Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
завідувачка кафедри кібербезпеки
та захисту інформації
_____Наталія ЛУКОВА-ЧУЙКО
«14» червня 2022р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

дипломної роботи
бакалавра
(назва освітнього ступеня)

галузь знань 12 Інформаційні технології
(шифр і назва галузі знань)

спеціальність 125 Кібербезпека
(код і назва спеціальності)

освітня програма Кібербезпека
(назва освітньої програми)

на тему: «Криптографічний модуль захисту інформації на базі підприємства критичної інфраструктури»

Виконавець: студент IV курсу, групи КБ-41

_____ **Андрій КУРОЄДОВ**
(підпис) (ім'я прізвище)

	Прізвище, ініціали	**Підпис**
Керівник	Лариса МИРУТЕНКО	

Нормоконтроль	Олександр ТОРОШАНКО	

Київ 2022

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
завідувачка кафедри кібербезпеки
та захисту інформації
_____Наталія ЛУКОВА-ЧУЙКО
«01» листопада 2021 р.

ЗАВДАННЯ
на виконання дипломної роботи

спеціальності 125 Кібербезпека
(код і назва спеціальності)

освітньої програми Кібербезпека
(назва освітньої програми)

Студентові **КБ-41** **Куроєдову Андрію Сергійовичу**
(група) (прізвище ім'я по-батькові)

Тема дипломної роботи Криптографічний модуль захисту інформації на базі підприємства критичної інфраструктури

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема дипломної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №5 від 29.10.2021 р.

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Алгоритм шифрування ДСТУ ГОСТ 28147:2009, дані про впровадження кіберзахисту об'єктів критичної інфраструктури, можливі кібератаки та способи захисту від них.

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Способи реалізації кіберзахисту на підприємства критичної інфраструктури, реалізовані кібератаки на об'єкти критичної інфраструктури та способи захисту від них, способи виявлення вразливостей в системах, криптографічний модуль захисту.

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність Створення криптографічного модулю захисту з використанням двофакторної автентифікації, який використовує алгоритм шифрування ДСТУ ГОСТ 28147:2009 для шифрування даних користувача при реєстрації в інформаційну систему підприємства.

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання: 01 листопада 2021 року

Завдання видав _____ (підпис) Лариса МИРУТЕНКО (ініціали, прізвище)

Завдання прийняв до виконання _____ (підпис) Андрій КУРОЄДОВ (ініціали, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Уточнення постановки задачі	29.10.2022 – 29.01.2022	*виконано*
2	Аналіз літератури	30.01.2022 – 12.02.2022	*виконано*
3	Аналіз засобів забезпечення кіберзахисту	13.02.2022 – 22.02.2022	*виконано*
4	Дослідження основних атак та способи захисту від них	23.02.2022 – 11.03.2022	*виконано*
5	Аналіз способів виявлення вразливостей ІКС	12.03.2022 – 19.04.2022	*виконано*
6	Огляд програмних засобів кіберзахисту	20.04.2022 – 26.04.2022	*виконано*
7	Розробка криптогрфачного модулю захисту інформації	27.04.2022 – 26.05.2022	*виконано*
8	Оформлення пояснювальної записки	27.05.2022 – 07.06.2022	*виконано*
9	Підготовка до захисту	08.06.2022 – 13.06.2022	*виконано*

Завдання видав _____ (підпис) Лариса МИРУТЕНКО (ініціали, прізвище)

Завдання прийняв до виконання _____ (підпис) Андрій КУРОЄДОВ (ініціали, прізвище)

УДК 004.056.5

РЕФЕРАТ

Пояснювальна записка дипломної роботи складається зі вступу, трьох розділів, висновків, списку використаних джерел та додатків. Основний текст займає 57 сторінок, включає в себе зміст, вступ, три розділи дипломної роботи, висновки та список використаних джерел. Дипломна робота містить один додаток із загальною кількістю сторінок – 15. Пояснювальна записка містить 17 рисунків і 1 таблиці.

Метою роботи є аналіз видів кіберзахисту, які застосовуються на об’єктах критичної інфраструктури та розробка криптографічного модулю захисту інформації. Дана тема є актуальною, тому що об’єкти критичної інфраструктури є важливими для економіки та національної безпеки держави і саме тому, впровадження та підтримка засобів кіберзахисту є важливим завданням, оскільки кількість кібератак збільшується щодня.

Для досягнення мети необхідно виконати такі завдання:

- Проаналізувати, реалізацію та підтримку кіберзахисту на об’єктах критичної інфраструктури;
- провести аналіз реалізованих кібератак на об’єкти критичної інфраструктури, способи захисту від них та способи виявлення вразливостей на підприємстві;
- реалізувати програмний модуль з використанням двофакторної автентифікації та алгоритмом шифрування ДСТУ ГОСТ 28147:2009.

Об’єктом дослідження є процес дослідження заходів кіберзахисту, реалізованих на об’єктах критичної інфраструктури.

Предметом дослідження є забезпечення, реалізація та експлуатація заходів кіберзахисту на об’єктах критичної інфраструктури.

Практичною цінністю даної роботи є створення криптографічного модулю захисту з використанням двофакторної автентифікації, який використовує алгоритм шифрування ДСТУ ГОСТ 28147:2009 для шифрування даних користувача при реєстрації в інформаційну систему об’єкта критичної інфраструктури.

Методи дослідження:

- порівняння;
- аналіз нормативних документів щодо кібербезпеки;
- аналіз джерел інформації.

Ключові слова: кіберзахист, критична інфраструктура, вразливості, кіберінциденти, шифрування, алгоритм шифрування ДСТУ ГОСТ 28147:2009, кібербезпека, криптографічний модуль захисту.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

АС	–	атомна станція
ІКС	–	інформаційна та керуюча система
ЕО	–	експлуатуюча організація
ЯРБ	–	ядерна та радіаційна безпека
ПЗ	–	програмне забезпечення
ПТК	–	програмно-технічний комплекс
ТЗА	–	технічний засіб автоматизації
ТО	–	технічне обслуговування
КСЗІ	–	комплексна система захисту інформація
DoS	–	denial of service
DDoS	–	distributed denial of service
CDN	–	content delivery network

ЗМІСТ

ВСТУП……. 8
РОЗДІЛ 1 АНАЛІЗ КІБЕРЗАХИСТУ КРИТИЧНОЇ ІНФРАСТУРКУТУРИ…… 12
1.1 Забезпечення кібербезпеки в критичній інфраструктурі України……... 12
1.2 Загальні вимоги до кіберзахисту АЕС……..…… 13
1.3 Види засобів кіберзахисту критичної інфраструктури…… 15
1.4 Криптографічні засоби захисту інформації на об’єктах критичної інфраструктури…… 17
1.5 Забезпечення кіберзахисту на прикладі АЕС як об’єкта критичної інфраструктури…… 19
Висновки за розділом 1……... 20
РОЗДІЛ 2 ІСНУЮЧІ ЗАХОДИ КІБЕРЗАХИСТУ ОБ’ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ……... 21
2.1 Аналіз вразливостей ІКС на АЕС до атак та кіберзагроз…….. 21
2.2 Забезпечення координації між кіберзахистом та функціями ІКС АС…. 26
2.3 Оцінювання повноти та достатності заходів кіберзахисту ІКС…….. 27
2.4 Загальні проєктні заходи кіберзахисту ІКС…….. 31
2.5 Загальні заходи забезпечення кіберзахисту в процесі експлуатації….. 36
Висновки за розділом 2……... 39
РОЗДІЛ 3 ПРОГРАМНІ ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ…… 40
3.1 «ЛОЗА – 1» як засіб забезпечення кіберзахисту на АЕС…… 40
3.2 Розробка криптографічного захисту інформації з використанням двофакторної аутентифікації…….. 42
Висновки за розділом 3……... 56
ВИСНОВКИ……. 57
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ…… 58
ДОДАТКИ…… 63
ДОДАТОК А……..... 63

ВСТУП

Критична інфраструктура – це певна кількість об’єктів, які являються надважливими для країни в економічній сфері та сфері національної безпеки. Нанесення шкоди об’єкту критичної інфраструктури може негативно вплинути на національні інтереси та економіку України в цілому. Тому кіберзахист даної галузі займає одне з головних місць для фахівців з кібербезпеки та державних органів та спеціальних організацій.

Атомні електричні станції – як сукупність окремих об’єктів, являються критичною інфраструктурою і їх захист має забезпечуватись належним чином. В наш час атомна енергетика відіграє надзвичайно важливу роль в житті людей по всьому світу. Мета атомної енергетики це виготовлення електричної та теплової енергії за допомогою ядерних реакцій. Цим процесом займаються атомні електростанції та різні агентства, такі як The World Association of Nuclear Operators (WANO) і International Atomic Energy Agency (IAEA). Головне завдання даних підприємств, це безпечне та постійне виготовлення енергії, і це все не можливо без захисту конфіденційної інформації.

В Україні атомна енергетика – це надважлива частина для розвитку економіки і вироблення електричної енергії. Завдяки різним організаціям в цій сфері, основна мета яких – це успішне та безпечне продукування, країна забезпечує себе і країни-імпортери електроенергією і таким чином розвивається в цій сфері, що допомагає підтримувати хороші відношення між США, Францією, Словаччиною, Угорщиною та іншими країнами.

Атомна енергетика в Україні формувалась ще при СРСР в 70-ті – 80-ті роки минулого століття і була зв’язана з військовою та промисловою сферою СРСР, коли почалось активне забудування територій держави атомними станціями (АЕС). Першою атомною електростанцією на території держави була Чорнобильська атомна електрична станція (ЧАЕС) з перший блоком №1, який було введено в експлуатацію

в 1977 році. Після успішного початку почалося активне будівництво Хмельницької, Південноукраїнської, Запорізької та Рівненської станцій [1, 2].

На сьогоднішній день в Україні в експлуатації перебувають 15 енергоблоків 13 – з реакторами типу ВВЕР-1000 та 2 – ВВЕР-440. Загальна потужність даних реакторів складає близько 27% від потужності всіх електростанцій країни і це 13835 МВт [1]. Енергоблоки України можна побачити в табл. 1

Таблиця 1.1

Ядерні енергоблоки України

Блок	Тип установки	Встановлена потужність (МВт)	Дата запуску	Завершення проектного терміну експлуатації
Запорізька АЕС				
1	ВВЕР 1000/320	1000	10.12.1984	23.12.2025
2	ВВЕР 1000/320	1000	22.07.1985	19.02.2026
3	ВВЕР 1000/320	1000	10.12.1986	05.03.2027
4	ВВЕР 1000/320	1000	18.12.1987	04.04.2028
5	ВВЕР 1000/320	1000	14.08.1989	27.05.2020
6	ВВЕР 1000/320	1000	19.10.1995	21.10.2026
Рівненська АЕС				
1	ВВЕР 440/213	420	22.12.1980	22.12.2030

продовження таблиці 1.1

2	ВВЕР 440/213	415	22.12.1981	22.12.2031
3	ВВЕР 1000/320	1000	21.12.1986	11.12.2037
4	ВВЕР 1000/320	1000	10.10.2004	07.06.2035
Південноукраїнська АЕС				
1	ВВЕР 1000/302	1000	31.12.1982	02.12.2023
2	ВВЕР 1000/338	1000	06.01.1985	31.12.2025
3	ВВЕР 1000/320	1000	20.09.1989	10.02.2020
Хмельницька АЕС				
1	ВВЕР 1000/320	1000	22.12.1987	13.12.2028
2	ВВЕР 1000/320	1000	08.08.2004	07.09.2035

Для всіх з цих енергоблоків АЕС було проведено спеціальною комісією з питань безпеки, детальний аналіз кібербезпеки. Було виявлено, що енергоблоки експлуатуються безпечно з допустимим рівнем ризику. Вимоги по забезпеченню безпеки реакторних установок, які організація передбачувала при побудові та запуску своїх об’єктів виконуються та перевіряються згідно стандартів. В разі виявлені слабких місць безпеки і відхилення від вимог нормативних документів являються не значними і не потребують негайної зупинки роботи підприємства і виправлення даних проблем. Дані перевірки повинні проходити на регулярній основі з чітко встановленими термінами командою експертів [1].

Тому, постійно має вестися удосконалення в даній сфері, підприємство, у цьому випадку АЕС, має постійно вдосконалювати системи захисту інформації, використовувати новітні розробки, адже проблема захисту інформації являється як ніколи дуже актуальною.

РОЗДІЛ 1
АНАЛІЗ КІБЕРЗАХИСТУ КРИТИЧНОЇ ІНФРАСТУРКУТУРИ

1.1 Забезпечення кібербезпеки в критичній інфраструктурі України

Для реалізації кібербезпеки на підприємствах критичної інфраструктури потрібно чітко розуміти всі можливі ризики в цій сфері і поставити певні задачі для досягання поставленої мети.

Основними задачами із забезпечення безпеки даних на об’єктах критичної інфраструктури держави є [3]:

- визначити загрози безпеки інформації та виявити всі можливі вразливості у програмному та апаратному забезпеченні підприємства;
- оцінити реальну захищеність об’єкта критичної інфраструктури на даний момент;
- розробити певні вимоги щодо забезпечення безпеки інформації в сфері критичної інфраструктури;
- після розробки різноманітних засобів захисту, потрібно реалізувати ці заходи захисту інформації на підприємстві;
- підготувати досвідчених та готових до будь якого розвитку подій фахівців із забезпечення безпеки інформації в критичній інфраструктурі;
- здійснювати постійний контроль та моніторинг в сфері забезпечення кібербезпеки на підприємстві;
- ознайомитись з нормативним та правовими аспектами в сфері забезпечення безпеки інформації в критичній інфраструктурі;
- ознайомитися з інформаційними, матеріально-технічними та науково-технічними матеріалами с галузі безпеки інформації;
- після успішного впровадження засобів захисту потрібно постійно покращувати і розвиватись в сфері забезпечення кіберзахисту на об’єкті критичної інфраструктури.

Напрями забезпечення кібербезпеки:

Під час визначення основних напрямів забезпечення кібербезпеки на підприємстві, можна визначити, що першим правильним кроком буде створення дієвого механізму координації зусиль органів влади та підрозділів самого підприємства, які повинні впроваджувати та підтримувати безпеку під час експлуатації певних об’єктів.

Окрім того, обов’язково потрібно вводити заходи на галузевому, державному та регіональному рівнях з організаційного, нормативно-правового та науково-методичного забезпечення, а саме [3]:

- Розробка Стратегії забезпечення кібербезпеки критичної інфраструктури.
- Розробка та виконання державних цільових програм для забезпечення безпеки інформації.
- Розробка та затвердження Державного реєстру об’єктів критичної інфраструктури України.
- Ведення постійного державного контролю за станом забезпечення кібербезпеки на підприємстві критичної інфраструктури держави.
- Здійснення інформаційного, матеріально-технічного та науково-технічного забезпечення кібербезпеки на об’єкті критичної інфраструктури держави.
- Виконання загальнодержавних заходів та вимог для забезпечення сталого функціонування об’єкту критичної інфраструктури.
- Здійснення законодавчого регулювання відносин в галузі кібербезпеки на підприємстві.
- Здійснення загального та методичного керівництва у галузі забезпечення безпеки інформаційних систем критичної інфраструктури держави.

1.2 Загальні вимоги з кіберзахисту АЕС

До загальних вимог кібербезпеки АЕС можна віднести наступне [4]:

1. За захист інформаційної та керуючої система атомної станції відповідає ЕО (експлуатуюча організація) на всьому шляху життя ІКС (інформаційна та керуюча

система) (під час впровадження, модифікації, експлуатації, ТО (технічне обслуговування), ремонтування, випробування інформаційних систем та складових і ПЗ (програмне забезпечення) на АС (атомна станція)). Кібербезпеку ІКС АС має забезпечувати відокремлений підрозділ на станції і до його складу мають входити фахівці, які мають певний рівень досвідченості, для виконання основної задачі - забезпечення кібербезпеки і ЯРБ (ядерна та радіаційна безпека) [4].

2. Захист ІКС має передбачати такі заходи як [4]:

- адміністративний, технічний;
- програмний (ідентифікація та авторизація, антивірусне ПЗ);
- програмно-технічний (системи виявлення вторгнень, фаерволи).

Ці заходи захисту будуть забезпечувати [4]:

- повідомляти про всі можливі шкідливі дії системи захисту інформаційних систем, складових цих систем, мережевих пристроїв, програмного забезпечення, інформації;
- використання систем спостереження, ідентифікації та взаємодії на шкідливі моменти для того, щоб мінімізувати можливі наслідки;
- зменшення впливу наслідків шкідливого втручання, яке включає заходи з повернення до правильної роботи інформаційних та керуючих систем, складових цих систем і мережевих пристроїв.

Заходи, які забезпечують кіберзахист можуть гарантувати, що всі випадкові дії та помилки працівників не погіршать кіберзахист систем і не підвищать вразливість інформаційних систем, складових цих систем та ПЗ до шкідливого впливу.

3. На етапі проєкту інформаційних систем визначаються програмні заходи захисту, які в майбутньому впроваджуються в процесі створення програмного забезпечення, програмно-технічних комплексів та технічних засобів. Після цього всі системи мають відповідати та виконувати поставлені вимоги з кібербезпеки на всіх подальших етапах життєвого циклу систем [4].

4. Надсилання інформації між ІКС АС та кризовими центрами АС має захищатися та контролюватися з використанням всіх можливих пристроїв захисту [4].

Також, важливою складовою забезпечення кібербезпеки АС це дотримуватися культури кіберзахисту. Директори організації мають впровадити культуру кіберзахисту в загальну культуру безпеки об’єкта [4]. Основа культури захисту – це те, що виконавець, який буде забезпечувати функціонування атомною станцією має чітко розуміти, що загрози реальні і потрібно впроваджувати всі можливі способи захисту. Ця культура впроваджується шляхом тренування фахівців на станції для їх розвитку в сфері кібербезпеки.

Оцінка культури кіберзахисту формує правила [4]:

- вимоги кібербезпеки задокументовані та зрозумілі для робітників;
- ведеться документація всіх дій використання інформаційних систем, складових цих систем та програмного забезпечення;
- дотримуватись заходів захисту – необхідність і робітники це усвідомлюють;
- використання систем, складових цих систем та програмного забезпечення впроваджує кіберзахист цих засобів відповідаючи базовим принципам та процедурам безпеки.

1.3 Види засобів кіберзахисту критичної інфраструктури

Для забезпечення кіберзахисту на об’єкті критичної інфраструктури були написані певні вимоги, які спираються на досвід країн ЄС та Сполучених Штатів Америки та пов’язані з міжнародними стандартами NIST, НАТО та ЄС з питань забезпечення кібербезпеки.

Засоби захисту повинні впроваджуватись та удосконалюватись на всіх стадіях життєвого циклу підприємства критичної інфраструктури. Керівник або власник підприємства, в свою чергу повинен проводити регулярні незалежні аудити інформаційної безпеки, а у випадку надзвичайних подій, наприклад, кібератак та кіберінцидентів, має проінформувати встановлені державні органи (Центральне управління СБУ або відповідний регіональний підрозділ СБУ та Державна служба спеціального зв’язку та захисту інформації України), які в свою чергу мають відреагувати на виклик та протидіяти зловмиснику.

Проведення незалежного аудиту в сфері кібербезпеки – це операція, яка проводиться незалежними фахівцями в сфері кібербезпеки та оцінює ступінь захищеності підприємства критичної інфраструктури на наявність можливих вразливостей та факторів, які здатні призвести до негативних наслідків [5].

Група експертів виконує сканування та тестування на можливість проникнення в систему об’єкта критичної інфраструктури; оцінює стійкість засобів захисту від методів соціальної інженерії (таким як фішинг та інші) [6]. Приділяється увага до існуючої документації на об’єкті, в якій вказані чіткі кроки в певних ситуаціях; чи відповідають вже впроваджені системи захисту міжнародним стандартам; до всіх виявлених кіберзагроз, які були спрямовані на підприємство в минулому. Всі ці кроки являють собою детальний аналіз всіх складових кіберзахисту [5].

Для проведення аудиту керівник об’єкта має надати доступ до всіх складових, які підлягають аудиту.

Такими складовими є [5]:

- документація з питань кібербезпеки (політика кібербезпеки, вимоги та накази з питань безпеки тощо);
- доступ до апаратної частини (сервери, робочі станції фахівців, периферія, мережеве обладнання);
- доступ до програмного частини (інформація про ПЗ, ОС встановлені на робочі станції та сервери);
- доступ до засобів захисту ІКС (налаштування засобів, виробник, дані про обслуговування).

Після ретельного аналізу зі сторони комісії виноситься висновок з характеристикою рівня захищеності на поточний час і з врахуванням рівнів ризику для об’єкта та можливими втратами. Маючи висновки комісії, власник або керівник може запровадити певні дії для запобігання тих чи інших проблем, в залежності від висновку після проведення аудиту [5].

Ще одним способом кіберзахисту – є використання антивірусних програмних засобів та брандмауерів.

Антивірусні програмні засоби мають використовуватись на об’єктах критичної інфраструктури для забезпечення безпеки на робочих станціях та серверах. За допомогою даного способу можна захиститись від шкідливого ПЗ, вірусу тощо. Антивірус здійснює постійне сканування і в разі виявлення підозрілого матеріалу – заблокує доступ до цього матеріалу [5].

Головна умова використання антивірусного програмного забезпечення – це те, що критична інфраструктура має використовувати тільки підтверджені та стандартизовані державними службами антивіруси [5].

Брандмауер або міжмережевий екран – це ще один спосіб забезпечення кіберзахисту в мережі. Його основна мета – це контролювати трафік, який надходить та виходить з мережі до робочих станцій та серверів [7]. На об’єктах критичної інфраструктури потрібно сегментувати мережу та після цього обмежити доступ між сегментами мережі за допомогою міжмережевих екранів [4]. Таким чином, мережеві пакети даних будуть підконтрольні і у випадку виявлення шкідливого пакету, його буде заблоковано міжмережевим екраном.

1.4 Криптографічні засоби захисту інформації на об’єктах критичної інфраструктури

Криптографічний захист інформації – це спосіб захисту інформації, при якому відкритий текст шифрується використовуючи різний алгоритм шифрування, наприклад, шифр Цезаря, для приховування і за допомогою певного ключа відкритий текст можна відновити у звичайний вид.

Криптографічні системи зазвичай можна класифікувати на основі таких трьох важливих характеристик [8]:

1) тип операцій з перетворення відкритого тексту в зашифрований;

2) число ключів, що використовуються;

3) метод обробки відкритого повідомлення.

Для криптографічного захисту інформації шифр має виконувати певні вимоги, наприклад, статистична безпека алгоритмів, проста процедура шифрування й

розшифрування інформації, надійність бази алгоритмів, незначна надмірність інформації за рахунок шифрування, нескладна реалізація [8].

Криптографічні засоби захисту розрізняються за типами, а саме [9]:

- апаратні засоби – це засоби захисту, криптографічна межа якого вказується периметром апаратного забезпечення;
- програмні засоби – криптографічна межа яких обмежується компонентами програмного забезпечення;
- вбудовані засоби;
- гібридні програмні засоби;
- гібридні вбудовані засоби.

Підприємство саме вибирає, які засоби криптографічного захисту потрібно впровадити. В залежності від цілей криптографічного захисту можна обрати засоби для шифрування інформації, засоби для виготовлення ключів даних, засоби для захисту від несанкціонованого доступу в системи підприємства, засоби для надання електронних довірчих послуг тощо [10].

В Україні на даний час стандартизовані певні криптографічні засоби захисту інформації, наприклад, «Калина» описаний в ДСТУ 7624:2014, алгоритм симетричного блокового перетворення; алгоритм криптографічного перетворення ГОСТ 28147-2009; FIPS-197; ітеративна криптографічна геш-функція ДСТУ 7564:2014; «Стрибог» описаний в ГОСТ 34.11-2018. Всі ці алгоритми захисту інформації рекомендовано використовувати на об’єкті критичної інфраструктури.

За допомогою методів захисту інформації, підприємство може захиститись від можливого вторгнення, викрадення, чи пошкодження спеціального обладнання, що може призвести до збою чи відключення цього обладнання, до збору конфіденційної інформації, за допомогою якої можна виявити слабкі місця для подальшого вторгнення або продати інформацію в Даркнеті, все залежить від мотивів та цілей нападника.

1.5 Забезпечення кіберзахисту на прикладі Рівненської АЕС, як об’єкта критичної інфраструктури

Рівненська АЕС – є одним з найбільших підприємством критичної інфраструктури і являється одним з найбільших в Україні. Відноситься до державного підприємства «НАЕК «Енергоатом» (Національна атомна енергогенеруюча компанія).

Щороку, підприємство виробляє близько 20 млрд кВт електроенергії, що становить 24% від виробництва атомними електростанціями або 13% від загального виробництва електроенергії в Україні. Таким чином, правильне та безупинне функціонування Рівненської АЕС це ключ успіху для компанії [11].

Для безпечного та безупинного функціонування підприємства на етапі його будівництва та в подальшому, створюється КСЗІ (Комплексна система захисту інформації або системи інформаційної безпеки з підтвердженою відповідністю), яка передбачається постановою Кабінету Міністрів України «Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури».

Захист інформації на такому підприємстві як АЕС являється дуже важливим завданням, так як АЕС являється об’єктом критичної інфраструктури і відіграє стратегічну роль для України.

Також, для захисту інформації, для несанкціонованого доступу в систему на Рівненський АЕС використовується спеціальне ПЗ (програмне забезпечення) «ЛОЗА».

Для шифрування на даному підприємстві критичної інфраструктури використовуються різні алгоритми хешування, наприклад, алгоритм SHA-512.

Функції хешування приймають на вхідні дані і виробляється дайджест. Дайджест – являє собою вихідні дані довільної довжини. SHA-512 – алгоритм дайджесту повідомлень. Він використовується для обчислення хеш – значення. Хеш-функція бере блок даних та повертає бітовий рядок фіксованого розміру (хешовані дані) [12].

Висновок за розділом 1

Підсумовуючи все вище сказане, АЕС як об’єкт критичної інфраструктури являється дуже важливим стратегічним об’єктом для держави і забезпечення безпеки інформації виступає одним з головних завдань для підприємства.

Сьогодні, реалізація та забезпечення кіберзахисту вимагає постійне покрашення вже існуючих правових, організаційних та технічних механізмів регулювання суспільних відносин, які виникають у інформаційній сфері. Для того, щоб виконати це завдання на практиці, необхідно розвивати кадровий потенціал в галузі кібербезпеки та розвиток національної галузі інформаційних технологій. Потрібно визначити об’єкт критичної інфраструктури, вирішити проблеми кіберзахисту на всіх етапах життєвого циклу підприємства, розробити різні методики модернізації та вдосконалення критичної інформаційної інфраструктури, далі потрібно систематизувати та покращувати нормативно-правові акти Кабміну та органів виконавчої влади.

Використовуючи всі можливі криптографічні та комплексні системи захисту (Лоза-1, алгоритми криптографічного перетворення ДСТУ ГОСТ 28147:2009, FIPS-197, ітеративні криптографічні геш-функції ДСТУ 7564:2014, SHA – 512, та «Стрибог» описаний в ГОСТ 34.11-2018), додаткові спеціальні програмні рішення, корпорація може забезпечити протидію зловмисним діям та захистити себе від кібератаки, таким чином, це призведе до успішної та ефективної роботи підприємства і як наслідок процвітання держави.

РОЗДІЛ 2
ІСНУЮЧІ ЗАХОДИ КІБЕРЗАХИСТУ ОБЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

2.1 Виявлення вразливостей ІКС на АЕС до атак та кіберзагроз

Щодня на об’єкти критичної інфраструктури України здійснюється десятки, інколи і сотні кібератак з різних точок світу, найпоширеніші кіберінциденти надходять з російської федерації.

В список найпоширеніших кібератак можна віднести [13]:

- DoS - атаки;
- DDoS - атаки;
- фішинг;
- поширення шкідливого програмного забезпечення.

DoS – атака (або «Відмова в обслуговуванні») це кібератака, ціль якої спричинити перенавантаження та порушення функціоналу систем, сервісів та іншого. Перенавантаження реалізовується шляхом направлення на ціль максимально великої кількості трафіку даних. DoS проводиться з одного хосту та направляються на певні системи та мережі [14].

До особливостей даної атаки можна віднести її помітність, так як переглянувши записи лог - файлів можна одразу виявити безліч направлених з одного хосту пакетів даних. Також, ще однією особливістю є те, що її можна з легкістю запобігти шляхом заблокуванням хосту, з якого надходять пакети даних адміністратором мережі, який аналізує весь трафік [15].

DoS стала популярною через свою легкість в реалізації та великим втратам для жертви. Сама атака не несе прямої загрози для сервера, але несе за собою фінансові втрати через серверне обслуговування та в разі відмови та можливу втрату прибутку через напад [14].

DDoS - атака (розподілена атака відмови в обслуговуванні) є різновидом DoS, але при цьому атака виконується з декількох хостів на одну систему або сервіс [14].

Під час реалізації даної атаки дуже складно виявити, що є її джерелом, тому що зловмисник використовує декілька зв'язаних між собою хостів чи ботів, які надсилають дані [16]. Зазвичай, атаки ведуться з вражених вірусами хостів звичайних користувачів, які не підозрюють, що стали зброєю хакера. Але нещодавно з'явились нові методи атак, за допомогою розумних гаджетів (чайників, кавоварок тощо). Оскільки вони мають доступ до мережі, то можуть використовуватись для атаки [17].

Всі ці хости, боти та інші інструменти будують ботнет – це єдина мережа, якою керує зловмисник зі свого головного комп'ютера, кількість таких пристроїв в цій мережі може сягати мільйонів. Така структура допомагає зловмиснику управляти всіма пристроями і координувати їх дії [15].

Державна служба спеціального зв'язку та захисту інформації України постійно бореться з даним типом атак, оскільки їх кількість за останній час збільшилась в рази та їх метою є об'єкти критичної інфраструктури.

Для захисту від даного типу атак потрібно запровадити фільтрацію всього трафіку, це допоможе відсортувати підозрілі пакети даних та заблокувати їх, використовувати балансувальник навантаження на системи – це пристрій, який при підозрілому трафіку сам виявить не навантажений сервер та перенаправить користувача на нього, автоматизація перевірки мережевого трафіку також допоможе своєчасно зупинити атаку. Також, потрібно розподіляти трафік за допомогою CDN (Content Delivery Network), що дозволить прискорити обробку даних та запитів за рахунок розподілення зберігання контенту [15].

Фішинг – це вид шахрайства, за допомогою якого зловмисник отримую доступ до конфіденційної інформації. Хакер за рахунок довірливості чи неуважності жертви, змушує її надати самій доступ до конфіденційної інформації [18].

Зловмисник може підробити email, який буде копією оригіналу і як наслідок, користувач введе свою інформацію, не підозрюючи, що надав свої дані хакеру [19]. Інший спосіб – це переадресація жертви на фішинговий сайт, який дуже схожий на

оригінальний. Фішингові повідомлення виконують таку ж саму функцію, як і email [18].

Для запобігання фішингу потрібно використовувати тільки перевірені сайти, постійно перевіряти повідомлення та email, які отримує користувач. Всі підозрілі посилання потрібно уникати та ні в якому разі не переходити за ними [20].

Поширення шкідливого програмного забезпечення – це ПЗ, запуск якого призводить до негативних наслідків для системи (блокування системи, крадіжка або шифрування даних, використання чужих конфіденційних даних в своїх цілях, використання систем для реалізації атак) [21].

Шкідливе програмне забезпечення буває різного типу, наприклад, backdoor, який надає віддалений доступ зловмиснику, троянській кінь чи хробак [22].

Для запобігання цієї атаки потрібно постійно робити резервні копії систем, що допоможе в випадку зараження системи відновитись до моменту, де вірус ще не зміг проникнути в систему. Потрібно запобігти запуску всіх підозрілих файлів в системі, так як запуска можу завдати негативних наслідків тощо [23].

Для виявлення вразливостей в ІКС на атомній станції слід дотримуватись таких етапів [4]:

1. Виявлення і документація потенційно можливих кіберзагроз і вразливостей кібербезпеки ІКС, всіх компонентів ІКС та ПЗ має проводитись під час кожного етапу життєвого циклу ІКС на АС [4].

2. Розробник програмних компонентів здійснюватиме всі необхідні заходи з виявлення потенційних загроз та захисту від несанкціонованого доступу до ПТК, ТЗА, а ЕО – до інформаційних та керуючих систем і їх компонентів (чи наявні/або відсутні замки та пломби на шафах, який стан сигналізації) [4].

3. Розробники засобів захисту оцінюватиме порядок та засоби контролю доступу користувачів до програмних комплексів, технічних засобів автоматизації, програмного забезпечення, а експлуатуюча організація в свою чергу до інформаційних систем, складових цих система та програмного забезпечення. Під час цієї перевірки можна виявити, що в всіх цих засобах захисту та захисних комплексах [4]:

- впроваджено методи автентифікації та авторизації користувачів в системи та забезпечено перевірку на анонімність доступу до всіх системи захисту;
- реалізовано процедуру надання доступу тільки до певного переліку функцій та конфіденційної інформації за принципом мінімальних привілеїв;
- зменшено до мінімуму шанс встановлення віддаленого доступу до складових і програмного забезпечення інформаційних систем захисту поза меж атомної станції та впроваджено захист від несанкціонованого доступу;
- реалізовано перевірку облікових записів користувачів на відсутність обхідних записів з найвищими привілеями;
- в разі чотирьох неправильних спроб авторизації користувачів, їх облікові записи підпадають блокуванню та перевірці, це зазначено в документації керування об’єкта про спробу отримання доступу до інформаційних систем, складових цих систем і спеціального програмного забезпечення;
- впроваджено певні вимоги до паролів для облікових записів користувачів;
- реалізовано етапи створення, модифікації та модернізації, перевірки та знищення облікового запису;
- встановлено правила перевірка доступу користувача, який зареєстрований в системі.

4. Розробники систем захисту мають здійснювати всі можливі дії з ідентифікації загроз і запобіганню несанкціонованих підключень, включаючи дистанційні, зовнішнього обладнання, (наприклад, сервісного обладнання, робочих станцій, принтерів та зовнішніх носіїв інформації) до інформаційних систем, їх складових та програмного забезпечення [4].

5. Всі дії з моніторингом та ідентифікацією загроз, оцінкою захисту локальної мережі має виконувати з заданою періодичністю організація, яка володіє об’єктом відповідно до цих Вимог використовуючи перевірки [4]:

- правильність визначення периметру кіберзахисту;
- правильність конфігурації мережевих пристроїв;
- впровадження засобів моніторингу, засобів безпеки та регулювання доступу до портів на мережевих пристроях;

- наявність або відсутність сегментації мережі;
- наявність брандмауерів (firewall) з метою поділу локальної мережі та перевірка стану підключень в обхід цих брандмауерів;
- наявність/відсутність демілітаризованої зони;
- використання процедури фільтрування пакетів даних, які надходять та виходять;
- правила розмежування доступу користувачів.

6. Розробники систем захисту мають оцінювати всі заходи та процедури, які реалізовують захист, в тому числі чи наявні або відсутні [4]:

- довірених фахівців, які беруть участь в забезпеченні кібербезпеки в організаційній структурі підприємства;
- документів з кібербезпеки;
- документація процедури бекапу та поновлення даних;
- порядку проведення оцінки кібербезпеки;
- етапи ідентифікації та авторизації користувача;
- документації з простою мережевою будовою;
- реалізація перевірки даних, які надходять та виходять;
- спостереження інцидентів.

7. Розробники мають оцінювати всі заходи та процедури для реалізації кібербезпеки створення програмних комплексів, технічних засобів, програмного забезпечення, а саме чи наявні або відсутні [4]:

- відповідальні фахівці, які впроваджують кібербезпеку на АС;
- документів з кібербезпеки, які описують етапи виготовлення програмних комплексів, технічних засобів і програмного забезпечення на підприємстві;
- локальна мережа сфери виготовлення, яка відокремлена від інших мереж розробників;
- системи кіберзахисту від несанкціонованого доступу, а саме, перевірки фахівців, які розробляють програмного забезпечення, технічних засобів та програмно-технічних комплексів);

- порядку управління секретною інформації;
- контроль користування зовнішніх носіїв інформації та інших пристроїв на підприємстві;
- вимог виконання оцінки кібербезпеки;
- виконання фіксації і виправлення знайдених інцидентів.

8. Всі результати, які були виявлені по вразливостям програмного забезпечення, технічних засобів та програмно-технічних комплексів мають документуватись розробниками у певному звіті і надалі враховуватись в планах захисту розробників [4].

9. Висновки, які включають знайдені ризики та вразливі місця інформаційних систем, складових цих систем та програмного забезпечення фіксуються в документах організацією та надається оцінка з кібербезпеки. При виявленні, що впроваджений захист являється неповним і досі наявні вразливі місця, експлуатуюча організація визначає додаткові засоби захисту, які компенсують наявні вразливості в інформаційних системах [4].

2.2 Забезпечення координації між кіберзахистом та функціями ІКС АС

Всі засоби забезпечення кібербезпеки, їх відмова і технічне обслуговування ніяк не матимуть негативного характеру (перешкоджання, затримка, зміна) на людино-машинний інтерфейс, функціонал інформаційних систем, який являється важливим для кібербезпеки станції, під час правильної роботи станції і в ситуаціях, які порушують нормальний стан об’єкта [4].

Також, мають забезпечуватись запобігання негативного впливу засобів захисту, які використовуються в певних інформаційних та керуючих системах. Реалізація захисту в ІКС виконується переважно за допомогою використання зовнішніх засобів кіберзахисту.

Розробники програмних комплексів захисту, технічних засобів автоматизації, програмного забезпечення мають аналізувати всі можливі чинники, які негативно

впливатимуть на системи і здатні порушити функціонал цих систем. Висновки після проведення

Результати проведеного аналізу та показані в ПТК, ТЗА, ПЗ заходи запобігання негативному впливу засобів кіберзахисту на функціонування та характеристики ІКС відображаються в плані кіберзахисту розробника [4].

В процесі випробування з кібербезпеки на майданчику, розробник підтверджуватиме відсутність всіх негативних характеристик, які впливають на функціонування та характеристики ІКС. Всі випробування та тести проводитимуться за програмою та методикою, погодженими Державною інспекцією ядерного регулювання України [4].

2.3 Оцінювання повноти та достатності заходів кіберзахисту ІКС

Для оцінки повноти та достатності заходів кіберзахисту інформаційних систем слід зазначити наступні кроки [4]:

1. Група осіб, яка створюється спеціально, має виконати оцінку повноти і достатності заходів захисту під час покращення або запровадження нових систем. До цієї групи входять представники організації (фахівці з експлуатації та обслуговування інформаційних систем на АС), розробники програмного забезпечення, технічних засобів та програмно-технічних комплексів [4].

ЕО реалізовує організацію та виконання первинного оцінювання відповідності повноти та достатності заходів захисту діючих систем, які вже в експлуатації на станції, у межах аналогічної окремої процедури та за допомогою ризик-інформованого підходу [4].

Оцінка повноти та достатності заходів захисту інформаційних систем на АС реалізовується заради підтвердження виконання певних заходів захисту від потенційно можливих загроз та атак. У разі виявлення недостатньо впроваджених заходів безпеки, потрібно визначити вимоги для додаткового встановлення заходів захисту [4].

2. Оцінка відповідності чи вистачає заходів захисту інформаційних та керуючих систем має виконуватись за допомогою методів для отримання інформації [4]:

огляд документів (політики безпеки, ПЗ та планів захисту інформаційних систем, звітів з оцінки кібербезпеки, навчальних матеріалів з захисту, ТД по інформаційним та керуючим системам, інвентарних списків технічних засобів, перевірки контролю доступу, мережевої архітектури, перевірок про інциденти та оцінка ризиків);

розмови з робітниками (адміністративне керівництво, оперативний і ремонтний персоналом, фахівці з кібербезпеки);

обстеження інформаційних та керуючих систем, їх складових та локальної мережі.

3. Оцінка чи відповідають передбачені у документації заходи захисту всім можливим вимогам проводитиметься під час аналізу всієї документації. Також, додатково треба оцінювати чи відповідає поточний стан кібербезпеки ідентифікованим загрозам та атакам [4].

4. Розмови з працівниками спрямовані на оцінку їх обізнаності з політиками і програмами захисту інформаційних та керуючих система станції, ефективності підготовки кадрів на рахунок кібербезпеки, сприйняття працівників загроз і ризиків, готовність до реагування на інциденти, розподілення обов’язків та відповідальності, ефективності культури кіберзахисту, заходів конфіденційності інформації [4].

5. Оцінка заходів кібербезпеки, чи реалізовані зони захисту, контроль доступу до інформаційних та керуючих систем, складових та програмних засобів, поточна мережева архітектура, перевірка та ТО інформаційних та керуючих систем атомної станції, управління конфігараціями, моніторинг та реєстрація інцидентів кібербезпеки – це все, що відбувається у процесі обстеження та перевірки [4].

6. Під час збору інформації проводиться оцінка [4]:

- політик, програм та планів захисту інформаційних та керуючих систем і звітів з їх виконання;
- порядку, обсягу і результатів аналізу загроз і їх можливих наслідків;

- використання диференційованого підходу для впровадження засобів захисту, визначення рівнів захисту;
- наявності оцінки ризиків і забезпечення відповідних заходів кіберзахисту.

7. У процесі оцінки відповідності всіх систем захисту інформаційних та керуючих систем на підприємстві виконується аналіз [4]:

- обізнаність працівників з політиками і ПЗ захисту інформаційних та керуючих систем станції, готовності працівників на рахунок забезпечення кібербезпеки і наявності відповідальних осіб, які мають забезпечувати захист;
- поділу обов'язків та прав доступу до систем;
- чи наявний інвентарний перелік всіх систем, їх складових, мережевого обладнання, програмних засобів, класифікація з кібербезпеки, відомостей про їх фізичне розміщення;
- виконання адміністративного, технічного і програмного захисту і моніторингу несанкціонованого доступу до систем, складових, мережевого обладнання, ПЗ і експлуатаційно-відновного резерву;
- в якому порядку використовуються випробувальні, налагоджувальні пристрої, портативні засоби та зовнішні носії даних у місцях експлуатації систем та складових;
- процедури усунення пошкоджених технічних засобів та знищення носіїв даних;
- обмеження прав доступу користувачам згідно з принципом найменших привілеїв;
- несанкціонованого доступу до інформаційних та керуючих систем, їх складових, програмного забезпечення та інформації через мережу, модеми, точки дротового/бездротового підключення, порти, незаблоковані технічні засоби автоматизації;
- виявлення вразливостей за рахунок проведення аналізів і тестів;
- чи достатньо реалізовано у системах заходів захисту відповідно планам кібербезпеки інформаційних та керуючих систем атомної станції;

- впровадження резервних заходів у разі, якщо важливі заходи захисту не можуть застосовуватись у межах конкретної системи;
- процедур впровадження та покращення систем, їх складових, покращення та встановлення нового програмного забезпечення і оцінка впливу цих змін на кібербезпеку;
- наявність в розробника ПТК, ПЗ, ТЗА систем менеджменту із забезпечення захисту, що стандартизовані розробниками;
- заходів впровадження захисту під час встановлення систем, і частин;
- програмних засобів та результатів тестування захисту програмних комплексів, технічних засобів, програмного забезпечення у розробників після виготовлення та тестування інформаційних систем на атомній станції;
- засобів, які реалізують захист інформаційних систем під час ТО;
- документація дій фахівців на виявлені інциденти кібербезпеки, враховуючи загрози ззовні та всередині організації.

8. Використовуючи ризико-інформований підхід для оцінки стану захисту на діючих інформаційних системах, організація має виконувати оцінку можливих ризиків для знаходження вразливих місць, які відносяться до даних систем, та встановлює всі можливі наслідки після успішної реалізації зловмисних дій. Всі заходи захисту реалізовуються на висновках після тестування можливих ризиків в інформаційних системах [4].

На етапі оцінки ризиків знаходяться та записуються певні поєднання загроз, вразливих місць та наслідків, після аналізування чого, реалізовуються додаткові засоби захисту, які допоможуть запобігти і пом’якшити можливі наслідки після атак на інформаційні системи [4].

Оцінка можливих ризиків інформаційних та керуючих система включає: [4]

- встановлення загальних умов та вимог використання інформаційних систем;
- знаходження та встановлення характеру загрози;
- моніторинг системи на наявність вразливих місць;
- оцінка можливостей створення шкідливих подій;
- оцінка впливу після реалізації шкідливих дій;

- оцінка рівнів можливих ризиків;
- встановлення рівнів припустимих ризиків;
- реалізація контрзаходів;
- встановлення конкретних ризиків і оцінка сумісного впливу цих ризиків на системи АС.

Правила для оцінки захисту інформаційних систем з використанням ризико-інформованого підходу встановлюються і конкретизуються в програмних засобах захисту і підтримуються в працездатному стані [4].

9. Після проведення оцінки та тестування кіберзахисту на об’єкті, створюється звіт з результатами і погоджується Державною інспекцією ядерного регулювання України.

На етапі оцінки та створення звіту реалізовується захист конфіденційних даних, а саме, використовується позначення, зберігання, передача та видалення матеріалів, записів, проєктів звіту та кінцевого висновку. Використовуються обмеження щодо використання електронних пристроїв і носіїв даних під час підготовки звіту [4].

2.4 Загальні проєктні заходи кіберзахисту ІКС

До загальних проєктних заходів кіберзахисту інформаційних та керуючих систем слід віднести [4]:

1. Створення програмно-технічних комплексів, технічних засобів автоматизації і ПЗ повинно передбачити можливі вразливості та реалізувати загальні та додаткові засоби захисту. На етапі проєктування беруться до уваги результати виявлення всіх можливих вразливих місць програмних комплексів, технічних засобів та програмного забезпечення [4].

2. Повинні виконуватись всі можливі заходи для зниження прихованих функцій у спеціальному ПЗ, ПТК і ТЗА. Обов’язково потрібно проводити детальні аналізи програмного коду власного виробництва і тести програмного забезпечення для підтвердження відсутності прихованих функцій в засобах та комплексах захисту [4].

3. Програмне забезпечення має пройти процедуру верифікації відповідно до всіх Вимог з ядерної та радіаційної безпеки до інформаційних і керуючих систем, які важливі для безпеки атомної станції. Під час етапу верифікації програмного забезпечення проводиться тестування реалізації у програмному забезпечені інформаційних систем і складових засобів захисту. Має перевірятись чи присутній негативний вплив засобів захисту для реалізації функцій інформаційних та керуючих засобів, які являються важливими для безпеки атомної станції [4].

4. Повинно забезпечуватись відсутність будь-якого впливу ПТК, ТЗА, ПЗ, що розробляються для використання в складі певної системи керування, на захист безпеки інших ІКС [4].

5. На етапі проектування засобів захисту і програмного забезпечення має враховуватись, що зв’язок між системами різних ступенів захисту відбувається з сторони інформаційних систем вищого ступеня захисту. У програмно-технічних комплексах, технічних засобах, програмному забезпеченні за допомогою проєктних заходів реалізовується мінімізація негативного впливу з боку інших інформаційних систем [4].

Проєктні заходи повинні визначатись з метою реалізації достатньої впевненості в тому, що кіберзахист засобів та комплексів безпеки, які створюються для реалізації в складі інформаційних та керуючих систем певного рівня захисту, не знижує свій функціонал через проведення шкідливих дій з боку інформаційних систем нижчого рівня захисту [4].

6. Обов’язково потрібно виконувати контроль та використовувати сигналізацію фізичного доступу до засобів захисту, зміни конфігурації цих засобів захисту тощо.

7. Засоби, які використовуються для мінімізації та зменшенню негативному впливу реалізуються на програмних комплексах, технічних засобах автоматизації, програмного забезпечення зі сторони спец пристроїв для тестів та ТО [4].

8. У програмно-технічних комплексах має мінімізуватись і обґрунтовуватись кількість точок доступу до локальної мережі.

9. Реалізовуються засоби захисту від несанкціонованого доступу до програмних комплексах, технічних засобах автоматизації, програмного забезпечення і мережевих пристроїв.

Впроваджуються необхідні системи, які обмежують доступ до програмованих елементів та їх складових.

10. Доступу користувача обмежується з урахуванням можливих наслідків ймовірних загроз, використовуючи принцип найменших привілеїв.

Доступ користувачів до засобів та комплексів захисту впроваджуються за допомогою технічного або програмного модулю автентифікації і авторизації. Тільки в разі успішної авторизації користувач зможе отримати доступ і можливість для корегування налаштувань у програмних комплексах, технічних засобах автоматизації та програмного забезпечення [4].

Людино-машинний інтерфейс (який використовується для експлуатації та ТО) має надавати доступ до програмного забезпечення лише після авторизації користувачів, використовуючи принцип найменших привілеїв.

Одночасно, перехоплення або змінення інформації, яка відображається використовуючи інтерфейс «людина-машина», яке спрямовується на запобігання чи затримку дій оператора, який виконує функції, які важливі для безпеки станції, унеможливлюється.

У програмному забезпеченні ІКС рівнів захисту К1, К2 використовується багатофакторна автентифікація, за допомогою технічних засобів на основі отримання конфіденційної інформації про знання (наприклад, пароль, код) і про особисті речі (наприклад, ключ, карта з вбудованим чипом). У програмному забезпеченні інформаційних система рівня кіберзахисту К3 використовують не менше одного з вказаних вище способів автентифікації [4].

11. Мають визначатись можливі напрями покращення ПЗ, які здатні негативно вплинути на виконання функцій систем захисту. На етапі верифікації виконується підтвердження здатності знаходження проведеної модернізації. У програмних комплексах, технічних засобах автоматизації використовуються засоби, які перевіряють правильність модернізації [4].

12. Програмні комплекси, технічні засоби автоматизації, програмне забезпечення розробляються з урахуванням всіх можливих вразливих місць інформаційних систем.

Для рішень захисту, які були розроблені раніше, потрібно використовувати параметри і конфігурація, які мінімізуватимуть вразливі місця інформаційних систем.

Програмні і технічні засоби і їх елементи повинні обиратись, конфігуруватись та налаштовуватись для мінімізації вразливості систем, до складу яких входять ці програмні комплекси та технічні засоби автоматизації [4].

13. На етапі проєктування конфігурації і налаштування параметрів програмних пристроїв мають виконуватись ефективні заходи захисту щодо [4]:

- керування доступом користувача до функціоналу ПЗ і до технічних засобів;
- передачі інформації в інформаційні системи з меншим рівнем захисту;
- відстеження модернізацій програмного забезпечення та налаштування програмних комплексів і технічних засобів автоматизації.

14. Під час тестування захисту програмного та технічного засобів в їх кінцевих варіантах налаштування показується наскільки ефективні засоби захисту чи відсутній будь-який негативний вплив на функціонал систем захисту, які реалізовують та підтримують ядерну та радіаційну безпеку [4].

Проведення тестів, які підтверджують чи достатні і коректні впроваджені у системах заходів захисту і виявлення потенційно можливих вразливостей захисту програмних комплексів, технічних засобів і програмного забезпечення повинні виконуватись під час випробувань захисту [4].

Випробування захисту програмних комплексів, технічних засобів автоматизації та програмного забезпечення виконуються за погодженими Державною інспекцією ядерного регулювання України вимогами та правилами.

15. Заходи захисту кібербезпеки, які неможливо інтегрувати в програмні комплекси, технічні засоби автоматизації та програмне забезпечення реалізуються в складі інформаційних та керуючих систем окремо. Використання і ТО окремих пристроїв виконуються за допомогою додаткових адміністративних заходів управління [4].

16. Інформація, яка стосуватиметься розробки, створення, реалізації і використання програмних комплексів, технічних засобів автоматизації та програмного забезпечення ідентифікується і при потребі, вказується як інформація, стосовно якої потрібно забезпечити певні організаційні заходи кіберзахисту від несанкціонованого доступу, викрадання, зміни чи видалення [4].

17. В програмних комплексах, технічних засобах та ПЗ повинні реалізовуватись проєктні заходи захисту, які сприяють запобіганню несанкціонованого віддаленого доступу і повного унеможливлення віддаленого доступу до систем поза меж атомної станції та із загальної мережі доступу [4].

Віддалений доступ до програмних комплексів, технічних засобів та програмного забезпечення рівнів кіберзахисту К1, К2, К3 реалізовується при умові авторизації та автентифікації користувача з передбачених проєктом робочих місць, які відносяться до такого ж чи вищого рівня кіберзахисту, що й відповідні засоби захисту [4].

В певних випадках може допускатись віддалений доступ до засобів рівнів захисту К1, К2, К3 з передбачених проєктом робочих місць, які відносяться до нижчого рівня кіберзахисту ніж відповідні програмні комплекси, технічні засоби та програмне забезпечення при виконання певних умов [4].

18. Заборона модифікації даних на носіях.

19. Для використання програмно-технічних комплексів і технічних засобів обов’язково має використовуватися сертифіковане антивірусне програмне забезпечення.

Для ПТК або ТЗА рівнів кіберзахисту К1, К2 застосовуються організаційні та програмно-технічні засоби антивірусного захисту без антивірусів сторонніх виробників. Для ПТК і ТЗА рівня кіберзахисту К3 застосовуються організаційні та програмно-технічні засоби антивірусного захисту або антивірусне ПЗ сторонньої розробки [4].

Застосовувати сторонні антивірусні продукти можна в випадку підтвердження відсутності будь-якого негативного впливу на програмне забезпечення, технічні та інші засоби інформаційних та керуючих систем, який може негативно вплинути і

спричинити порушення функціонування і зміну характеристик ІКС, компонентів та програмного забезпечення. Також, розробники сторонніх антивірусних продуктів на регулярній основі випускають оновлення антивірусних баз даних [24].

2.5 Загальні заходи забезпечення кіберзахисту в процесі експлуатації

До загальних заходів забезпечення кіберзахисту на об’єктах критичної інфраструктури в процесі експлуатації слід віднести [4]:

1. На об’єкті критичної інфраструктури, як атомна станція повинні реалізовуватись засоби захисту, які відокремлюють інформаційні та керуючі системи та їх компоненти різних рівнів захисту кібербезпеки [4].

2. Будь-яка модифікація ІКС має плануватися та виконуватись з урахуванням потенційних загроз з боку кібербезпеки [4].

3. Важливо мінімізуватись максимально кількість точок доступу до локальних мереж на станції.

4. Необхідно реалізувати заходи виявлення несанкціонованого входу і підключення до інформаційних та керуючих систем, їх складових та локальної мережі, з подальшим блокування цих несанкціонованих дій та введення всіх інших вимог. Дані дії реалізуються і забезпечують запобігання порушенню вимог ЯРБ [4].

Доступ до інформаційних та інших систем і локальної мережі суворо інспектується для втручання в роботу систем осіб, які не пройшли етап автентифікації [4].

Контроль даного процесу виконується завдяки впровадженню заходів технічного захисту кібербезпеки (наприклад, замків на персональних шафах, контролю фізичного доступу на об’єкті), програмних засобів, які обмежують та виявляють несанкціонований доступ і виконують відповідні організаційні заходи, які повинні встановлюватись відповідно до рівнів захисту певних ІКС та складових [4].

5. Необхідно впровадити процедуру ідентифікації та реєстрації постійних або тимчасових змін в сфері оновлення програмного забезпечення, побудови та комунікації інформаційних та керуючих систем, доступу та підключення додаткових

ліній передачі даних для апаратних пристроїв і технічного обслуговування. Це потрібно для виявлення змін, які можуть завдати негативний вплив на захист [4].

6. Відновлення працездатності систем на станції після атак та шкідливого впливу ззовні виконується відповідно встановленого порядку дій. Повинні реалізовуватися заходи, які мінімізуватимуть ймовірність того, що вказаний порядок відновлення буде вразливим для тієї ж кібератаки [4].

7. Кожна модифікація чи зміна систем, їх складових або програмної складової має виконуватись відповідно до порядку, які визначені у Вимогах до проведення модифікацій ядерних установок та порядку оцінки їх безпеки [4].

8. ЕО має здійснювати постійний моніторинг захисту інформаційних систем, складових цих систем і програмного забезпечення для того, щоб швидко виявити загрозу, порушення нормального функціоналу інформаційних систем, несанкціонований доступ або зміну та оперативну відреагувати. Всі результати спостереження архівуються та захищаються від знищення чи зміни. Також, використовується інтерфейс «людина-машина», який підтримує персонал в процесі спостереження кібербезпеки, знаходження, фіксації та сигналізації про загрози в усіх режимах роботи підприємства [4].

9. Необхідно реалізувати заходи захисту та запобігання створення обхідного шляху передачі інформації між ІС та компонентами ІС різного рівня захисту через обладнання та лінії передачі даних, які використовуються для контролю, технічного обслуговування та відновлення [4].

10. ТО інформаційних та керуючих систем включає засоби забезпечення захисту та передбачає [4]:

- регулярні та почергові тести на кожному каналі систем, який виведено в технічне обслуговування;
- перегляд програмних подій роботи ІКС;
- оцінка і огляд стану компонентів систем;
- моніторинг функціонування інформаційних систем в режимі реального часу;
- дії з ідентифікації, попередження і зменшення наслідків деградації компонентів;

- дії з перевірки, ремонту або заміни компонентів, які вийшли з ладу.

Заходи захисту, функція яких – це попередження реалізації в інформаційну систему або її складових, програмного коду та інформації, які здатні негативно вплинути на функціонал систем реалізуються під час проведення ТО.

Також, реалізовуються заходи захисту обладнання, які аналогічні до певних, які застосовуються до відповідних систем, з урахуванням рівня її захисту. Категорично заборонено підключати обладнання для ТО, якщо це не є необхідним або не проводяться відповідні дії з ТО [4].

Якщо потрібно виконати певні дії з ТО інформаційних систем і потрібно тимчасово вимкнути певні засоби забезпечення захисту, на час проведення цих дій, потрібно прийняти компенсуючі заходи захисту.

Після закінчення ТО потрібно виконати перевірку конфігурації програмного забезпечення та значень установок задля попередження їх несанкціонованих змін [4].

11. Всі дії фахівців на етапі експлуатації, обслуговування та випробування інформаційних та керуючих систем мають контролюватися згідно з регламентованими на АЕС процедурами [4].

12. При використанні будь-яких змінних носіїв даних під час експлуатації, ТО або випробувань має здійснюватися контроль їх вмісту перед під’єднанням до ІС для того, щоб запобігти внесення до ІС програмного коду або даних, які мають шкідливий вплив на виконання функцій інформаційних систем, і після від’єднання від ІКС для запобігання несанкціонованому копіюванню, модернізації чи видалення з систем даних [4].

13. Під час заміни певних елементів ІС в процесі модифікації, технічного обслуговування або ремонту потрібно забезпечити вилучення замінених елементів, даних і програмного забезпечення для запобігання використанню цієї інформації для підготовки та реалізації атак. Якщо неможливо вилучити дані та ПЗ із елемента ІКС, то тоді потрібно ці елементи знищити або зберігати з дотриманням відповідних заходів фізичного захисту, захисту кібербезпеки і захисту від несанкціонованого доступу [4].

Висновки за розділом 2

Забезпечення засобів захисту кібербезпеки на атомній електростанції є важливою частиною життєвого циклу об’єкта критичної інфраструктури.

Для забезпечення безпеки на підприємстві критичної інфраструктури потрібно проаналізувати всі ризики та виконати наступні задачі як:

- визначити загрози для безпеки;
- провести оцінку поточної ситуації з захищеністю на об’єкті;
- розробити та виконувати певні вимоги щодо безпеки інформаційних та інших систем на АС;
- реалізувати всі розроблені засоби захисту;
- підготувати обізнаний персонал для роботи з реалізованими технологіями;
- здійснювати безперервний моніторинг кіберзахисту;
- регулярно проводити планове технічне обслуговування засобів захисту, їх складових, модернізацію системи захисту.

Також, потрібно забезпечити фізичний захист певних складових підприємства, наприклад, серверну кімнату чи електричні шафи тощо. Обмеження доступу до локальної мережі позитивно вплине на цілісність кібербезпеки. Постійний моніторинг трафіку, який надходить до ІКС, ПТК та інших систем може забезпечити своєчасну зупинку шкідливих дій та їх наслідків для функціонування засобів захисту.

Усі створені та реалізовані програмно-технічні комплекси, технічні засоби автоматизації та програмне забезпечення повинні передбачати можливі вразливості та вжити загальні та резервні системи захисту. Всі засоби захисту проходять процес верифікації згідно певних вимог в сфері захисту кібербезпеки на об’єкті критичної інфраструктури. Під час цієї операції відбувається тестування та обстеження систем на різні дефекти, які негативно впливатимуть на функціонал.

РОЗДІЛ 3
ПРОГРАМНІ ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ

3.1 «ЛОЗА – 1» як засіб забезпечення кіберзахисту на АЕС

ЛОЗА - 1 – це спеціально розроблений комплекс програмних засобів, який використовують для захисту від несанкціонованого доступу інформації на підприємстві, яка міститься в текстових документах та електронних таблицях [25].

Система може забезпечувати захист будь - яких інших даних – на рівні папок операційної системи для даних на жорсткому диску, та на рівні розділу диска – для даних на зовнішніх дисках [26].

Дана система захисту інформації містить засоби, які необхідні для побудови КСЗІ (комплексної системи захисту інформації) в автоматизованих системах.

Лоза – 1 може надавати послуги в безпеці які зазначені на рис. 3.1 та 3.2 [25].

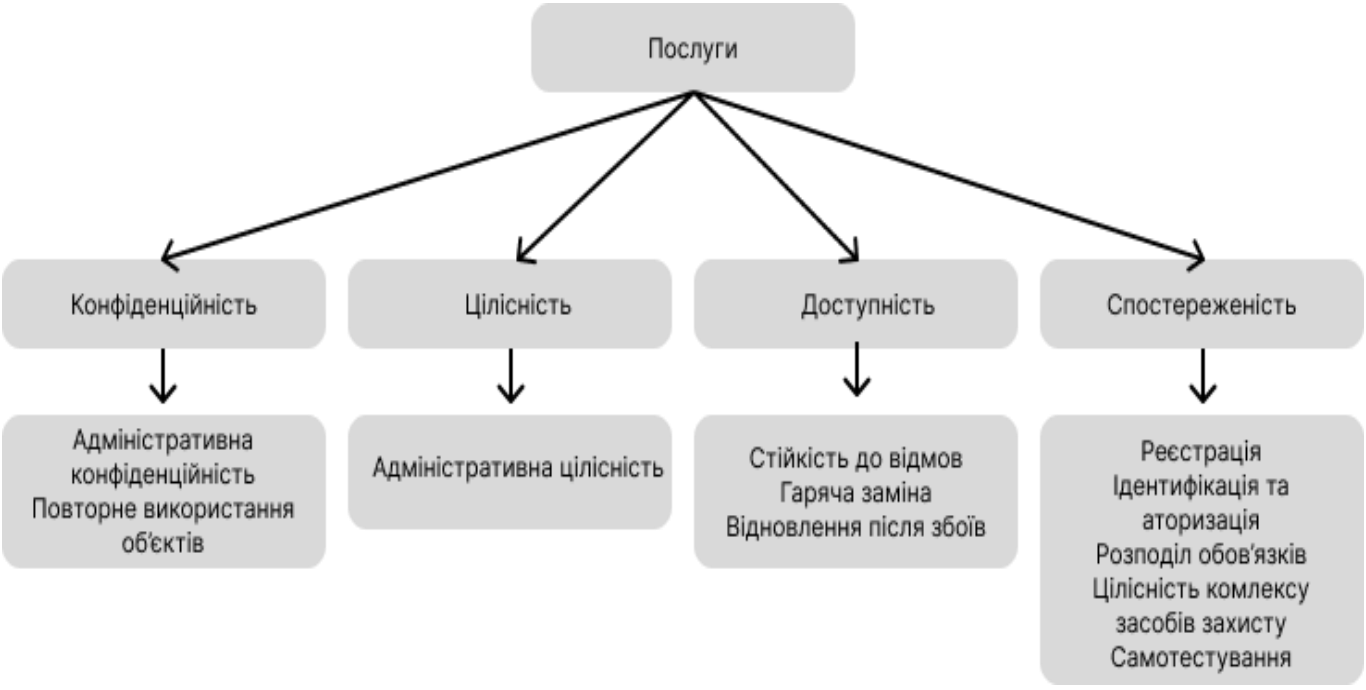

Рисунок 3.1 – Профіль системи ЛОЗА-1 "Підвищена безпека"

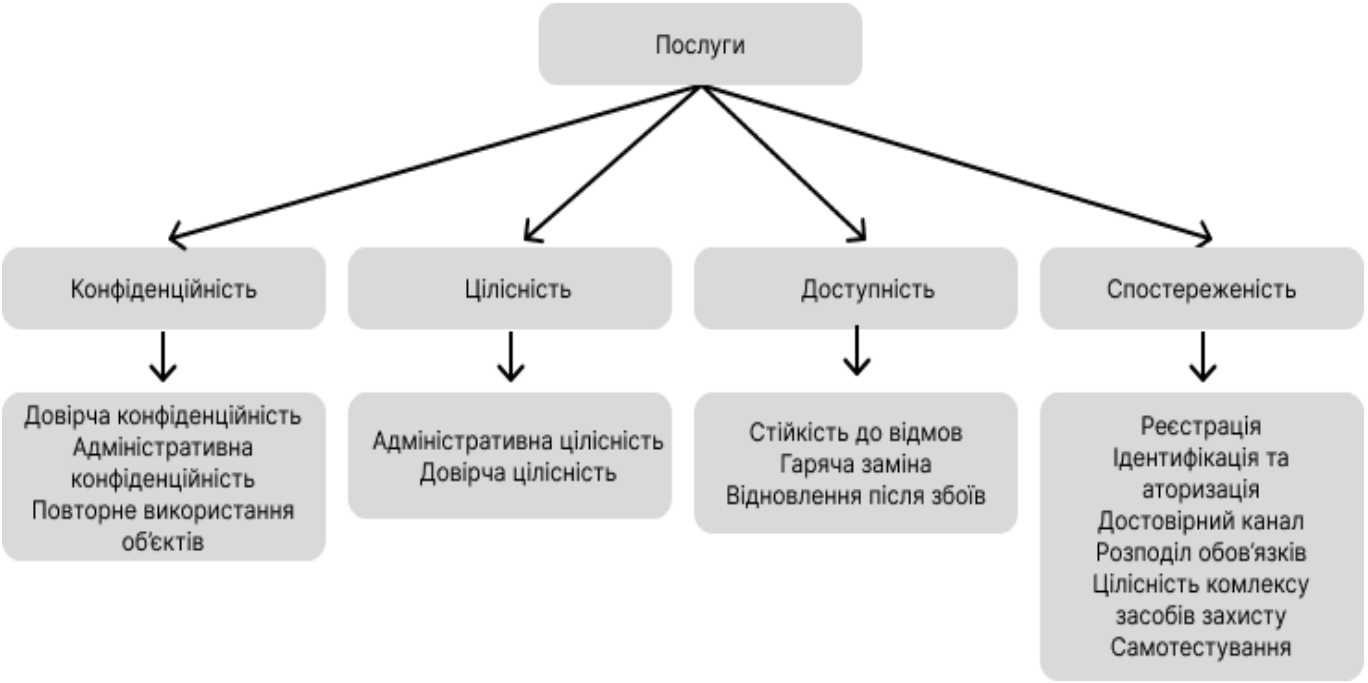

Рисунок 3.2 – Профіль системи ЛОЗА-1 "Стандартна безпека"

Дане спеціальне програмне рішення використовується на всіх популярних і всім відомим ОС (Операційних системах) таких як: Microsoft Windows 7 (32bit 64bit) Microsoft Windows 8.1 (32bit 64bit, Microsoft Windows Server 2008 R2 (64bit), Microsoft Windows Server 2012 R2 (64bit), Microsoft Windows Server 2016 (64bit), Microsoft Windows Server 2019 (64bit) та Microsoft Windows 10 (32bit 64bit) [26].

В Україні окрім «ЛОЗА – 1», як програмний комплекс захисту інформації використовують «ГРИФ», який має 4 версії [27]. Даний програмний комплекс використовується для захисту інформації з обмеженим доступом, яка зберігається в інформаційних системах на підприємствах критичної інфраструктури [28, 29].

«ЛОЗА – 1» використовує метод двофакторної аутентифікації користувачів в систему для підвищення безпеки. Двофакторна аутентифікація – це використання користувачам систем двох доказів особистості, при підтверджені яких можна отримати доступ до системи [30].

Використовуючи диск, флеш накопичувачу, запис інформації в базу даних та через внутрішню пам'ять комп'ютера. Всі ці способи мають свої недоліки, які можуть негативно вплинути на процес авторизації користувачів в систему.

Зовнішній диск має великі габаритні розміри, схильний до фізичного впливу та пошкоджень, таким чином, він проявляє себе з слабкого боку. Флеш-накопичувач має невеликі габаритні розміри, що являється плюсом, але він, як і зовнішній диск, має періодично проходити перевірки на змогу використання в певних програмних засобах, тобто, чи не призведе використання флеш-носія та зовнішнього диску до негативних наслідків для функціонування програмних засобів. Запис даних користувачів в базу даних та в внутрішню пам'ять комп’ютера – це зручний спосіб авторизації, але його недолік, це змога системного адміністратора без відома користувача заволодіти конфіденційною інформацією (логін, пароль) та здійснити несанкціонований вхід в систему з ціллю викрадення, модифікації чи знищення інформації. Таким чином, для запобіганню даних вразливих місць на етапі авторизації програмного забезпечення «ЛОЗА - 1» було запропоновано програмний модуль захисту інформації для авторизації в системі.

3.2 Розробка криптографічного захисту інформації з використанням двофакторної аутентифікації

Для забезпечення кіберзахисту систем на об’єктах критичної інфраструктури можна реалізувати модуль захисту, який використовує двофакторну аутентифікацію, яка дозволить захистити конфіденційні дані в системах підприємства.

Дане програмне рішення дозволить вирішити мінуси в способах авторизації програмного засобу «ЛОЗА – 1» завдяки двофакторній аутентифікації через надсилання коду [31] в сторонньому програмному застосунку та завдяки криптографічному алгоритму ДСТУ ГОСТ 28147:2009, який було прийнято як національний стандарт в Україні [32].

Даний алгоритм захисту був розроблений в 1987 році і використовувався як стандарт шифрування інформації в СРСР. В 2009 році він був стандартизований в Україні і отримав назву ДСТУ ГОСТ 28147:2009 [33].

ГОСТ 28147:2009 являється стандартом симетричного шифрування. Також, так як і DES [34], цей шифр – блоковий, де інформація шифрується, використовуючи

схему Фейстеля [35] шістдесяти чотирьох бітними блоками з використанням 256-бітного ключа шифрування [36]. А також, в шифрі реалізовано 32 раунди перетворень [37].

Структура шифру поділяється на [38]:

- основний крок – це перелік дії, які реалізовуються в кожному базовому циклі;
- базові цикли («32-З», «32-Р», «16-З»,) – різняться числом повторів основного кроку і порядком використання елементів ключа. Цифри 32 чи 16 – це кількість повторів основного кроку, а букви З і Р позначають різновид використання елементу ключа.
- режими роботи – це певні методи, які запроваджують криптостійкість, та які беруть результати шифрування попередніх блоків для шифрування наступних.

В криптографічному алгоритмі використовується різні режими, а саме [39]:

- проста заміна;
- гамування;
- гамування з зворотнім зв’язком;
- обчислення імітовставки.

Основні переваги ДСТУ ГОСТ 28147:2009 [40]:

- ефективна реалізація і звідси висока швидкодія.
- безперспективність атак перебору;
- використання захисту від нав'язування помилкових даних (вироблення імітовставки).

Таким чином, даний алгоритм шифрування являється дуже доречним для використання і для забезпечення захисту даних користувача.

Опис програми: криптографічний модуль містить вкладку реєстрації користувача в систему (рис. 3.3 – 3.4), вікно про успішну реєстрацію (рис. 3.5), вкладку входу в систему (рис. 3.6 – 3.7) вікно для отримання коду (рис. 3.8), яке надсилається користувачу через сторонній додаток (рис. 3.9) та інформаційне вікно (рис. 3.10), яке інформує користувача про успішний вхід.

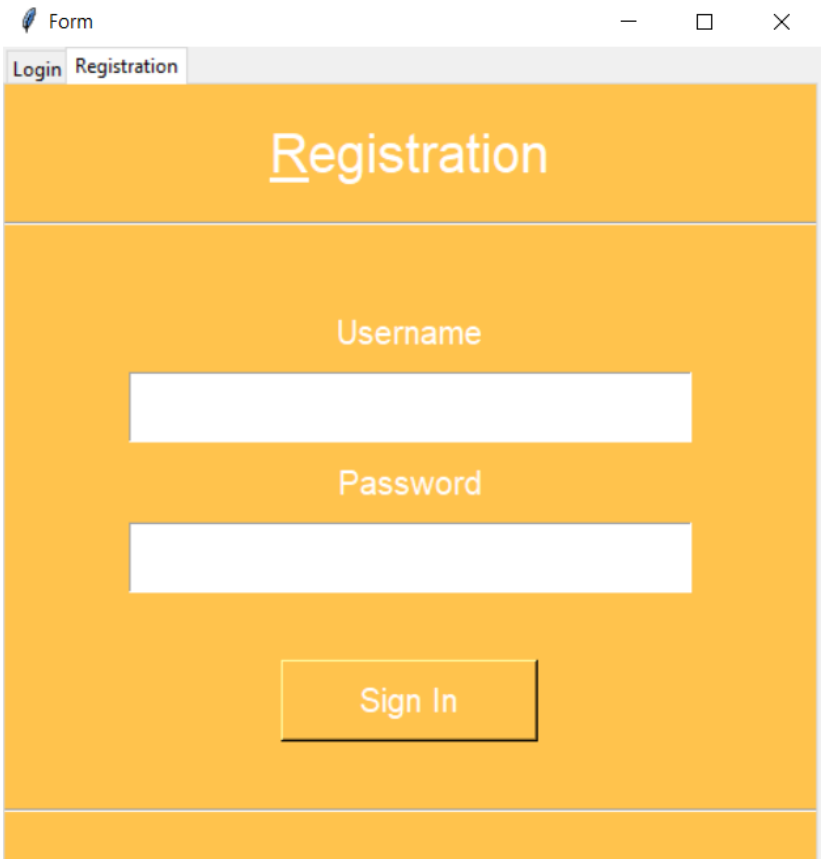

Рисунок 3.3. Вікно реєстрації користувача в систему

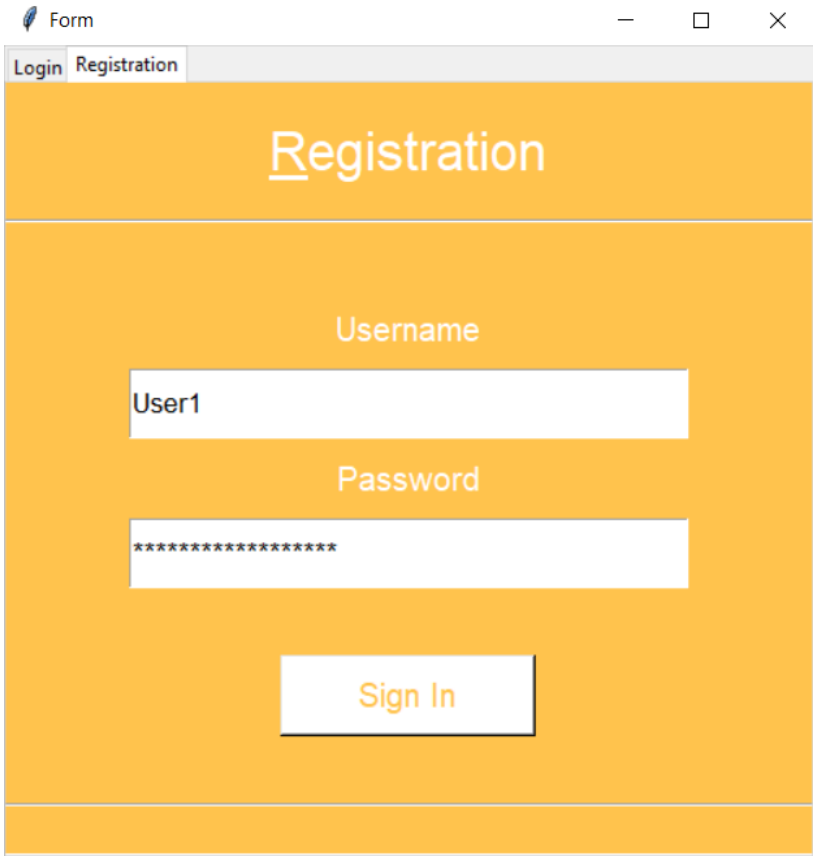

Рисунок 3.4. Процес реєстрації користувача в системі

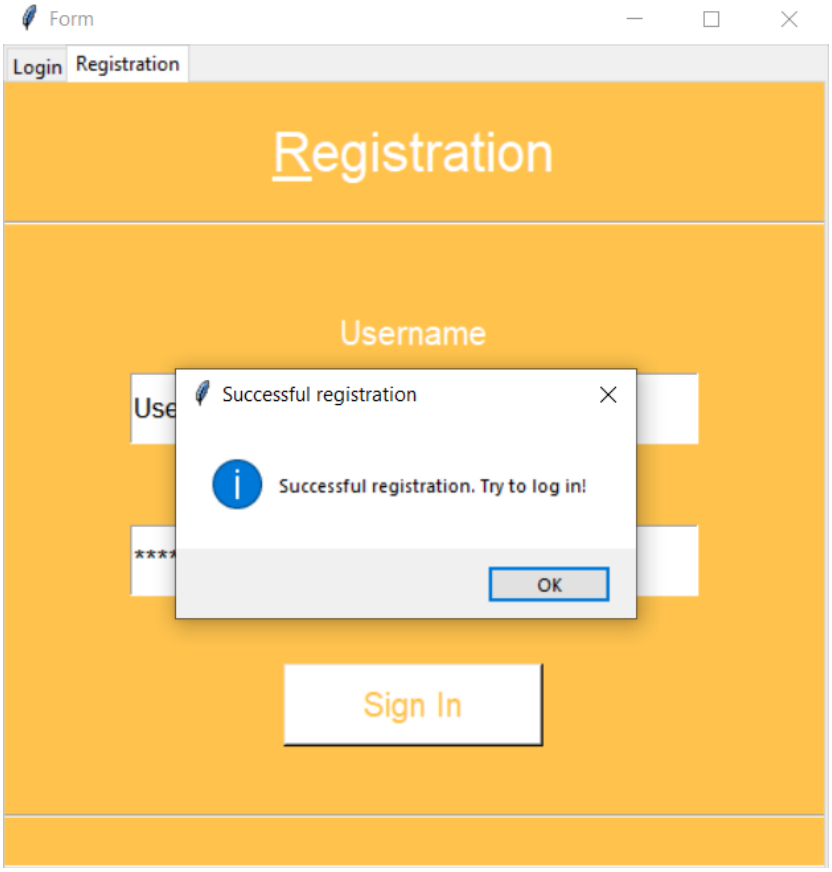

Рисунок 3.5. Успішна реєстрація користувача

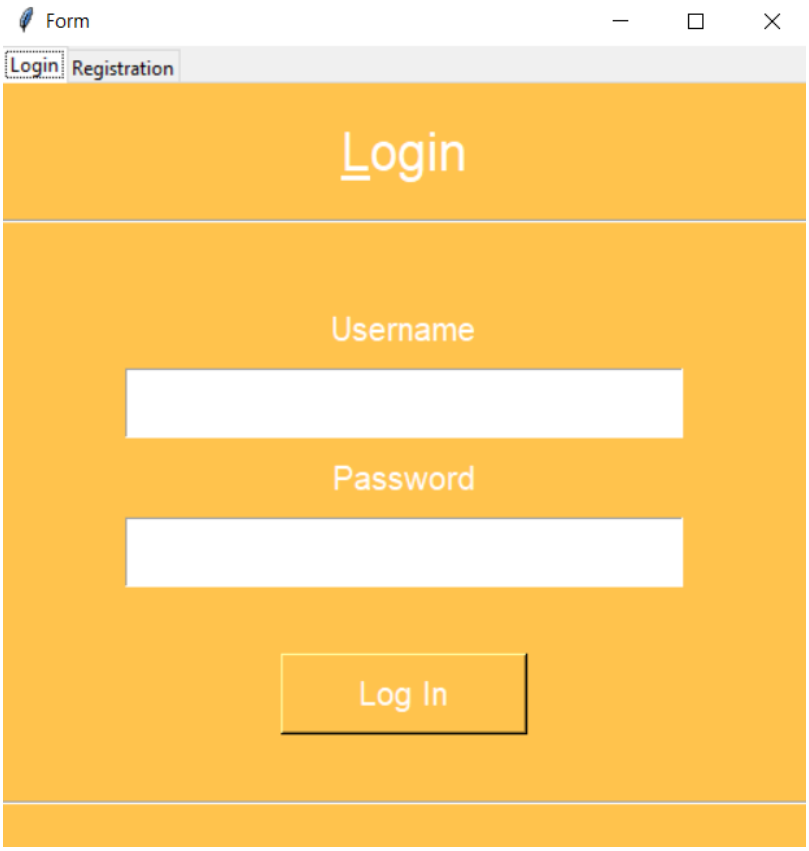

Рисунок 3.6 – Вікно авторизації користувача в системі

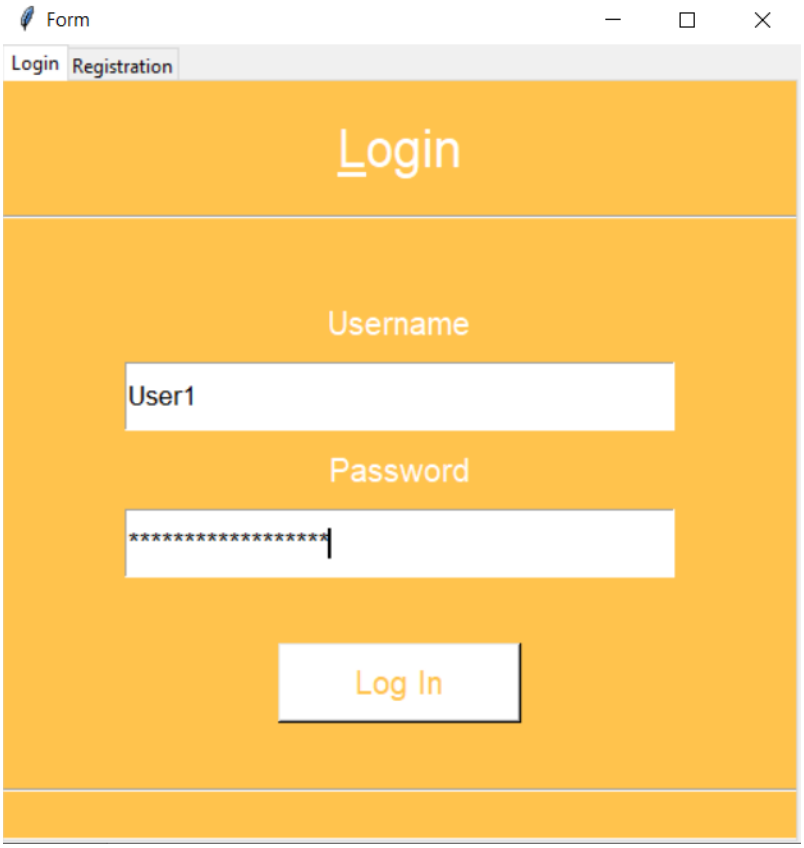

Рисунок 3.7 – Авторизація користувача

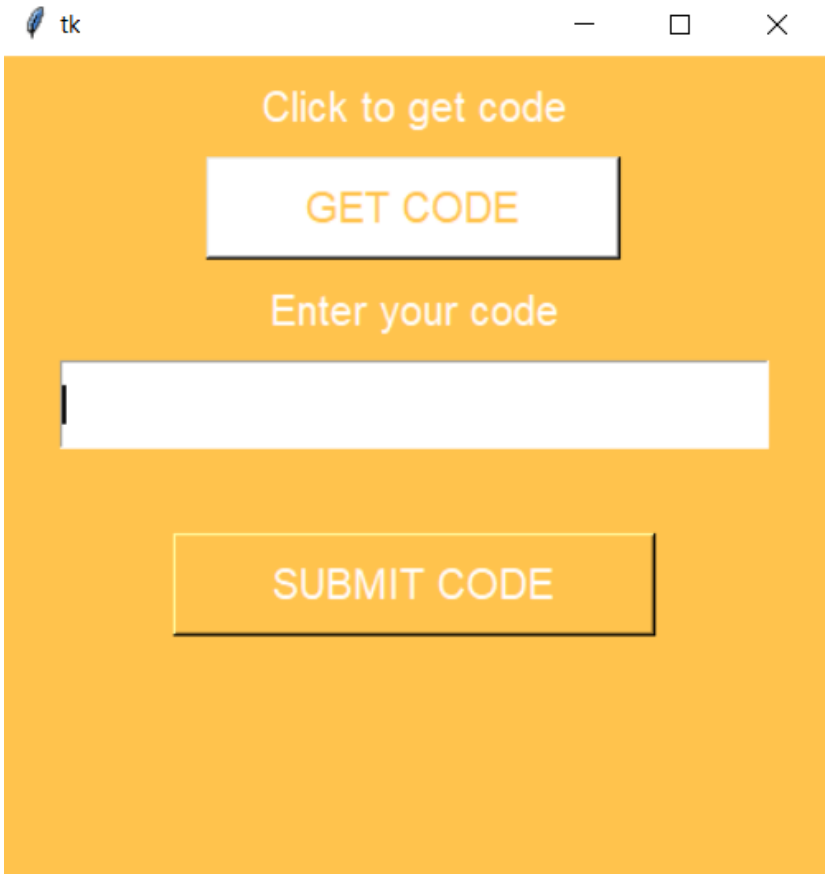

Рисунок 3.8 – Отримання коду безпеки

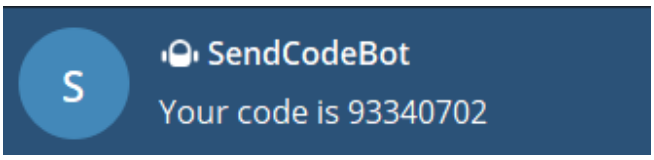

Рисунок 3.9 – Код безпеки для двофакторної авторизації

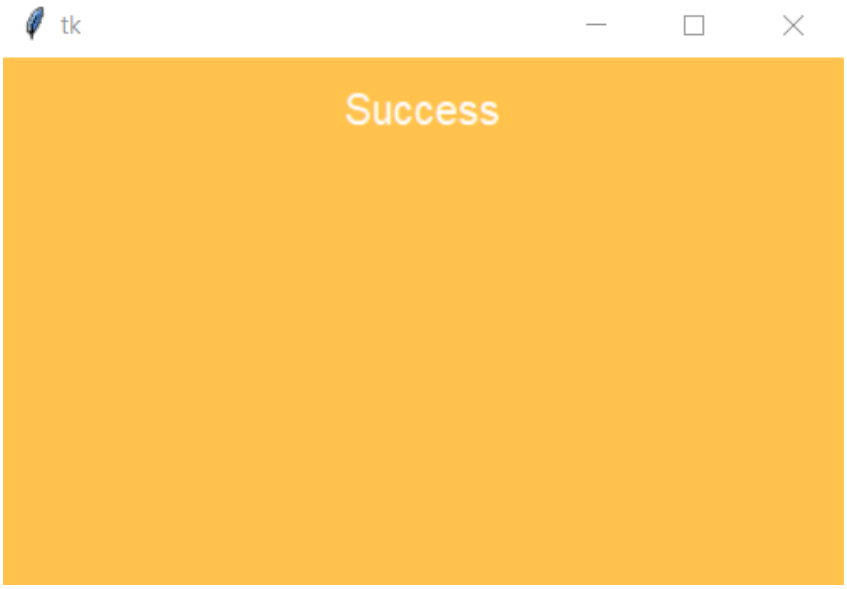

Рисунок 3.10 – Успішна авторизація користувача

Всі дані введені користувачем зберігаються в базі даних (логін та пароль). Після успішної реєстрації користувач переходить на іншу вкладку входу в систему. При успішному вході в систему користувач отримує можливість отримати код для двофакторної аутентифікації. Код надсилається користувачу в сторонній додаток і таким чином, користувач може увійти в систему після введення правильного коду.

Функція кнопки «Зареєструватись» в вкладці реєстрації successful_signin(). В даній функції створюється sql – запит в базу даних, куди записуються логін та пароль користувача. Пароль перетворюється в двійкову систему числення використовуючи функцію text_to_bits(), після чого пароль користувача передається у функцію шифрування алгоритму ДСТУ ГОСТ 28147:2009 zashifr_zamena() – режим шифрування простої заміни. Функція zashifr_zamena(text, key) на вході налічує ключ для шифрування та пароль в двійковому форматі. Цикл for x in range(8): keys.append(key[x*32:(x+1)*32]), key = keys розбиває весь ключ на 8 підключів. left_side = block_data[:32] і right_side = block_data[32:] – це блок, який ділиться на

праву та ліву частини. Цикл for i in range(32): - 32 раунди самого алгоритму шифрування, де викликається функція шифрування самого блоку, куди передається відповідний ключ ashifr_block_data(right_side, key[i % 8]). left_side, right_side = right_side, left_side використовуються для зміни місцями правої та лівої частини в кінці кожного раунду шифрування. Строка allCodedPassword += left_side+right_side – це додавання результату шифрування блоку в змінну. А строка codedInSymb += codedBinInCodedSymbols(allCodedPassword) являється перетворенням результату з двійкового формату в символи. Функція шифрування блоку zashifr_block_data(block, k), яка викликається в функції zashifr_zamena(). Операція ксор блоку і ключа за модулем 2 використовується в строці коду block = xor32(block, k). Цикл for i in range(8): blocks.append(zamina_s_table(s_table[i], block[i*4:(i+1)*4])) – заміна блоків на S – блоки. Після чого відбувається циклічний зсув на 11 біт вліво за допомогою строки block = zsuv(block, 11).

Функція successful_login() це функція для кнопки «ЛОГІН». Використовуючи sql – запит вона зчитує інформацію з базт даних і порівнює її з тою, яку вводив користувач при реєстрації. Якщо інформація відповідає один одній, в цьому випадку відкривається нове вікно, яке виконує запит коду для авторизації. Для порівняння даних, які ввів користувач з даними в базі даних потрібно виконати шифрування введеного паролю, який перетворюється в двійковий формат числення з використанням функції text_to_bits() і виконується шифрування за допомогою функції zashifr_zamena(). Далі цей шифрований пароль порівнюється з паролем, яким знаходиться в базі даних. При збігу цих двох паролів, тоді створюється нова форма за допомогою функції secondfactor().

Функція secondfactor() – це функція, яка створює вікно де потрібно отримати код для двофакторної автентифікації. В даному вікні кнопка «GET CODE» при натисканні виконується функція send_message(). Дана функція генерує випадковий код з шести цифр – randint(10000000, 99999999). За допомогою додаткового ПЗ «Телеграм» використовуючи чат-бот надсилаються дані користувачу використовуючи строки r = requests.post(url, data={ "chat_id": id, "text": text}). Після чого надісланий код записується в базу даних використовуючи sql – запит: sql =

"UPDATE data SET code=? WHERE id=?" db_c.execute(sql, (code, id_db)). Після чого користувач вводить надісланий код для двофакторної авторизації і натискає кнопку «SUBMIT CODE». При натисканні викликається функція checkCode(), яка використовуючи sql – запит і дані з бази даних перевіряє чи співпадає введений код з кодом в базі даних. Якщо результат перевірки позитивний – створюється нове вікно з успішним входом користувача та надписом «Success».

Загальну блок-схему програми можна побачити на рис. 3.11

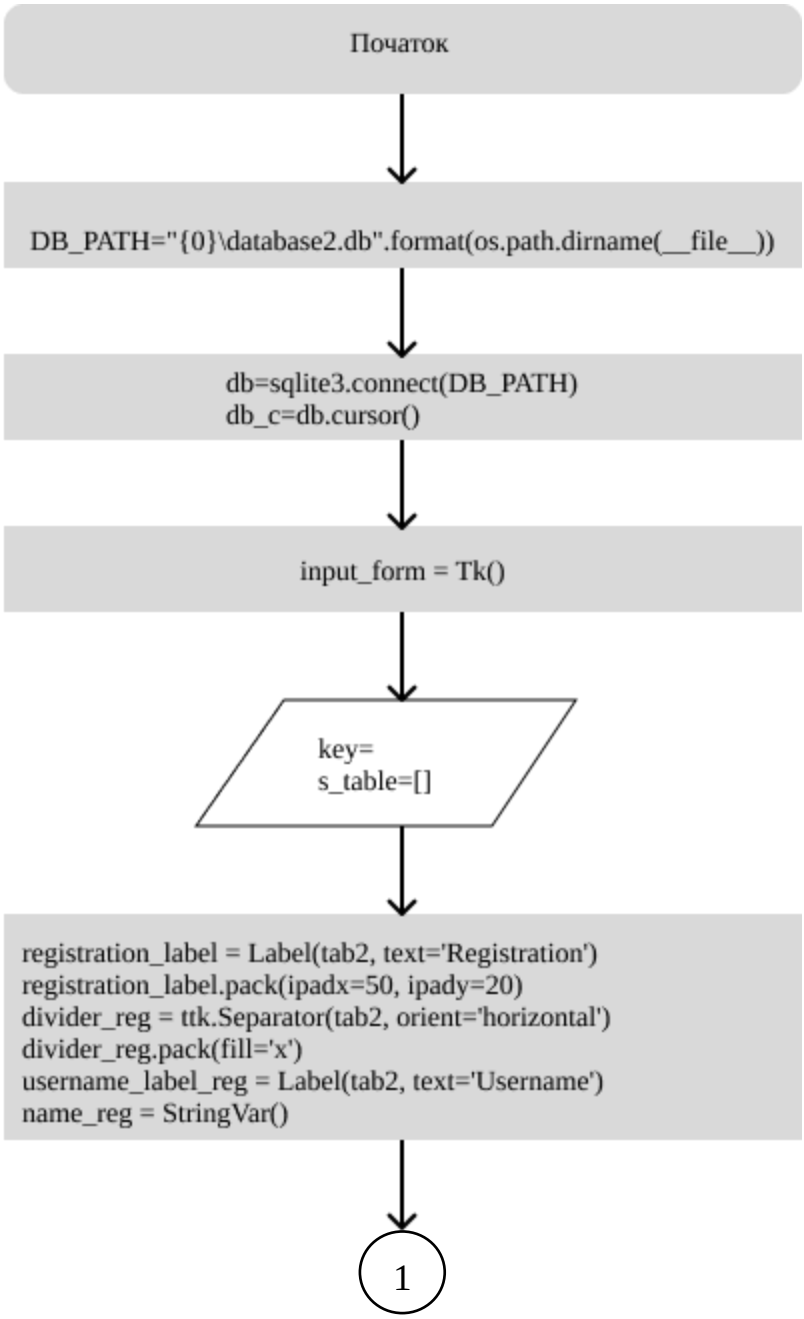

Рисунок 3.11 – Загальний опис програми

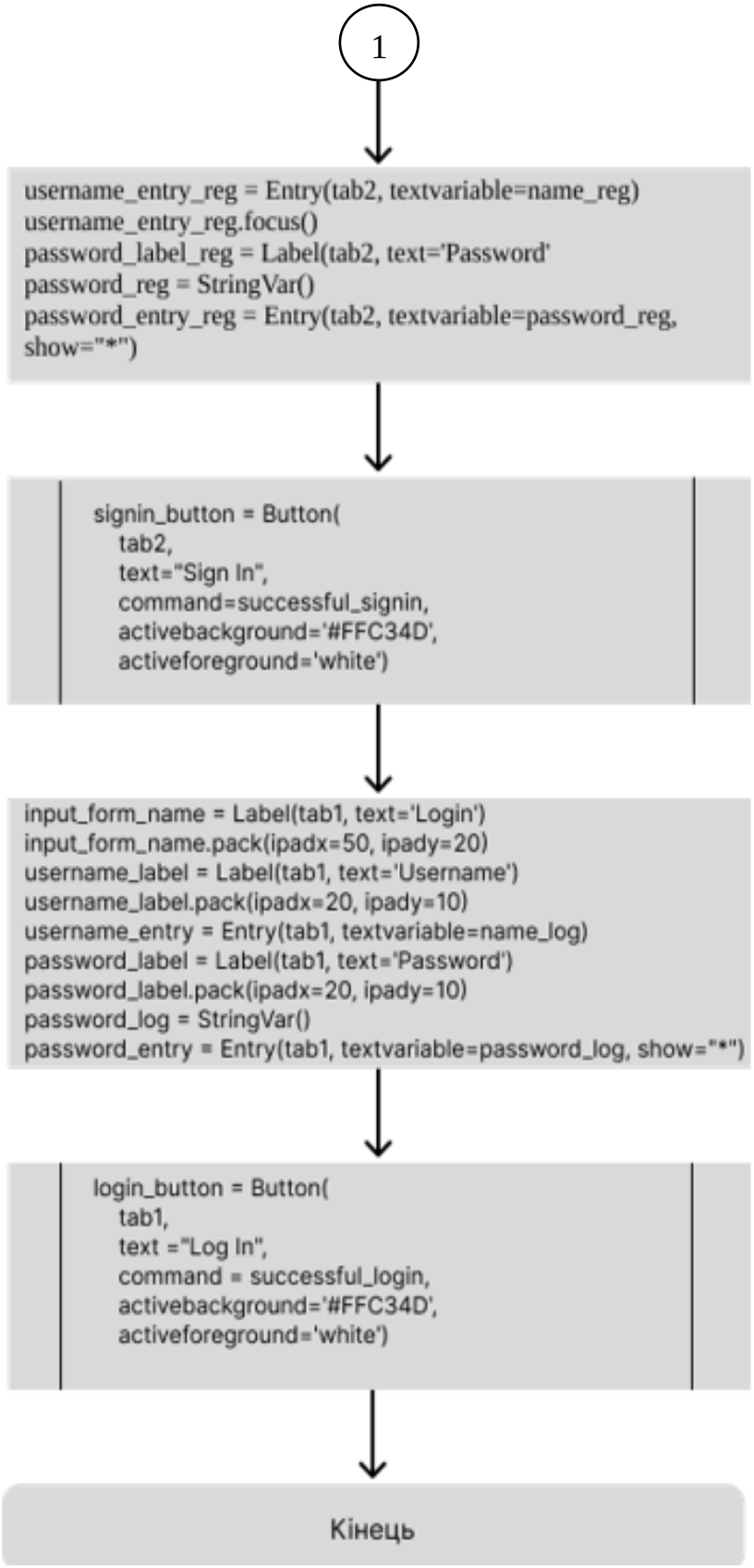

Рисунок 3.11 (продовження) – Загальний опис програми

Блок-схему для кнопки «Login» можна побачити на рис. 3.12

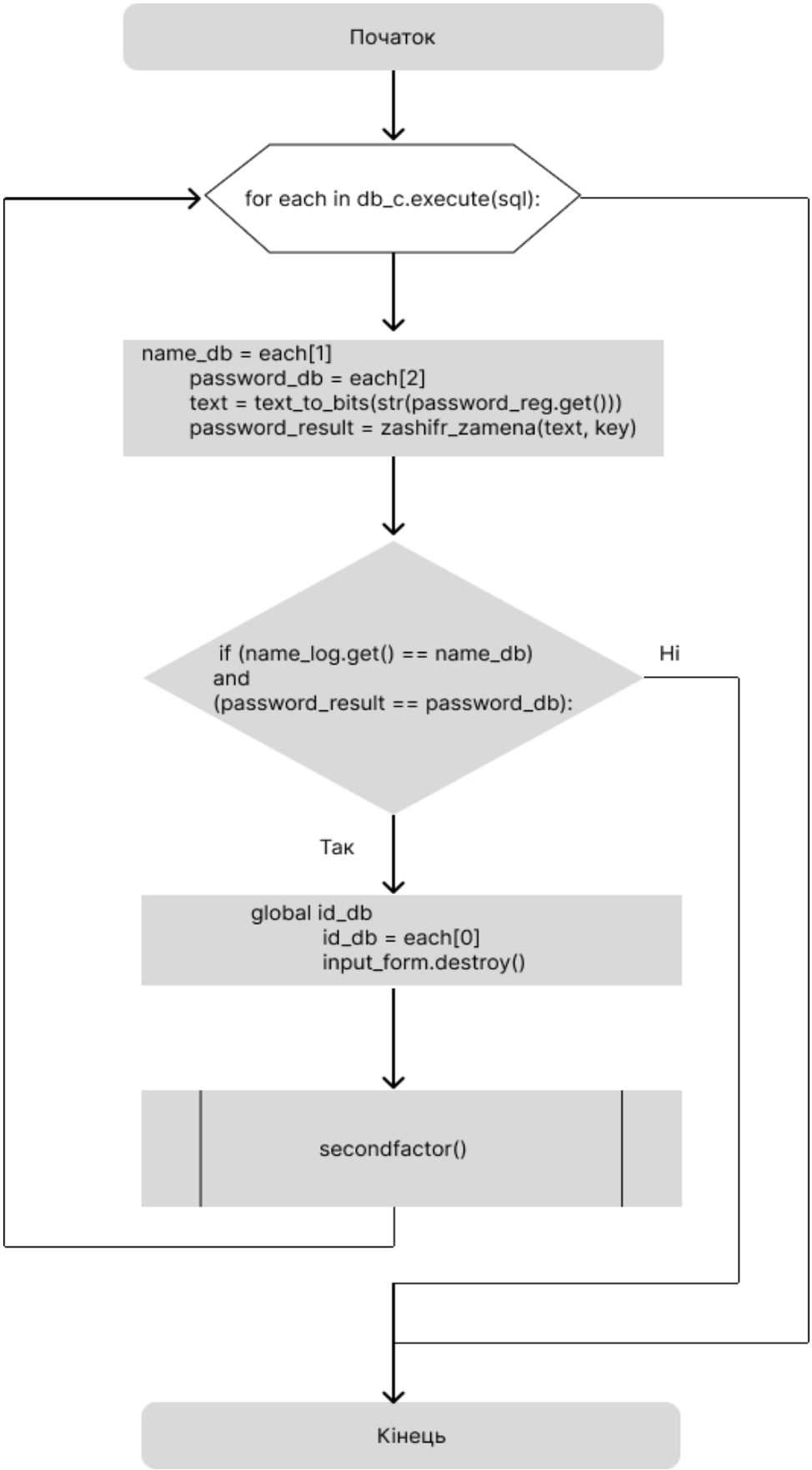

Рисунок 3.12 – Опис кнопки «Login»

Блок-схему для функції шифрування zashifr_zam() показано на рис. 3.13

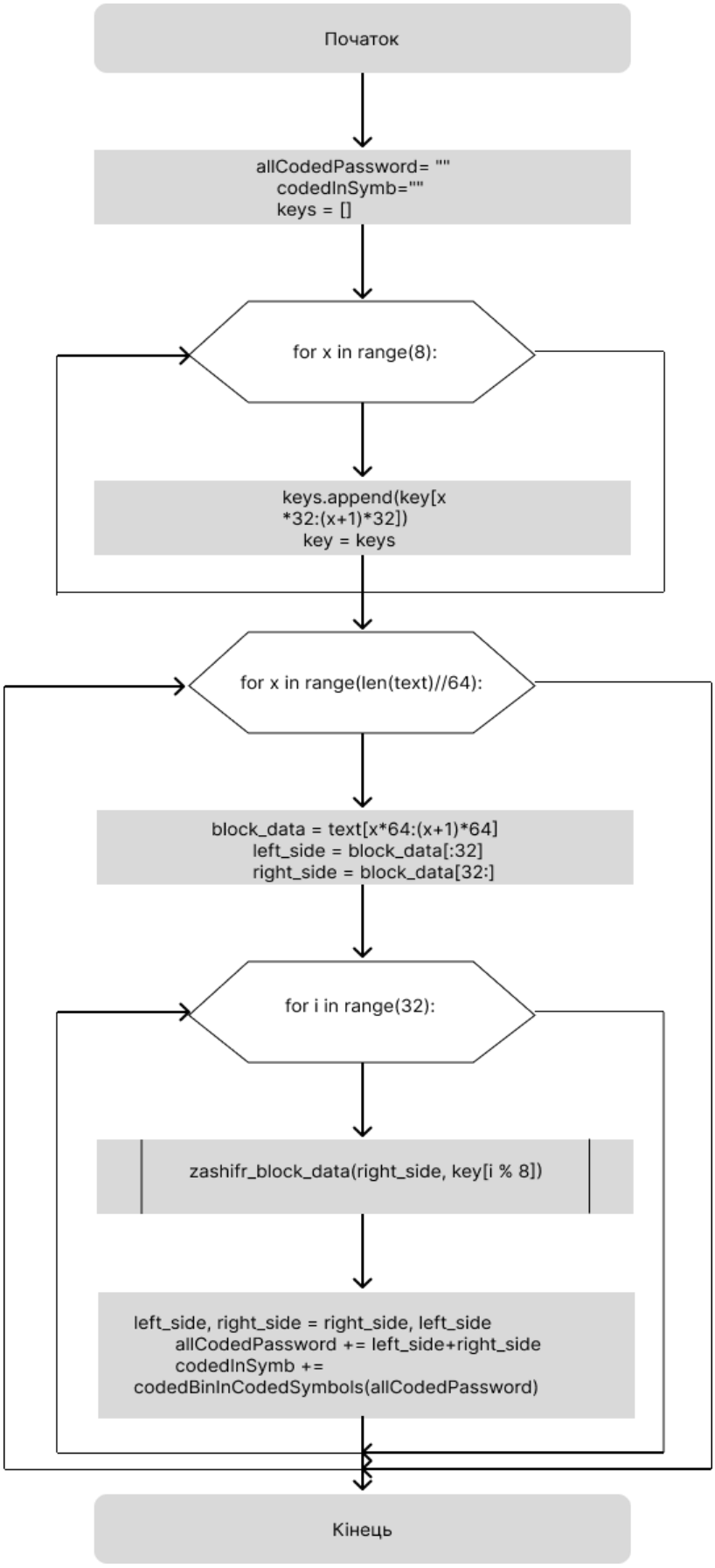

Рисунок 3.13 – Схема для функції шифрування zashifr_zam()

Блок-схема функції zashifr_block_data() для функції шифрування zashifr_zamena() показано на рис. 3.14

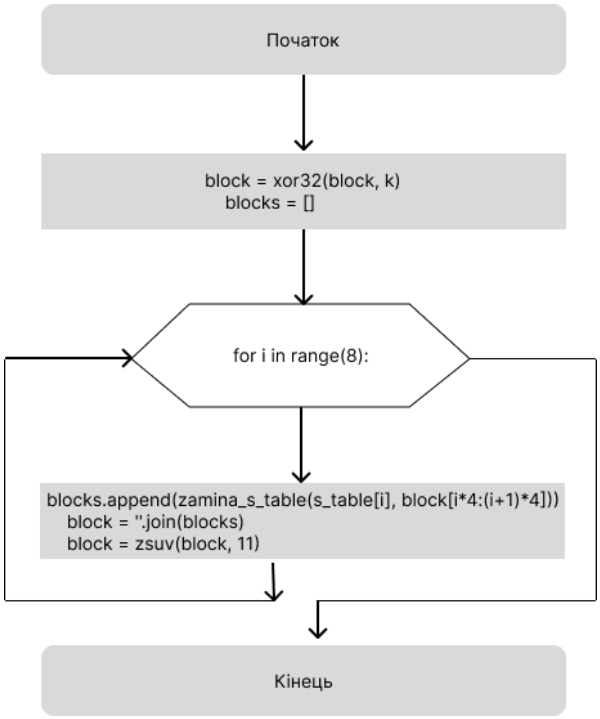

Рисунок 3.14 – Схема для функції zashifr_block_data()

Блок-схему для кнопки «Sign in» можна побачити на рис. 3.15

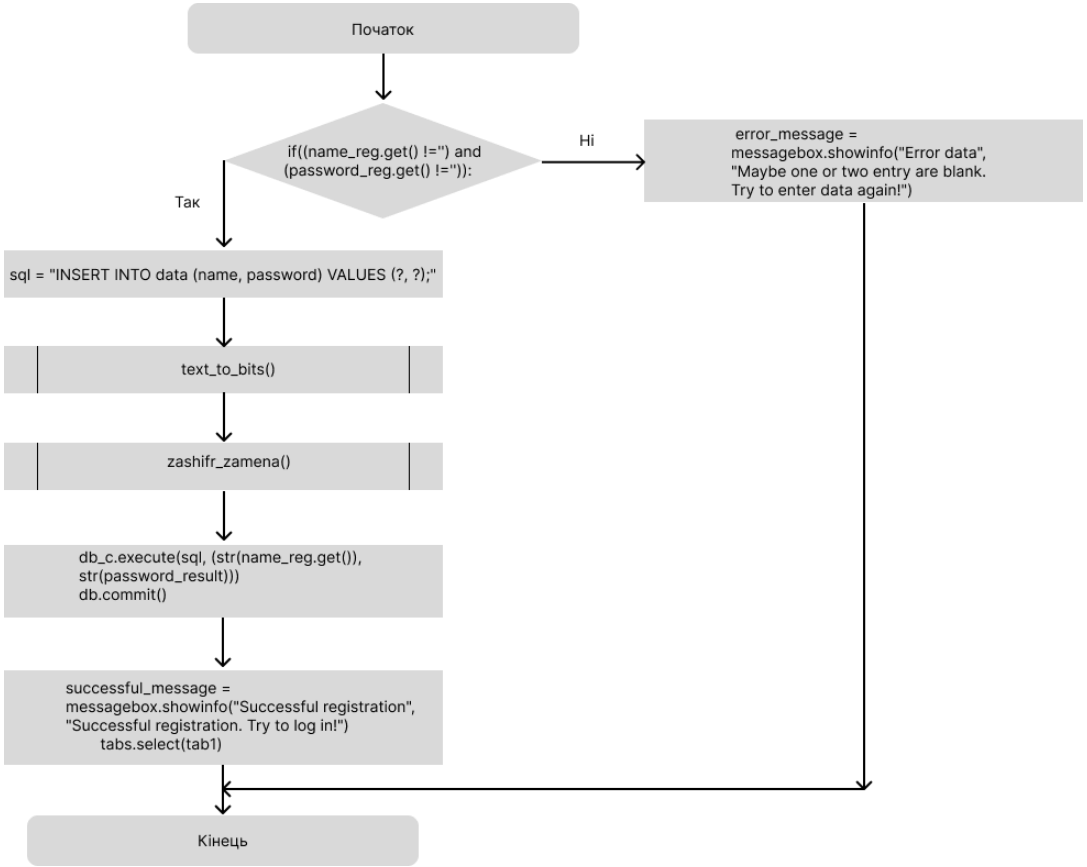

Рисунок 3.15 – Опис кнопки «Sign In»

Блок-схему для функції send_message() показано на рис. 3.16

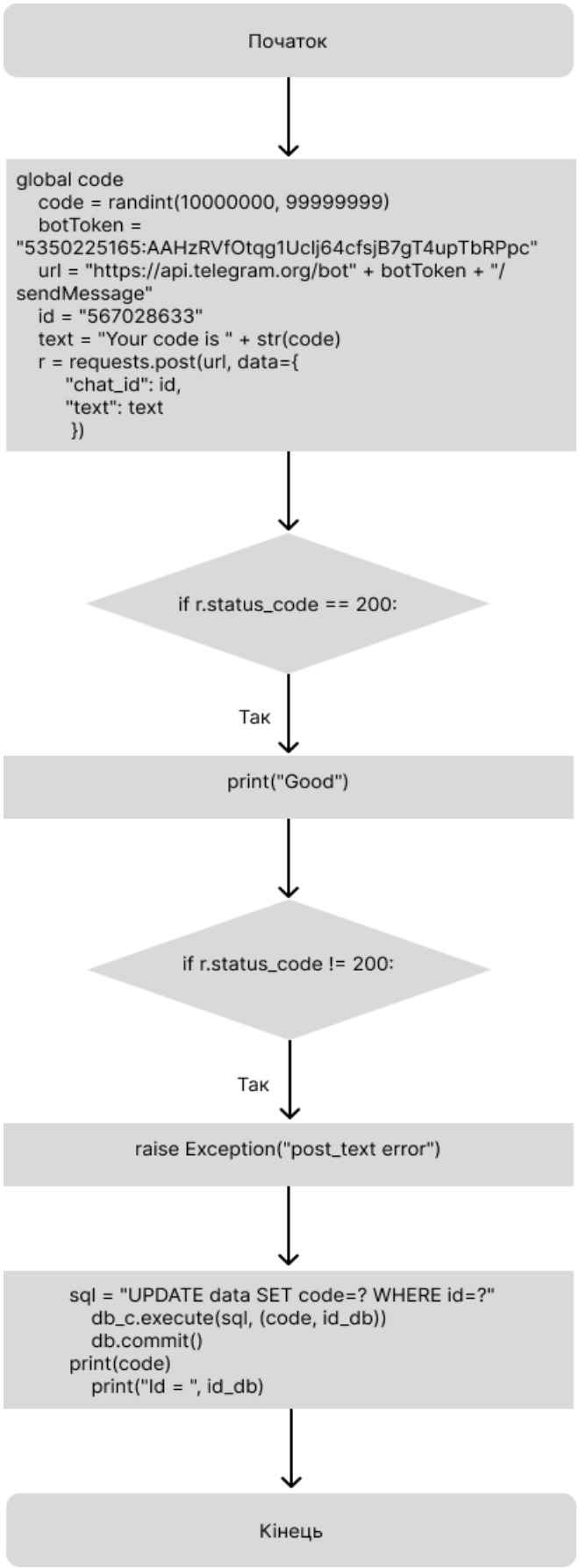

Рисунок 3.16 – Блок-схема для функції send_message()

Блок-схему для функції checkCode() можна побачити на рис. 3.17

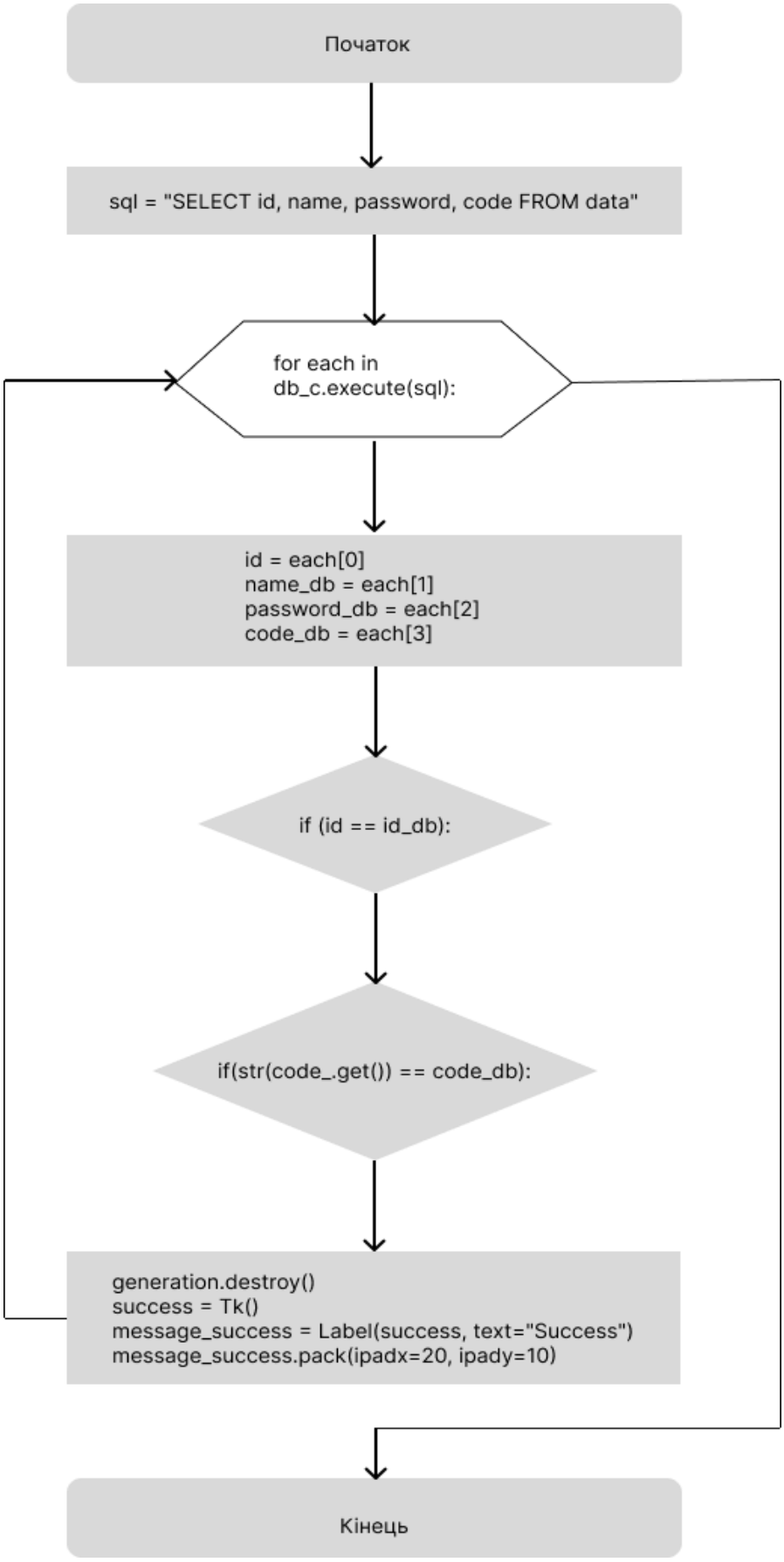

Рисунок 3.17 – Опис схеми для функції checkCode()

Висновок за розділом 3

В третьому розділі було розглянуто спеціальне програмне забезпечення «ЛОЗА – 1», яке використовується для захисту від несанкціонованого доступу інформації на підприємстві, яка міститься в текстових документах та електронних таблицях. Проаналізували роботу даного програмного засобу та виявили слабкі місця на етапі авторизації користувачів, а саме використання зовнішніх носіїв даних (дисків, флеш-носіїв) для реалізації двофакторної аутентифікації та запис даних в пам'ять комп’ютерів. Було розроблено та продемонстровано криптографічний модуль захисту інформації з використанням двофакторної автентифікації та алгоритмом шифрування ДСТУ ГОСТ 28147:2009.

ВИСНОВОК

Під час написання дипломної роботи проаналізовано реалізацію та підтримку кіберзахисту на об’єкти критичної інфраструктури, способи виявлення та боротьби з вразливостями, які можуть завдати негативних наслідків для організації.

Було виявлено, що забезпечення кіберзахисту на об’єктах критичної інфраструктури реалізується шляхом впровадження різноманітних засобів кіберзахисту (програмними комплексами, технічними засобами та програмним забезпеченням). Проведено аналіз реалізованих атак зловмисниками на критичну інфраструктуру (DoS, DDoS, фішинг та поширення шкідливого програмного забезпечення) та способи боротьби з ними. Виявлено, що постійний моніторинг систем, оперативне реагування на інциденти та правильна експлуатація засобів захисту буде позитивно сприяти на функціонування підприємства.

Для реалізації криптографічного модулю захисту інформації було створено програмний застосунок на мові python, який використовує двофакторну автентифікацію для входу користувача в інформаційну систему та метод шифрування ДСТУ ГОСТ 28147:2009, який виконує шифрування даних, наданих користувачем (паролю), що підвищить надійність захисту.

Таким чином, мета дипломної роботи досягнута та всі поставлені завдання виконанні.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Сайт з питань ядерної безпеки, радіаційного захисту та нерозповсюдження ядерної зброї [Електронний ресурс] Режим доступу – https://www.uatom.org/zagalni-vidomosti

2. Атомна індустрія України (Експертний огляд) [Електронний ресурс] Режим доступу – https://network.bellona.org/content/uploads/sites/3/2017/12/ATOM_UKR_site2.pdf

3. Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури [Електронний ресурс] Режим доступу – https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text

4. Вимоги до кіберзахисту інформаційних та керуючих систем атомних станцій для забезпечення ядерної та радіаційної безпеки. [Електронний ресурс] Режим доступу – https://zakon.rada.gov.ua/laws/show/z0395-22#Text

5. Стаття: Рой Я.В, Мазур Н. П та Складанний П. М. АУДИТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ – ОСНОВА ЕФЕКТИВНОГО ЗАХИСТУ ПІДПРИЄМСТВА. 2018. №1. ст. 87-89 [Електронний ресурс] Режим доступу – https://csecurity.kubg.edu.ua/index.php/journal/article/view/23/64

6. Аудит інформаційної безпеки на об’єктах критичної інфраструктури може стати обов’язковим [Електронний ресурс] Режим доступу – https://biz.ligazakon.net/news/180936_audit-nformatsyno-bezpeki-na-obktakh-kritichno-nfrastrukturi-mozhe-stati-obovyazkovim

7. Мережеві екрани та рішення захисту мережі [Електронний ресурс] Режим доступу – https://amind.ua/merezhevi-ekrany-ta-zahyst-merezhi

8. Криптографічний захист інформації [Електронний ресурс] Режим доступу – https://www.znanius.com/3851.html

9. ТЕХНІЧНИЙ РЕГЛАМЕНТ засобів криптографічного захисту інформації [Електронний ресурс] Режим доступу –

https://www.kmu.gov.ua/storage/app/uploads/public/601/286/214/60128621415cd223194591.pdf

10. Про затвердження Зводу відомостей, що становлять державну таємницю Електронний ресурс] Режим доступу – http://search.ligazakon.ua/l_doc2.nsf/link1/RE35674.html

11. Рівненська АЕС [Електронний ресурс] Режим доступу – https://www.rnpp.rv.ua/

12. SHA – 2 [Електронний ресурс] Режим доступу – https://uk.wikipedia.org/wiki/SHA-2

13. За півроку фахівці Держспецзв'язку заблокували 1,7 млн мережевих атак на держоргани [Електронний ресурс] Режим доступу – https://cip.gov.ua/ua/news/za-pivroku-fakhivci-derzhspeczv-yazku-zablokuvali-1-7-mln-merezhevikh-atak-na-derzhorgani

14. Відмінність DOS-атак від DDOS-атак [Електронний ресурс] Режим доступу – https://eternalhost.net/blog/hosting/dos-i-ddos-ataki

15. DoS чи DDoS: як атакують держсайти та бізнес. [Електронний ресурс] Режим доступу – https://mind.ua/openmind/20236357-dos-chi-ddos-yak-atakuyut-derzhsajti-ta-biznes

16. DoS vs. DDoS [Електронний ресурс] Режим доступу – https://www.fortinet.com/resources/cyberglossary/dos-vs-ddos

17. Що таке DDoS-атаки та яку мету вони переслідують [Електронний ресурс] Режим доступу – https://infocom.ua/%D1%89%D0%BE-%D1%82%D0%B0%D0%BA%D0%B5-ddos%D0%B0%D1%82%D0%B0%D0%BA%D0%B8/

18. Що таке фішинг і як від нього захиститись? [Електронний ресурс] Режим доступу – https://www.fg.gov.ua/articles/50140-shcho-take-fishing-i-yak-vid-nogo-zahistitis.html

19. What Is Phishing? [Електронний ресурс] Режим доступу – https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html

20. Що таке фішинг та як не стати жертвою зловмисників. [Електронний ресурс] Режим доступу – https://18000.com.ua/blogs/shho-take-fishing-ta-yak-ne-stati-zhertvoyu-zlovmisnikiv/

21. Загальні рекомендації щодо зменшення наслідків від впливу шкідливого програмного забезпечення. [Електронний ресурс] Режим доступу – https://cert.gov.ua/recommendation/2502

22. Learn IT: Malware [Електронний ресурс] Режим доступу – https://www.techtarget.com/whatis/reference/Learn-IT-Malware#:~:text=Typically%2C%20malware%20is%20distributed%20in,code%20on%20a%20Web%20site.

23. Поширення шкідливого програмного забезпечення. [Електронний ресурс] Режим доступу – https://wikis.fandom.com/uk/wiki/%D0%9F%D0%BE%D1%88%D0%B8%D1%80%D0%B5%D0%BD%D0%BD%D1%8F_%D1%88%D0%BA%D1%96%D0%B4%D0%BB%D0%B8%D0%B2%D0%BE%D0%B3%D0%BE_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BD%D0%BE%D0%B3%D0%BE_%D0%B7%D0%B0%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%BD%D1%8F

24. КІБЕРБЕЗПЕКА. АСПЕКТ 4: КОМП’ЮТЕРНІ ВІРУСИ [Електронний ресурс] Режим доступу – https://www.mil.gov.ua/ukbs/shhodenni-kiberzagrozi/kompyuterni-virusi.html

25. Товариство з обмеженою відповідальністю Науково-дослідний інститут Автопром. Система захисту інформації ЛОЗА -1. версія ПАСПОРТ ЛОЗА-1.ПД.01. [Електронний ресурс] Режим доступу –https://docplayer.net/90605324-Tovaristvo-z-obmezhenoyu-vidpovidalnistyu-naukovo-doslidniy-institut-avtoprom-sistema-zahistu-informaciyi-loza-1-versiya-pasport-loza-1-pd-01.html

26. СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ ЛОЗА™-1, ВЕРСІЯ 4. [Електронний ресурс] Режим доступу – http://avtoprom.kiev.ua/avtoprom/ua/content/%D0%A1%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0-

%D0%B7%D0%B0%D1%85%D0%B8%D1%81%D1%82%D1%83-%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%97-%D0%9B%D0%9E%D0%97%D0%90%E2%84%A2-1-%D0%B2%D0%B5%D1%80%D1%81%D1%96%D1%8F-4

27. Програмний комплекс ГРИФ. [Електронний ресурс] Режим доступу – https://mybiblioteka.su/tom2/10-15594.html

28. Інститут Комп'ютерних Технологій [Електронний ресурс] Режим доступу – http://www.ict.com.ua/?lng=1&sec=8&art=41

29. Інститут Комп'ютерних Технологій [Електронний ресурс] Режим доступу – http://ict.com.ua/?lng=1&sec=8&art=51

30. Що таке MFA — багатофакторна аутентифікація? [Електронний ресурс] Режим доступу – https://datami.ua/shho-take-mfa-bagatofaktorna-autentifikatsiya/

31. Two-Factor Authentication (2FA) from Duo [Електронний ресурс] Режим доступу – https://duo.com/product/multi-factor-authentication-mfa/two-factor-authentication-2fa

32. ДСТУ ГОСТ 28147:2009 Система обробки інформації. [Електронний ресурс] Режим доступу – http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=55943

33. ГОСТ 28147 – 89. [Електронний ресурс] Режим доступу – https://uk.wikipedia.org/wiki/%D0%93%D0%9E%D0%A1%D0%A2_28147-89

34. ШИФР DES [Електронний ресурс] Режим доступу – https://stud.com.ua/179769/informatika/shifr

35. Мережа Фейстеля. [Електронний ресурс] Режим доступу – https://uk.unionpedia.org/%D0%9C%D0%B5%D1%80%D0%B5%D0%B6%D0%B0_%D0%A4%D0%B5%D0%B9%D1%81%D1%82%D0%B5%D0%BB%D1%8F

36. Що таке 256-бітове шифрування? [Електронний ресурс] Режим доступу – https://uk.theastrologypage.com/256-bit-encryption

37. ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ. [Електронний ресурс] Режим доступу – https://ela.kpi.ua/bitstream/123456789/23896/1/TZI_book.pdf

38. Алгоритм криптографічного перетворення (ГОСТ 28147-89). [Електронний ресурс] Режим доступу – https://usts.kiev.ua/wp-content/uploads/2020/07/dstu-host-28147-2009.pdf

39. ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ. [Електронний ресурс] Режим доступу – https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/36506/1/%D0%9F%D0%86%D0%94%D0%A0%D0%A3%D0%A7%D0%9D%D0%98%D0%9A%20%D0%97%D0%86%D0%9A%D0%A1_2021.pdf

40. ГОСТ 28147-89. [Електронний ресурс] Режим доступу – https://www.wiki.uk-ua.nina.az/%D0%93%D0%9E%D0%A1%D0%A2_28147-89.html

ДОДАТОК А

Програмний код криптографічного модулю захисту інформації

```
from tkinter import *
from tkinter import messagebox
import tkinter as tk
from tkinter import ttk
import sqlite3
import os
import requests
from random import randint

DB_PATH = "{0}\database2.db".format(os.path.dirname(__file__))
db = sqlite3.connect(DB_PATH)  # connect to database
db_c = db.cursor()   # виконання sql запитів
#sql = "CREATE TABLE [IF NOT EXISTS] data ( id INTEGER NOT NULL UNIQUE, name TEXT NOT NULL, password TEXT NOT NULL, code TEXT, PRIMARY KEY(id AUTOINCREMENT))"
#db_c.execute(sql)
# creating new window with form login
input_form = Tk()
# favicon
# input_form.iconbitmap('registration.ico')
# Title
input_form.title("Form")
# size of window
input_form.geometry("500x500")

# Таби(вкладки) для вибору вікна або логіну або реєстрації
```

```
# Tkinter в Python.
tabs = ttk.Notebook(input_form)
tab1 = tk.Frame(tabs, background='#FFC34D')
tab2 = tk.Frame(tabs, background='#FFC34D')
tabs.add(tab1, text='Login')
tabs.add(tab2, text='Registration')
tabs.pack(expand=1, fill="both")

#Вхідні дані
key="0100100101111010001001001011100110101010001101001011011010110010101010100011011110100010001101111010100110110111101101101011001010111010000110100001101001011011100110011101010101011100110110010101100110011101010110110001000110011011110111001001001101011001010"

#Режим простої заміни
s_table = [ #S-блоки
                    [4, 10, 9, 2, 13, 8, 0, 14, 6, 11, 1, 12, 7, 15, 5, 3],
                    [14, 11, 4, 12, 6, 13, 15, 10, 2, 3, 8, 1, 0, 7, 5, 9],
                    [5, 8, 1, 13, 10, 3, 4, 2, 14, 15, 12, 7, 6, 0, 9, 11],
                    [7, 13, 10, 1, 0, 8, 9, 15, 14, 4, 6, 12, 11, 2, 5, 3],
                    [6, 12, 7, 1, 5, 15, 13, 8, 4, 10, 9, 14, 0, 3, 11, 2],
                    [4, 11, 10, 0, 7, 2, 1, 13, 3, 6, 8, 5, 9, 12, 15, 14],
                    [13, 11, 4, 1, 3, 15, 5, 9, 0, 10, 14, 7, 6, 8, 2, 12],
                    [1, 15, 13, 0, 5, 7, 10, 4, 9, 2, 3, 14, 6, 11, 8, 12],
          ]
def text_to_bits(password):
    passwInBits = ""
    countAdd=""
    if len(password) < 8:
        for i in range(8 - len(password)):
```

```
            countAdd += '0'
        elif( len(password) > 8 and len(password)<16):
            for i in range(16 - len(password)):
                countAdd += '0'
        elif (len(password) > 16 and len(password) < 32):
            for i in range(32 - len(password)):
                countAdd += '0'

        password += countAdd

        for symbol in password:
            countAdd=""
            textInBin = format(ord(symbol), 'b')
            if len(textInBin) < 8:
                for i in range(8 - len(textInBin)):
                    countAdd += '0'
                textInBin = countAdd + textInBin
            passwInBits += textInBin
        return passwInBits

    def codedBinInCodedSymbols(password):
        p = ''
        passw = [password[:8], password[8:16], password[16:24], password[24:32],
password[32:40], password[40:48], password[48:56], password[56:64]]
        for part in passw:
            part = int(part, 2)
            if (part <= 160 and part >= 127):
                part -= 80
            elif (part <= 32 and part >= 0):
                part += 80
```

```
        elif (part >= 161):
            part = 99
        p += chr(part)
    return p

def bin_to_dec(data): # переведення числа з двійкової системи в десяткову
    return int(data, 2)

def dec_to_bin(data, l): # переведення числа з десяткової системи в двійкову
    dviy = ''
    while data > 0:
        dviy = str(data % 2) + dviy
        data = data // 2
    while len(dviy) < l:
        dviy= '0' + dviy
    return dviy

def xor(x, y): # ксор за модулем 2
    for i in range(len(x)):
        x = x[:i] + ('0' if x[i] == y[i] else '1') + x[i+1:]
    return x

def xor32(x, y): # ксор за модулем 2^32
    x = "0b" + x
    y = "0b" + y
    Xxor32Y = (int(x, 2) + int(y, 2)) % 2 ** 32
    Xxor32Y = format(Xxor32Y, 'b')
    countAdd=""
    if len(Xxor32Y) < 32:
        for i in range(8 - len(Xxor32Y)):
```

```
            countAdd += '0'
        Xxor32Y = countAdd + Xxor32Y
    x += Xxor32Y
    return x

def zamina_s_table(s, text): # заміна S-блоків
    text = bin_to_dec(text)
    return dec_to_bin(s[text], 4)

def zsuv(text, count): # Циклічний зсув вліво на 11 біт
    return text[count:] + text[:count]

#Зашифрування
def zashifr_block_data(block, k): #шифрування для кожного раунду(вхід це права частина і ключ)
    block = xor32(block, k) # ксор блоку з ключем за модулем 2^32
    blocks = []      #створений масив для зберігання результатів кожного зашифрування блоку
    for i in range(8):
        blocks.append(zamina_s_table(s_table[i], block[i*4:(i+1)*4])) # заміна 8 S блоків по 4 біти
    block = ''.join(blocks)
    block = zsuv(block, 11) #циклічний зсув на 11 біт вліво
    return block

def zashifr_zamena(text, key):   #шифрування в режимі простої заміни
    allCodedPassword= ""
    codedInSymb=""
    keys = [] # створений массив для 8 ключів по 32 біта
    for x in range(8): #масив для розбиття одного ключа на 8 підключів
```

```
            keys.append(key[x*32:(x+1)*32])
        key = keys
        for x in range(len(text)//64): # ділимо весь текст на 64 біти
            block_data = text[x*64:(x+1)*64]
            left_side = block_data[:32] # ліва частина
            right_side = block_data[32:] # права частина
            for i in range(32):  #32 раунда для шифрування
                right_side = zashifr_block_data(right_side, key[i % 8])
                left_side, right_side = right_side, left_side  #зміна місцями, R-результат шифрування блоку він стає лівою частиною, а L стає правою частиною
            allCodedPassword += left_side+right_side  #результат зашифрування тексту
            codedInSymb += codedBinInCodedSymbols(allCodedPassword)
        print("Result: ",codedInSymb)
        return codedInSymb

    # -TAB2 REGISTRATION-----------------------------------------------------------------------

    # Label "Registration" заголовок в вкладці
    registration_label = Label(tab2, text='Registration')
    registration_label['bg'] = '#FFC34D'
    registration_label['font'] = ('Roboto'', 25')
    registration_label['fg'] = 'white'
    registration_label['underline'] = 0
    registration_label.pack(ipadx=50, ipady=20)

    # Divider
    divider_reg = ttk.Separator(tab2, orient='horizontal')
    divider_reg.pack(fill='x')
```

```
# Blank label для відступу
blank_label_reg = Label(tab2, text='  ')
blank_label_reg['bg'] = '#FFC34D'
blank_label_reg.pack(ipadx=20, ipady=10)

# Label for username input
username_label_reg = Label(tab2, text='Username')
username_label_reg['font'] = ('Roboto'', 15')
username_label_reg['bg'] = '#FFC34D'
username_label_reg['fg'] = 'white'
username_label_reg.pack(ipadx=20, ipady=10)

# Text Entry for username  - ввод тексту
name_reg = StringVar()
username_entry_reg = Entry(tab2, textvariable=name_reg)
username_entry_reg['font'] = ('Roboto'', 13')
username_entry_reg.pack(ipadx=80, ipady=10)
username_entry_reg.focus()

# Label for password input
password_label_reg = Label(tab2, text='Password')
password_label_reg['font'] = ('Roboto'', 15')
password_label_reg['bg'] = '#FFC34D'
password_label_reg['fg'] = 'white'
password_label_reg.pack(ipadx=20, ipady=10)

# Text Entry for password
password_reg = StringVar()
password_entry_reg = Entry(tab2, textvariable=password_reg, show="*")
password_entry_reg['font'] = ('Roboto'', 13')
```

```
    password_entry_reg.pack(ipadx=80, ipady=10)

    # Blank label
    blank_label_reg = Label(tab2, text='  ')
    blank_label_reg['bg'] = '#FFC34D'
    blank_label_reg.pack(ipadx=20, ipady=10)

    # function for button
    def successful_signin():
        if((name_reg.get() !='') and (password_reg.get() !='')):
            #sql_id = "SELECT id FROM data"
            #for each in db_c.execute(sql_id):
            #    id_u = each[0]
            # id = int(id_u) + 1
            sql = "INSERT INTO data (name, password) VALUES (?, ?);"

            text = text_to_bits(str(password_reg.get()))
            password_result = zashifr_zamena(text, key)
            db_c.execute(sql, (str(name_reg.get()), str(password_result)))
            db.commit()

            successful_message = messagebox.showinfo("Successful registration",
"Successful registration. Try to log in!")
            tabs.select(tab1)
        else:
            error_message = messagebox.showinfo("Error data", "Maybe one or two entry
are blank. Try to enter data again!")

    # Button SIGN IN
    signin_button = Button(
```

```
        tab2,
        text="Sign In",
        command=successful_signin,
        activebackground='#FFC34D',
        activeforeground='white')
    signin_button['bg'] = "white"
    signin_button['fg'] = '#FFC34D'
    signin_button['font'] = ('Roboto", 15')
    signin_button['state'] = 'active'
    signin_button.pack(ipadx=40, ipady=5)

    # Blank label
    blank_label_reg = Label(tab2, text='  ')
    blank_label_reg['bg'] = '#FFC34D'
    blank_label_reg.pack(ipadx=20, ipady=10)

    # Divider
    divider_reg = ttk.Separator(tab2, orient='horizontal')
    divider_reg.pack(fill='x')

    # -TAB1 LOGIN-----------------------------------------------------------------------------------
---------
    # Label "Login"
    input_form_name = Label(tab1, text='Login')
    input_form_name['bg'] = '#FFC34D'
    input_form_name['font'] = ('Roboto", 25')
    input_form_name['fg'] = 'white'
    input_form_name['underline'] = 0
    input_form_name.pack(ipadx=50, ipady=20)
```

```
# Divider
divider = ttk.Separator(tab1, orient='horizontal')
divider.pack(fill='x')

# Blank label
blank_label_ = Label(tab1, text='  ')
blank_label_['bg'] = '#FFC34D'
blank_label_.pack(ipadx=20, ipady=10)

# Label for username input
username_label = Label(tab1, text='Username')
username_label['font'] = ('Roboto'', 15')
username_label['bg'] = '#FFC34D'
username_label['fg'] = 'white'
username_label.pack(ipadx=20, ipady=10)
# Text Entry for username
name_log = StringVar()
username_entry = Entry(tab1, textvariable=name_log)
username_entry['font'] = ('Roboto'', 13')
username_entry.pack(ipadx=80, ipady=10)
username_entry.focus()

# Label for password input
password_label = Label(tab1, text='Password')
password_label['font'] = ('Roboto'', 15')
password_label['bg'] = '#FFC34D'
password_label['fg'] = 'white'
password_label.pack(ipadx=20, ipady=10)
# Text Entry for password
password_log = StringVar()
```

```
password_entry = Entry(tab1, textvariable=password_log, show="*")
password_entry['font'] = ('Roboto", 13')
password_entry.pack(ipadx=80, ipady=10)

# Blank label
blank_label = Label(tab1, text='  ')
blank_label['bg'] = '#FFC34D'
blank_label.pack(ipadx=20, ipady=10)

def send_message():
    global code
    code = randint(10000000, 99999999)

    botToken = "5350225165:AAHzRVfOtqg1Uclj64cfsjB7gT4upTbRPpc"    # token який дав BotFather
    url = "https://api.telegram.org/bot" + botToken + "/sendMessage"
    id = "567028633"   # id tg
    text = "Your code is " + str(code)
    r = requests.post(url, data={
        "chat_id": id,
        "text": text
         })
    if r.status_code == 200:
        print("Good")
    if r.status_code != 200:
        raise Exception("post_text error")

    sql = "UPDATE data SET code=? WHERE id=?"
    db_c.execute(sql, (code, id_db))
    db.commit()
```

```
    print(code)
    print("Id = ", id_db)

def checkCode():
    sql = "SELECT id, name, password, code FROM data"
    for each in db_c.execute(sql):
        id = each[0]
        name_db = each[1]
        password_db = each[2]
        code_db = each[3]
        if (id == id_db):
            if(str(code_.get()) == code_db):
                generation.destroy()
                success = Tk()
                success['bg'] = '#FFC34D'
                success.geometry("400x400")
                message_success = Label(success, text="Success")
                message_success['font'] = ('Roboto",30')
                message_success['fg'] = 'white'
                message_success['bg'] = '#FFC34D'
                message_success.pack(ipadx=20, ipady=10)

def secondfactor():
    global generation
    generation = Tk()
    generation['bg'] = '#FFC34D'
    generation.geometry("400x400")
    code = Label(generation, text="Click to get code")
    code['font'] = ('Roboto",30')
    code['fg'] = 'white'
```

```
code['bg'] = '#FFC34D'
code.pack(ipadx=20, ipady=10)
get_button = Button(
    generation,
    text="GET CODE",
    command=send_message,
    activebackground='#FFC34D',
    activeforeground='white')
get_button['bg'] = "white"
get_button['fg'] = '#FFC34D'
get_button['font'] = ('Roboto", 15')
get_button['state'] = 'active'
get_button.pack(ipadx=40, ipady=5)

# Label for code input
code_label = Label(generation, text='Enter your code')
code_label['font'] = ('Roboto", 15')
code_label['bg'] = '#FFC34D'
code_label['fg'] = 'white'
code_label.pack(ipadx=20, ipady=10)

# Text Entry for code
global code_
code_ = StringVar()
code_entry = Entry(generation, textvariable=code_)
code_entry['font'] = ('Roboto", 13')
code_entry.pack(ipadx=80, ipady=10)
code_entry.focus()
# Blank label
blank_label__ = Label(generation, text='  ')
```

```
    blank_label__['bg'] = '#FFC34D'
    blank_label__.pack(ipadx=20, ipady=10)
    # Button to submit code
    submit_button = Button(
        generation,
        text="SUBMIT CODE",
        command=checkCode,
        activebackground='#FFC34D',
        activeforeground='white')
    submit_button['bg'] = "white"
    submit_button['fg'] = '#FFC34D'
    submit_button['font'] = ('Roboto", 15')
    submit_button['state'] = 'active'
    submit_button.pack(ipadx=40, ipady=5)

# function for button
def successful_login():
    sql = "SELECT id, name, password FROM data"
    for each in db_c.execute(sql):
        # id_db = each[0]
        name_db = each[1]
        password_db = each[2]
        text = text_to_bits(str(password_reg.get()))
        password_result = zashifr_zamena(text, key)
        if (name_log.get() == name_db) and (password_result == password_db):
            global id_db
            id_db = each[0]
            input_form.destroy()
            secondfactor()
```

```
# Button LOG IN
login_button = Button(
    tab1,
    text ="Log In",
    command = successful_login,
    activebackground='#FFC34D',
    activeforeground='white')
login_button['bg'] = "white"
login_button['fg'] = '#FFC34D'
login_button['font'] =  ('Roboto", 15')
login_button['state'] = 'active'
login_button.pack(ipadx=40, ipady=5)

# Blank label
blank_label__ = Label(tab1, text='  ')
blank_label__['bg'] = '#FFC34D'
blank_label__.pack(ipadx=20, ipady=10)

# Divider
divider_ = ttk.Separator(tab1, orient='horizontal')
divider_.pack(fill='x')

# Opening tab2 - Registration
tabs.select(tab2)

# launch form
input_form.mainloop()
```