціальний	Саксонов Г.М.			
економічний	к.е.н., доц. Пілова Д.П.			
Рецензент				
Нормоконтролер	ас. Конограй Н.О.			

Дніпро
2021

ЗАТВЕРДЖЕНО:
завідувач кафедри безпеки
інформації та телекомунікацій
_____ д.т.н., проф.Корнієнко В.І.
«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студенту *Черненку Єгору Юрійовичу* **академічної групи** *125-17-2*
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

на тему ***Система захисту інформації виробничої дільниці ЧПУ ТОВ «Техноком»***

затверджену наказом ректора НТУ «Дніпровська політехніка» від 07.06.2021 № _317-с_

Розділ	Зміст	Термін виконання
Розділ 1	Проведено аналіз структури АСУТП, підсистеми ЧПУ в АСУТП, аналіз особливостей АСУТП з точку зору ІБ. Проаналізовано стандарти в області захисту інформації АСУТП та виявлені загрози ІБ в підсистемі ЧПУ	07.03.2021-29.04.2021
Розділ 2	Проведено обстеження виробничої дільниці ЧПУ, аналіз та оцінка інформаційних ризиків, модель порушника і загроз, заходи безпеки та рекомендації, висновки до спеціальної частини	30.04.2021-31.05.2021
Розділ 3	Проведення економічних розрахунків для підтвердження економічної доцільності розробки заходів безпеки та рекомендацій, та ефекту впровадження контролю фізичного доступу до ЧПУ та візуальний контроль виконання керуючих програм на ЧПУ	01.06.2021-10.06.2021

Завдання видано _____ _____
(підпис керівника) (прізвище, ініціали)

Дата видачі: 07.01.2021р.

Дата подання до екзаменаційної комісії: 14.06.2021р.

Прийнято до виконання _____ Черненко Є.Ю.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 64 с., 12 рис., 11 табл., 5 додатків, 22 джерела.

Об’єкт дослідження: виробнича дільниця ЧПУ ТОВ “Техноком”

Предмет дослідження: політика безпеки інформації об’єкта інформаційної діяльності (ОІД).

Мета роботи (проекту): підвищення рівня захисту інформації в ІТС ТОВ “Техноком”

Методи розробки: спостереження, порівняння, аналіз, опис.

У першому розділі проведено аналіз структури АСУТП, підсистеми ЧПУ в АСУТП, аналіз особливостей АСУТП з точку зору ІБ. Проаналізовано стандарти в області захисту інформації АСУТП та виявлені загрози ІБ в підсистемі ЧПУ.

У спеціальній частині проведено обстеження виробничої дільниці ЧПУ, проаналізовані та оцінені інформаційні ризики. Також розроблено модель загроз та модель порушника безпеки інформації, сформовані основні положення політики безпеки інформації для комплексної системи захисту інформації, та розроблені заходи безпеки, такі як: контроль фізичного доступу до ЧПУ і візуальний контроль виконання керуючих програм на ЧПУ.

В третьому розділі проведені економічні розрахунки для підтвердження економічної доцільності розробки заходів безпеки та рекомендацій, та ефекту впровадження контролю фізичного доступу до ЧПУ та візуальний контроль виконання керуючих програм на ЧПУ.

ІНФОРМАЦІЙНА БЕЗПЕКА АСУТП, ЧПУ, ОБ'ЄКТ ЗАХИСТУ, АНАЛІЗ РИЗИКІВ, МОДЕЛЬ ПОГРОЗ, МОДЕЛЬ ПОРУШНИКА, ПОЛІТИКА БЕЗПЕ

РЕФЕРАТ

Объяснительная записка: 64 с., 12 рис., 11 табл., 5 приложений, 22 источника.

Объект исследования: производственный участок ЧПУ ООО "Техноком".

Предмет исследования: политика безопасности информации объекта информационной деятельности (ОИД).

Цель работы (проекта): повышение уровня защиты информации в ИТС ООО "Техноком".

Методы разработки: наблюдение, сравнение, анализ, описание.

В первом разделе проведен анализ структуры АСУТП, подсистемы ЧПУ в АСУТП, анализ особенностей АСУТП с точки зрения ИБ. Проанализированы стандарты в области защиты информации АСУТП и выявленные угрозы ИБ в подсистеме ЧПУ.

В специальной части проведено обследования производственного участка ЧПУ, проанализированы и оценены информационные риски. Также разработана модель угроз и модель нарушителя безопасности информации, сформированы основные положения политики безопасности информации для комплексной системы защиты информации, и разработаны меры безопасности, такие как: контроль физического доступа к ЧПУ и визуальный контроль выполнения управляющих программ на ЧПУ.

В третьем разделе проведены экономические расчеты для подтверждения экономической целесообразности разработки мер безопасности и рекомендаций, и эффекта внедрения контроля физического доступа к ЧПУ и визуальный контроль выполнения управляющих программ на ЧПУ.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АСУТП, ЧПУ, ОБЪЕКТ ЗАЩИТЫ, АНАЛИЗ РИСКОВ, МОДЕЛЬ УГРОЗ, МОДЕЛЬ НАРУШИТЕЛЯ, ПОЛИТИКА БЕЗОПАСНОСТИ

ABSTRACT

Explanatory note: 64 p., 12 figures, 11 tables, 5 applications, 22 sources.

Object of research: production site of CNC LLC "Technocom".

Subject of research: information security policy of the object of information activity (OID).

Purpose of work (project): increasing the level of information protection in ITS LLC "Technocom".

Development methods: observation, comparison, analysis, description.

In the first section the analysis of the structure of the control system, the CNC subsystem in the control system, the analysis of the features of the control system from the point of view of IS is carried out. The standards in the field of information protection of the control system and the identified threats of IS in the CNC subsystem are analyzed.

In the special part of the inspection of the CNC production site, information risks are analyzed and assessed. A threat model and an information security intruder model have also been developed, the basic provisions of the information security policy for an integrated information security system have been developed, and security measures have been developed, such as control of physical access to CNC and visual control of CNC control programs.

In the third section, economic calculations are performed to confirm the economic feasibility of developing security measures and recommendations, and the effect of the introduction of control of physical access to the CNC and visual control of the implementation of control programs on the CNC.

INFORMATION SECURITY ACS, CNC, OBJECT OF PROTECTION, RISK ANALYSIS, THREAT MODEL, VIOLER'S MODEL, SECURITY POLIC

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АСУТП – автоматизована система управління технологічним процесом;

АРМ – автоматизоване робоче місце;

ІС – інформаційна система;

ІТС – інформаційна-телекомунікаційна система;

НСД – несанкціонований доступ;

ІБ – інформаційна безпека;

ІзОД – інформація з обмеженим доступом;

ЛОС – локальна обчислювальна мережа;

СЗІ – система захисту інформації;

ОС – операційна система;

ОСРЧ – операційна система реального часу;

ПЗ – програмне забезпечення;

ПБІ – політика безпеки інформації;

КП – керуюча програма;

ЧПУ – числове програмне управління;

СЧПУ – станки з числовим програмним управлінням;

РВТ – рукав високого тиску;

СКУД – система контролю управління доступу;

ОІД – об’єкт інформаційної діяльності

ЗМІСТ

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи;

ДОДАТОК Б. Огляд стандарту безпеки промислових систем управління NIST SP 800-82;

ДОДАТОК В. Перелік документів на оптичному носії;

ДОДАТОК Г. Відгуки керівників розділів;

ДОДАТОК Ґ. Відгук керівника кваліфікаційної роботи.

ВСТУП

На відміну від традиційних систем інформаційних технологій, в автоматизованих системах управління технологічними процесами (АСУТП) існує досить тісний взаємозв'язок автоматизованих систем з фізичними процесами і виконавчими пристроями. Визначальною відмінністю від традиційних інформаційних систем є характерне управління процесами і фізичними об'єктами в режимі реального часу, тоді як звичайні адміністративні системи управляють інформацією, і в більшості випадків не критичні до часу її обробки. Для забезпечення безпеки АСУТП вкрай рідко використовуються традиційні методи захисту інформації, оскільки вони, як правило, породжують надмірність обчислень і можуть уповільнити або зовсім зупинити відправку та отримання керуючого сигналу.

Робота обладнання з числовим програмним управлінням (ЧПУ) входить до АСУТП, що дозволяє значно збільшити продуктивність, виключити ймовірність впливу людського фактору і поліпшити якість продукції. Наявність програмованого обладнання в кілька разів збільшує ефективність виробництва і значно скорочує витрати. При цьому ключову роль відіграє інформація, яка визначає технологічний процес, а застосовувані в них методи захисту більшою мірою відносяться до забезпечення технологічної безпеки.

На сьогоднішній день проведено безліч досліджень, присвячених кібервразливостям промислових систем управління – зокрема, контролерів АСУТП, маніпуляції з якими можуть викликати порушення в роботі керованих систем. Якщо влаштувати таємну атаку, яка внесе зміни в виробництво деталей, то вона може привести до зміни їх характеристик, що не відповідає розрахунковим. При цьому такі модифікації можуть бути непомітні при стандартних умовах їх тестування, що надалі може привести до катастрофічних наслідків при їх використанні.

Ця дипломна робота присвячена аналізу інформаційних загроз виробничої дільниці ТОВ “Техноком”, обладнаній верстатами з ЧПУ, і розробці заходів по їх зменшенню.

1 СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Аналіз структури АСУТП

Автоматизована система управління - комплекс програмних і програмно-апаратних засобів, призначених для контроля за технологічним і виробничим обладнанням (виконавчими пристроями) і виробленими ними процесами, а також для управління таким обладнанням і процесами. Автоматизовані виробничі лінії є невід'ємним атрибутом сучасного машинобудівного виробництва. Усі АСУ можна розділити на три групи: автоматизовані системи управління технологічними процесами (АСУТП), автоматизовані системи управління (АСУП) і інтегровані АСУ.

Автоматизовані системи управління технологічними процесами - це системи, призначені для вироблення і реалізації керуючих впливів на технологічний об'єкт управління, згідно з прийнятим критерієм.

АСУТП логічно поділяють на три рівні:

– верхній рівень, або рівень візуалізації, диспетчеризації та збору даних;

– середній рівень, або рівень контролерів;

– нижній рівень, або рівень контрольно-вимірювального обладнання.

Функції АСУТП підрозділяються на керуючі, інформаційні та допоміжні і реалізуються на трьох інформаційних рівнях [1].

На верхньому рівні (рівень корпоративної мережі) за участю оперативного персоналу вирішуються завдання диспетчеризації процесу, оптимізації режимів, підрахунку техніко-економічних показників виробництва, візуалізації та архівування процесу, діагностики і корекції програмного забезпечення системи. Верхній рівень АСУТП реалізується на базі серверів і робочих станцій.

На середньому рівні вирішуються завдання автоматичного управління і регулювання, пуску і зупинки обладнання, логіко-командного управління, аварійних відключень і захистів. Середній рівень реалізується на основі програмованих логічних контролерів.

Нижній (польовий) рівень АСУТП забезпечує збір даних про параметри технологічного процесу і стану обладнання, і реалізує управлінський вплив. Основними технічними засобами нижнього рівня є датчики і виконавчі пристрої, станції, пускачі, кінцеві вимикачі і перетворювачі частоти [2].

Для функціонування АСУТП необхідна взаємодія наступних її компонентів:

– технічне забезпечення;

– програмне забезпечення;

– інформаційне забезпечення;

– організаційне забезпечення;

– операційний персонал;

Технічною освітою і програмним забезпеченням АСУТП називають повну сукупність технічних і програмних засобів, достатніх для її функціонування і реалізації системою всіх її функцій.

Інформаційне забезпечення АСУТП складається з:

– інформації про стан технологічного процесу;

– системи класифікації та кодування технологічної та техніко-економічної інформації;

– масиву даних і документів;

До операційного персоналу відносяться технологи-оператори та експлуатаційний персонал, який забезпечує правильне функціонування комплексу технічного і програмного забезпечення.

Телекомунікації в АСУТП представляються мережами передачі даних, які умовно поділяються на два рівні: верхній рівень і нижній.

Мережі верхнього рівня використовують для передачі даних між контролерами, серверами та робочими станціями. Основний стандарт мереж верхнього рівня – Ethernet. Причина широкого використання цього стандарту в тому, що з допомогою Ethernet легко об’єднують обладнання верхнього рівня АРМ і сервери, як і у більшості випадків є персональними комп'ютерами. Також перевагою мереж Ethernet є велика

швидкість передавання даних.

У програмному комплексі АСУТП і мережі верхнього рівня використовують такі заходи захисту: ведення архіву повідомлень, захист інформації вбудованими інструментами протоколу Ethernet, самодіагностика програмно-технічних засобів, захист від несанкціонованого доступу за допомогою паролю.

Головною функцією мережі нижнього рівня є забезпечення взаємодії між контролерами обладнання та віддаленою периферією їх управління.

1.2 Підсистема ЧПУ в АСУТП

Специфікою автоматизованого виробничого обладнання з ЧПУ є наявність керуючого модуля, який комплектується мікроконтролерами, відповідальними за дії приводів. Алгоритм дій верстата визначає керуюча програма. Крім самої програми комп'ютер верстата містить дані про обладнання, матеріали і режими різання. На різних етапах підготовки виробничих потужностей і безпосередньо виробництва деталей (виробів, вузлів і т.д.) в системах автоматизованого проектування формуються файли даних. Першим етапом є розробка тривимірної моделі і креслень в системах автоматизованого проектування (CAD-системах). При цьому файли даних зберігаються у внутрішньому поданні CAD-системи на АРМ технологічного персоналу. Наступним етапом є формування керуючої траєкторії в CAM-системі, яка також зберігається у внутрішньому поданні CAM-системи в файлі проекту обробки або в CL-файлі. Для перетворення керуючої траєкторії в керуючу програму для верстата з ЧПУ застосовується постпроцесор. Отримана керуюча програма зберігається в текстовому файлі на АРМ технологічного персоналу.

Спрощено описана схема показана на рисунку 1.1.

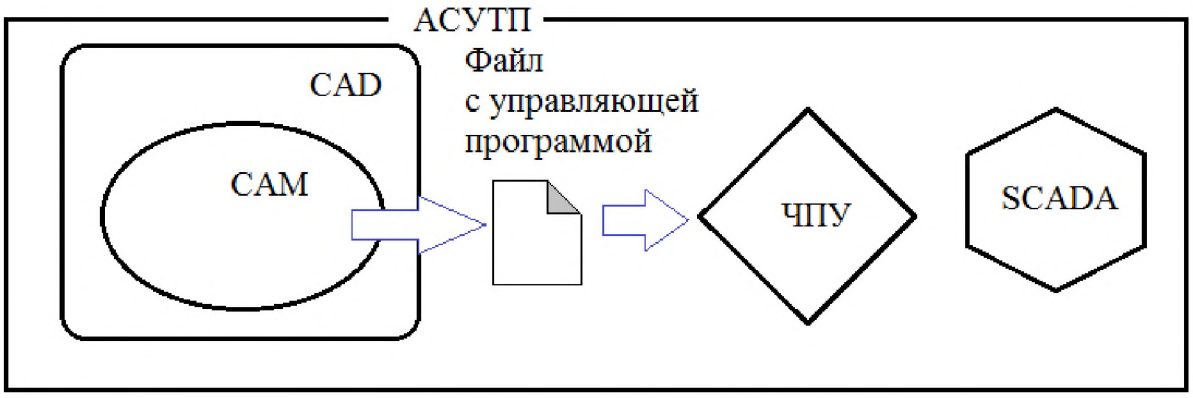


Рисунок 1.1 – Спрощено схема АСУТП

Верстат з ЧПУ дозволяє створювати деталі, які мають різні форми: від простих до максимально складних. Використання такого обладнання у виробництві значно підвищує рівень продуктивності і якість продукції, що випускається. Для роботи верстатів з ЧПУ потрібні керуючі програми. Вони служать для створення майбутніх виробів, введення команд управління і читання інструкцій, написаних спеціальною мовою програмування. Керуюча програма для верстатів з ЧПУ служить для контроля над верстатом і забезпечує автономний або напівавтономний процес обробки заготовок. Завдяки їй існує можливість з високою точністю проводити якісні деталі складної форми без технологічних помилок.

Спеціально програмне забезпечення дає можливість звільнити оператора від постійного стеження за робочим обладнанням та необхідності щохвилини контролювати процес. Таке ПЗ містить в собі набір команд, які безперервно надходять на верстат з ЧПУ. Команди дозволяють в автоматичному режимі:

- переміщати інструменти,
- переміщати деталі в системі координат,
- контролювати швидкість обробки.

В якості точки відліку для подальших дій кожного разу приймається положення виконавчого інструменту, яке він займав раніше. Для кожного виду заготовок пишеться окрема програма. Щоб її створити, потрібно встановити на комп'ютер спеціальне програмне забезпечення - CAM / CAD.

CAM (система автоматизованого виробництва) - спеціальна програма, що працює з CAD об'єктами - трьохвимірні об'єкти на основі заданих даних. CAM-програма конвертує цифрові об'єкти CAD в зрозумілі верстату команди в форматі G-code. G-code це безпосередньо керуюча програма для верстатів з ЧПУ - набір команд для обладнання. Часто CAD / CAM поставляються у вигляді одного програмного пакета, або заздалегідь підготовлені для простої інтеграції в програмно-апаратні комплекси та спільної роботи.

На рисунку 1.2 вказано G-код для верстата з ЧПУ.

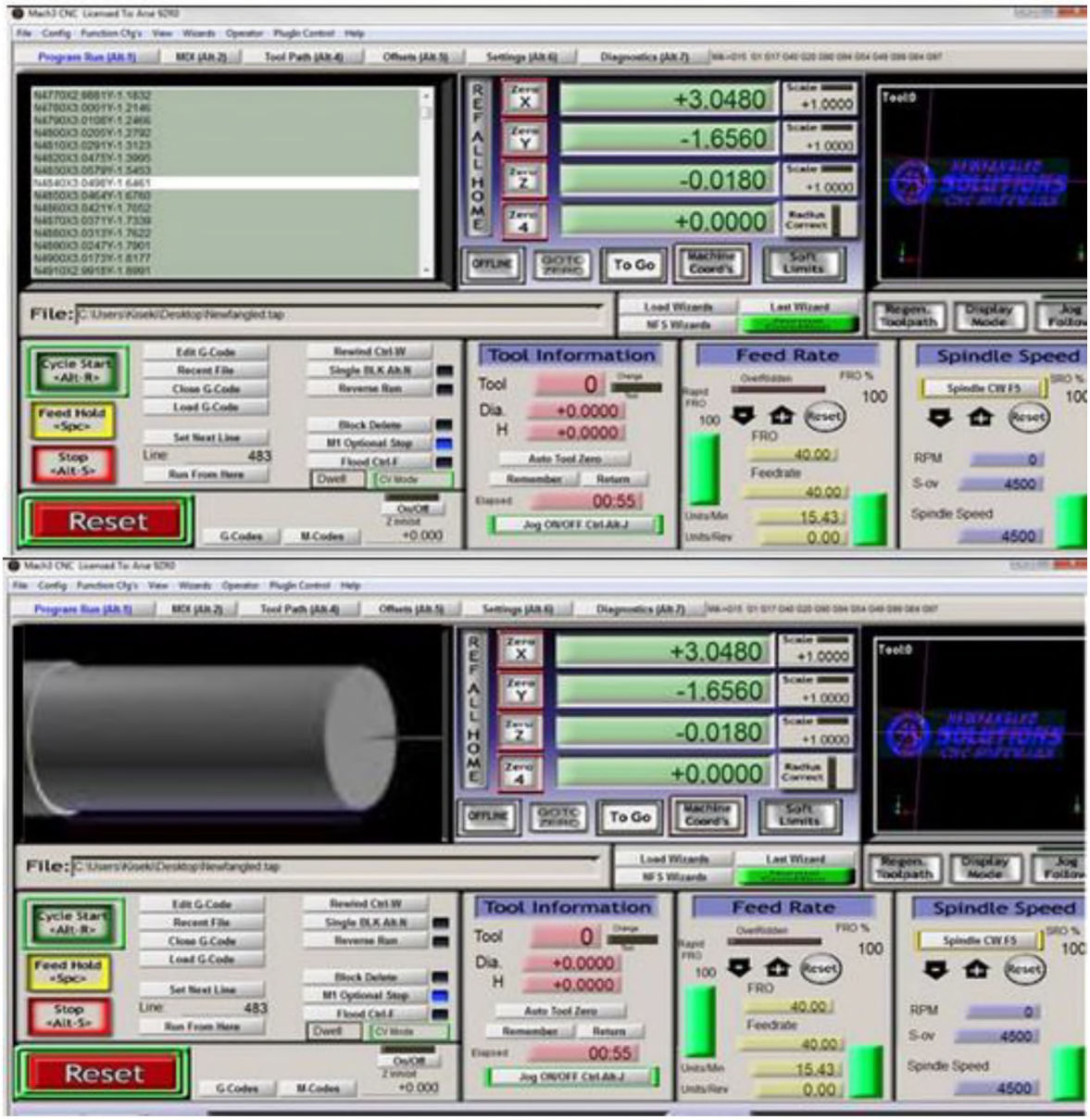


Рисунок 1.2 – G-код для верстата з ЧПУ

Постановка завдань для всіх систем ЧПУ відбувається з використанням універсальної мови програмування у вигляді керуючого програмного коду, який називають G-кодом. Керуюча програма складається з послідовного набору кадрів, кожен з яких відповідає за один крок в роботі верстата.

Готові завдання для обробки деталей є ланцюжок окремих G-команд. Основні команди мови називають підготовчими, їх рівно 100: від G00 до G99. Наприклад, лінійна інтерполяція, функція G01, використовується для включення режиму руху робочого інструменту паралельно осі. Для старту режиму функціонування в дюймової системі служить функція G20, а для переходу в міліметри застосовують код G21.

За допомогою команд, перетворених в G-код, відбувається:

– лінійне і круговий рух робочих елементів верстата з певною швидкістю (регулювання напрямку обертання, корекція діаметра або радіуса руху інструменту);

– виконання типових послідовностей (стандартні отвори і різьблення);

– налаштування параметрів: систем координат верстата, площин роботи, числа обертів робочого інструмента, швидкості подачі.

Система G-кодів для ЧПУ являє собою високорівневу мову. Програма містить список команд, розташованих в певній послідовності, і може при необхідності редагуватися в будь-якому текстовому редакторі. Алгоритм роботи ЧПУ задається набором команд, розташованих в установленому порядку. Програми, створені на основі G -код для верстатів з ЧПУ, відрізняються жорсткою структурою. Окремі команди групуються в кадри; в деяких з них команда може бути одна, в інших – кілька.

Елементарні команди в кадрах виконуються в один і той же проміжок часу, але зазвичай розташовуються в такій послідовності:

– підготовчі;

– установка координат пересування;

– завдання обробного режиму;

– технологічні.

Підготовчі програмні коди мають різні функції і управляють різними технологічними операціями. Так, деякі з них встановлюють лінійну або кругову швидкість переміщення робочих органів обладнання, а інші задають режими обробки деталі. З їх допомогою вказуються значення параметрів, і здійснюється управління координатними системами: відносної і абсолютної.

Приклад простої керуючої програми в G-кодах показаний на рисунку 1.3.

Кадры УП	Описание кадра
%	Символ начала программы
O0001 (PAZ)	Номер программы (0001) и ее название (PAZ)
N10 G21 G40 G49 G54 G80 G90	Строка безопасности
N20 M06 T01 (FREZA D1)	Вызов инструмента № 1
N30 G43 H01	Компенсация длины инструмента № 1
N40 M03 S1000	Включение оборотов шпинделя (1000 об/мин)
N50 G00 X3 Y8	Ускоренное перемещение в опорную точку T1
N60 G00 Z0.5	Ускоренное перемещение инструмента В Z0.5
N70 G01 Z-1 F25	Перемещение на глубину 1 мм на подаче 25 мм/мин
N80 G01 X3 Y3	Перемещение инструмента в точку T2 (25 мм/мин)
N90 G01 X7 Y3	Перемещение инструмента в точку T3 (25 мм/мин)
N100 G01 X7 Y8	Перемещение инструмента в точку T4 (25 мм/мин)
N110 G01 Z5	Подъем инструмента вверх в Z5 (25 мм/мин)
N120 M05	Выключение оборотов шпинделя
N130 M30	Завершение программы
%	Символ конца программы

Рисунок 1.3 – Програма обробки заготовки в G-кодах

Основу комп'ютеризованої системи управління технологічним обладнанням складає ядро системи ЧПУ. Сьогодні це, як правило, персональний комп'ютер промислового виконання, функціонуючий на базі ОСРЧ [3].

Формат файлу визначається конкретним типом обладнання і постпроцесора. Перенесення керуючої програми на стійку ЧПУ можливе різними способами:

– безпосереднім введенням управляючої програми на стійці;

– через послідовний порт;

– через flash-накопичувач;

– через Ethernet-контролер.

Таким чином, з огляду на тісну інтеграцію CAD / CAM-систем і стійок ЧПУ в умовах сучасного машинобудівного виробництва, зловмисники мають широкі можливості для крадіжки даних на будь-якому етапі підготовки виробництва і безпосередньо в ході виробництва. АРМ технологічного персоналу, як правило, знаходяться в контрольованій зоні – в охоронюваному будинку, під відеоспостереженням. Самі АРМ мають програмні засоби захисту – система ідентифікації й автентифікації, журнали обліку і контролю доступу та т.д.

Усередині рівнів АСУТП можна виділити наступні основні інформаційні потоки:

– інформація від датчиків вимірювання передається до контролера;

– від контролера до пристрою магістральної передачі інформації (комутатор, радіомодуль);

– від пристрою передачі даних до сервера;

– від сервера до SCADA-серверу в локальній мережі;

– від SCADA-серверу інформація передається диспетчеру АСУТП.

SCADA - це програмний пакет, призначення для розробки чи забезпечення роботи у режимі реального часу систем збору, обробки, зображення та архівування інформації про об'єкт моніторингу чи управління.

Зараз існує багато варіантів SCADA-систем різного роду та призначення.

1.3 Аналіз особливостей АСУТП з точки зору ІБ

Забезпечення інформаційної безпеки на виробництві має свої нюанси, пов'язані зі специфікою автоматизованих систем управління підприємством і з особливістю протікання виробничих процесів. Інформаційна безпека має на увазі стан захищеності даних від трьох основних загроз: порушення конфіденційності, зміна інформації, і її доступності. Але стосовно виробничого підприємства значущість цих загроз змінюються, оскільки в цьому випадку інформація відіграє роль інструменту управління. Визначальною відмінністю від традиційних інформаційних систем,

характерне управління процесами і фізичними об'єктами, тоді як звичайні адміністративні системи управляють інформацією. Увага концентрується на фізичних процесах, а не на інформаційних об'єктах. Інформаційні потоки повинні забезпечити безперервність і безаварійність процесу виробництва. Зазіхання на автоматизовані системи управління підприємством здійснюються найбільш часто саме з метою призупинити виробництво або втрутитися в його роботу і викликати аварію. Це обумовлює особливий підхід до організації системи ІБ на виробництві.

З огляду на особливості АСУТП з точки зору ІБ виділяють наступні основні особливості захисту АСУТП:

– при створенні систем захисту АСУТП на перший план виходить завдання забезпечення цілісності та доступності. Питання забезпечення конфіденційності, як правило, неактуальне з огляду на те, що сама по собі інформація, що циркулює в АСУТП, не представляє інтересу для потенційного зловмисника;

– для захисту АСУТП необхідно застосовувати спеціалізовані засоби, які не впливали б на сам технологічний процес і в той же час враховували його специфіку з точки зору виявлення дій зловмисника;

– для захисту АСУТП повинні залучатися фахівці, які не тільки розбиралися б у питаннях ІБ, а й розуміли специфіку захищуваних технологічних процесів.

На підставі аналізу літературних джерел і матеріалів розміщених в інтернеті виділені наступні основні особливості інформаційної безпеки виробництва з АСУТП:

– на промисловому виробництві знаходиться велика кількість споживачів інформації різних типів, як користувачів, так і пристроїв, при цьому вона передається по безлічі каналів і у великій кількості форматів. Крім комп'ютерів та елементів інфраструктури об'єктами управління стають виробничі одиниці. Ними можуть бути і верстати з ЧПУ, системи життєзабезпечення і т.д.;

– на відміну від традиційних ІС, АСУТП виявляється системою реального часу. Час реакції і спрацьовування на виклики завжди критично, неприйнятні втрати даних

або затримки їх передачі. Вкрай важливо своєчасне спрацьовування в аварійних ситуаціях;

– система завжди розподілена, її одиниці можуть бути важкодоступні, інформація передається по безлічі каналів зв'язку;

– для АСУ неприпустимі перерви в роботі, перезавантаження як метод вирішення проблем не застосовується, технічні роботи плануються заздалегідь за умови запуску дублюючих рішень;

– безпека людей і обладнання, безвідмовність мають пріоритет над конфіденційністю і цілісністю даних. Інформаційна безпека концентрується на безперервності процесу обміну інформацією і збереженні її цілісності;

– для АСУ частіше використовуються спеціалізовані, а не загальнодоступні операційні системи. Вони позбавлені більшості відомих хакерам вразливостей, але не містять вбудованих модулів безпеки;

– велику небезпеку становить і те, що на комп'ютерах, які керують обладнанням, застосовуються старі версії операційних систем і сервісів. У деяких випадках оновити систему було не можна, оскільки виробниче ПЗ вимагало чітко визначеної версії операційної системи;

– системні ресурси АСУ обмежені, вони призначені суворо для управління промисловими об'єктами і не мають ресурсів для розгортання обчислювальних потужностей або модулів безпеки;

– в АСУТП виникає безліч вразливостей, ймовірність використання яких при різних інцидентах інформаційної безпеки прямо пропорційна важливості і значущості об'єкта. Про наслідки таких інцидентів важко судити, оскільки дуже багато що залежить від конкретних цілей зловмисника, а вони варіюються від крадіжки конфіденційної інформації до порушення технологічних процесів, здатного послужити причиною зупинки всього промислового комплексу в цілому;

– комунікації в рамках АСУ проходять по спеціалізованим протоколам не реалізованих в офісних ІС;

– для забезпечення безпеки АСУТП вкрай рідко використовуються криптографічні рішення, оскільки вони, як правило, породжують надмірність обчислень і можуть уповільнити або зовсім зупинити відправку та отримання керуючого сигналу;

– експлуатація та підтримка АСУ здійснюються тільки розробниками;

– при розробці більшості автоматизованих систем управління малося на увазі, що вони не будуть змінюватися в майбутньому. Системи, сконфігуровані 20 років тому, до цих пір функціонують в первозданному вигляді, а програмне забезпечення, що використовується в АСУТП, часто не оновлювалося роками. Багато виробників навіть рекомендують не оновлювати ПЗ, якщо система працює справно, оскільки будь-яка зміна може призвести до збоїв в роботі системи управління;

– реалізація будь-яких стратегій захисту може перестати працювати без залучення постачальника програмного забезпечення для системи. Вартість модернізації з метою підвищення захисту може виявитися дуже високою, тільки ліцензування і сертифікація змін можуть зайняти до 10% від загальної вартості проекту впровадження.

Особливості функціонування промислових інформаційних мереж породжують і особливості спрямованих на них загроз. Такі відмінності породжують різні підходи в питаннях забезпечення інформаційної безпеки.

Нижче описані основні підсистеми забезпечення інформаційної безпеки АСУТП:

– підсистема мережевої безпеки. Іноді її ділять на дві системи – міжмережевого екранування і виявлення вторгнень. У таких випадках мається на увазі, що в АСУТП буде впроваджено додаткове обладнання - міжмережеві екрани і система виявлення вторгнень;

– підсистема двухфакторної (багатофакторної) автентифікації;

– підсистема забезпечення цілісності;

– підсистема швидкого відновлення конфігурацій і даних;

– підсистема запобігання витоків конфіденційної інформації;

– підсистема управління патчами;

– підсистема управління мобільними пристроями;

– підсистема управління неструктурованими даними;

– підсистема аналізу захищеності;

– підсистема криптографічного захисту.

Перші три ІБ-підсистеми є ключовими в АСУТП, оскільки дозволяють найбільш ефективно зберігати доступність автоматизованої системи управління. Найчастіше побудова комплексної системи безпеки починається з забезпечення цілісності - відповідні завдання регламентуються додатковими стандартами і проводами, зокрема NIST SP 800-12, 800-40 та 800-94.

1.4 Стандарти в області захисту інформації АСУТП

Діяльність у сфері технічного захисту інформації регламентується та регулюється Конституцією України, а саме переліком Законів та других нормативно-правових АКТІВ.

Згідно ЗУ «Про інформацію» захист інформації це сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї. Також згідно цього закону несанкціоновані дії щодо інформації в системі це дії, що провадяться з порушенням порядку доступу до цієї інформації, установленого відповідно до законодавства.

Таким чином інформація, що циркулює в АСУТП також потрапляє під цей закон.

Стандарт ISA 99 / IEC 62443

Описує технічні вимоги до кібербезпеки складових АСУТП. Стандарт специфікує вимоги по 4-м рівням:

1) Загальні положення: визначають відповідні концепти, моделі й термінологію, а також цілі та метрики з безпеки;

2) Політики і процедури: встановлюються конкретні правила в рамках програми безпеки. Тут з'являються правила, що відповідають рівню АСУТП;

3) Системи і технології: тут розглядаються конкретні технології, інструменти і практики, які стосуються АСУТП;

4) Компоненти: цей рівень специфікує вимоги з безпеки на рівні окремо взятого пристрою - це особливо важливо для розробки нових механізмів управління.

Стандарт NIST

Стандарт NIST не висуває жодних формальних вимог, а лише пропонує набір методик і рекомендацій. Він містить:

– предметні рекомендації, що дають уявлення про те, з чого слід почати і як найбільш ефективно побудувати систему захисту в цілому;

– спрощені моделі зловмисника і загроз АСУТП;

– великий розділ за типовими загрозами і вразливостями АСУТП;

– рекомендації відносно створення і реалізації програми забезпечення безпеки АСУТП;

– докладний опис архітектури АСУТП і загальний опис підсистеми безпеки;

– всеосяжний розділ, присвячений всім класичним підсистемам інформаційної безпеки (контроль над доступом, ідентифікація і аутентифікація, антивірусний захист, мережі, аудит, криптографія та ін.

Огляд стандарту NIST SP 800-82 наведено в додатку Б.

1.5 Загрози ІБ в АСУТП

Основні проблеми інформаційної безпеки АСУТП, що виділяються експертами [4] виникають з наступних причин:

– слабкий захист від загрози несанкціонованого доступу (паролі);

– незадекларовані можливості SCADA;

– відсутність контролю управляючих впливів (сукупність параметрів);

– використання бездротових комунікацій;

– відсутність чітких меж між різними сегментами мережі;

– несвоєчасне або некоректне оновлення програмного забезпечення;

– дистанційні методи управління;

– Web - технологій використовуваних на верхньому рівні АСУТП.

Одна з найбільших компаній в світі, що займається розробкою виробничих об'єктів, Siemens, запропонувала вичерпну класифікацію загроз інформаційній безпеці на виробництві [5]:

– несанкціоноване використання віддаленого доступу до процесу управління виробничим об'єктом. Канали зв'язку АСУ зазвичай не мають достатнього захисту;

– хакерські атаки, що направляються через корпоративні (офісні) інформаційні мережі. Між каналами управління АСУ та офісною інформаційною системою існують сполуки, які можуть бути використані зловмисниками;

– атаки на стандартні компоненти інфраструктури мереж управління АСУ. Операційні системи, сервери додатків, бази даних мають уразливості, які не завжди своєчасно усуваються розробниками і добре відомі хакерам. Якщо в архітектурі АСУ є такі компоненти, вони можуть бути використані для атаки;

– DDoS-атаки. Масовані розподілені атаки відмови в обслуговуванні часто використовуються для руйнування мережевих з'єднань і для порушення нормальної роботи АСУ;

– помилки персоналу, навмисний саботаж і пошкодження компонентів системи управління. Ризики в цій ситуації, при наявності у зловмисника доступу до АСУ, серйозні і непередбачувані;

– впровадження вірусних і інших шкідливих програм через з'ємні носії особами, допущеними до обслуговування обладнання, часто це співробітники сервісних організацій. Прикладом реалізації ризику стало масове зараження АСУ, в тому числі об'єктів ядерної інфраструктури Ірану, вірусом Stuxnet;

– читання, запис і зміна повідомлень в мережах АСУ. Компоненти АСУ підтримують мережевий обмін даними з використанням незахищених тестових повідомлень. Це створює можливість без труднощів зчитувати тестові повідомлення і вносити в них несанкціоновані зміни;

– несанкціонований доступ до ресурсів. Якщо в АСУ передбачена слабка система ідентифікації і автентифікації, треті особи можуть отримати доступ до ресурсів;

– атака на мережеві компоненти з поширенням на об'єкти промислової інфраструктури;

– технічні несправності, аварії, природні катаклізми.

Одним з поширених підходів до побудови ІБ-систем АСУТП є ешелонований захист, який включає в себе такі рівні:

– фізична безпека (обмеження фізичного доступу до панелей управління, диспетчерських та інших приміщень, пристроїв, кабелів);

– мережева безпека. В нього входять мережева інфраструктура (наприклад, міжмережеві екрани з вбудованими сенсорами систем запобігання вторгнення) і засоби захисту, інтегровані в мережеве обладнання (комутатори і маршрутизатори);

– безпека робочих станцій і серверів (управління оновленнями ПЗ, застосування антивірусного ПЗ, видалення невикористовуваних додатків, протоколів і сервісів);

– безпека додатків (автентифікація, авторизація та аудит при доступі до додатків);

– безпека пристроїв (контроль над змінами і обмеження доступу).

Особливу увагу приділяють мережному рівню. Багато компонентів АСУТП підключені до мережевої інфраструктури IP / Ethernet, але для них не завжди можлива установка засобів забезпечення ІБ, таких як антивіруси або системи запобігання вторгнень на рівні хоста.

1.6 Загрози ІБ в підсистемі ЧПУ

Робота обладнання з числовим програмним управлінням (ЧПУ) дозволяє значно збільшити продуктивність, виключити ймовірність впливу людського фактора і поліпшити якість продукції. Наявність програмованого обладнання в кілька разів збільшує ефективність виробництва і значно скорочує витрати. При цьому ключову роль відіграє інформація, яка визначає технологічний процес. Застосовувані в системах ЧПУ методи захисту більшою мірою відносяться до забезпечення технологічної безпеки. З боку користувача ці методи захисту можна розділити умовно на видимі і невидимі [6]. До видимих відносяться виділення зони відповідальності і забезпечення рівня доступу до функціоналу системи по ключу (програмному або апаратному). Це запуск певних режимів роботи верстата з системою ЧПУ, редагування механічних властивостей, використання інструментів налаштування і діагностики системи і т.д. Машинні параметри розділені на рівні доступу (оператор, наладчик, системний інженер, інженер служби технічної підтримки та ін.). Залежно від рівня доступу конкретний машинний параметр може бути: прихований для користувача, доступний тільки для читання або доступний для читання і запису. Верстатобудівникам і кінцевим користувачам надається можливість шифрування підпрограм і верстатних циклів, що, в тому числі запобігає відображенню програмного коду і технологічних параметрів на екран під час його виконання. Нові версії вбудованого ПЗ поставляються тільки після надання доказів, що наявні в системі ЧПУ помилки заважають роботі технологічного обладнання.

До невидимих для користувача методам захисту відносяться: закриття певних портів, безпечна робота з флеш-накопичувачами і локальною мережею через спеціалізовані утиліти копіювання даних, резервування даних в разі зникнення живлення і т. д.

Технологічне обладнання в виробничих приміщеннях, як правило, не оснащено комплексними системами забезпечення інформаційної безпеки. Фізичний доступ до

обладнання мають всі співробітники даного підприємства (цеху). Також на підприємствах часто не контролюється процес перенесення даних з АРМ технологічного персоналу на стійки ЧПУ і носії, з допомогою яких здійснюється ця процедура. Обслуговуючі компанії, які здійснюють пуско-наладку, технічне обслуговування і ремонт обладнання, також мають практично необмежений доступ до обладнання під час проведення робіт, в тому числі і за допомогою віддаленого доступу до нього.

Системи безпеки ЧПУ мають наступні особливості:

– складність організації захищеного з'єднання для безпечної взаємодії під час виконання завантаження керуючих програм, тому що, в більшості випадків, використовуються протоколи, які не підтримують захищені з'єднання;

– реалізація класичних сервісів передачі файлів (FTP, SMB і інші), які використовуються для завантаження УП, в СЧПУ часто несе в собі відомі уразливості проектів з відкритим вихідним кодом, на базі яких вони побудовані, навіть якщо у вихідному проекті дана уразливість вже усунена;

– багато СЧПУ від зарубіжних виробників мають штатні інструменти віддаленого управління і моніторингу, які дозволяють зловмисникові: звернутися до вмісту пам'яті і досліджувати її на предмет залишкової інформації, яка може містити критичні дані (головним чином, УП) здійснювати НСД з можливістю переконфігурування обладнання та модифікації УП, використовувати різні НДМ, залишені виробником, у шкідливих цілях;

– мережевий стек ОС, що використовуються в СЧПУ, часто має схильність до традиційних мережевих атак (DoS, DNS spoofing, розміщення несанкціонованих DHCP-серверів, мережевих шлюзів) у периметрі цехової ЛВС;

– характеристики мережевих параметрів СЧПУ (MAC-адреси, доступних мережевих сервісів, відбитки стека TCP / IP) і його штатних конфігураційних параметрів дозволяють успішно проводити мережеву розвідку С ЧПУ віддаленим зловмисником.

У підсистемах ЧПУ можна виділити три види інформації, які впливають на роботу обладнання:

1) Дані про налаштування обладнання та дані про діагностику його роботи;

2) Інформація про геометричні параметри оброблюваних заготовок і виготовлені з них деталі або вузли;

3) Інформація про режими обробки.

Більш детальна класифікація інформації в ЧПУ приведена на рисунку 1.4

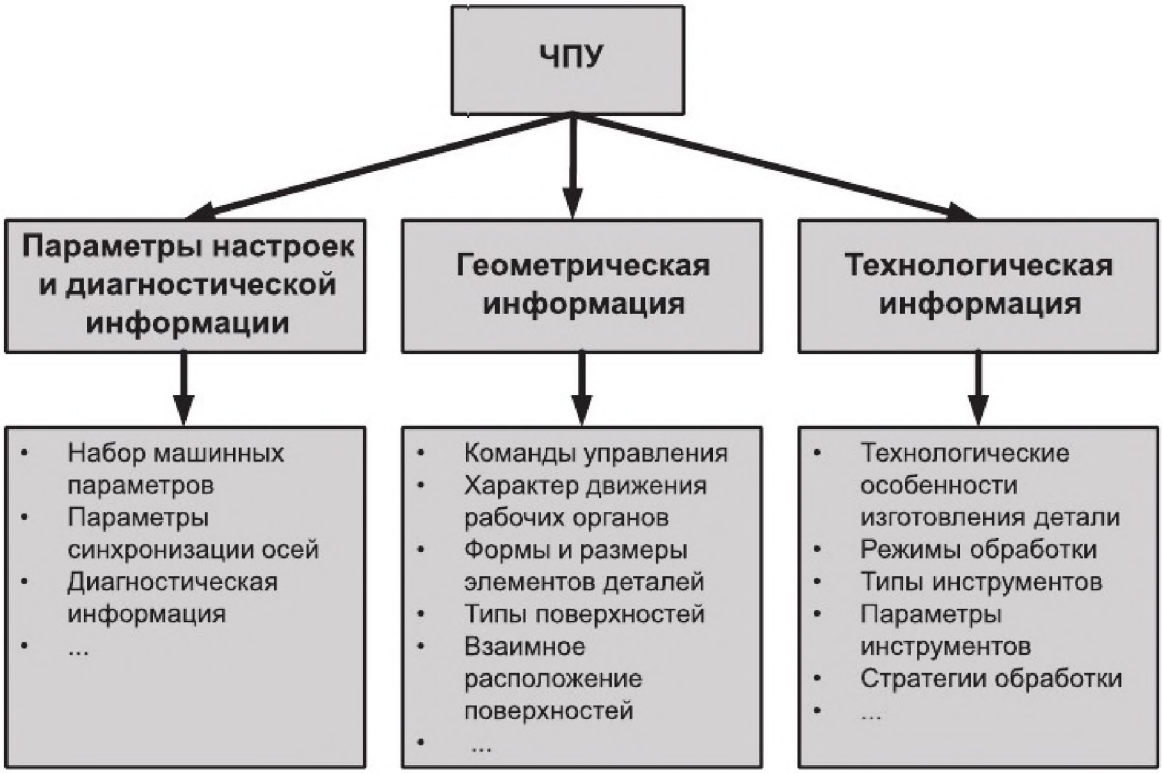


Рисунок 1.4 – Інформація в системі ЧПУ

Виділяють наступні загрози безпеки підсистем з ЧПУ [7]:

– порушення конфіденційності - розкрадання керуючих програм, збір відомостей про номенклатуру та обсяги виробництва виробів і т.д.;

– порушення цілісності - як керуючих програм з метою зміни виконуваних ними функцій, так і параметрів налаштування обладнання, масовий брак, приведення в непридатність дорогих заготовок, обробного інструменту, виконавчих механізмів верстатів, і т.д.;

– порушення доступності неможливості запуску виконання керуючої програми, постійні відмови СЧПУ або його окремих елементів, простій дорогого обладнання;

– контроль місця розташування обладнання з ЧПУ (для обладнання від іноземних виробників).

1.7 Постановка завдання

Мета дипломного проекту – обґрунтування методів забезпечення інформаційної безпеки і оцінки інформаційної захищеності підсистеми ЧПУ малого виробничого підприємства.

На період виконання дипломного проекту були сформовані та поставлені наступні задачі:

– на підставі доступних літературних видань і матеріалів, розміщених в інтернеті провести аналіз технологічної та інформаційної структури АСУТП і її особливостей з точки зору інформаційної безпеки. Метою такого аналізу є надання загального уявлення про наявність потенційних можливостей щодо забезпечення захисту інформації, виявлення компонентів АСУТП, які вимагають підвищених вимог до захисту інформації і впровадження додаткових заходів захисту;

– проаналізувати існуючі стандарти і нормативні документи в області захисту інформації стосовно АСУТП в цілому і до верстатів з ЧПУ зокрема;

– провести обстеження виробничої дільниці ТОВ "Техноком" і виконати аналіз та оцінку інформаційних ризиків на ній;

– розробити заходи щодо зменшення виявлених загроз інформаційної безпеки на цій технологічній ділянці.

1.8 Висновок

У першому розділі було розглянуто проблему захисту інформації в АСУТП, які використовують ЧПУ. Проведено аналіз їх особливостей з точки зору ІБ і описані можливі загрози в АСУТП. Проведено аналіз нормативно-правових документів у цій сфері. Поставлені задачі дипломної роботи.

Подано на аналіз перелік нормативно-правових актів та стандартів в області захисту інформації АСУТП, що є правовою основою забезпечення безпеки інформації. Проведено аналіз структури АСУТП з точку зору інформаційної безпеки. Приведені задачі дипломної роботи, а саме: проаналізувати існуючі стандарти і нормативні документи в сфері захисту інформації стосовно АСУТП. Проаналізувати існуючі загрози ІБ в АСУТП та в підсистемі ЧПУ та розробити заходи безпеки та рекомендації щодо підвищення рівню захисту інформації.

2 СПЕЦІАЛЬНА ЧАСТИНА

2.1 Обстеження виробничої дільниці ЧПУ

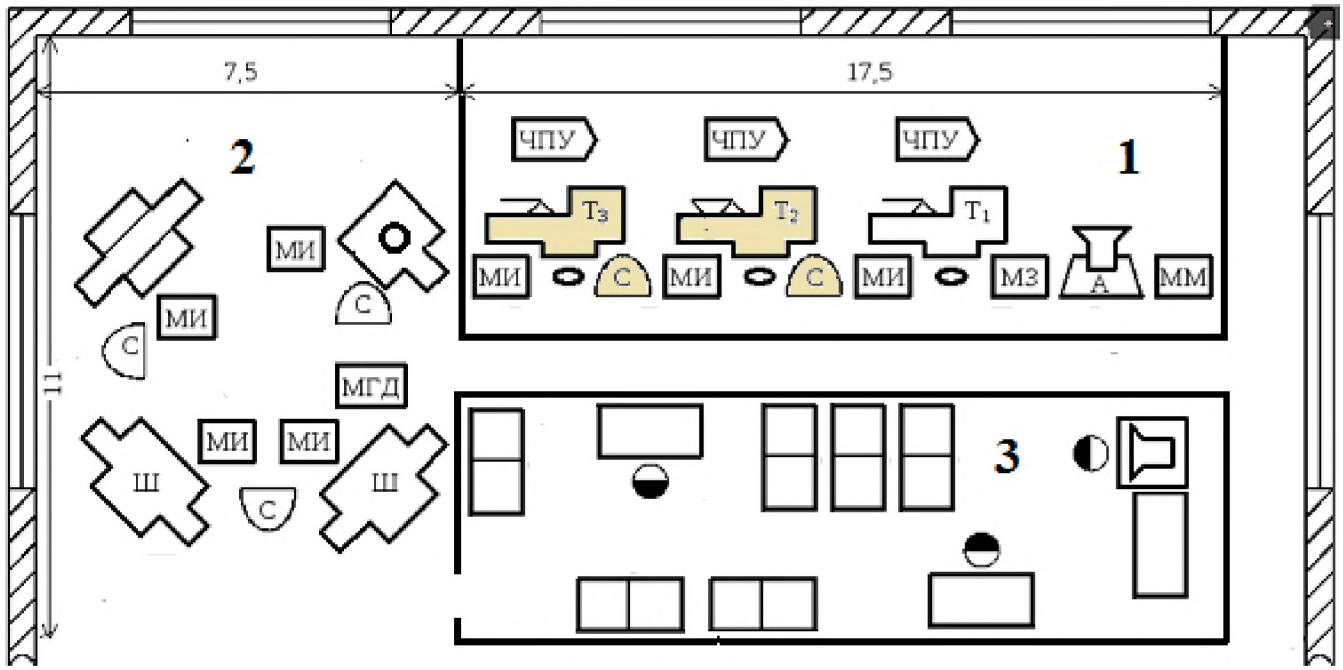
Під час проведення обстеження розглянуто фізичне середовище виробничої дільниці з ЧПУ, середовище користувачів системи проектування та експлуатації обладнання з ЧПУ. Приводиться опис кожного середовища функціонування.

2.1.1 Опис об'єкта інформаційного захисту

Об'єктом інформаційної діяльності є виробнича дільниця, яка представляє собою виробничий підрозділ ЧПУ ТОВ «Техноком», що об'єднує ряд робочих місць і де здійснюється процес з виготовлення рукавів високого тиску.

Рукав високого тиску (РВТ) – це гнучка частина трубопроводу, яка використовується для підведення до них робочих рідин. На виробничій ділянці ТОВ «Техноком» виробляє виготовлення металевих елементів РВД (фітинги, перехідники, з'єднання) і їх опресовування. До якості цих елементів пред'являються досить жорсткі вимоги, оскільки такі вироби повинні витримувати високі показники тиску. На цій ділянці використовується різнотипове обладнання, яке розташовується по ходу технологічного процесу. Робочі місця спеціалізуються на виготовленні певного виду деталей і збірці готової продукції, і розбиті на три зони – слюсарну, токарну і інструментальну (рисунок 2.1). У токарній зоні встановлені 3 верстати з ЧПУ, один з яких знаходиться в не робочому стані. В інструментальній зоні розташовується персональний комп'ютер, на якому виконується виробничий і бухгалтерський облік, а також підготовка керуючих програм для верстатів ЧПУ. На ділянці зайняті робітники різних спеціальностей і їх відповідальний виконавець- майстер ділянки. Крім цього в штаті ділянки за сумісництвом числиться програміст ЧПУ, який викликається в разі розробки нової керуючої програми або обслуговування комп'ютера. Виробнича ділянка розташована в не охоронюваному приміщенні колишнього інструментального цеху ВАТ «Дніпропетровський завод. Червоний профінтерн» розташованого за

адресою вул. Червонозаводська, 1. Територія заводу не охороняється. На прохідній заводу проводиться тільки контроль виїжджаючого автотранспорту.



Умовні позначення:

1 – Токарна зона, 2 – Слюсарна зона, 3 – Інструментальна зона

Рисунок 2.1 – Планування виробничої дільниці

Відповідно до НД ТЗІ 1.6-005-2013 «Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці», для даного об’єкта інформаційного захисту встановлюється категорія IV (четверта), адже на об'єкті технічними засобами обробляється інформація с обмеженим доступом, що не становить державної таємниці.

2.1.2 Опис апаратного та програмного забезпечення

ПК: Процесор Intel Celeron Dual Core J1800 (2.41 ГГц) / RAM 4 ГБ / HDD 100 ГБ.

Материнська плата: Asus J1800I-C.

Принтер: Canon i-SENSYS LBP6000.

ОС: Windows XP(без ліцензії)

Програмне забезпечення: Mozilla Firefox (ліцензія), 1С Бугалтерія (без ліцензії), WinRAR (ліцензія), EMCO Compact 5 CNC Simulator (безкоштовний), DOSBOX, текстові редактори та інше.

EMCO Compact 5 CNC Simulator – це симулятор токарного оброблення на верстаті з ЧПУ. Симулятор систем с ЧПУ – програми призначені для перевірки керуючих програм на помилки і візуалізації профілю обробки і переміщення обробного інструменту в реальному часі (рисунок 2.2).

Рисунок 2.2 – Симулятор EMCO Compact 5 CNC Simulator

Розробка управляючих програм проводиться за допомогою текстового редактора з подальшою їх перевіркою за допомогою симулятора і виготовлення контрольних зразків безпосередньо на ЧПУ.

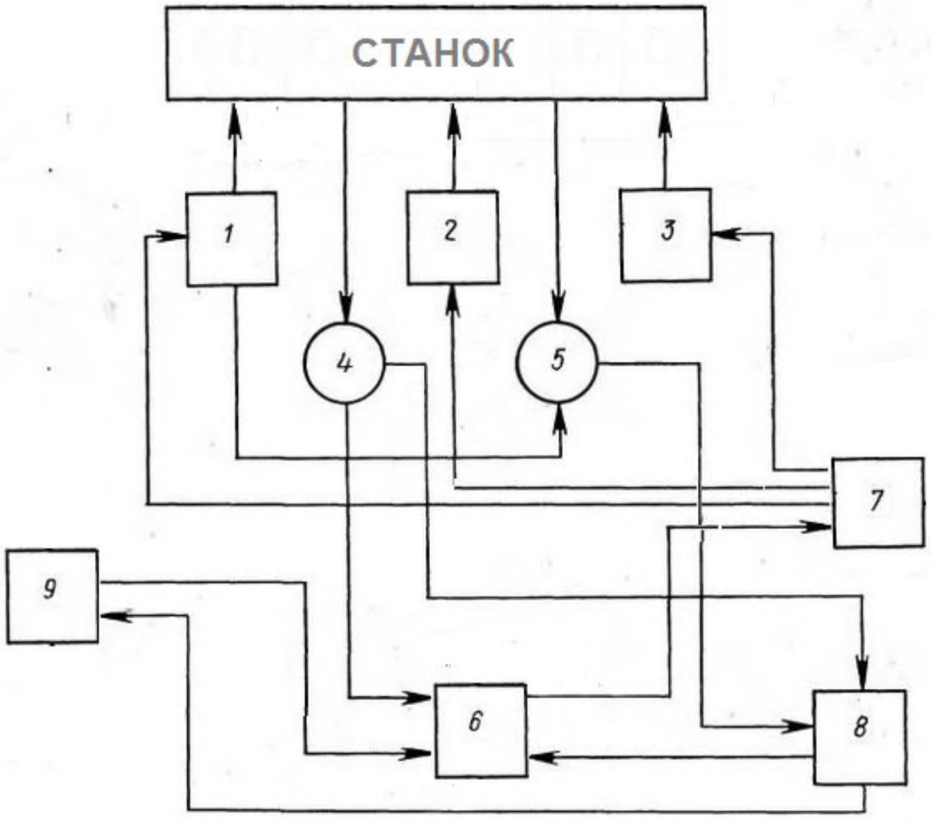
2.1.3 Опис верстатів типу 16А20Ф3

Токарні верстати з ЧПУ серії 16А20Ф3 призначені для токарної обробки в автоматичному режимі зовнішніх і внутрішніх поверхонь деталей, типу тіл обертання із ступінчастим і криволінійним профілем різної складності за заздалегідь складеною керуючої програмою. Область застосування верстата – дрібносерійне та серійне

виробництво. Токарні верстати з ЧПУ серії 16А20Ф3 випускалися з 1985 -1992 роки на заводі «Червоний пролетар», який на сьогоднішній день припинив своє існування. Зовнішній вигляд нового верстата і цього ж верстата, встановленому на виробничій ділянці після майже 20 років експлуатації, капітального ремонту та модернізації, наведені на малюнку 2.3 – зовнішній вигляд верстата з ЧПУ серії 16А20Ф3.

Рисунок 2.3 – Зовнішній вигляд верстата з ЧПУ серії 16А20Ф3

Вузли верстата включають в себе електричну частину (електродвигун і електричні пристрої управління), а також механічну частину для передачі руху робочих органів станків з ЧПУ. Електрообладнання призначається для того, щоб приводити в рух агрегати і механізми, автоматично управляти ними, контролювати їх стан, а також виробляти технічну діагностику і сигналізацію. На рисунку 2.4 показана функціональна схема електроустаткування верстата. Залежно від призначення всі електричні елементи, які входять до складу електроустаткування верстата з ЧПУ, підрозділяються на командні, логічні, захисні, виконавчі, джерела живлення і перетворювач напруг. До складу електроустаткування входять: електропривод головного руху 1; електропривод подачі 2; допоміжні електроприводи для створення обертального і поступального руху механізмів 3; датчики технологічних параметрів 4; датчики зворотних зв'язків електроприводів, що перетворюють параметри електроприводів в їх електричні сигнали 5.



Умовні позначення:

1 – електропривід головного руху, 2 – електроприводи подачі, 3 – допоміжні електроприводи, 4 – датчики технологічних параметрів, 5 – датчики зворотних зв'язків електроприводів, 6 – електроавтоматика верстата, 7 – комутаційна апаратура, 8 – пристрій електричного блокування, діагностики і контролю, 9 – консоль управління верстатом

Рисунок 2.4 – Функціональна схема електроустаткування верстатів з ЧПУ

Консоль управління верстатом містить монітор, клавіатуру, кнопки управління, дисковод для 3.5' дискет і COM-порт для сполучення з зовнішніми пристроями. Її основні функції:

– введення оперативних команд за допомогою клавіш клавіатури;

– введення команд запуску, зупинки і скидання;

– введення даних в умовах команд, за допомогою клавіатури;

– введення даних і програмного забезпечення (програм «part program»), опцій програмного забезпечення і т.д.) за допомогою дискет;

– виведення на екран даних та всіх оперативних умов системи;

– контроль середовища ЧПУ.

Пристрої діагностики і контролю (7) служать для контролю та індикації основних робочих режимів, а також для захисту верстата з ЧПУ в аварійному режимі. Автоматичні контролюючі пристрої вимірюють геометричні розміри оброблюваних деталей і видають команди на продовження або закінчення обробки. Для управління верстатами в різних режимах і контролю станів їх механізмів, служать пульти управління. Числове програмне управління для переміщень інструменту, управління головним приводом і допоміжних команд вводяться в пам'ять системи управління з клавіатури консолі оператора (8), а також з 3.5' дискети зовнішньої пам'яті або COM-порту з зовнішнього пристрою і можуть коригуватися з пульта оператора ЧПУ з візуалізацією на панелі цифрової індикації. До об’єктів інформаційного захисту належать два види інформації:

1) Геометрична інформація, яка задає інформацію обладнання з ЧПУ, що включає команди управління, інформацію, що описує форму, розміри елементів деталі і інструментів, їх взаємне положення в просторі для вирішення завдань по контролю за розміщенню та використанню файлів КП.

2) Технологічна інформація – інформація, що описує технологічні особливості виготовлення деталі і містить відомості про характер руху робочих органів керованого устаткування, їх синхронізацію і режимах руху.

2.2 Аналіз та оцінка інформаційних ризиків

2.2.1 Модель порушника

Модель порушника представляє собою опис можливих дій порушника, який складається на основі аналізу типу зловмисника, рівня його повноважень, знань,

теоретичних та практичних можливостей. Порушників прийнято поділяти на зовнішніх і внутрішніх. До внутрішніх належать співробітники, користувачі інформаційної системи, які можуть наносити шкоду інформаційним ресурсам як ненавмисно/навмисно; технічний персонал, який обслуговує будівлі і приміщення; персонал, який обслуговує технічні засоби. Зовнішні порушники це сторонні особи, які знаходяться поза контрольованою зоною організації або не авторизовані для використання даної комп'ютерної системи. Змістовна модель порушника відображає причини й мотивацію дій порушників, переслідувані ними цілі і загальний характер дій у процесі підготовки і здійснення порушення інформаційної безпеки. До побудови моделі порушника приймаємо, що реалізація загрози може бути на будь-якому етапі циклу використання інформації обмеженого доступу. У нашому випадку це чотири етапи - розробка ПЗ, перенесення його в ЧПУ, інсталяція ПЗ і його експлуатація. Також в нашому випадку порушник – це один або декілька фізичних осіб, що навмисно здійснюють в системі неправомірні дії, які направлені на модифікацію або компрометацію ПЗ ЧПУ. Змістовна модель порушника у вигляді специфікацій відображена в таблицях 2.1...2.6. Модель порушника – таблиця 2.7.

Таблиця 2.1 - Категорії порушників

Позначення	Визначення категорії	Потенційний рівень загрози
П1	Особи, яким не передбачено доступ до технічних та програмних засобів, але які мають можливість незалежної розробки ПЗ для ЧПУ	5
П2	Особи, яким передбачено доступ до ІзОД, але які не мають можливість розробки ПЗ для ЧПУ	3
П3	Особи, які забезпечують працездатність технічних засобів ЧПУ	5
П4	Авторизовані користувачі ЧПУ	3
П5	Технічний персонал, який обслуговує приміщення (електрики, прибиральники тощо), в яких розташовані ЧПУ	2

У колонці «Рівень загроз» зазначених таблиць наведено рейтингову оцінку загроз порушника (можливих збитків). Рівень загрози характеризується наступними категоріями:

1 – незначний;

2 – низький;

3 – середній;

4 – високий;

5 – неприпустимо високий.

Таблиця 2.2 – Специфікація моделі порушника за місцем дії

Позначення	Характеристика місця дії порушника	Рівень загроз
Д1	Усередині приміщень, але без доступу до програмних та технічних засобів	5
Д2	За межею приміщень, але без доступу до технічних засобів	2
Д3	З робочих місць користувачів	3
Д4	З доступом у зону зберігання баз даних, архівів	2

Таблиця 2.3 – Специфікація моделі порушника за мотивами здійснення порушень

Позна-чення	Мотив порушення	Рівень загроз
М1	Корисливий інтерес за рахунок підвищення продуктивності	5
М2	Корисливий інтерес за рахунок виготовлення неврахованої продукції	5
М3	Самоствердження за рахунок компрометації ПО	4
М4	Самоствердження за рахунок компрометації обладнання ЧПУ	4
М5	Безвідповідальність/необачність	3

Таблиця 2.4 – Специфікація моделі порушника за рівнем кваліфікації та обізнаності

Позначення	Основні кваліфікаційні ознаки порушника	Рівень загроз
К1	Володіє низьким рівнем знань, але вміє працювати за технічними засобами	2
К2	Має навички щодо користування ПК на рівні користувача	4
К3	Володіє знаннями щодо: функціонування засобів та механізмів обробки інформації та, що використовуються на ІТС та їх недоліків	5

Таблиця 2.5 – Специфікація моделі порушника за часом використання ПЗ

Позначення	Характеристика можливостей порушника	Рівень загроз
Ч1	Під час розробки	3
Ч2	Під час переносу в ЧПУ	5
Ч3	Під час налаштування та інсталяції	4
Ч4	Під час експлуатації	1

Таблиця 2.6 – Специфікація моделі порушника за показником можливостей використання засобів та методів подолання системи захисту

Позначення	Характеристика можливостей порушника	Рівень загроз
З1	Використовує пасивні технічні засоби перехвату інформації без її модифікації	4
З2	Використовує технічні засоби активного впливу з метою модифікації інформації та компонентів, дезорганізації систем обробки інформації	5
З3	Має фізичний доступ до компонентів ІТС, але не є авторизованим користувачем ІТС	4

Таблиця 2.7 – Модель порушника

Позначення	Визначення категорії	Характер дій порушника					Рівень загроз
		Мотив	Кваліфікація	Можливості	Час	Місце	
П1	Особи, яким не передбачено доступ до технічних та програмних засобів, але які мають можливість незалежної розробки ПЗ для ЧПУ	М4 М5	К2, К3	З2, З1	Ч1	Д1	2
П2	Особи, яким передбачено доступ до ІзОД, але які не мають можливість розробки ПЗ для ЧПУ	М1, М2 М3	К3	З1, З2, З3	Ч2 Ч3	Д2	4
П3	Особи, які забезпечують працездатність технічних засобів ЧПУ	М1, М2	К1, К2	З2, З3	Ч3	Д1	4
П4	Авторизовані користувачі ЧПУ	М3, М5	К2, К3	З1	Ч3	Д1	5
П5	Технічний персонал, який обслуговує приміщення (електрики, прибиральники тощо), в яких розташовані ЧПУ	М1	К3	З3	Ч4	Д1	1

2.2 Модель загроз

Відповідно до Закону України "Про основи національної безпеки України", до джерел загроз інформаційній безпеки зокрема належить розкриття інформаційних ресурсів, порушення їх цілісності, спричинення збоїв у роботі комп'ютерного обладнання та мережевого устаткування. За походженням джерела загроз бувають природного та техногенного характеру та класифікуються за такими аспектами інформаційної спрямованості:

Загрози конфіденційності (К) – інформація з обмеженим доступом стає відомою особі, яка немає повноважень доступу до неї, тобто неправомірний доступ до інформації;

Загрози цілісності (Ц) – інформація піддається модифікації, тобто неправомірна зміна даних;

Загроза доступності (Д) – блокування своєчасному доступу до інформації, тобто унеможливлення або ускладнення доступу до інформації;

Змістовна модель загроз у вигляді шкали оцінки відображена в таблицях 2.8 та 2.9.

Таблиця 2.8 – Шкала оцінки можливості реалізації загроз

Коефіцієнт можливості реалізації загрози	Характеристика
1	Практично неможливо
2	Реалізація загрози малоймовірна
3	Реалізація загрози можлива, але недоцільна
4	Реалізація загрози можлива та доцільна
5	Висока ймовірність реалізації загрози

Таблиця 2.9 – Шкала оцінки критичності наслідків від реалізації загроз

Оцінка критичності наслідків	Характеристика
1	Не критичні
2	Низька критичність
3	Середня критичність
4	Вагома критичність
5	Неприпустимо висока критичність

Після детального вивчення особливостей ОІД, аналізу ризиків підприємства та моделі порушника було складено загальну модель загроз (таблиця 2.10) та на її основі виявлено суттєві та несуттєві для ДПРЧ-11 загрози інформаційній безпеці.

Таблиця 2.10 – Модель загроз

Найменування загрози та її опис	Джерело	Вразливість	Наслідки	По-ру-шує	Коефіціє Можли-вості реалізації	Крити-чність наслі-дків	Оці-нка заг-рози
Несанкціонований доступ до параметрів налаштувань Загроза полягає в несанкціонованому отриманні доступу до обладнання з ЧПУ	Зовнішні Внутрішні	Недотримання режиму доступу у приміщеннях та до обладнання ЧПУ	Необхідність проведення ремонтних робіт ЧПУ представником виробника	К	2	5	7
Порушення підготовчих команд. Загроза полягає в зміні ланцюжка команд або інструкцій, виконуваних безпосередньо з пульта управління ЧПУ	Внутрішні	Не реалізована послуга автентифікації та ідентифікації	Призупинення роботи	Ц	5	2	7

Продовження таблиці 2.10 – Модель загроз

Найменування загрози та її опис	Джерело	Вразливість	Наслідки	По-ру-шує	Коефіцієн Можли-вості реалізації	Крити-чність наслі-дків	Оці-нка заг-рози
Порушення керуючої програми. Загроза полягає в зміні підготовчих,технологічних або керуючих команд пересування інструменту в G-коді безпосередньо з пульта управління ЧПУ	Внутрішні	Не реалізована послуга автентифікації та ідентифікації	Призупинення роботи	Ц,Д	5	2	7
Підміна G-кодів при перенесенні керуючої програми в ЧПУ	Внутрішні		Шкода іміджу підприємства, призупинення роботи	Ц,Д	4	1	5
Втрата зовнішніх носіїв інформації с G-кодами виготовлених деталей	Внутрішні	Відсутні правила роботи з зовнішніми носіями інформації	Призупинення роботи	К,Д	2	5	7

Якщо перелік цих загроз буде реалізований за допомогою вказаних у таблиці 2.10 вразливостей і призведуть до порушення конфіденційності, цілісності або доступності, негативними наслідками будуть зупинення роботи підприємства або її значне уповільнення.

2.3 Заходи безпеки та рекомендації

2.3 Загальна специфікація політики безпеки

Заходи безпеки поділяються на 18 груп [8], кожна з груп включає заходи безпеки, які пов’язані з загальною її темою. Контроль безпеки може включати аспекти нагляду за ручними процесами, діями працівників, автономними механізмами. Нижче наведені всі 18 груп, пов’язаних з безпекою:

1) Контроль доступу. Це процес надання або відхилення конкретних запитів на отримання та використання інформації та пов'язаних з нею послуг з обробки інформації для фізичного доступу до даних в середовищі інформаційної системи.

2) Обізнаність та тренування. Політики та процедури для забезпечення того, щоб всім користувачам інформаційної системи було надано відповідне навчання з питань безпеки щодо їх використання в системі та збереження точних записів про навчання.

3) Аудит та підзвітність. Незалежний огляд та експертиза записів та заходів для оцінки адекватності системного контролю, забезпечення дотримання встановленої політики та оперативних процедур, а також рекомендації щодо необхідних змін у контролі, політиці або процедурах.

4) Оцінка безпеки та авторизація. Визначення гарантії того, що вказані елементи керування виконуються правильно, працюють як задумано, і видають бажаний результат.

5) Планування форс-мажорів. Політики та процедури, призначені для підтримки або відновлення бізнес-операцій, включаючи комп'ютерні операції,

можливо в альтернативному місці, у випадку надзвичайних ситуацій, збоїв системи або аварій.

6) Керування конфігураціями. Політики та процедури для контролю модифікацій апаратного забезпечення, прошивки, програмного забезпечення та документації для забезпечення захисту інформаційної системи від неналежних змін до, під час і після впровадження системи.

7) Ідентифікація та автентифікація. Процес перевірки ідентичності користувача, процесу або пристрою за допомогою використання певних облікових даних (наприклад, паролів) як передумова для надання доступу до ресурсів в IT-системі.

8) Дії при інцидентах. Політики та процедури, які відносяться до тренування відповіді, тестування, керування, слідкування, звітності та підтримки роботи сервісів при інцидентах.

9) Підтримка. Політики та процедури для управління всіма аспектами підтримки інформаційної системи.

10) Захист носіїв даних. Політики та процедури для забезпечення безпечного зберігання даних. Контроль за доступом, маркуванням, зберіганням, транспортуванням, знищенням та переробкою носіїв даних.

11) Фізичний захист та захист довкілля. Політики та процедури, що стосуються фізичного доступу, доступу до передавання та відображення даних разом з контролем за середовищем роботи.

12) Планування. Розробка та підтримка плану забезпечення безпеки інформаційної системи шляхом виконання оцінок, визначення та впровадження засобів безпеки, призначення рівнів безпеки та реагування на інциденти.

13) Безпека персоналу. Політики та процедури категоризації, визначення придатності, транспортування, покарання та звільнення.

14) Оцінка ризиків. Процес виявлення ризиків для операцій, активів або фізичних осіб шляхом визначення ймовірності виникнення, наслідків впливу та

додаткового контролю безпеки, який би пом'якшив цей вплив.

15) Придбання систем та сервісів. Розподіл ресурсів для забезпечення безпеки інформаційних систем протягом всього життєвого циклу системи та розробки політики придбання на основі результатів оцінки ризиків, включаючи вимоги, критерії розробки, процедури тестування та супутню документацію.

16) Захист системи та комунікацій. Механізми захисту засобів передавання даних.

17) Цілісність системи та інформації. Політики та процедури захисту інформаційних систем та їх даних від заміни даних використовуючи перевірку функціональності, цілісності даних, вияву проникнення у систему, виконання шкідливого коду, попередження про небезпеку.

18) Програмне управління. Надає заходи управління безпекою на рівні всієї організації, а не тільки на інформаційно-системному рівні.

2.3.1 Заходи безпеки

На верстаті з ЧПУ існує ряд завдань, які можна вирішувати за допомогою системи управління допоміжних пристроїв електроавтоматики. До цих завдань відносяться: забезпечення безпеки, розмежування прав доступу, дистанційні видачі команд і управління периферійним обладнанням верстата. Для вирішення завдань надання фізичного доступу до технологічного устаткування ЧПУ в роботі [9], запропоновано використання одноплатного комп'ютера. Одноплатний комп'ютер - комп'ютер, зібраний на одній друкованій платі, на якій встановлені мікропроцесор, оперативна пам'ять, системи введення-виведення та інші модулі, необхідні для функціонування комп'ютера. Одноплатні комп'ютери виготовляються в якості систем для розробників або освіти або для використання в ролі промислових або вбудованих комп'ютерів.

У цій дипломній роботі запропонована система, яка розширює можливості окремого одноплатного комп'ютера не тільки в якості системи управління

периферійним обладнанням, а й як підсистема інформаційної безпеки ділянки ЧПУ. Ця система повинна забезпечувати наступні завдання:

– ідентифікацію, автентифікацію та фізичний контроль доступу до ЧПУ;

– механізм захисту при передачі G-коду в ЧПУ;

– цілісність G-коду в ЧПУ;

– моніторинг виконання G-коду.

В якості одноплатного комп'ютера пропонується використання дешевого комп'ютера Raspberry Pi 3 по управлінням ОС Raspberry Pi. На Raspberry Pi 3 встановлений 64-х бітний процесор BCM2837 на архітектурі ARM Cortex-A53 з тактовою частотою 1,2 ГГц і модулем оперативної пам'яті на 1 ГБ. Процесор і пам'ять розміщені безпосередньо на процесорі. Процесор включає в себе також двоядерний графічний співпроцесор, який забезпечує відкрите апаратне прискорення і декодування. Забезпечуються наступні входи\виходи:

– цифровий аудіо / відео вихід: HDMI;

– композитний аудіо / відео вихід;

– USB порти: USB 2.0 × 4;

– WiFi: 802.11n;

– Ethernet: 10/100 Мб RJ45;

– bluetooth: Bluetooth 4.1, Bluetooth Low Energy;

– роз'єм дисплею: Display Serial Interface (DSI);

– роз'єм відеокамери: MIPI Camera Serial Interface (CSI-2);

– карта пам'яті: MicroSD;

– інтерфейс (порти) введення-виведення.

RaspberryPi - комп'ютер, який отримав високу популярність багато в чому, завдяки наявності вбудованого інтерфейсу введення / виводу. Інтерфейс введення / виводу може виконувати 3 функції: подачу електрики певної напруги, заземлення та прийом / відправлення сигналів.

В Raspberry Pi встановлюється Linux – така операційна система, яка в плані

безпеки переганяє всі інші популярні ОС з наступних причин:

– файлова система Linux надійно захищена паролем. Здійснювати будь-які дії зі зміни файлів може тільки користувач з правами superuser або root. Але, на відміну від Windows, зайти в систему від імені адміністратора і працювати під цим записом постійно в Linux не вийде;

– надійна система доступу також забезпечує захист від вірусів поки користувач не включив режим superuser. А оскільки він включається тільки за допомогою терміналу і просунутий користувач Linux точно знає, що він робить то у вірусів мало шансів на проникнення в систему;

– лінуксоподібні ОС мало поширені і тому кількість вірусів під цю систему незрівнянно менше ніж під інші ОС.

На рисунку 2.5 показаний зовнішній вигляд одноплатного комп'ютера RaspberryPi 3.

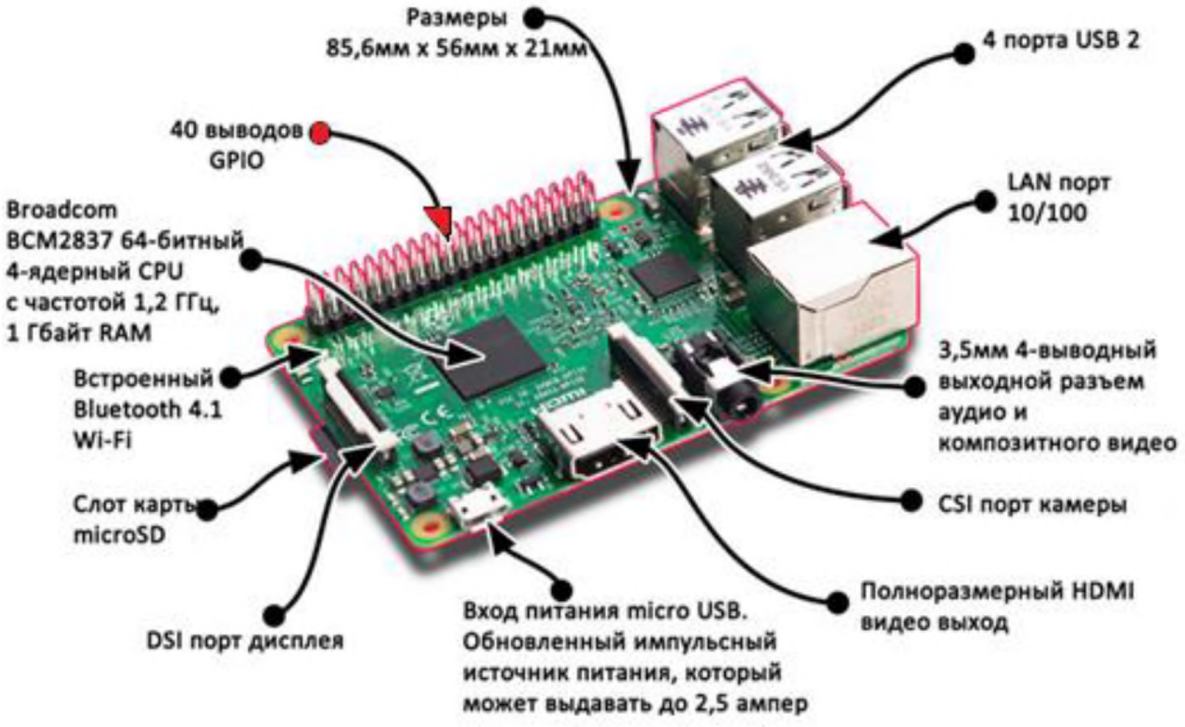


Рисунок 2.5 – Зовнішній вигляд одноплатного комп'ютера RaspberryPi 3

Запропонована в дипломній роботі підсистема інформаційної безпеки ділянки ЧПУ з

використанням одноплатного комп'ютера може забезпечити такі завдання безпеки:

– контроль фізичного доступу до обладнання з ЧПУ;

– контроль цілісності керуючих програм з G-кодом;

– візуальний контроль виконання керуючих програм.

2.3.2 Контроль фізичного доступу до ЧПУ

Фізичний доступ до ЧПУ здійснюється за допомогою індивідуальних RFID ключів.

RFID або Radio Frequency IDentification (радіочастотна ідентифікація) – це метод віддаленого зберігання і отримання інформації шляхом передачі радіосигналів за допомогою пристроїв, званих RFID-мітками.

Принцип роботи RFID-систем досить простий. Дані системи включають в себе два основних компоненти: зчитувач (рідер) і ідентифікатор (мітка, брелок). Ідентифікатор містить електронний чіп (з унікальним кодом) і антену. Коли ідентифікатор потрапляє в поле дії зчитувача, від першого до другого по радіоканалу передається код. Отримавши код ідентифікатора, зчитувач пересилає його в контролер СКУД (системи контролю та управлінням доступом), де автоматично приймається рішення про допуск. Історично СКУД була першим об'єктом застосуванням технології RFID. Більшість подібних систем використовують пасивні мітки і працюють в низькочастотному діапазоні, хоча останнім часом все частіше зустрічаються інтерактивні системи на частотах 13,56 МГц.

Схема використання RFIF ідентифікації в верстатах з ЧПУ (рисунок 2.6) передбачає управління пристроями блокування верстата в залежності від сигналу про допуск одержуваних від RFID рідера через RaspberryPi на контролери управління електроавтоматікой верстата.

Рисунок 2.6 – Схема використання RFIF ідентифікації в верстатах з ЧПУ

Контроль цілісності керуючих програм з G-кодом здійснюється за рахунок наступної організаційної процедури перенесення керуючих програм в ЧПУ: у запропонованій підсистемі безпеки передбачається наявність трьох типів користувачів, що мають різний рівень доступу до елемента підсистеми. У таблиці 2.11 показані рівень доступу для різних користувачів.

Таблиця 2.11 – Рівні доступу користувачів

Користувач	Елемент підсистеми
Відповідальний виконавець	RaspberryPi(root), ПК
Розробник G-кода	ПК, CAM\CAD
Оператор ЧПУ	RaspberryPi(user),ЧПУ

Керуючі програми (файли, які містять G-код) розроблені за допомогою CAD \ CAM на персональному комп'ютері, переносяться в RaspberryPi за допомогою флеш-накопичувача тільки відповідальним виконавцем, що має права суперкористувача. Також формується набір файлів таких керуючих програм, що визначають номенклатуру виготовлених деталей на ділянці. В RaspberryPi встановлюється спеціальна програма-встановник, що дозволяє вибрати з набору керуючих програм потрібну, і скопіювати її в пристрій управління ЧПУ. Доступ до цієї програми, яка встановлюється засобами ОС RaspberryPi, мають тільки відповідальний виконавець і оператори ЧПУ.

Таким чином, процес перенесення керуючої програми розбивається на дві операції – записи керуючої програми в RaspberryPi і копіювання її в систему управління ЧПУ. При цьому оператором ЧПУ може бути виконана тільки операція копіювання керуючої програми в ЧПУБ, його доступ до інших програм в RaspberryPi заборонений. Розбиття процесу перенесення керуючих програм за допомогою одноплатного комп'ютера дозволяє застосувати і інші методи перевірки цілісності файлів – перевірка контрольної сумою або шифрування.

2.3.3 Візуальний контроль виконання керуючих програм на ЧПУ

Це новий витік у розвитку систем безпеки сучасного металообробного обладнання. За допомогою такого контролю можна здійснювати запис всієї інформації, що відображається па пульті верстата, а саме:

– номер поточної керуючої програми;

– поточний кадр керуючої програми;

– час початку і кінця роботи ЧПУ;

– основні сигнали електроавтоматики і аварійні стани;

– номер активного інструменту і інші динамічні параметри роботи верстатів.

На рисунку 2.7 показана принципова схема використання одноплатного комп'ютера RaspberryPi 3 в підсистемі інформаційної безпеки виробничої дільниці ЧПУ.

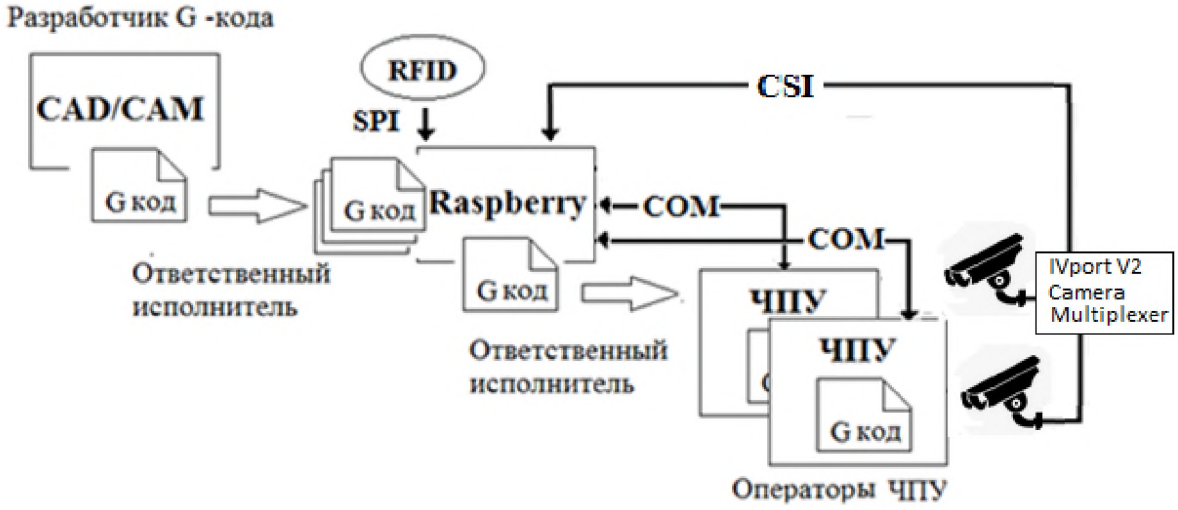


Рисунок 2.7 – Схема використання одноплатного комп'ютера RaspberryPi 3

RaspberryPi злився з кожним верстатом ЧПУ по інтерфейсу RS-232. RS-232 – послідовним інтерфейсом (COM-порт), призначеним для обміну байтовою інформацією. В даний час використовується для підключення до комп'ютерів широкого спектру обладнання, невибагливого до швидкості обміну, особливо при значній відстані його від комп'ютера і відхиленні умов застосування від стандартних.

RS-232 забезпечує передачу даних і деяких спеціальних сигналів між терміналом і комунікаційним пристроєм на відстань до 15 метрів. Так як в одноплатні комп'ютери RaspberryPi не мають штатного COM-порту, то в цьому інтерфейсі використовується перехідник- адаптер USB на COM-порт. З цього дво-керованого каналу від RaspberryPi в систему управління ЧПУ можуть передаватися файл з G-кодом керуючої програмою і код фізичного доступу з обладнання до ЧПУ. Від системи управління ЧПУ в одноплатний комп'ютер передається інформація.

Для підключення до RaspberryPi зчитувача RFID використовується інтерфейс SPI. SPI – (послідовний периферійний інтерфейс, шина SPI) послідовний синхронний стандарт передачі даних в режимі повного дуплексу, призначений для забезпечення простого і недорогого високошвидкісного сполучення мікроконтролерів і периферії. Наприклад, в якості периферії може бути: дисплей, різні датчики, FLASH пам'ять, SD карта і т.д. SPI також іноді називають чотирьох проводним інтерфейсом, так як використовуються чотири лінії зв'язку. Цей інтерфейс дозволяє налаштувати «гірляндне» підключення відразу декількох сумісних пристроїв, використовуючи при цьому всього одну групу контактів – шляхом присвоєння всім цим пристроям різних адрес.

Камери відеоспостереження приєднується до плати мікрокомп'ютера RaspberryPi кабелем-шлейфом до гнізда CSI (послідовний інтерфейс камери). Цей порт забезпечує передачу відеоданих з високою роздільною здатністю зі швидкістю до 30 кадрів в секунду і може бути програмно змінена. Для підключення декількох камер може бути використана плата IVport V2 Camera Multiplexer, що дозволяє підключати до чотирьох офіційних Pi-камер до однієї плати RaspberryPi.

Схема інтерфейсів RaspberryPi показана на рисунку 2.8.

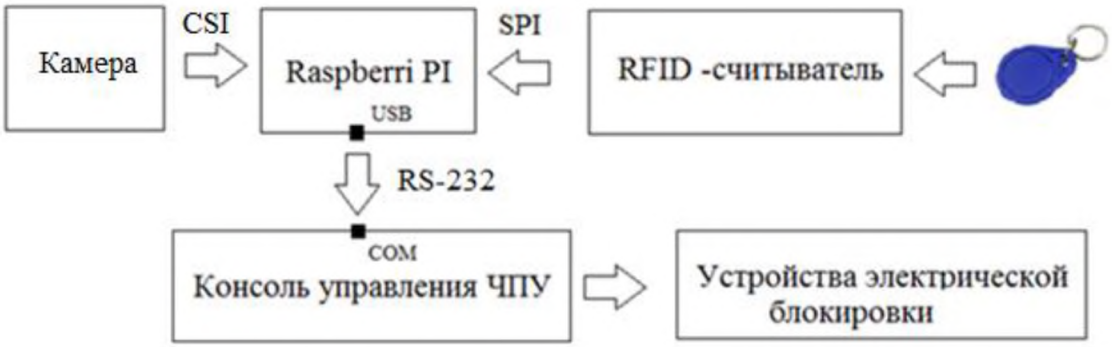


Рисунок 2.8 – Схема інтерфейсів RaspberryPi

2.4 Висновок

В спеціальній частині провели обстеження виробничої дільниці ЧПУ, описали об'єкт інформаційного захисту, описали апаратне та програмне забезпечення, провели опис верстатів типу 16А20Ф3, провели аналіз та оцінку інформаційних ризиків, склали модель загроз та модель порушника, ввели заходи безпеки та рекомендації, а саме загальна специфікацію політики безпеки та заходи безпеки, ввели контроль фізичного доступу до ЧПУ та візуальний контроль виконання керуючих програм на ЧП.

3 ЕКОНОМІЧНИЙ РОЗДІЛ

Метою виконання економічного розділу є економічне обґрунтування доцільності запровадження політики безпеки та рекомендацій, а саме контролю фізичного доступу до ЧПУ та візуальний контроль виконання керуючих програм на ЧПУ.

3.1 Економічне обґрунтування доцільності впровадження політики безпеки інформації.

Визначення трудомісткості розробки політики безпеки інформації.

$$t = t_{тз} + t_{в} + t_{а} + t_{вз} + t_{озб} + t_{овр} + t_{д}\text{ , годин,} \quad (3.1)$$

де $t_{тз}$ - тривалість складання ТЗ на розробку ПБІ = 21 година;

$t_{в}$ - тривалість розробки концепції безпеки інформації у організації = 24 години;

$t_{а}$ - тривалість процесу аналізу ризиків = 26 годин;

$t_{вз}$ - тривалість визначення вимог заходів, методів та засобів захисту = 17 годин;

$t_{озб}$ - тривалість виробу основних рішень з забезпечення БІ = 27 годин;

$t_{овр}$ - тривалість організації виконання відновлювальних робіт і забезпечення неперервного функціонування організацій = 25 годин;

$t_{д}$ - тривалість документального оформлення ПБ = 16 годин;

$t=21+24+26+17+27+25+16 = 156$ годин.

Розрахунок витрат на створення ПБІ

Витрати на розробку політики безпеки інформації Крп складаються з витрат на заробітну плату спеціаліста з інформаційної безпеки Ззп і вартості витрат машинного часу, що необхідний для розробки політики безпеки інформації Змч.

$К_{рп} = З_{зп} + З_{мч} = 24960+48 = 25008$ грн.

$З_{зп} = t*З_{пр} = 156*160 = 24960$ грн.

де t – загальна тривалість розробки політики безпеки, годин=156;

$З_{іб}$ – середньогодинна заробітна плата спеціаліста з інформаційної безпеки з

нарахуваннями, грн/годину = 160 грн.

Вартість машинного часу для розробки політики безпеки інформації:

Змч= tд*Смч=16*3 = 48 грн.

де tд – трудомісткість підготовки документації на ПК, годин;

Смч – вартість 1 години машинного часу ПК, грн./година.

Вартість 1 години машинного часу:

Смч = 0,6* 2*1,68 + ((5696*0,3)/1920) + ((1750*0,1)/1920) = 3 грн.

Встановлена потужність = 0,6 кВт;

Кількість задіяних робочих станцій при написанні політики = 2;

Тариф на електроенергію = 1,68 грн/кВт*год.;

Залишкова вартість ПК на поточний рік = 5696 грн;

Річна норма амортизації на ПК = 0,3;

Річна норма амортизації на ліцензійне програмне забезпечення = 0,1;

Вартість ліцензійного програмного забезпечення = 1750 грн;

Річний фонд робочого часу = 1920.

Капітальні (фіксовані) витрати на створення політики безпеки інформації:

К = Кпр + Кзпз + Кпз + Каз + Кнавч + Кн = 47308 грн.

де Кпр – вартість розробки політики інформаційної безпеки та залучення для цього зовнішніх консультантів = 0 тис. грн;

Кзпз – вартість закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ) = 8000 тис. грн;

Крп - вартість розробки політики = 25008 грн;

Каз – вартість закупівлі апаратного забезпечення та допоміжних матеріалів = 12 тис. грн;

Кнавч – витрати на навчання технічних фахівців і обслуговуючого персоналу = 0 грн.

Кн – витрати на встановлення обладнання та налагодження системи інформаційної

безпеки = 2300 грн.

Розрахунок поточних витрат

Річні поточні витрати на функціонування системи інформаційної безпеки:

$$С = Св + Ск + Сак \text{ , грн.} \quad (3.2)$$

де Св - вартість відновлення й модернізації системи = 0 грн.

Сак - витрати, викликані активністю користувачів системи інформаційної безпеки. Сак = 0 грн.

Витрати на керування системою інформаційної безпеки:

$$Ск = Сн + Са + Сз + Сел + Со + Стос, \text{ грн.} \quad (3.3)$$

Витрати на навчання адміністративного персоналу й кінцевих користувачів визначаються = Сн = 0 грн.

Річний фонд амортизаційних відрахувань:

Са = 2000 грн (50000 грн / 25 років)

Річний фонд заробітної плати інженерно-технічного персоналу, що обслуговує систему інформаційної безпеки (Сз), складає:

Сз = Зосн + Здод, грн.

Основна заробітна плата спеціаліста з інформаційної безпеки 16200 грн. Виконання робіт вимагає залучення спеціаліста на 0,25 ставки.

Сз = (16200·12 + 16200·12·0,1)·0,25= 53460 грн.

З 01.12.2021 р. Ставка ЄСВ для всіх категорій платників складає 22%.

Сєв = 47308·0,22 = 10408 грн.

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року (Сел), визначається за формулою:

Сел = Р·Fр·Ц = 1935 грн.

де Р – встановлена потужність апаратури інформаційної безпеки = 0,6 кВт;

Fр – річний фонд робочого часу системи інформаційної безпеки = 1920 год.;

Це – тариф на електроенергію = 1,68 грн./кВт за годину.

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної

безпеки:

Стос = 47308·0,01 = 473 грн.

Витрати на керування системою інформаційної безпеки визначаються:

Ск = 0+2000+53460+10408+1935 + 473 = 68276 грн.

С= 0+68276+0 = 68276 грн.

Таким чином, річні поточні витрати на функціонування системи інформаційної безпеки складають 68276 грн.

3.2 Оцінка можливого збитку від атаки на вузол або сегмент мережі

Оцінка величини збитку:

tп – час простою вузла або сегмента корпоративної мережі внаслідок атаки, 3 години;

tв – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, 4 години;

tви – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, 2.5 год;

Зо – заробітна плата обслуговуючого персоналу (адміністраторів та ін.), 18000 грн./міс.;

Зс – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, 15000 грн./міс.;

Чо – чисельність обслуговуючого персоналу (адміністраторів та ін.), 2 особи;

Чс – чисельність співробітників атакованого вузла або сегмента корпоративної мережі, 8 осіб.;

О – обсяг збитку атакованого вузла або сегмента корпоративної мережі, 5,5 млн. грн. у рік;

Пзч – вартість заміни встаткування або запасних частин, грн;

I – число атакованих сегментів корпоративної мережі, 1;

N – середнє число атак на рік, 5.

Упущена вигода від простою атакованого сегмента корпоративної мережі становить:

$$U = Пп + Пв + V, \quad (3.4)$$

де Пп – оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі, грн;

Пп = ((15000·8)/176)·3 = 2046 грн,

де F – місячний фонд робочого часу (при 40-а годинному робочому тижні становить 176 ч).

Пв – вартість відновлення працездатності вузла або сегмента корпоративної мережі (переустановлення системи, зміна конфігурації та ін.), грн;

V – втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі, грн.

Витрати на відновлення працездатності вузла або сегмента корпоративної мережі включають кілька складових:

Пв = Пви + Ппв + Пзч,

де Пви – витрати на повторне уведення інформації, грн.;

Ппв – витрати на відновлення вузла або сегмента корпоративної мережі, грн;

Пзч – вартість заміни устаткування або запасних частин, 0 грн.

Пви = ((15000·8)/176)·2,5 = 1705 грн.

Ппв = ((18000·2)/176)·4 = 818 грн.

Витрати на заміни встаткування або запасних частин можуть скласти 2320,50 грн.

Тоді витрати на відновлення працездатності вузла або сегмента корпоративної мережі складуть:

Пв = 1705 + 818 + 0 = 2523 грн.

Втрати від зниження очікуваного обсягу прибутків за час простою атакованого вузла або сегмента корпоративної мережі визначаються виходячи із середньогодинного обсягу прибутку і сумарного часу простою сегмента корпоративної мережі:

V = (5500000/2080)·(3+4+2,5) = 25120 грн.

де Fг – річний фонд часу роботи філії (52 робочих тижні, 5-ти денний робочий тиждень, 8-ми годинний робочий день) становить близько 2080 год.

U = 2046 + 2523 + 25120 = 29689 грн.

Загальний збиток від атаки на сегмент корпоративної мережі організації складе:

B = 1·5·29689 = 148445 грн.

3.2.1 Загальний ефект від впровадження системи інформаційної безпеки

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної:

$$E=B\cdot R - C, \quad (3.5)$$

де B– загальний збиток від атаки у разі перехоплення інформації = 148445 грн.;

R – вірогідність успішної реалізації атаки на сегмент мережі, частки одиниці = 55%;

C – щорічні витрати на експлуатацію системи інформаційної безпеки = 68276 грн.

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки:

E = 148445·0,55 – 68276 = 13369 грн.

3.3 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки:

де B – загальний ефект від впровадження системи інформаційної безпеки грн.;

K – капітальні інвестиції за варіантами, що забезпечили цей ефект, грн.

Коефіцієнт повернення інвестицій ROSI:

ROSI = 148445 / 47308 = 0,31 частки одиниці,

Проект визнається економічно доцільним, якщо розрахункове значення коефіцієнта повернення інвестицій перевищує величину річної депозитної ставки з урахуванням

інфляції:

$$ROSI > (Nдеп – Nінф)/100), \quad (3.6)$$

де Nдеп – річна депозитна ставка, (8%);

Nінф – річний рівень інфляції, (5%).

Розрахункове значення коефіцієнта повернення інвестицій:

0,31 > (8 – 5)/100 = 0,03.

Термін окупності капітальних інвестицій То показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи інформаційної безпеки:

Т = 1/0,31 = 3,2 роки.

3.4 Висновок

Розробка та впровадження політики інформаційної безпеки для ТОВ «Техноком» є економічно доцільним, оскільки коефіцієнт повернення інвестицій ROSI складає 0,31 на 1 грн., що означає отримання 0,31 грн. економічного ефекту на кожну гривню капітальних вкладень. Термін окупності при цьому складатиме 3,2 роки. Капітальні витрати складають 47308 грн, а поточні 68276 грн.

ВИСНОВКИ

АСУ ТП – автоматизована система управління технологічними процесами, в якій існує досить тісний взаємозв'язок автоматизованих систем з фізичними процесами і виконавчими пристроями. Для забезпечення безпеки АСУТП вкрай рідко використовуються традиційні методи захисту інформації. Маніпуляції з АСУ ТП можуть викликати порушення в роботі керованих систем – може привести до зміни характеристик, що не відповідає розрахунковим. При цьому такі модифікації можуть бути непомітні при стандартних умовах їх тестування, що надалі може привести до катастрофічних наслідків при їх використанні.

Згідно ЗУ «Про інформацію» несанкціоновані дії щодо інформації в системі це дії, що провадяться з порушенням порядку доступу до цієї інформації, установленого відповідно до законодавства. Таким чином інформація, що циркулює в АСУТП також потрапляє під цей закон. Тому було прийнято рішення про створення комплексної системи захисту інформації.

У першому розділі проведено аналіз структури АСУТП, підсистеми ЧПУ в АСУТП, аналіз особливостей АСУТП з точку зору ІБ. Проаналізовано стандарти в області захисту інформації АСУТП та виявлені загрози ІБ в підсистемі ЧПУ.

У спеціальній частині проведено обстеження виробничої дільниці ЧПУ, проаналізовані та оцінені інформаційні ризики. Також розроблено модель загроз та модель порушника безпеки інформації, сформовані основні положення політики безпеки інформації для комплексної системи захисту інформації, та розроблені заходи безпеки, такі як: контроль фізичного доступу до ЧПУ і візуальний контроль виконання керуючих програм на ЧПУ.

В третьому розділі проведені економічні розрахунки для підтвердження економічної доцільності розробки заходів безпеки та рекомендацій, ефекту впровадження контролю фізичного доступу до ЧПУ та візуальний контроль виконання керуючих програм на ЧПУ.

ПЕРЕЛІК ПОСИЛАНЬ

1. Визначення, функції та склад АСУТП [Електронний ресурс] // АСУТП: сайт. - Ресурс доступу: https://automation-system.ru/main/ll-asutp/asu-tp/46-41 -opredelenie-funkczii-i-sostav-asutp.html.

2. Структура розподіленої АСУ ТП [Електронний ресурс] // Teh-Lib.Ru: зб. техн. ст. - Ресурс доступу: http://www.teh-lib.ru/atpip/struktura-raspredeljonnoj-asu-tp/Vse-stranitsy.html.

3. Проблематика інформаційної безпеки автоматизованого виробництва. Огляд: IT-безпеку, квітень 2016. Ресурс доступу: https://www.itweek.ru/security/article/detail.php?ID=185094

4. Хемілтон Тернер, Жюль Вайт, Хайме Камелія, Крістофер Вільямс, Брендон Еймос. «Чи надійні сучасні виробничі системи? Відкриті системи». СУБД 2015 № 03 - Ресурс доступу: https://www.osp.ru/os/2015/03/13046899

5. Гончар С.Ф. Аналіз ймовірності реализации загроза захисту інформації в автоматизоване системах управління технологічним процесом // Захист інформації. - 2014. - том 16, № 1. - С. 40-46.

6. Гончар С.Ф. Визначення актуальних загроз безпеці інформації у автоматизова-них системах управління технологічними процесами захисту інформації, том 17. - Ресурс доступу: http://jrnl.nau.edu.ua/index.php/ZI/article/view/9519

7. Сергій Гончар, Геннадій Леоненко, Олексій Юдін «Загальна модель загроз безпеці інформації АСУТП - Правове, нормативне та Метрологічне забезпечення системи захисту інформації в Україні», вип. 1 (29), 2015-го

8. Анікеєнко В. Безпека АСУ ТП і контроль прівілегіроіанних користувачів. Ресурс доступу: http: www.anti-mafware.ru

9. ВОРОНЦОВ А. Автоматизовані системи управління технологічними процессами. Зап. безпеки: інформ. бюл. "Інфоснстемі Джет". Інформаційна безпека промисловим

об'єктом. Ресурс доступу: http: www.anti-mafware.ru

10. Лукацький А. Стандарти безпеки АСУ ТП. Ресурс доступу: http://www.slideshare.net/CiscoRu/ss-8690963

11. Астахов А. Аналіз захищеності корпоративних автоматизованих систем [Електронний ресурс] / А. Астахов // Мистецтво управління інформаційною безпекою Режим доступу: http://iso27000.ru/chitalnyi-zai/audit-informacionnoi-bezopasnosti/analiz-zaschischennosti-korporativnyh-avtomatizirovannyh-sistem.

12. С.Н. Григорєв, Г.М. Мартинов СИСТЕМА ЧПУ: СУЧАСНІ ВИКЛИКИ, ІНФОРМАЦІЙНІЙ І ТЕХНОЛОГІЧНІЙ БЕЗПЕЦІ "АВТОМАТИЗАЦІЯ В ПРОМИСЛОВОСТІ" 2016. Режим доступу: https://elibrary.ru/item.asp?id=26168249

13. Кібербезпека АСУ ТП. Огляд спеціалізованих накладених засобів захисту Максим Небайкін Максим Небайкін Ресурс доступу: https://www.anti-malware.ru/analytics/Market_Analysis/ICS-security-review

14. ФАТКІЕВА Р.Р. Моделювання автоматизованих технологічних процесів в умовах інформаційних загроз Науковий вісник НГТУ тому 70, № 1, 2018, с. 167-176 Vol. 70, No. 1, 2018, pp. 167-176 ІНФОРМАТИКА, ОБЧИСЛЮВАЛЬНА ТЕХНІКА І УПРАВЛІННЯ

15. Опублікований стандарт з вимогами до безпеки компонентів АСУ ТП. «Цифрова підстанція» Ресурс доступу: http://digitalsubstation.com/blog/2018/09/26/opublikovan-standart-s-trebovaniyami-k-bezopasnosti-komponentov-asu-tp/

16. Олег Сафрошкін "Захист АСУ ТП" - Журнал "Information Security / Інформаційна безпека" # 2, 2014 Ресурс доступу:http://itsec.ru/articles2/Oborandteh/zaschita-asu-tp

17. Верескун М.В. ЗАБЕЗПЕЧЕННЯ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПРОМИСЛОВИХ ПІДПРИЄМСТВ, Економіка і Організація управління • No 1 (17) - 2 (18)

18. Домарев В.В. "Безпека інформаційних технологій. Методологія створення

систем захисту" - К.: ТОВ "ТИД" ДС ", 2002. - 688 с.

19. Висновок з Відповідей на опитуванні про впровадження правил безпеки інформаційних систем та мереж: до культури безпеки 2012. [Електронний ресурс] - Режим доступу: http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/R

20. Нежметдінов Р.А., Ковальов І.А., Харясов А.В. Розробка способу ідентифікації користувача верстата з ЧПУ на основі застосування зовнішніх обчислювальних пристроїв. ФГБОУ ВО «МГТУ СТАНКИН»[Електронний ресурс] - Режим доступу: www.esa-conference.ru

21. Система моніторингу верстатів з ЧПУ. [Електронний ресурс] - Режим доступу: http://cnc-vision.ru

22. Методичні рекомендації до Виконання кваліфікаційних робіт бакалаврів спеціальності 125 Кібербезпека / Упоряд .: О.В. Герасіна, Д.С. Тимофєєв, О.В. Кручінін, Ю.А. Мілінчук - Дніпро: НТУ «ДП», 2020. - 47 с.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	1	
5	А4	Стан питання. Постановка задачі	28	
6	А4	Спеціальна частина	17	
7	А4	Економічний розділ	9	
8	А4	Висновки	1	
9	А4	Список літератури	2	
10	А4	Додаток А	28	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	
14	А4	Додаток Ґ	2	

ДОДАТОК Б. Огляд стандарту безпеки промислових систем управління NIST SP 800-82

Стандарт інформаційної безпеки (ІБ) промислових систем управління NIST SP 800-82 Rev містить перелік функцій системи захисту інформації промислових систем управління і посилання на відповідні стандарти і може бути використаний при створенні систем захисту інформації.

У шести розділах даного стандарту представлені:

1) Короткий огляд промислових систем управління, їх зв'язок зі SCADA, розподіленими системами управління і програмованими логічними контролерами. Промислові системи можуть бути повністю автоматичними або ж в роботі системи може брати участь людина. Прикладом систем, в роботі якої бере участь людина, є автоматизовані системи управління технологічним процесом (АСУТП).

2) Коротко описана еволюція промислових систем управління і їх поступова інтеграція з IT-системами.

3) Наводиться опис промислових систем управління, в тому числі компонентів, що використовуються в промислових системах управління.

4) Описано чинники, що впливають на інформаційну безпеку промислових систем управління.

5) Описано чинники, які необхідно врахувати при захисті промислових систем управління.

6) Наведена таблиця розходжень між IT системами і промисловими системами управління.

7) Наводяться список різних систем управління, які схожі з промисловими системами та інформаційна безпека яких також забезпечуватися на основі стандарту NIST SP 800-82. До таких систем управління, в тому числі, відносяться АСУТП.

8) Представлені базові поняття управління ризиками, засновані на стандартах NIST SP 800-39, NIST SP 800-37 і NIST SP 800-30. Крім базових понять в розділі також

представлені рекомендації та керівництва з управління ризиками стосовно ІБ промислових систем управління.

9) Описуються методи по розробці програми забезпечення ІБ промислових систем управління: опис переваг впровадження системи захисту інформації, опис потенційних наслідків від реалізованих атак і представлення програми забезпечення ІБ керівництву компанії.

10) Наводяться рекомендації по розробці і впровадженню програм забезпечення ІБ промислових системах управління, які включають в себе традиційні для управління ризиками частини: ідентифікація та визначення цінності активів; вибір заходів захисту; аналіз і оцінка ризиків; впровадження заходів захисту.

11) Описано підходи до забезпечення мережевої безпеки і не відносяться до мережевої безпеки:

– загальні положення по сегментації і поділу мереж; захист мережевого периметра;

– односпрямовані шлюзи;

– додано підрозділи по рекомендованим правилами для шлюзів безпеки для протоколів DHCP, SSH, SOAP;

– автентифікація і авторизація;

– аудит системи, моніторинг і ведення журналів подій;

– виявлення інцидентів і реагування на них, відновлення системи.

У додатках стандарту приведено:

Додаток А і В - містить список абревіатур і список термінів;

Додаток С містить інформацію про погрози, вразливості і інциденти ІБ промислових систем управління.

Загрози розділені на 4 типи (по типу джерела загроз). Для кожного типу загроз можна прочитати коротке пояснення і характеристики.

У стандарті розглядаються наступні типи вразливостей:

– вразливості політик і процедур;

– вразливості архітектури;

– вразливості в конфігураціях пристроїв і процедурі обслуговування;

– фізичні уразливості;

– вразливості ПЗ;

– вразливості комунікацій і обчислювальних мереж.

Для кожного типу наводиться не тільки список відповідних вразливостей, а й умови, які сприяють їх виникненню.

Додаток D наведені посилання на ресурси, які містять інформацію, пов'язану із забезпеченням захисту промислових систем управління.

Додаток E включає список механізмів і технологій, які можуть застосовуватися при забезпеченні захисту промислових систем управління, в тому числі АСУ ТП.

Додаток G являє механізм проектування системи захисту для промислових систем управління які згруповані по наступних напрямках:

1. Управління доступом;
2. Інформування та навчання персоналу;
3. Аудит та облік;
4. Оцінка безпеки;
5. Управління конфігураціями;
6. Планування дій на випадок непередбачених ситуацій;
7. Ідентифікація та автентифікація;
8. Реагування на інциденти;
9. Обслуговування;
10. Захист знімних носіїв інформації;
11. Фізичний захист і охорона навколишнього середовища;
12. Планування;
13. Безпека персоналу;
14. Управління ризиками;
15. Інвентаризація систем і сервісів;

16. Захист промислової системи управління і мереж передачі даних;

17. Цілісність промислової системи управління та інформації;

18. Засоби управління системою забезпечення ІБ промислової системи управління.

Для кожного напряму наводиться список заходів захисту, які можна застосувати для забезпечення ІБ промислових систем управління.

ДОДАТОК В. Перелік документів на оптичному носії

1. Пояснювальна_записка_Черненко.doc
2. Пояснювальна_записка_Черненко.pdf
3. Презентація_Черненко.pptx

ДОДАТОК Г. Відгуки керівників розділів

Відгук керівника економічного розділу:

Керівник розділу _____ _____
(підпис) (ініціали, прізвище)

ДОДАТОК Ґ. Відгук керівника кваліфікаційної роботи

Відгук

на кваліфікаційну роботу студента групи 125-17-2 Черненка Єгора Юрійовича на тему: «Система захисту інформації виробничої дільниці ЧПУ ООО «Техноком»

Керівник кваліфікаційної роботи: доц. Горєв В.М.

Керівник спеціального розділу: Саксонов Г.М.