Міністерство освіти і науки України

Харківський національний університет імені В.Н. Каразіна

Факультет комп’ютерних наук

Спеціальність 125 «Кібербезпека»

Освітня програма «Безпека інформаційних та комунікаційних систем»

«Допущено до захисту»

В.о. зав. кафедрою БІСТ

Ольга МЕЛКОЗЬОРОВА

_____

« » 2023 р.

Пояснювальна записка

до кваліфікаційної роботи магістра

на тему: «Дослідження та аналіз методів забезпечення захисту персональних даних в системах електронного голосування»
«Research and analysis
of methods of ensuring the protection of personal data in electronic voting systems»

оцінка « »

Голова ЕК

Олександр ЛЕМЕШКО _____

Керівник : к.т.н., доцент Єсіна М.В.

Рецензент : к.т.н. Бобух В. А.

Виконавець : студент(ка) групи КБ-61

_____

Маджа В. В.

Харків – 2023

РЕФЕРАТ

Дипломна робота другого (магістерського) рівня вищої містить 75 сторінок, 3 рисунка, 4 таблиці. Перелік посилань нараховує 43 найменування.

Актуальність роботи. Актуальність теми дослідження зумовлено стрімким розвитком інформаційних технологій в галузі цифровізації фізичної інформації та необхідністю якісного та стійкого захисту оцифрованої інформації в умовах використання систем електронного голосування.

Метою роботи є визначення та аналіз ефективних методик, технологій та механізмів захисту персональних даних для їх впровадження та ефективного використання в системах електронного голосування.

Об'єктом дослідження дипломної роботи є процес захисту персональних даних в системах електронного голосування.

Предметом розробки є модель безпеки для систем електронного голосування України.

Результати роботи та їх новизна. Результатом дослідження є систематизація знань щодо механізмів захисту персональних даних, які використовуються в країнах, що безпосередньо займаються дослідженнями в цій галузі, для створення об'єктивних даних щодо можливостей використання таких механізмів у розбудові цифрової інфраструктури України.

Рекомендації щодо використання результатів роботи. Проаналізовані методи та механізми в комплексі надають можливість створити надійну систему не лише в області електронного голосування. Запропоновані комбінації методів та технологій можуть бути використані для практичних реалізацій.

Значущість роботи та висновки. Для України вкрай важливо створювати та розвивати цифрову інфраструктуру. Таким чином будується справжня демократія, а якість життя зростає. Позбавлення людей від необхідності створювати живі черги, та виконання їх конституційних прав: як голосування, є основними показниками демократії і покращень у житті.

Припущення про можливі напрямки розвитку. Проаналізовані механізми можуть та повинні бути використані і в інших галузях цифровізації, деякі з них мають бути впровадженні безпосередньо в процес планування та реалізації. Це відноситься до соціальної та адміністративної інфраструктури.

Ключові слова: ЕЛЕКТРОННЕ ГОЛОСУВАННЯ, ГОЛОСУВАННЯ, Е-ГОЛОСУВАННЯ, ІНТЕРНЕТ ГОЛОСУВАННЯ, ГОЛОСУВАННЯ ЧЕРЕЗ ІНТЕРНЕТ.

ABSTRACT

The thesis of the second (master's) level of higher education contains 75 pages, 3 figures, 4 tables. The list of references includes 43 items.

Relevance of the work. The relevance of the research topic is due to the rapid development of information technology in the field of digitalization of physical information and the need for high-quality and sustainable protection of digitized information in the context of electronic voting systems.

The purpose of the study is to identify and analyze effective methods, technologies and mechanisms for protecting personal data for their implementation and effective use in electronic voting systems.

The object of research of the thesis is the process of personal data protection in electronic voting systems.

The subject of development is a security model for electronic voting systems in Ukraine.

Results and novelty. The result of the study is the systematization of knowledge about the mechanisms of personal data protection used in countries that are directly involved in research in this area to create objective data on the possibilities of using such mechanisms in the development of Ukraine's digital infrastructure.

Recommendations for using the results of the work. The analyzed methods and mechanisms in combination make it possible to create a reliable system not only in the field of electronic voting. The proposed combinations of methods and technologies can be used for practical implementation.

Significance of the work and conclusions. It is extremely important for Ukraine to create and develop digital infrastructure. This is how true democracy is built and the quality of life improves. Saving people from the need to create long queues and fulfilling their constitutional rights, such as voting, are the main indicators of democracy and improvements in life.

Assumptions about possible directions of development. The analyzed mechanisms can and should be used in other areas of digitalization, and some of them

should be implemented directly in the planning and implementation process. This applies to social and administrative infrastructure.

Keywords: ELECTRONIC VOTING, VOTING, E-VOTING, INTERNET VOTING, VOTING VIA THE INTERNET.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ 8
ВСТУП 9
1 ЕЛЕКТРОННЕ ГОЛОСУВАННЯ, ВИЗНАЧЕННЯ, РОЗУМІННЯ ТА МІЖНАРОДНЕ ЗАСТОСУВАННЯ 11
1.1 Визначення електронного голосування та як його використовують у світі 11
1.2 Реалізація електронного голосування в Естонії 13
1.3 Реалізація електронного голосування в Японії 15
1.4 Реалізація електронного голосування в Аргентині 17
2 АНАЛІЗ ТА ДОСЛІДЖЕННЯ МЕТОДІВ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ 19
2.1 Що таке персональні дані та загальні механізми їх захисту 19
2.1.1 CIA тріада 21
2.1.2 Домени кібербезпеки 21
2.1.3 Захист мережі 23
2.1.4 Загрози, механізми та моделі захисту 27
2.1.4.1 Вразливості, загрози та ризики 27
2.1.4.2 Соціальна інженерія, захист працівників 28
2.1.4.3 Операційний центр безпеки (SOC) 29
2.1.4.4 Веб-захист 31
2.1.4.5 Шифрування 32
2.1.4.6 Посилення безпеки 33
2.1.4.7 Хмарна безпека 34
2.1.5 Фреймворки 34
2.1.6 Управління ризиками 36
2.1.7 Життєвий цикл безпечної розробки програмного забезпечення 39
2.1.8 Механізми захисту персональних даних систем електронного голосування 43

2.2 Міжнародний досвід застосування механізмів захисту персональних даних на прикладі Естонії 44
3 МОЖЛИВІ ПРОБЛЕМИ В РЕАЛІЗАЦІЇ СИСТЕМ ЕЛЕКТРОННОГО ГОЛОСУВАННЯ 47
3.1 Соціальні проблеми 47
3.2 Законодавче підґрунтя 48
3.3 Технічні вимоги та проблеми 49
3.4 Безпека 50
4 МОДЕЛЬ І АРХІТЕКТУРА СИСТЕМИ ЕЛЕКТРОННОГО ГОЛОСУВАННЯ 52
4.1 Модель загроз 52
4.2 Модель порушника 57
4.3 Децентралізація та резервування 62
4.4 Блокчейн 65
4.5 Смарт-контракти 67
4.6 Рекомендації та пропозиції 68
ВИСНОВКИ 70
ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ 71

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ID	identification
IDS	Intrusion Detection System
CIA	Confidentiality, Integrity, Availability
IPS	Intrusion Prevention System
OSI	Open Systems Interconnection
NAC	Network Access Control
IAM	Identity Access Manager
VPN	Virtual Private Network
DLP	Data Leak Prevention
SIEM	Security Information and Event Manager
SOAR	Security Orchestration, automation and response
NDR	Network Detection and Response
SOC	Security Operation Center
SDLC	Software Development Life Cycle
SSDLC	Secure Software Development Life Cycle
C2 (CC)	Command & Control
TTP	Tactics, Techniques and Procedures

ВСТУП

Актуальність теми. Сьогоднішні тенденції у час, коли інформаційний потік рухається мережею Інтернет, а кожен має у кишені комп'ютер, викликають необхідність у системах, безпека яких не ставиться під сумнів. Цифровізація суспільства є невідворотнім процесом розвитку. Системи електронного голосування є лише одним з багатьох кроків на шляху цього процесу. Україна останні роки активно розвиває цифровізацію, для того, щоб спростити процеси, у яких частіше використовуються паперові документи. Персональні дані людей переносяться у системи типу «Дія». Звісно всім довелось довіритись цій системі у часи пандемії та війни, коли ускладнились процеси з паперовими документами, і повірити, що персональні дані захищені. Наступним кроком у цифровізації як раз може стати волевиявлення суспільства шляхом голосування через мережу Інтернет.

Наразі є низка країн, які рухаються у напрямі впровадження необхідних законодавчих та технічних механізмів для створення систем електронного голосування, які будуть достатньо стійкими для протистояння сучасним загрозам у вигляді зловмисних хакерських груп.

Мета кваліфікаційної роботи полягає в аналізі механізмів захисту персональних даних, які активно використовуються у західних країнах, для пошуку оптимальних рішень із впровадження та побудови надійних систем, які забезпечують безпеку, конфіденційність та цілісність даних.

Результатом роботи буде окреслення сучасних рішень для вирішення проблем з забезпечення безпеки персональних конфіденційних даних користувачів систем електронного голосування.

Публікації:

1) Маджа В.В, Пономар В.А. Методи захисту персональних даних у системах електронного голосування. Збірник матеріалів конференції «Захист інформації і безпека інформаційних систем», Львівська політехніка, Львів - 2023

1 ЕЛЕКТРОННЕ ГОЛОСУВАННЯ, ВИЗНАЧЕННЯ, РОЗУМІННЯ ТА МІЖНАРОДНЕ ЗАСТОСУВАННЯ

1.1 Визначення електронного голосування та як його використовують у світі

Паперовим голосуванням вже сотні років, вони всім знайомі і всі знають як ця система працює. Завдяки багаторічному використанню є можливості впровадження більш стійких засобів захисту таких голосувань. Але є негативна сторона таких виборів, оскільки всі знають як ця система працює, всі так само знають її слабкі сторони, які дуже часто експлуатуються корумпованими особами. Система голосувань повинна відповідати багатьом вимогам, але можна чітко і точно виділити дві – анонімність і довіра. Забезпечення анонімності є дуже важливим, адже виборець, наприклад, на виборах президента, після затвердження свого голосу не повинен зіткнутися з тиском і погрозами із опозиційної сторони. Довіру заслуговують системи, які є надійними, прозорими і зрозумілими, незалежно від технічних аспектів і складності.

Електронне голосування – це різновид конституційного волевиявлення громадян для обрання осіб на вищі державні пости, пости регіонального значення та інші. Відрізняється від традиційного використанням електронних компонентів у виборчому процесі. І одразу можна сказати, що така система має достатньо недоліків. Довіру до програмного забезпечення і обладнання, яке використовується, зі сторони виборців буде важко отримати. В теорії ця система може бути «з відкритим кодом» і кожен, хто забажає може подивитися як вона працює. Це викличе нову проблему – зворотню інженерію [17] (обернену розробку), і будь-який хакер, який володіє необхідними навичками зможе знайти критичні вразливості системи. А також однією з ключових проблем можна назвати проблему тестування, адже повноцінний тест всієї системи буде відбуватися безпосередньо під час виборів, і в такій ситуації може бути

застосована Zero-day attack (атака нульового дня). Також популярний блогер YouTube Том Скотт у своєму відео «Чому електронні голосування все ще погана ідея» висвітлює проблему заражених вірусами пристроїв, які можуть бути причиною витоку персональних даних.

На 2023 рік, є 28 країн з 178, що опитувалися, які впровадили та використовують електронне або Інтернет-голосування. З них 18 країн проводять голосування на всіх рівнях – регіональних, адміністративних та президентських. Ще 4 країни використовують електронне голосування лише для менш значущих посад, таких як лідери продовольчих галузей, торгових союзів і т.д. Існують і країни, які розпочали рух у напрямку диджиталізації виборів на початку 2000-х років, але не змогли вирішити проблеми безпеки, через що програми Е-голосувань були закриті [23].

Загально кажучи, є два варіанти впровадження електронного голосування. Країни як Естонія впроваджують та використовують більш просунуте представлення – голосування через Інтернет, коли людина може зробити це з будь-якої точки країни або світу, зробити це максимально просто і без зайвих витрат часу, наприклад, через телефон, використовуючи електронні документи для автентифікації. Можливість голосувати через Інтернет також надає можливість віддати свій голос людям з обмеженими можливостями, які не мають фізичної можливості прийти на виборчу дільницю, що дозволяє уряду отримувати інформацію про воління їх народу в повному обсязі.

Другий варіант є більш застарілим, але є країни, що досі користуються такими методами та модифікують їх з точки зору безпеки, наприклад, варіант при якому для голосування використовують електронні машини, які на вході отримують документи виборця, а на виході надають йому можливість проголосувати та підтвердження голосу.

Також існує гібридна система, коли використовуються машини, але вони є лише проміжними вузлами у голосуванні, така система вимагає обов’язково приходити на виборчу дільницю, але голосувати ви можете лише через спеціальну машину, яка відправляє ваш голос на сервер, де він обробляється.

Кожна така ідея та система має свої переваги та недоліки. Ця робота насамперед націлена на дослідження систем, які надають можливість бути відсутнім на виборчий дільниці, використовувати лише свій телефон, або інший наявний пристрій, адже саме такі системи мають найбільше потенціалу, насамперед через те, що майже кожна людина має ПК у себе у кишені, який можна використати не тільки для дзвінків та смс, а надати йому більше свободи та сенсу. Вибір саме таких систем обумовлюється світовими тенденціями до цифровізації суспільства і обставинами, такими як пандемія COVID-19 та війнами. Особливо заслуговує уваги питання безпеки таких систем, адже при впровадженні голосувань через пристрої на дільниці, їх можна захищати фізично, тим часом Інтернет голосування потребує більш просунутого захисту на багатьох рівнях.

У цій роботі будуть розглянуті популярні рішення різних країн, як проводяться вибори, в якому режимі та за якими алгоритмами. Таким чином можна буде визначити помилки, яких може припуститися Україна при впровадженні схожих методів та використовуючи схожі технології.

1.2 Реалізація електронного голосування в Естонії

Естонія є найкращим прикладом розвитку загалом електронного документообігу та комп'ютеризації суспільства. Шлях такого розвитку розпочався на початку нульових, з 1996 року розпочалося стрімке зростання кількості Е-послуг, створюється перша система електронного банкінгу, було запропоновано схему використання національних ID карт з унікальним ідентифікаційним номером, затверджуються електронно-цифрові підписи і нарешті у 2005 році проводиться перше електронне голосування. У 2016 році для журналу Wired Тааві Котка, на той момент головний інформаційний директор уряду Естонії, дав коментар “Третя частина населення країни голосує через Інтернет...” [34].

З кожним роком кількість населення, яке віддає свої голоси через Інтернет зростає, так, згідно інформації з офіційного сайту E-estonia можна дізнатися, що у 2023 році було проведено голосування, де взяло участь онлайн понад 50% виборців при загальній явці у 64%. Очевидним є те, що більшість з людей, які

використовують Е-голосування – є підлітки та молоде покоління, від 16 до 25-30 років. Тобто, той прошарок суспільства, якому найлегше розібратися з новими технологіями, та ті, хто не хоче або не може витрачати час на відвідування ділянки голосування.

З інтерв'ю директорки програми з кібербезпеки Естонії Епп Маатен можна дізнатися, як саме працює система електронного голосування та як забезпечується безпека конфіденційних даних. Насамперед кожен виборець повинен ідентифікуватися у системі з використанням державного ID. Україна має схожу систему ідентифікації у додатку “Дія” через BankID. Один виборець може змінювати свій вибір безліч разів до кінця голосування, кожен новий голос замінює попередній, це зроблено для зменшення ризиків голосування проти волі. Для голосування у системі використовуються низка безпекових компонентів, таких як урядове електронне посвідчення особи, реєстр виборців, а також голоси шифруються ще до передачі на сервер, щоб убезпечити дані при несанкціонованому проникненні у канал передачі даних. Весь комплекс електронного обладнання, яке використовують при голосуваннях також використовується у повсякденних операціях, тому це дає змогу комплексно розробляти захисні механізми для кожного елементу окремо, що забезпечує міцний захист та відсутність дір для хакерів. Тобто, підсумовуючи, Естонія використовує три основні умови електронних голосувань: надійні інструменти електронної ідентифікації, політична консолідація та наявність консенсусу і очевидно електронний ресурс такий як сховища даних, обладнання для верифікації і т.д. [41].

Для проведення голосування використовують електронні національні ідентифікаційні карти. ID картки, що використовують при голосуваннях були розроблені для роботи на інтегральній схемі, Java чіп платформах та захищені із застосуванням 2048 бітного ПІН-кода. Картки спроможні створювати підписи, використовуючи SHA1/SHA2 [3]. Людина, що буде брати участь у голосуванні, повинна завантажити програму голосування, автентифікувати дані, використовуючи електронний паспорт, та, якщо вона за законом має право голосувати – вона отримає список кандидатів, і голосування для нього

розпочнеться. Після завершення процедури, голос виборця буде зашифровано з використанням виборчого відкритого ключа та підписується особистим ключем виборця. Після чого, голос відправляється на сервер, що контролюється естонським урядом [8].

1.3 Реалізація електронного голосування в Японії

Перше електронне голосування в Японії було проведене у 2002 році, з того часу десять місцевих урядів провело загалом до двадцяти п'яти електронних голосувань. Почалось усе із запропонування "Стратегії e-Japan", яка полягала у побудові електронного уряду у 2001 році. З того часу було багато спроб створення "електронної демократії" у країні, саме у той час, дивлячись на Естонію, зростала цікавість до Е-послуг. На жаль, система не стала популярною, скоріше за все, це пов'язано з кількістю населення, що старше 65-ти років (35,6 млн осіб з 125,7 млн), якому важче пристосуватися до електронних девайсів.

В Японії використовувалися Електромагнітні Записувачі для голосування. Процедура голосування була наступною [24]:

- Виборець приходить на виборчу дільницю з "вхідним квитком" який він/вона отримав поштою заздалегідь;
- У приймальні виборець здає квиток, його дані звіряються з реєстром виборців;
- Після ідентифікації, виборцю надається картка для голосування;
- Виборець вставляє картку у пристрій, після чого отримує доступ до голосування;
- Виборець обирає кандидата зі списку, використовуючи сенсорний екран. (Зазначається, що є можливість не обирати кандидатів, та натиснути на "пропустити голосування");
- Виборець підтверджує свій голос;
- Результат голосування записується на електромагнітному носії, що знаходиться усередині машини для голосування;

- Після чого виборець витягує картку з машини. Процес голосування закінчено, картку повертають до адміністрації.

У той час, система мала три фази впровадження:

1) Виборець голосує через електронну машину на виборчій дільниці;

2) Виборець має змогу голосувати не тільки на тій дільниці, до якої він приписаний;

3) Виборець має змогу голосувати поза дільницею з використанням ПК або смартфону.

Саме перша фаза і була імплементована у систему Японії. При такій побудові, машини не були підключені до мережі Інтернет, а отже не було трафіку, який би могли перехопити зловмисники. Можливість сфальсифікувати голос майже відсутня. Але у такій архітектурі була проблема – треба знайти метод доставки інформації до машини, що буде рахувати голоси. Очевидним методом було виймання носія з машини голосування і доставка його до машини рахування, але такий метод нічим не відрізнявся від звичайного паперового, і мав ті самі недоліки.

Другим методом стало під’єднання машин до мережі, у першій фазі він не використовувався, бо були проблеми з безпекою. Але вже друга фаза включала в себе під’єднання до захищеної мережі для передачі інформації про голосування. Також це дозволило би розповсюджувати інформацію про кандидатів, а також спростило ідентифікацію виборців за допомогою реєстрації у мережі і дозволило б виборцям голосувати поза межами дільниці, до якої вони приписані.

Третьою фазою було впровадження повного голосування через мережу Інтернет. Тоді будь-яке Інтернет-з’єднання можна було використовувати, а не тільки виділену лінію, можливі проблеми з безпекою були очевидними. Також в такому разі, всі дільниці стають непотрібні, а для голосування виборець точно повинен мати ПК або смартфон. На той час ще й вставало питання ідентифікації виборців та їх автентифікація у системі. В той час було не зрозуміло як ідентифікувати людину, та взагалі бути впевненим, що саме вона сидить перед комп’ютером. Тоді був варіант впровадження верифікації за

допомогою криптографії з відкритим ключем, або біометричних даних, як відбиток пальця. І знову виникало питання, оскільки в третій фазі не було наглядачів за процесом, чи є голос виборця результатом його волі, або його могли примусити, тоді це було важке питання для Японії.

Судячи з розвитку технологій, зараз, можна сказати, що третя фаза могла бути впроваджена [24]. Однак вона є так само не дуже реалістичною. На 2018 рік, була впроваджена лише перша фаза, і у цей рік було проведено останні місцеві електронні вибори у Префектурі Аоморі.

1.4 Реалізація електронного голосування в Аргентині

Перші тести електронного голосування були проведені у 2003 році, тоді провінція Буенос-Айрес використала таку систему для людей, що не є громадянами країни, але мають три і більше років резидентства. В тому ж році найменша провінція країни Тіерра дель Фуего використала електронне голосування для муніципальних виборів. Такі вибори викликали обурення деяких кандидатів, та звичайно багато заяв про необхідність перерахунку голосів через ненадійність такої системи. Не дивлячись на такі заяви, система витримала критику і в деяких провінціях відмовилися від стандартного алгоритму голосування за допомогою паперу та конвертів. У 2009 році провінція Сальта стала першою, яка використала електронне голосування для повного електорального складу у провінційних виборах, а це не менше 850 тисяч виборців [31].

Система розвивалася і мала багато переваг у порівнянні з традиційною системою. Основною перевагою є швидкість підрахунку голосів, що дозволяє відстежувати результати виборів в реальному часі. Звісно є проблеми, сам уряд країни визнає можливості технологічних збоїв у роботі, та можливість програмної фальсифікації голосів, використовуючи вразливості системи.

Алгоритм голосування дуже схожий на інші країни, які використовують машини підрахунку та голосування [42]:

1) Виборець надає ідентифікаційні дані;
2) Після чого отримує електронний бюлетень;

3) Виборець заходить у темну кімнату, де вставляє бюлетень у пристрій для голосування;

4) Використовуючи сенсорний екран, виборець голосує за кандидата (Також є можливість не голосувати, але пройти реєстрацію у виборах);

5) Після вибору, виборцю надається можливість перевірити та підтвердити свій голос;

6) Пристрій видає виборцю спеціальну картку з вбудованим чіпом;

7) Просканувавши картку тим самим пристроєм, виборець може знову перевірити правильність голосу;

8) Далі виборець вкидає карту у скриньку з голосами, отримуючи акт, який є доказом голосування.

Для підрахунку голосів, представники виборчої дільниці повинні пропустити картки через сканер, якій підсумує голоси, ці дані вже традиційно надсилаються поштою у центр підрахунку.

Аналізуючи алгоритм роботи, можна вже побачити можливі вразливості такої побудови системи, адже людина у момент голосування знаходиться одна у кімнаті, чим може скористатися зловмисник. Використовуючи апаратні технології є можливість підключення до пристрою, чим можна нашкодити як носіям інформації, так і фальсифікувати вибори.

2 АНАЛІЗ ТА ДОСЛІДЖЕННЯ МЕТОДІВ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

2.1 Що таке персональні дані та загальні механізми їх захисту

Для початку визначимо, що таке персональні дані. Персональні дані [9] – будь-яка інформація яка може потенційно ідентифікувати конкретну персону. Будь-яка інформація, яка дозволяє відрізнити одну особу від іншої і може бути використана для деанонімізації до цього анонімних даних, також кваліфікується як персональна інформація. До персональної інформації відноситься: ПІБ, адреса, електронна пошта, номер телефону, дата народження, номер паспорту, фото, відбиток пальця, номер ліцензії водійського посвідчення, номера кредитних або дебетових карт, ідентифікаційний номер та інші. Виходячи з цього списку можна поділити інформацію на дві категорії: ту, яка при витоку даних не несе загрози особі, та на ту, виток якої може нести матеріальні, психологічні або інші збитки для особи – власника даних. Саме тому персональна інформація повинна бути захищена.

Персональні дані кожної людини так чи інакше використовуються різноманітними установами. Кожна така установа, яка буде збирати/зберігати/оброблювати персональну інформацію, повинна слідувати правилам, які встановлюються законами країни. В Україні це регулюється законом України від 2010 р., редакції 27.10.2022 «Про захист персональних даних» [4].

Європейський союз у 2018 році увів у роботу Загальний Регламент Захисту Даних (GDPR) для захисту персональних даних. Ключові вимоги закону включають наступне [21]:

- Попереднє погодження повинне бути отримано перед збиранням будь-якої персональної інформації: тобто обов’язково повинно бути попередження особи, чию інформацію буде зібрано, про те, що її інформація буде зібрана і

оброблена. Також повинно бути окреслено чи буде інформація зберігатися чи буде видалена після обробки.

- Персональна інформація повинна зберігатися у мінімальному вигляді і збиратися тільки тоді, коли це необхідно: будь-яка установа повинна зберігати тільки ту інформацію, яка потрібна їй для обробки без надлишкової.
- Необхідно вжити відповідних заходів захисту для персональних даних, що зберігаються: заходи захисту персональної інформації повинні відповідати всім нормам і стандартам.

Рис 2.1 – GDPR кваліфікація

Під словом «загальні» механізми захисту, маються на увазі такі, що є основою при побудові тієї чи іншої системи, та, які будуть важливими для будь-якої системи. У даному контексті це може бути будь-яка система, від звичайної локальної мережі до, в нашому випадку, системи електронного голосування. Не важливо, яке це саме Е-голосування, як вже зазначалося вище, в Інтернеті чи фізичне із застосуванням електронних компонентів.

2.1.1 CIA тріада

Для ефективного захисту персональних даних необхідно керуватися основною моделлю кібербезпеки, а саме CIA тріадою (Конфіденційність, Цілісність і Доступність).

Конфіденційність – забезпечує впевненість, що дані захищені від несанкціонованого доступу.

Цілісність – вказує, що дані правильні, автентичні та точні.

Доступність – означає, що особа, яка авторизована на отримання інформації, отримає її без перешкод.

Важливо пам’ятати, що зазвичай будь-яка атака націлена саме на ці три стовпи кібербезпеки. Існує так звана DAD тріада [36], що являє собою повну протилежність вищезазначеній моделі.

Розкриття (Disclosure) – є протилежністю конфіденційності, тобто розголошення конфіденційних даних і є посягання на конфіденційність.

Зміна/деформація (Alteration) – є протилежністю до цілісності. Зміна інформації становить загрозу її цілісності.

Знищення (Destruction) – є протилежністю доступності. Знищення інформації або знищення можливості доступу до неї.

2.1.2 Домени кібербезпеки

Згідно сертифікації Certified Information System Security Professional (CISSP) існує 8 доменів кібербезпеки [6], кожен домен відповідає за конкретну сферу відповідальності. Спеціаліст з кібербезпеки може відноситися до одного, або одразу декількох доменів, відносно його навичок, знань і досвіду. Коректна робота спеціалістів доменів як одне ціле забезпечує здатність організації/компанії і т.п. керувати захистом критично важливих активів і даних компанії, і реагувати на зміни. До цих доменів відноситься [1]:

1) Безпека та управління ризиками (Security and Risk Management): виходячи з назви, домен відповідає за пом’якшення ризиків, будь-яких, як репутаційних, фінансових, так і технічних. Також відповідає за впровадження політик безпеки, нормативних вимог та незалежних стандартів. Безпосередньо

перетинається із законами, правилами та вимогами, етичним очікуванням, щоб мінімізувати недбалість, зловживання чи шахрайство.

2) Безпека активів (Asset security): Активи як персональні дані повинні бути надійно захищені. Не зважаючи, де і як вони зберігаються та як передаються. Компанії повинні мати політики та процедури, які надають невпевненості, що дані належно зберігаються, оброблюються, передаються та знищуються.

3) Безпека архітектури та інженерії (Security architecture and engineering): Відповідає за належну архітектуру як обладнання, так і програмного забезпечення. Потребує впровадження особливих політик та принципів кібербезпеки як OWASP principles та NIST Risk management framework [39].

4) Безпека зв'язку та мережі (Communication and Network Security): відповідає за те, що передача даних організації є безпечною, незалежно від того відбувається вона через мережу або фізично. Відноситься до всіх комунікації.

5) Керування ідентифікацією та доступом (Identity and access management): Основне завдання – впевнитись, що системи організації захищені на стільки, на скільки можливо, за допомогою обмеження прав доступу користувачів до того мінімуму, який потрібен для роботи. Загальна мета – знизити ризики системі та даним в цілому.

6) Оцінка безпеки та тестування (Security Assessment and Testing): Допомагає знаходити нові та кращі шляхи пом'якшення загроз, ризиків та вразливостей.

7) Операції безпеки (Security Operations): Поєднує в собі великий спектр можливих заходів для реакції на інцидент безпеки. Найбільший домен, який відповідає за моніторинг системи, збирання та аналіз логів, запобігання втручань у систему, менеджмент інцидентів, оновлення політик безпеки, тренування персоналу, пост-інцидентні заходи та розслідування інцидентів. Розслідування розпочинається одразу після того як інцидент був ідентифікований, якщо це активна атака – спочатку вона пом'якшується та зменшується її потенціал до подальшої ескалації. Як тільки загроза була

нейтралізована – починається процес збору цифрових та фізичних «доказів» і подальше розслідування.

8) Безпека розробки програмного забезпечення (Software development security): Потребує впровадження практик з безпечного програмування, щоб створювати безпечні додатки та сервіси, тестування та пошук загроз.

Розуміння цих доменів є важливим для кожного спеціаліста з кібербезпеки, адже так чи інакше кожен з них працює в одному з них. Необхідно швидко приймати рішення, які практики з яких доменів потрібно використати саме під час конкретного інциденту або при розробці продукту/програмного забезпечення/веб-ресурсу або сервісу.

2.1.3 Захист мережі

Як вже було зазначено вище, захист персональних даних в нашому випадку в основному буде відбуватися на сховищах даних, які будуть постійно під'єднанні до мережі. Звісно дуже важливо правильно обрати сховище або сервер для збереження персональних даних, але набагато важливіше створити коректну систему безпеки, яка буде забезпечувати захист на всіх рівнях моделі OSI. Очевидно, що в даному випадку ці дані будуть більш коректними для системи голосування через мережу Інтернет. Коротко про можливі механізми для кожного рівня моделі:

1) Фізичний рівень (Physical layer): Для забезпечення захисту даних на цьому рівні використовуються фізичні методи, інженерні ресурси та компоненти мережі такі як модеми, хаби та кабелі. Відповідно, потребує особливої уваги до компонентів обладнання серверних установок.

2) Канальний рівень (Data link layer): На цьому рівні варто звертати увагу на безпеку локальної мережі. Унеможливлювати несанкціонований доступ неверифікованого персоналу, обмежувати доступ до інтерфейсів управління. Є необхідність в моніторингу трафіку із завданням перевірки коректності пакетів протоколів.

3) Мережевий рівень (Network layer): Рівень характеризується використанням Firewall для моніторингу вхідного та вихідного трафіку. В системах Е-голосування через мережу Інтернет – є одним з найважливіших

компонентів захисту. Коректне налаштування брандмауеру є істотним, адже інакше локальна мережа не буде захищена від можливих найпростіших в реалізації атак. Використання Subnet додасть захисту, адже розбиття мережі на окремі ділянки з окремим захистом створить більш істотні труднощі для зловмисників, та надасть команді безпеки час на реакцію.

4) Транспортний рівень (Transport layer): Оскільки рівень забезпечує передачу пакетів даних протоколами, такими як TCP, додатковим фактором захисту буде система моніторингу трафіку, для вчасної реакції на можливі DoS або DDoS атаки.

5) Сеансовий рівень (Session layer): Рівень забезпечує комунікацію між двома пристроями, а отже захист «тунелю» комунікації має важливе значення, бо перехоплення пакетів під час передачі даних може створити ситуацію витоку даних. Тунель комунікації повинен бути захищеним криптографічними методами.

6) Рівень представлення даних (Presentation layer): Відповідає за представлення даних у формі, яка буде зрозуміла людині. Цей рівень використовує шифрування та стиснення даних. Для забезпечення гідного рівня безпеки, при втраті даних, зловмисник не повинен розшифрувати дані та мати змогу їх прочитати. Отже шифрування повинне проводитися за допомогою надійних алгоритмів, які не можуть бути розшифровані без закритих ключів або біометричних ключів.

7) Прикладний рівень (Application layer): Останній, але не менш важливий з точки зору безпеки даних рівень. Оскільки він відповідає за взаємодію користувача з мережею, необхідно використовувати захищені протоколи, як HTTPS, SSH і т.д. Оскільки для Е-голосування у мережі цей рівень означає взаємодію користувача з веб-ресурсом, основну увагу потрібно приділяти безпеці веб-додатка.

Основа безпеки мереж фокусується на двох концепціях: автентифікація та авторизація. Існує безліч інструментів, технологій та підходів для забезпечення та оцінки цих двох ключових концепцій і виходу за рамки забезпечення

безперервності і надійності. Безпека мереж містить три базові рівні контролю для забезпечення максимально доступного управління безпекою:

- Фізичний рівень: контроль фізичної безпеки запобігає неавторизованому фізичному доступу до мережевих приладів, кабелів та всіх поєднаних компонентів.
- Технічний рівень: елементи керування безпекою даних запобігають несанкціонованому доступу до мережевих даних, як-от встановлення тунелів і впровадження рівнів безпеки.
- Адміністративний рівень: адміністративні засоби контролю безпеки забезпечують узгодженість операцій безпеки, таких як створення політик, рівнів доступу та процесів автентифікації.

У цих рівнях контролю є два основні підходи та кілька елементів. До підходів відносять: контроль доступу та контроль загроз.

Ключові елементи контролю доступу описані у таблиці 2.1:

Таблиця 2.1 – Елементи контролю доступу

Елемент контролю	Опис
Брандмауер (Фаєрвол)	Контролює вхідний та вихідний мережевий трафік, використовуючи заздалегідь створені безпекові правила. Створений для блокування підозрілого/шкідливого трафіку та загроз прикладного рівня, дозволяючи чистий та очікуваний трафік.
Контроль мережевого доступу (NAC)	Призначений для перевірки приладу відповідності встановленим правилам та характеристикам перед підключенням до мережі.
Керування ідентифікацією та доступом (IAM)	Керує ідентифікацією активів і доступом користувачів до систем і ресурсів мережі.
Балансування навантаження	Контролює використання ресурсів для розподілення задач та для покращення загальної обробки даних.

Продовження таблиці 2.1 – Елементи контролю доступу

Мережева сегментація	Створює та контролює сегментацією мережі, для ізоляції користувачів відповідних рівнів доступу, покращує безпеку мережі в цілому.
Віртуальні приватні мережі (VPN)	Створює та контролює зашифровані канали зв’язку між приладами у мережі.
Модель нульової довіри (Zero Trust)	Пропонує налаштування та реалізацію доступу на мінімально можливому рівні без шкоди для робочого процесу.

Ключові елементи контролю загроз описані у таблиці 2.2:

Таблиця 2.2 – Елементи контролю загроз

Елемент контролю	Опис
Системи виявлення та запобігання вторгнення (IDS/IPS)	Перевіряє трафік та створює оповіщення (IDS) або перериває з’єднання (IPS), коли знаходить аномалію/загрозу.
Системи запобігання втрати даних (DLP)	Перевіряє трафік та блокує спроби вилучення чутливої інформації.
Захист приладу (Кінцевої точки)	Захист усіх типів пристроїв, які підключаються до мережі, використовуючи багаторівневий підхід (шифрування, антивірус, DLP, IDS, IPS і т.д.).
Хмарний захист	Захист хмарних/онлайн ресурсів систем від загроз та витоку даних шляхом впровадження та використання відповідних контрзаходів.
Система SIEM	Технологія, яка допомагає виявленню загроз та управлінню інцидентами, використовуючи контекстний аналіз подій.

Продовження таблиці 2.2 – Елементи контролю загроз

Система SOAR	Технологія, яка допомагає координувати та автоматизувати завдання між різними людьми та інструментами для виявлення аномалій, загроз та вразливостей.
Аналіз мережевого трафіку та NDR	Перевірка трафіку або перехоплення трафіку для виявлення аномалій та загроз.

2.1.4 Загрози, механізми та моделі захисту

2.1.4.1 Вразливості, загрози та ризики

Основні терміни [1]: вразливість, загроза та ризик, хоч і є схожими, але кардинально відрізняються конструктивно. Загроза – будь-які обставини або події, які можуть негативно вплинути на активи компанії чи організації. Загрозою вважається і зловмисник. В свою чергу ризик – це будь-що, що може вплинути на конфіденційність, цілісність або доступність активу. Активи, в цьому контексті, поділяються на три підгрупи: з низьким, середнім та високим рівнем ризику. Активи з низьким рівнем ризику – це інформація, яка не завдасть шкоди репутації та не матиме фінансових наслідків у разі витоку. Активи з середнім рівнем ризику – це такі, які не доступні публічно, і їх витік може спровокувати деяку шкоду фінансам та репутації організації. В свою чергу, як вже зрозуміло, активи з високим рівнем ризику – це інформація, яка захищається нормативними актами та законами, яка при витоку буде мати особливо негативні наслідки для організації, її репутації та фінансів. В свою чергу, вразливість – це слабкість, яка може бути використана загрозою для зламу.

Рис. 2.2 – Приклад реалізації ризику, загрози та вразливості

Вплив, який може виникнути при використанні вразливостей зловмисником, може бути, як вже зазначалось вище, фінансовим, репутаційним, і окремо крадіжкою конфіденційних даних. Фінансова шкода може варіюватись в залежності від атаки та її наслідків, так само як і репутаційна. Тоді як конфіденційні дані – є активом, зберігання якого само по собі є ризиком. Втрата таких даних в результаті витоку інформації несе серйозні наслідки, як підміна особистих даних зловмисником для подальшої ескалації атаки та збільшення потенційних збитків.

У контексті безпеки систем електронних голосувань, важливо зрозуміти, що такі системи будуть дуже цікаві зловмисникам. Оскільки через них проходять персональні дані користувачів, а ця інформація є ключовою для будь-якого хакера. Використовуючи особисті дані можна проникати у будь-які установи або сервіси. Підміна даних або деперсоніфікація є одними з основних причин зламу користувачів у соціальних мережах. У цьому випадку, системи голосування є навіть більш цікавими, адже через них курсує багато важливої і цікавої персональної інформації.

2.1.4.2 Соціальна інженерія, захист працівників

Механізми захисту в основному будуються виходячи з можливих вразливостей, які зловмисники можуть і будуть використовувати для

проникнення у системи з метою викрадення, ушкодження/видалення/шифрування або підміни даних.

Будь-який хакер одразу може вказати на першу і основну вразливість будь-якої системи – люди. Соціальна інженерія – перший і основний вид атаки на організацію з метою отримання чутливої інформації, який виконують зловмисники. Наразі є найскладнішим, адже кожна атака буде унікальною в залежності від людини. Для запобігання такого роду вразливості необхідно впровадити активну роботу з персоналом, висвітлення проблем кібербезпеки серед робітників, та навчання з метою зменшення ризиків. До соціальної інженерії входить багато атак, таких як медіа-фішинг, фізична інженерія, стратегічна інженерія і т.д.

Результатом такої атаки може бути отримання інформації для втручання у внутрішні системи організацій, або інформації про робітників компанії, які є більш впливовими та на яких теж можливо направити соціальну атаку. Активно використовується сучасними хакерами, бо люди зазвичай є передбачуваними, і ведуть себе шаблонно при деяких обставинах.

Здається, що системи електронного голосування не мають такої проблеми, але сервери повинні кимось обслуговуватися, а отже є людські ресурси, які можна експлуатувати зловмиснику.

2.1.4.3 Операційний центр безпеки (SOC)

Для забезпечення захисту, істотним є створення підрозділу кібербезпеки, завданням якого буде безпосереднє створення, моніторинг та підтримка системи. В цей підрозділ повинні входити декілька команд, для розподілення завдань. Політика безпеки повинна визначати місце кожної команди під час інциденту, щоб максимально швидко та ефективно відповісти на загрозу та пом’якшити ризики. Це завдання припадає на Playbook [22], або на керівництво щодо застосування, яке будується на основі вимог системи, та можливих вразливостей, які можуть бути використані зловмисниками для втручання у систему.

Сьогоднішні тенденції розвитку зловмисниками вірусних додатків та програм, підштовхує все більше компаній до впровадження операційних

центрів з безпеки або Security Operation Center (SOC). Впровадження центру має бути невід'ємною частиною побудови стійкої системи захисту будь-яких даних, адже одразу використовує багато інструментів для перевірки, аналізу та реакції на інциденти. SOC виконує п’ять основних операцій [10]: генерація подій (евентів) безпеки, збирання, зберігання, аналіз та реакція. За кожну з цих операцій відповідає конкретний модуль:

- Генерація подій (евентів) безпеки – включає в себе моніторинг систем, генерацію записів (логів) дій в системі в режимі реального часу, для цього використовуються системи IDS, SIEM та інші інструменти моніторингу та аналізу систем.
- Збирання та зберігання – після генерації подій, їх збирають з інструментів генерації і надалі структурують та зберігають на серверах, для подальшого аналізу за необхідністю.
- Аналіз та реакція – при виникненні інциденту, спеціалісти центру безпеки проводять аналіз зібраних подій та ведуть розслідування для встановлення причин цієї події. Після точного встановлення цих подій, будується звіт, в якому вказують на причини та можливі шляхи виправлення системи, таким чином проходить реакція на інцидент, після якої проводиться відновлення системи після інциденту.

Автоматизація – є важливою складовою побудови надійної системи захисту. Означає використання технологій для зменшення роботи людей при виконанні звичних та повторюваних завдань [1]. Такими системами є вже вище зазначені Intrusion Detection Systems (IDS) або системи виявлення вторгнень, які в режимі реального часу перевіряють активність системи та сповіщають адміністраторів при можливому вторгненні. Security Information and Event Management (SIEM), спеціалізовані системи, які є обов’язковими для впровадження [37], надають аналіз сповіщень безпеки в реальному часі, які генеруються мережевим обладнанням та додатками. Завдяки таким системам компанія зможе швидко та ефективно реагувати на різного роду події безпеки, як при спробі зламу, так і при звичайних помилках у роботі системи.

2.1.4.4 Веб-захист

При побудові системи, такої як електронне голосування в мережі Інтернет, важливо зауважити, що така система буде будуватися на основі веб-ресурсу, до якого буде мати доступ кожен охочий, бо саме це зробить її більш прозорою. А отже, в такій ситуації будемо мати справу з веб-вразливостями, які на даний момент є найбільш небезпечними одразу після соціальної інженерії. Кожні 5 років компанія OWASP [29] надає звіт з топ-10 веб-вразливостей, які найчастіше використовувалися зловмисниками. Цей документ є важливим при створені веб-серверів та веб-сайтів для розуміння можливих точок відмови системи. Звіт на сьогоднішній день описано на рис. 2.3:

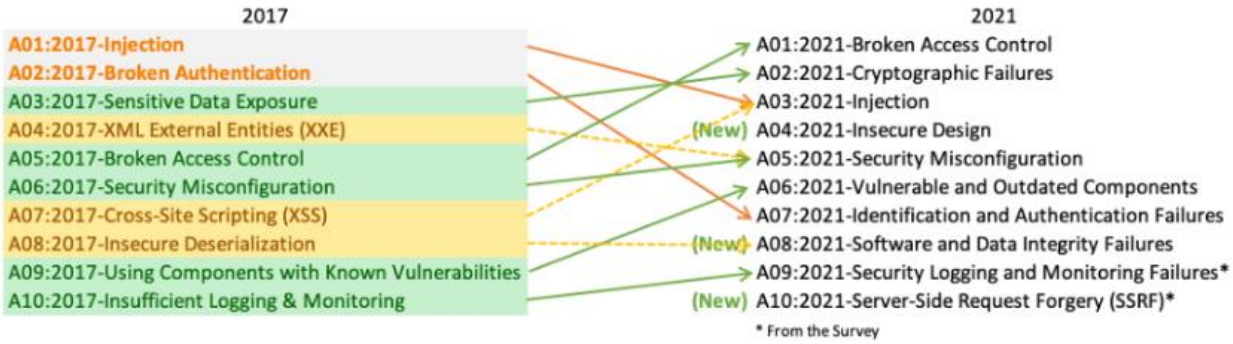

Рис 2.3 – Топ-10 веб-вразливостей згідно OWASP

Виходячи з цих вразливостей, компанії зазвичай користуються послугами тестувальників на проникнення (penetration tester), яких вони наймають або створюють постійні команди всередині компанії. Саме завдяки команді тестувальників можна зрозуміти, які вразливості на даний момент існують саме у вашій системі, саме на цей момент часу, і швидко їх «закрити».

Звісно всі вразливості неможливо просто прибрати, вони будуть завжди і з кожним роком будуть знаходити нові, саме тому тестувальники є важливою складовою системи захисту, бо веб-вразливості мають характер постійного оновлення і впровадження.

OWASP також має дуже важливу документацію щодо принципів безпеки веб-ресурсів, вона складається з шести пунктів [1]:

1) Мінімізувати площу атаки – що відноситься до всіх потенційних вразливостей, які можуть бути використані зловмисниками.

2) Принцип найменших привілеїв – означає що користувач буде мати найменш можливі привілеї, які необхідні йому для виконання щоденних задач.

3) Захист у глибину – організації повинні мати різні механізми та системи контролю безпеки, які пом’якшують ризики та загрози.

4) Розділення обов’язків – критичні зобов’язання повинні розподілятися на багато людей, які в свою чергу слідують пункту 2.

5) Безпека повинна бути простою – необхідно уникати непотрібних та надто ускладнених рішень.

6) Виправляти проблеми безпеки необхідно правильно – коли відбувається інцидент безпеки, необхідно знайти першопричину, стримати вплив атаки, виявити вразливість, що була використана, провести тести та переконатися, що усунення пройшло успішно.

Ще одним з важливих механізмів захисту є впровадження команди Threat hunter. Це спеціалісти, які ще на етапі розробки програмного забезпечення або веб-ресурсів будуть проводити роботи з пошуку можливих загроз, які будуть використані проти вашої системи у майбутньому. Чому така команда є особливо важливою на початковому етапі? Через те, що відомі на момент початку роботи загрози можуть вже бути не актуальні в силу впроваджених засобів захисту, але вже на момент випуску кінцевого продукту можуть бути знайдені загрози та вразливості, які не були належним чином захищені, і до вашої системи може бути застосована атака нульового дня.

Важливо розуміти, що вищеописані механізми захисту необхідні при побудові системи з веб-застосунком, хоча електронне голосування є сезонною системою, при використанні веб-сервісів, система буде працювати завжди, а отже потребує постійного захисту.

2.1.4.5 Шифрування

Один з найнадійніших механізмів збереження даних – шифрування [19]. Це є процес перетворення інформації з відкритого тексту у гешований код за допомогою ключа, що робить вихідний текст не читабельним. Розшифрування можливе лише за умови використання того самого ключа. Цей процес мінімізує ризики під час обробки та передачі зашифрованих даних, через відсутність

автентичного ключа у третіх осіб. Зашифровані дані будуть зберігатися надійно і буде неможливо отримати несанкціонований доступ до них без вірного ключа.

Наразі існує безліч алгоритмів шифрування, кожен має свої переваги та недоліки, деякі швидші, деякі надійніші. Але правило шифрування одне – чим довші за довжиною вхідні дані, тим надійніше шифрування, тим важче його зламати (або неможливо взагалі). Описувати роботу кожного алгоритму не є ціллю цієї роботи, адже шифрування не буде основним механізмом захисту у методі, що пропонується.

2.1.4.6 Посилення безпеки

Посилення безпеки [1] – це процес, в результаті якого зменшується вразливість систем та площа атак. Посилити безпеку можливо в багатьох аспектах системи, але в основному цей процес використовується в наступному:

- обладнання;
- операційні системи;
- додатки;
- комп’ютерні мережі;
- бази даних (БД).

Що саме означає посилення безпеки в контексті зменшення вразливості системи? Рівно те, про що було описано вище у попередніх пунктах, але більш комплексно, використовуючи плани, систематизацію та тестування. Наприклад, для зміцнення (посилення) обладнання буде використовуватись активне оновлення самого обладнання на фізичному рівні і його фізичний захист. Посилення операційних систем потребує також постійного оновлення, використання сторонніх актуальних систем захисту (антивірус, двохфакторна автентифікація і т.п.), використання віртуальних машин, або пісочниць для тестування. До посилення мереж можна віднести фільтрацію портів, обмеження мережевого доступу, шифрування, бекапування, оновлення і т.д.

При побудові систем електронного голосування дуже важливо проводити посилення безпеки кожного окремого аспекту.

2.1.4.7 Хмарна безпека

Зазвичай хмарні сервіси дуже спрощують використання деяких застосунків або програм. У нашому випадку хмарні сервіси можливо використовувати як сховище даних. Звісно це дорогий варіант, але він може бути надійнішим, ніж звичайне фізичне сховище.

Безпека в хмарних сервісах досягається за допомогою коректної конфігурації системи, коли використовуються тільки ті сервіси, які є необхідними для роботи конкретного проєкту, і не робить усю систему надто складною. Одним з найважливіших механізмів у роботі хмарного сховища є Identity Access Management (IAM) – що є колекцією процесів та технологій які допомагають організаціям керувати цифровими персональними даними у їх середовищі. А також авторизує процес використання користувачами різних хмарних сервісів.

Обирати хмарні сервіси може бути корисним не тільки через простоту, а й через політику розподілення безпеки, що означає, що провайдер хмарних сервісів бере на себе частину безпеки, і несе за неї відповідальність. Такий підхід дозволяє будувати міцний захист, але об’єктивно створює більше загроз, при розірванні з’єднання.

2.1.5 Фреймворки

Фреймворки інформаційної безпеки [12] надають вичерпну кількість документації, яка окреслює підхід організації до інформаційної безпеки і визначають як безпека впроваджується, керується та посилюється. Включає в себе:

- Політики: окреслюють цілі, принципи та керівні документи для досягнення конкретних цілей організації;
- Стандарти: документи, що встановлюють спеціалізовані вимоги або специфікації для конкретного процесу, продукту або сервісу;
- Настанови: документи, що надають рекомендації та найкращі практики для досягнення конкретних цілей або завдань;

- Процедури: набір конкретних кроків для виконання конкретного завдання або процесу;
- Базиси: набір мінімальних безпекових стандартів або вимог, які повинна виконувати і використовувати система організації.

Зазвичай такі документи вже існують, і організації керуються вже створеними фреймворками. Але іноді є необхідність створити свої, для специфічних завдань або для конкретної компанії. В такому разі існують кроки для розробки таких документів:

1) Визначення обсягів та мети: необхідно визначити, що документ буде покривати та для чого він потрібен, як, наприклад, політика паролів – необхідна для забезпечення надійності та безпеки паролів користувачів.

2) Дослідження та огляд: необхідно досліджувати чинні закони, регуляції, стандарти індустрії та найкращі практики, щоб бути певним, що документ є релевантним. Важливо дослідити документи, які вже існують для запобігання дублікатів.

3) Складання документу: на цьому кроці розроблюється план і починається складання документу, в дотриманні найкращих практик для написання чітких і лаконічних політик, процедур, стандартів, інструкцій і базисів. На цьому етапі також необхідно переконатися, що документ є коректним, практичним і, що він відповідає цілям організації.

4) Огляд та схвалення: готовий документ необхідно, щоб перевірили зацікавлені сторони такі, як експерти з конкретних напрямків та вище керівництво. Згідно відгуків проводиться корекція документу і знову проводиться огляд і остаточне схвалення.

5) Впровадження і комунікація: всі працівники та зацікавлені сторони яким необхідно знати про новий документ, повинні знати про нього. Необхідно переконатися, що вони розуміють свої ролі і обов’язки щодо впровадження документу. На цьому етапі рекомендується розробка програми навчання та впровадження її для підвищення обізнаності працівників для гарантування розуміння та дотримання документа.

6) Перегляд та оновлення: документ потребує регулярного перегляду та оновлень для переконання, що він залишається актуальним та практичним. Важливо коригувати документ і на основі відгуків, і на основі загроз, які з’являються під час його роботи.

2.1.6 Управління ризиками

Зберігати персональні дані користувачів – великий ризик, дані можуть стати ціллю для зловмисників, і тому важливо розуміти як адекватно сприймати цей ризик, контролювати його і створювати безпечну середу для роботи.

Якщо розглядати ризики з точки зору звичайної людини, то це є певна ймовірність того, що щось небажане або шкідливе може статися через якісь дії або події [35]. Будь-яка активність тягне за собою певний рівень ризику. В будь-якій ситуації ризиками можна управляти трьома шляхами: запобігання, прийняття, зменшення. Виходячи з назв зрозуміло, що при запобіганні ризиків – будуть створюватися умови, при яких ризик не має ймовірності статися, а при її виникненні, будуть проводитися заходи для запобігання ризику. Прийняття – означає, що ймовірність ризику приймається, і активність не припиняється навіть при достатньо високій ймовірності. Зменшення вимагає постійного моніторингу ризиків для вчасного зменшення ймовірності його виникнення.

На допомогу в управлінні ризиками приходять фреймворки, як вже зазначалось, це вичерпна документація, а отже використовується в низці методологій. Для управління ризиками використовуються в основному такі методології:

- NIST SP 800-30: Розроблена Національним інститутом стандартизації. Включає в себе ідентифікацію і оцінку ризиків, визначення ймовірностей та впливу ризиків, а також розробку планів реагування на ризики.
- Facilitated Risk Analysis Process (FRAP): Спрощений процес аналізу ризиків – методологія, що включає аналізування ризиків групою зацікавлених осіб у команді.
- Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE): Методологія оцінки ризиків, яка базується на основі процесу

визначення пріоритетів активів на основі їх критичності для організації, і визначення загроз і вразливостей, які можуть впливати на ці активи.

- Failure Modes and Affect Analysis (FMEA): Зазвичай використовується в інженерії, передбачає визначення потенційних збоїв у системах або процесах, а також аналіз наслідків від збоїв або відмов і ймовірність їх виникнення.

Згідно вищевказаного фреймворку, NIST SP 800-30 є чотири основні процеси управління ризиками, а саме [28]: окреслення ризику, оцінка ризику, відповідь на ризик, моніторинг ризику.

Окреслення ризику – процес, коли організація визначає «рамки» в яких ризик має місце, контекст в якому виникає ризик. Для окреслення, необхідно відповісти на такі питання:

1) Які є припущення щодо загрози або вразливості, яка ймовірність їх появи і які можливі наслідки?

2) Які є обмеження щодо оцінки, реагування та моніторингу ризику?

3) Які прийнятні рівні ймовірності ризику, який прийнятний ступінь невизначеності?

4) Які бізнес-функції мають найвищий пріоритет, які можливі компроміси щодо ризиків?

Під час процесу оцінки ризиків важливо пам’ятати, що ризики можуть бути рукотворні, природні та технічні. З природними та рукотворними все зрозуміло, а технічні потребують деякого пояснення. До технічних ризиків відносяться ті, що викликаються технологічними відмовами, несправностями або вразливостями: відсутність електроспоживання, відмови програмного забезпечення або обладнання, витоки даних і т.д. Отже під час другого процесу управління ризиків необхідно розглянути такі питання:

1) Які ризики необхідно враховувати?

2) З якими вразливостями вони пов’язані?

3) Яким буде вплив та наслідки, якщо вразливість буде використана ризиком?

4) Яка ймовірність використання вразливості?

Наприклад, можна розглянути два результати процесу описаного вище, для ризику природного характеру і рукотворного:

1) Ризик: повінь

Вразливість: офіс знаходиться біля річки.

Вплив: офісні приміщення та обладнання будуть зруйновані або непридатні для використання.

Ймовірність: незначна.

2) Ризик: вірус-вимагач

Вразливість: дані зберігаються на серверах.

Вплив: втрата доступу до баз даних або самих даних.

Ймовірність: висока.

Процес відповіді на ризики фокусується на тому, як організації будуть відповідати на ризики, які окреслюються в процесі оцінки ризиків. З можливих відповідей виділяються чотири:

- Уникнення ризику – якщо компанія вирішає прибрати активність, яка може призвести до ризику, вона уникає його;
- Розподілення ризику – компанія може вирішити, що можливі ризики надто серйозні, і вона не зможе самостійно їх витримати, тоді вона може придбати страхування;
- Пом’якшення ризику – компанія інвестує у контрзасоби для зменшення можливих ризиків до прийнятного рівня;
- Прийняття ризику – іноді контрзасоби є надто складними та дорогими для впровадження, а ризик не є надто критичним, в такому разі можна прийняти ймовірність виникнення ризику.

Але важливо, що ігнорування ризику не є прийнятним варіантом. А прийняття ризику в свою чергу не є його ігноруванням, це означає, що ризик був проаналізований, як його ймовірність, так і його вплив, і навіть контрзасоби. Однак прийняття означає, що є причини залишити все як є.

Вже після оцінки ризику, розуміння його впливів, контрзасобів і відповідей на нього, впроваджується процес моніторингу. Є багато причин необхідності такого процесу, навіть, коли всі необхідні засоби захисту від

ризику були впровадженні. Моніторинг допоможе знайти та додати нові ризики, виключити ризики, які більше не несуть загрози або проаналізувати контрзасоби, які впроваджені проти ризиків, що вже існують.

Процес моніторингу включає в себе наступні сфери:

- Моніторинг ефективності: впроваджене рішення проти ризику може бути ефективним лише на момент його впровадження. За допомогою моніторингу ефективності можна точно зрозуміти чи є впроваджені механізми ефективними для оцінених ризиків, і чи коректно він пом’якшується.
- Моніторинг змін: зміни щодо ризиків можуть бути пов’язані зі змінами у бізнес-моделі або змінами у інформаційній системі. А будь-які такі зміни несуть за собою утворення нових ризиків.
- Моніторинг відповідності: використання нових законів, документів та фреймворків буде мати відповідні наслідки, і тому нові політики повинні бути впроваджені

Деякі з цих процесів є швидкоплинними, деякі доволі тривалими, але кожен важливий. Правильним рішенням буде створення команди управління ризиків, для того, щоб вони виконували безпосередньо свої функції, але це є індивідуальним рішенням кожної організації.

2.1.7 Життєвий цикл безпечної розробки програмного забезпечення

При будь-якій архітектурі, система електронного голосування буде мати своє програмне забезпечення, і процес його розробки повинен стати початком планування безпеки всієї системи голосування.

Під час життєвого циклу розробки ПЗ (далі SDLC) можна помітити, що тест безпеки проводиться дуже пізно. Вразливості та помилки дуже пізно стають явними, що в свою чергу робить доволі дорогим та тривалим процес їх вирішення та полагодження. В багатьох випадках тестування безпеки не розглядається на безпосередньо етапі тестування, і тому більшість помилок і вразливостей знаходять кінцеві користувачі вже після публікації програмного забезпечення і його використання. Моделі Secure SDLC (SSDLC) спрямовані на те, щоб тестування безпеки і її впровадження було на кожному етапі життєвого циклу розробки.

Інститут систем і наук IBM досліджував питання дороговартості процесу виправлення помилок на різних етапах розробки [14] і виявив, що на етапі впровадження ПЗ, виправлення помилок коштує у 6 разів дорожче, ніж на етапі проектування. В той самий час на етапі тестування цей процес буде коштувати у 15 разів дорожче, і у 100 разів на етапах обслуговування і експлуатації. Варто зазначити, що раннє виявлення вразливостей дуже знижує бізнес-ризики.

SSDLC включає в себе впровадження процесів як тестування безпеки та інших активностей у безпосередній процес розробки. До прикладів входить написання вимог безпеки на тому ж рівні як і функціональних вимог і проведення аналізу архітектурних ризиків на етапі проектування життєвого циклу розробки. Фази SSDLC наступні [13]:

- Risk assessment (оцінка ризику) – на ранніх етапах життєвого циклу розробки важливо визначити міркування безпеки, які будуть сприяти моделі «безпечний-за-проектом» (secure-by-design).
- Threat modeling (моделювання загроз) – процес виявлення потенційних загроз, коли не існує належних контрзасобів. Є дуже ефективним у парі з оцінкою ризиків і під час етапу проектування [40].
- Code review (перегляд коду) – може бути ручним або автоматизованим. Важливий процес на етапах розробки, коли пишеться код.
- Security assessment (оцінка безпеки) – сюди відноситься тест на проникнення і оцінка вразливостей. Є формою автоматизованого тестування, яке допомагає ідентифікувати критичні шляхи у програмі, які можуть привести до вразливостей. Однак ці оцінки є гіпотетичними, оскільки не моделюють атаки. Однак тестування на проникнення навпаки визначає недоліки та намагається їх використати. Пентест виконується на етапах експлуатації та обслуговування після створення прототипу ПЗ.

Процеси оцінки ризиків та моделювання загроз були ширше розібрані в цій роботі, тому в цьому розділі буде описано процес безпечного програмування та оцінки безпеки.

Аналіз та огляд безпеки коду є дуже важливим, адже дослідження Verizon про [27] витоки даних показало, що 43% витоків відбуваються через атаки на

веб-додатки, деякі відбуваються через вразливості веб-додатків. Перевірка або сканування коду під час SSDLC, особливо у фазі впровадження допоможе підвищити стійкість та безпеку продукту без необхідності додаткових витрат на майбутні патчі (виправлення).

Сам процес перевірки безпеки коду означає, що код буде верифіковуватися та проходити валідацію для певності у тому, що вразливості, які будуть знайдені, можуть бути пом'якшені або прибрані, для унеможливлювання їх використання зловмисниками (загрозами). Перевіряти код можна вручну або автоматизовано. Ручну перевірку коду зазвичай здійснює експерт, який аналізує та перевіряє вихідний код строка за строкою, щоб знайти вразливості. Для отримання перевірки високої якості, експерту необхідно постійно комунікувати з командою розробників, для розуміння кожного аспекту ПЗ. Результатом аналізу буде звіт для розробників, де будуть зазначені необхідні виправлення.

Автоматичні системи аналізу коду поділяються на два типи – статичні та динамічні. Статичні перевіряють код без безпосереднього запуску програми, в свою чергу динамічні проводять огляд під час того як програма працює. Існує низка інструментів для аналізу коду, які часто використовуються розробниками:

1) SAST – Static Application Security Testing, метод прямого аналізу коду. Може знаходити помилки та вразливості навіть ще до того, як код буде імплементовано у ПО, якщо використовується на етапі розробки.

2) SCA – Software Composition Analysis, йде поруч із попереднім методом. Використовується для сканування залежностей, і допомагає знаходити і аналізувати будь-які open-source компоненти проекту. Наразі цей метод є одним з найважливіших для сучасних розробників.

3) DAST – Dynamic Application Security Testing, виходячи з назви є динамічним методом аналізу, який працює під час роботи програми і безпосередньо після компіляції коду, але не має доступу до вихідного коду. Зазвичай використовується як інструмент для сканування веб-додатків на предмет вразливостей безпеки. Під час пошуку може відправляти повідомлення розробникам з інформацією про знайдені вразливості. Працює як автоматична

система тестування на проникнення, емулюючи автоматизовані атаки, копіюючи поведінку зловмисників.

4) IAST – Interactive Application Security Testing, аналізує код на предмет вразливостей коли застосунок працює, і має доступ до коду безпосередньо. Інструмент використовується для аналізу і звітування щодо безпекових помилок мобільних та веб-додатків. Цей інструмент був створений для ігнорування лімітів SAST та DAST. Проводить тести в режимі реального часу як і DAST, але використовує систему перевірки коду як SAST і має можливість повідомляти про знайдені помилки.

5) RASP – Runtime Application Self Protection, розгортається на сервері та перевіряє вхідний та вихідний трафік, а також патерни поведінки кінцевого користувача для запобігання атак. На відміну від інших інструментів використовується на етапі релізу проекту, і фокусується на безпосередньо безпеці. Під час знаходження помилок у безпеці одразу сповіщає команду розробників або SOC і блокує доступ до запиту.

Розуміння, як працюють ці інструменти, дуже важливе, адже їх впровадження дуже спростить процес розробки, та зробить його більш безпечним на всіх етапах. Важливо також розуміти, на яких етапах SDLC потрібно впроваджувати ці інструменти, для цього є таблиця 2.3:

Таблиця 2.3 – Системи аналізу відповідно до етапів розробки

Етап розробки	SAST, SCA
Етап інтеграції	SCA
Етап прийняття	SAST, DAST
Етап пре-релізу	SAST, DAST, IAST
Реліз	RASP

2.1.8 Механізми захисту персональних даних систем електронного голосування

Отже, вищезазначені механізми та системи захисту персональних даних можна імплементувати у безпосередньо систему електронного голосування, підводячи підсумок, система повинна мати наступні механізми захисту:

- Фізичний захист місць зберігання даних, дотримування політики безпеки щодо персоналу та доступу.
- Надійна побудова мережі, з використанням налаштованого брандмауера або декількох на розрізі суб-мереж, постійним моніторингом трафіку, використовувати т.з. Playbook, або керівництво щодо використання, яке описує механізм дій при втручанні у системи зловмисників.
- Впровадження та активна робота підрозділу кібербезпеки, SOC, аналітиків безпеки та «мисливців» за загрозами, активна комунікація між підрозділами для досягнення мети з побудови та підтримки стійкої системи захисту інформації.
- Автоматизація – це впевненість, що жодна загроза, втручання, злам або будь-яка інша не бажана активність у вашій системі не пройде непоміченою, а всі безпекові інциденти будуть розслідувані та прийняті до уваги при оновленні механізмів та систем.
- Аудит безпеки. Такий аудит повинен проводитися не один раз, а систематично і часто. В кібербезпеці аудит [1] – означає перегляд засобів контролю безпеки, політики та процедур у порівнянні з набором очікувань. Тобто система за висновком аудиту повинна пройти всі тести та бути захищеною. Аудит проводиться як внутрішній, так і зовнішній.
- Використання фреймворків є важливим і необхідним, адже вони допомагають будувати повну і зрозумілу структуру системи безпеки.
- Управління ризиками – є важливою складовою всієї безпеки. Знаючи ворога, можна точно знати, де він вдарить, і як на це можна відповісти.
- Впровадження безпечного життєвого циклу розробки програмного забезпечення та тестування безпеки на кожному його етапі дозволить скоротити

витрати на майбутні виправлення помилок, та знижує ризики використання вразливостей.

- Проактивне та регулярне тестування на проникнення є важливою складовою оцінки ризиків та як механізм захисту від майбутніх загроз.

2.2 Міжнародний досвід застосування механізмів захисту персональних даних на прикладі Естонії

Передовою в сенсі захисту персональних даних, як вже зазначалось вище, є Естонія. Країна, яка дуже серйозно ставиться до захисту даних свого народу. Майже вся система державних установ та сервісів Естонії оцифрована. Така система має великі недоліки у сенсі безпеки, адже важливо прорахувати кожен аспект, для того, щоб захистити сенситивну інформацію.

Першим механізмом захисту персональних даних Естонії є Закон про захист персональних даних [30]. Саме він регулює, які дані кваліфікуються як персональні, як вони повинні оброблятися, де зберігатися, хто до них має доступ і багато деталей, які одразу не спадають на думку, але в комплексі заходів є дуже важливими. Право кожної люди на захист її персональних даних є конституційним правом.

Наступним механізмом безпеки є органи захисту персональних даних – Інспекція із захисту даних (DPI) [33]. Саме вона стежить за тим, щоб приватна інформація (персональні дані) людей була достатньо захищена. Також інспекція забезпечує достатній доступ до інформації про діяльність установ.

Одразу після основних законодавчих механізмів, йде дуже прискіпливий вибір персоналу. Вимоги до спеціалістів із захисту даних є доволі високими у порівнянні з іншими країнами ЄС. Всі ці вимоги також регламентуються Інспекцією з захисту даних і включають в себе необхідність знати [7]:

- Законодавство країни, та законодавчі настанови ЄС про захист даних;
- Принципи інформаційної безпеки, відповідні технології та розробки;
- Актуальні технології та розробки в сфері інформаційно-комунікаційних технологій та інформаційної безпеки, їх можливий вплив на організаційні процеси;

- Принципи та методи аналізу та профілювання даних, псевдонімізацію та анонімізацію;
- Системи та методи аналізу та управління ризиками;
- Основи та методи проведення оцінки впливу на захист даних;
- Відповідні джерела інформації (ЄС та національне законодавство);
- Як визначати ризики та складати плани дій для пом'якшення ризиків;
- Як керувати та координувати процеси захисту даних організації, включаючи розробку стратегії та інструкцій, а також впровадження принципів захисту даних;
- Як ідентифікувати та документувати операції з обробки даних і порушення, включаючи порушення, про які необхідно повідомляти наглядові органи.

Виходячи з інформації на офіційному сайті Естонії e-estonia.com [25], можна зрозуміти, що їх кібербезпека будується на трьох «стовпах»: e-ID, X-Road та KSI blockchain. Всі вони репрезентують комплекс механізмів захисту персональних даних, які утворюють екосистему кібербезпеки. E-ID дозволяє людям ідентифікувати себе інформаційно, і забезпечує індивідуальність та автентичність даних. ID-карта – основа електронної ідентифікації, яка є ідентифікаційним документом для будь-якого жителя або постійного резидента Естонії. На додаток до картки існує ще два механізми – MobileID та SmartID. ID-карта використовує інфраструктуру відкритого ключа. Ключі які необхідні для отримання електронного підпису та для ідентифікації зберігаються на чипі фізичної картки. Вони захищені ПІН кодами, які знає лише людина-власник картки. Використовується двох-факторна автентифікація, яка забезпечує неможливість викрадення персональних даних, у випадку викрадення картки або ПІН кодів.

Одним з ключових і найбільш важливих функцій e-ID – електронний підпис (ЕП) на основі контейнера, тобто інформація зберігається в незмінному форматі у контейнері типу AsiC-E, таким чином можливо зберігати в одному контейнері різні файли різних форматів, підписаних одним електронним

підписом. ЕП є машинозчитуваним, що допомагає автоматизувати низку сервісів та систем. Завдяки підпису зберігається цілісність даних.

Естонія не використовує великих супер-сховищ даних, натомість система X-Road, що основана на розподіленій архітектурі, забезпечує безпечний та ефективний обмін даними між базами даних та різними установами. Зберігає правило конфіденційності, установи, які не мають доступу до інформації, не отримають її. З 2001 року, система працює безперервно, і це є найбільшим доказом її ефективності.

KSI blockchain – технологія, яка допомагає забезпечувати цілісність даних. Вона записує усі зміни, тобто завжди відомо, коли та ким вони були зроблені. Технологія убезпечує державні мережі, історія не може бути переписана ніким і автентичність електронних даних може бути математично доведена. Це означає, що ніхто – ані хакери, ані системні адміністратори, навіть влада держави – не може маніпулювати даними без наслідків.

Система шифрування Естонії дозволяє безпечно передавати конфіденційну інформацію. Тип шифрування, який використовується, не розголошується, але він є короткочасним у використанні, бо термін дії eID сертифікату закінчується як і ключі розшифрування, які зберігаються на чипі. Зашифровані файли можуть бути надіслані через будь-які канали обміну інформації з повним забезпеченням конфіденційності, цілісності та доступності даних. Шифрування відбувається за допомогою ідентифікаційного коду отримувача. Розшифрування в свою чергу використовує його ж ПІН код.

3 МОЖЛИВІ ПРОБЛЕМИ В РЕАЛІЗАЦІЇ СИСТЕМ ЕЛЕКТРОННОГО ГОЛОСУВАННЯ

Досліджуючи мережу у пошуках наукових робіт з цієї теми, ми прийшли до висновку, що є чотири основні лінії проблем у впровадженні систем електронного голосування:

- Соціальні фактори, проблеми та обмеження;
- Законодавчі регулятори права та конституційні гарантії;
- Технічні можливості;
- Безпека.

Це означає, що система електронного голосування є складною системою, з великою кількістю різнотипних складових, відносно яких необхідно забезпечувати захист самої системи та інформації, що у ній циркулює. Ну і звісно забезпечувати правильне та безпечне функціонування самих цих складових.

3.1 Соціальні проблеми

Україна велика країна, з різними людьми, а отже ми не зможемо однаково впливати на кожного. Впровадження електронних онлайн голосувань буде неможливе, якщо воно буде єдиним видом виборів. Ця неможливість випливає через соціальні групи населення, менталітет і очевидно довіру.

Соціальні групи в даному випадку відіграють вирішальну роль. Люди, яким важко голосувати через Інтернет, з тих чи інших причин, не зможуть виконати своє конституційне право з волевиявлення, а отже вибори будуть не легітимні. Ця проблема потребує або використання змішаного формату голосувань, або впровадження систем навчання різних груп населення волевиявленню через таку форму голосування. Обидва варіанти є доволі складними в реалізації, але все ж таки змішана форма на початкових етапах буде більш прийнятною. Важливо розуміти, що з кожним новим поколінням,

цифровізація суспільства проходить простіше, адже навіть діти користуються цифровими пристроями.

Менталітет деяких верств населення, які можуть не довіряти такій системі теж є однією з великих проблем. Довіра досягається лише чесними прозорими виборами, що в свою чергу є технічним аспектом системи електронного голосування. Але дуже важко отримати довіру від громадян, адже неможливо повністю розкрити систему і те, як вона працює, з цього випливає недовіра виборців до системи. Якщо обговорювати використання програмного забезпечення (ПЗ) у вигляді додатку на смартфони та ПК, ми не можемо гарантовано отримати довіру до цього ПЗ, чи є воно надійним або навіть справжнім. Якщо використовувати методи доведення справжності, такі як контрольні суми, то не буде довіри до справжності контрольних сум. Це замкнуте коло недовіри можливо розірвати. Лише шляхом впровадження і тестування можна досягти деяких успіхів зі сторони підвищення явки на такі вибори.

3.2 Законодавче підґрунтя

При впровадженні систем електронного голосування перше, що повинно бути зроблено – законодавчі акти регуляції таких голосувань. Цей аспект є дуже індивідуальним залежно від багатьох факторів країни. Культура, менталітет, довіра до влади і багато інших факторів будуть впливати на ефективність законів.

Для України така тема не нова, у 2011 році впроваджувалась концепція ініціативи «Запровадження системи електронного голосування в України» [5] у Верховну Раду, де було зазначено, що на той момент (як і зараз) виборчий процес в Україні проходить через етапи, які є «громіздкими, витратними та вразливими», оскільки на всіх етапах існує великий вплив людського фактору, а отже існує велика недовіра з боку учасників виборчого процесу і навіть світової спільноти.

Електронні онлайн вибори повинні проводитися з дотриманням усіх міжнародних норм і прав людини [18]:

- Право таємниці вибору: виборець має право голосувати таємно, і держава повинна захищати це право, і унеможливлювати тиск на громадян через їх вибір. Окрім цього необхідно забезпечити право перевірити свій голос і результати виборів;
- Право на вільний вибір: кожна людина має право вільно обирати і висловлювати свою думку, без примусу чи впливу сторонніх осіб;
- Рівність виборчого права: система голосування повинна забезпечувати рівні умови – один виборець – один голос;
- Загальне виборче право: кожна людина, яка має право волевиявлення, повинна мати можливості це зробити, а також система повинна захищати права обранців, за яких віддаються голоси;
- Право обізнаності: кожен виборець повинен бути свідомої думки про те, як працює система, як вона рахує голоси та як проходить увесь виборчий процес.

На жаль, саме у цих правах виникає проблема, адже вони забезпечують демократію, прозорість і підвищують довіру суспільства до системи і до влади. Але технічно неможливо виконати деякі з них, наприклад, право обізнаності – неможливо розкривати увесь процес роботи системи, адже це дозволить загрозам у вигляді хакерів провести «обернену розробку» і знайти критичні вразливості системи. Так само система повинна забезпечувати незмінність голосу, але, якщо він був зроблений під примусом, він не є легітимним, через що виникає більше проблем з довірою.

3.3 Технічні вимоги та проблеми

Голосування через мережу Інтернет набагато складніше у реалізації, аніж за допомогою електронних машин для голосування. І важливо уточнити, що для таких машин існують стандарти, затвердженні відповідними органами, тоді як ніяких технічних стандартів для онлайн голосування не існує. І хоча NIST у 2011 році намагалися дослідити питання онлайн голосування [32], вони дійшли висновку, що такі системи є неможливими: «Через труднощі валідації та верифікації програмного забезпечення на віддалених серверах електронних

систем голосування та персональних комп'ютерів, набагато важче аудит таких систем і їх контроль». З того часу технічні засоби дуже покращилися, а отже є надія, що наразі такі системи є можливими.

Основними вимогами до системи електронного онлайн голосування є:

- Можливість безпомилково і безупинно працювати протягом виборчого процесу;
- Забезпечувати максимальний рівень безпеки даних;
- Зберігати історію голосувань для їх верифікації за необхідності;
- Можливість працювати при постійному доступі до мережі без помилок;
- Бути достатньо стійкою при можливих атаках;
- Надавати достатній рівень швидкодії та ефективності для роботи користувачів;
- Забезпечувати достатній рівень пропускної здатності;

Але існує проблема, яку ніхто не висвітлює, але вона з кожним роком стає все більш важливою – боти. Комп'ютерні програми, які намагаються маскуватись під людину – не нова технологія, але несуть серйозну загрозу для систем електронного голосування. Не дивлячись на двохфакторну автентифікацію виборців, все ще існує ймовірність використання таких ботів для фальсифікації результатів виборчого процесу. Можливо автоматичний тест Тюрінга (CAPTCHA) вирішить цю проблему, але розвиток ботів може створити серйозну загрозу легітимності виборів.

3.4 Безпека

Система, попри простоту процесу голосування, повинна мати складну, в сенсі можливості несанкціонованого проникнення, систему безпеки. Очевидно, що важливо враховувати безпосередню архітектуру проекту, на основі якого будується безпека. Якщо це веб-ресурс – потрібен стійкий захист мережевих каналів передачі даних і надійна база даних, для збереження інформації. Якщо це система на основі кліент-серверного додатку – будуть використані інші

інструменти. Розглянемо основні проблеми впровадження такої системи для цих варіантів.

Умовно розділимо варіанти на веб-сайт і додаток.

Веб-сайт – буде зручним інструментом для голосування. Потребує постійних ресурсів для підтримки, вимагає частого оновлення компонентів, які використовуються. З точки зору безпеки персональних даних – буде вимагати від користувача або мануального внесення особистих даних у поля вводу, або надсилати запит на отримання цих даних з джерел на пристрої (наприклад, додаток «Дія»). Такі маніпуляції не є безпечними, адже не виключена атака MitM (Man in the Middle) [38], при якій зловмисник зможе перехопити дані при передачі. Шифрування відповідних даних з подальшим розшифруванням на сервері обробки, хоча і є достатнім для забезпечення захисту, але не є ефективним з точки зору використання ресурсів машинних потужностей.

Додаток – є більш бажаним варіантом, хоча має свої недоліки. Додаток буде завжди на носії кожного виборця. Може мати доступ до персональних даних користувача одразу, не потребує їх попереднього шифрування для передачі. При використанні такої системи голосування буде відбуватися на стороні клієнта, відправлятися на сервер буде зашифрований блок даних, де буде вказано метадані та голос користувача. Гешовані дані користувача теж можуть бути передані для верифікації його голосу і забезпечення цілісності, бажано використовувати «сіль» для більш стійких гешів, які важче зламати. Але ключовим недоліком є те, що існує вірогідність того, що прилад користувача, на якому встановлено додаток може бути зламано/скомпрометовано, і на ньому може бути сплячий вірус, який чекає на передачу даних, або який полює на закриті ключі. На жаль, перевіряти кожен окремий прилад кожного окремого користувача неможливо, бо, якщо у додаток вбудовувати антивірусні механізми, він буде надто великих розмірів і процес оновлення та сканування буде дуже завантажувати носії. Отже, ця проблема існувала і буде існувати, а безпека пристроїв залишається відповідальністю кожного користувача окремо. В свою чергу, зі сторони розробників основною задачею буде створити додаток, який буде стійким до подібних вірусів.

4 МОДЕЛЬ І АРХІТЕКТУРА СИСТЕМИ ЕЛЕКТРОННОГО ГОЛОСУВАННЯ

У даному розділі розглядаються моделі, які використовуються при побудові системи і її архітектура. Розглядається як, використовуючи конкретні сучасні фреймворки і інструменти, будуються моделі загроз та моделі порушника. Розглянемо можливі архітектури такої системи і технології, які можна використати для забезпечення максимального рівня захисту для персональних даних.

Сучасні технології захисту персональних даних дають впевненість, що системи електронного голосування можуть існувати на практиці, і можуть бути ефективним інструментом волевиявлення громадян суспільства. Не дивлячись на всі проблеми, такі країни як Естонія розвивають цей напрямок, отже, може і Україна. Першість в цьому питанні наша країна вже не отримає, але зробити вагомий внесок може.

Перше, що важливо розуміти – довіра людей, хоч і є основним питанням працездатності проекту, не є ключовим аспектом в реалізації. Скоріше, ним навіть нехтують, бо неможливо внести щось нове, якщо завжди прислухатися до суспільства. На жаль для того, щоб будувати подібні системи в Україні, нам необхідно перебудовувати законодавство, впроваджувати нові стандарти захисту персональних даних, або хоча б ратифікувати і користуватися стандартами ЄС, що вже додасть нам інструментів для повної і якісної цифровізації суспільства.

Цей розділ покликаний проаналізувати те, як будуються інформаційні системи в інших країнах, які стандарти та інструменти використовуються для побудови моделей, як спростити цей процес і зробити його захищеним, щоб в результаті отримати якісний продукт.

4.1 Модель загроз

Модель загроз – результат аналізу можливих загроз, абстрактний структурований опис загроз. Може розглядатися як сукупність атак на основні

функціональні властивості захищеності інформаційних об’єктів – конфіденційність, цілісність і доступність, на систему в цілому чи її елементи. Моделювання загроз [36] – це систематичний підхід до виявлення, визначення пріоритету і усунення потенційних загроз безпеці. Моделюючи можливі сценарії атак і оцінюючи наявні вразливості взаємопов’язаних систем організацій, модель загроз дозволяє розробляти проактивні заходи безпеки та приймати якісні рішення щодо розподілу ресурсів. Цей процес і результат націлені на те, щоб зменшити загальний ризик безпеці, шляхом ідентифікації вразливостей і потенційних векторів атаки. Процес є дуже важливим для створення стійкої стратегії безпеки проти кібер-загроз, які постійно розвиваються.

Наразі цей процес є доволі простим та стандартизованим завдяки автоматизації. Існують фреймворки моделювання, наприклад, MITRE ATT&CK Navigator, який надає доступ до великої бази даних загроз, тактик та технік зловмисників, і дозволяє створювати свої моделі загроз для конкретних задач. Але існує і ручний високорівневий процес, який складається з наступних кроків:

- Визначення сфери застосування: визначення конкретних систем, застосунків та мереж, для яких модель будується.
- Ідентифікація активів: потребує розробки діаграм архітектури організації і її залежностей. Важливо встановити пріоритет активів за їх важливістю, яка в свою чергу базується на інформації, яку зберігає актив.
- Визначення загроз: визначити потенційні загрози, які можуть бути застосовані проти визначених активів, такі як кібер-атаки, фізичні атаки, соціальна інженерія або внутрішні загрози.
- Аналізування вразливостей і пріоритет ризиків: аналізувати вразливості базуючись на потенційному впливі ідентифікованих загроз у поєднанні з оцінкою існуючих засобів контролю безпеки. Отриманий список вразливостей і ризиків повинен бути розподілений за пріоритетом, базуючись на можливості їх використання та можливому впливі.

- Розробка і впровадження контрзасобів: розробити і впровадити контроль безпеки, щоб усунути ідентифіковані ризики. Такі засоби і заходи як контроль доступу, оновлення систем, регулярний огляд вразливостей, тощо.
- Моніторинг і оцінка: постійно тестувати і проводити моніторинг ефективності впроваджених контрзасобів і оцінювати успішність моделі загроз.

Слідуючи цим крокам компанія може отримати чітку модель загроз для ідентифікації та пом’якшення потенційних ризиків безпеки і експлуатацію вразливостей зловмисниками, тим самим впроваджуючи кращі і більш надійні системи.

MITRE ATT&CK поділяє техніки на 14 основних напрямків: розвідка, розробка ресурсів, початковий доступ, виконання, постійність, підвищення привілеїв, ухилення від захисту, доступ до облікових даних, виявлення, побічний рух, збір, командування та контроль, ексфільтрація, вплив. Кожен з цих напрямів має багато різних технік, які так чи інакше можуть і будуть використовувати зловмисники при плануванні, безпосередній атаці та після успішної або не успішної атаки.

Поміж традиційної моделі загроз існують інші фреймворки, які також використовуються для моделювання, але в більш широкому розумінні. Фреймворк DREAD [16], що є акронімом від: Damage, Reproducibility, Exploitability, Affected Users, Discoverability. Кожен з цих термінів відповідає за окремий пункт моделі. Фреймворк був створений компанією Microsoft, і хоча скоріше це інструмент оцінки ризиків, він є дуже важливим в моделюванні загроз, адже допомагає побудувати пріоритетність загроз та вразливостей.

Отже, опишемо кожен з пунктів/етапів окремо:

1) Damage (ушкодження): потенційна шкода, яка може стати результатом успішної експлуатації вразливості. Сюди входить втрата даних, відключення системи та репутаційні втрати. Відповідає на питання «На скільки поганою може бути атака?»

2) Reproducibility (відтворюваність): простота з якою потенційних хакер/зловмисник може успішно відтворити експлуатацію вразливості. Чим

вищий цей показник у конкретної загрози, тим вищий ризик її використання. Відповідає на питання «Як легко відтворити атаку?»

3) Exploitability (можливість експлуатації): рівень складності експлуатації вразливості, виходячи з таких факторів, як необхідні технічні навички, доступність інструментів або експлойтів, та час необхідний для виконання успішного зламу. Відповідає на питання «Скільки роботи необхідно для запуску атаки?»

4) Affected Users (вплив на користувачів): кількість людей/користувачів, на яких вплине використання вразливості загрозою. Відповідає на питання «Як багато людей буде під впливом атаки?»

5) Discoverability (можливості виявлення): простота знаходження вразливості для її експлуатації загрозою, враховуючи багато факторів. Відповідає на питання «Як легко знайти вразливість?»

Модель DREAD базується на суб'єктивній думці та оцінках експерта, який будує її. Однак, надійність таких суджень можна покращити виконуючи ряд настанов:

- Необхідно впровадження стандартизованого набору настанов і визначень для кожного етапу DREAD, що дозволить узгодити розуміння щодо того, як проводити оцінку вразливості. Це може бути досягнуто додатковими прикладами та сценаріями, які наочно показують як оцінювати вразливості за різних обставин.
- Важливо заохочувати співпрацю кількох команд. Організація конструктивного зворотного зв'язку від різких учасників допоможе обґрунтувати присвоєну оцінку, що призведе до більш точних даних.
- Використовувати фреймворк DREAD разом з іншими методологіями оцінки ризиків і регулярно оновлювати обрані методи та техніки для їх актуалізації і перевірки відповідності до організаційних вимог.

Використовуючи ці настанови, можна приборкати суб'єктивність оцінки та покращити точність оцінки ризиків.

Інший фремворк STRIDE [15], що теж був розроблений Microsoft, допомагає ідентифікувати та категоризувати потенційні загрози безпеки під час

розробки ПЗ та дизайну системи. STRIDE так само є акронімом від: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of service, Elevation of Privilege.

Опишемо окремо кожний пункт:

- Spoofing (Спуфінг): неавторизований доступ або імперсоналізація користувачів або систем (включає атаки фішингу).
- Tampering (Фальсифікація): неавторизована модифікація або маніпуляція даними або кодом.
- Repudiation (Відмова): можливість заперечити дію, що відбулася, зазвичай можливо через недостатній аудит та відсутність логування.
- Information Disclosure (Розкриття інформації): неавторизований доступ до сенситивної інформації – персональної або фінансової.
- Denial of Service (Відмова сервісу): порушення доступності системи, що заважає чесним користувачам отримати доступ.
- Elevation of privilege (Підняття привілей): неавторизоване підняття привілей доступу, що дозволяє загрозам/зловмисникам виконувати шкідливі дії у системі.

Систематичний аналіз цих шести категорій загроз дозволяє організації проактивно визначати потенційні вразливості своїх систем, додатків або інфраструктури, і вчасно зміцнювати усю систему безпеки. Зазвичай результатом аналізу буде таблиця маркерів, такого типу (таблиця 4.1).

Таблиця 4.1 – Приклад таблиці на основі STRIDE фреймворку

Сценарій	S	T	R	I	D	E
Використання SQL ін’єкцій		✓		✓		
Наповнення веб-серверу великою кількістю запитів					✓	

Для впровадження фреймворку STRIDE в моделювання загроз, важливо інтегрувати ці шість категорій загроз у систематичний процес для ефективної ідентифікації, оцінки та пом’якшення ризиків.

Варто зазначити, що системи електронного голосування потребують особливої уваги. Модель загроз повинна будуватися не абстрактно, а конкретно,

бо такі системи можуть використовуватися як на місцевих виборах, так і на президентських, що потребує більшої зосередженості на можливих загрозах і їх контрзасобах. Виходячи з обраної архітектури, більше уваги варто приділяти об’єктивним ризикам, кібер-групам, які є основною загрозою таких систем. Є впевненість, що хакер-одинак не зможе «пробити» захист так легко, як це зроблять організовані групи. Вони несуть основну загрозу.

4.2 Модель порушника

Моделлю порушника [1] називають формалізований або неформалізований опис дій порушника, який відображає його практичні та теоретичні можливості, апріорні знання, час та місце дії і т.д. Такі моделі є невід’ємною частиною інструментів пом’якшення загроз, адже у комплексі дозволяє повністю розуміти: які вразливості є в системі, які ризики представляють ці вразливості, як ці ризики будуть використовуватися загрозами, в нашому випадку порушниками, для досягнення конкретної мети. Виходячи з цих суджень можна припустити, що модель порушника повинна мати наступну інформацію:

- Хто може кваліфікуватись як порушник? Чи будь-яка людина може бути ним, або є конкретна категорія осіб?
- Який рівень навичок та знань необхідно мати порушнику для успішних дій проти системи?
- Які інструменти можуть бути використані порушником?
- Яка мета і кінцева ціль порушника?
- Звідки порушник може виконувати зловмисні дії проти системи?
- Можливий вплив дій порушника на систему.

Кожне з цих питань необхідно детально дослідити, бо розуміння порушника є основою контрзаходів, якщо дії порушника є зрозумілими для організації – на них простіше адекватно відповідати і швидко реагувати. Якщо ж дії порушника мають хаотичний або незрозумілий характер – то і можливий вплив на систему є невідомим, що саме собою є ризиком.

Кваліфікуватись як порушник може особа, яка може отримати несанкціонований доступ до систем організації, та відповідно може завдати шкоди системі або безпосередньо організації. Порушники можуть бути внутрішніми та зовнішніми:

- Внутрішній порушник – особа, яка може мати безпосередній доступ будь-якого рівня до систем. Зазвичай так кваліфікують співробітників компанії/організації. Результатом дій внутрішніх порушників може стати саботаж, корупція, шпіонаж і звісно несанкціонований доступ та витік даних.
- Зовнішній порушник – може бути будь-яка особа, яка не має відношення до компанії та яка може отримати несанкціонований доступ до систем або мереж організації, при чому навіть фізичний доступ розглядається як можливий.

В свою чергу до зовнішніх порушників можна віднести Advanced Persistent Threats (APT), або постійну просунуту загрозу. APT – група осіб, хакерів, порушників або зловмисників, які є достатньо організовані для створення постійної загрози будь-якій організації. Такі групи можуть бути найманими або ідейними. Їх підхід до зламів є доволі серйозним, вони мають значний досвід отримання несанкціонованого доступу, і як правило досліджують свої цілі заздалегідь і приділяючи цьому багато часу. Можуть залишатись «у тіні» довгий проміжок часу.

Іншою частиною зовнішніх порушників можна назвати Хактивістів – особи-одинаки, але мають змогу створювати колективну загрозу збираючись у групи. Мотивацією їх дій може бути як грошові винагороди, так і проста демонстрація можливостей, пропаганда хактивізму, революції у кіберпросторі або звичайна популярність.

На щастя, зазвичай порушники є доволі передбачуваними, і тому існує поняття «Cyber Kill Chain'», яке доволі складно коректно перекласти. Отже, поняття Kill Chain [26] – це військовий концепт, що визначає структуру атаки. Він складається з набору дій для атаки на ціль. У 2011 році компанія Martin Lockheed внесла фреймворк Cyber Kill Chain як основу для ідентифікації, крок-

за-кроком, дій порушників під час атак. Тобто теоретично, для досягнення успіху зловмисник повинен пройти кожен з кроків ланцюга.

Складові ланцюга наступні:

1) Розвідка – дослідження та збір інформації щодо жертви. Є фазою планування. Використовуються інструменти OSINT (Open-source intel). Під час цієї фази порушник збирає дані, проводить атаки фішингу, та досліджує працівників або людей, які мають доступ до системи-жертви. Досліджує інфраструктуру мережі та фізичний захист.

2) Озброєння – фаза, коли порушник проводить підготовчі дії щодо шкідливого ПЗ, шукає інструменти для зламу, або сам їх створює. Готує у коді можливості для бекдору. Впроваджує системи C2 у ПЗ.

3) Доставка – фаза при якій порушник обирає метод для «транспортування» шкідливих продуктів. І варіантів дійсно багато: фішинг, підкладні пристрої, фізичне проникнення і т.д.

4) Експлуатація – фаза безпосереднього отримання несанкціонованого доступу шляхом експлуатації знайдених на першій фазі вразливостей за допомогою ШПЗ, отриманого на другій фазі.

5) Встановлення – ця фаза використовується порушником для отримання постійної «точки входу» для себе у систему, на випадок, якщо його присутність буде помічена і основний канал буде закрито. Зробити це він може безліччю варіантів, один з яких – використання програм типу Metasploit.

6) Управління і контроль (C2) – після отримання доступу, та створення постійної точки входу, порушник створює канал віддаленого доступу для керування пристроєм жертви з C2 сервером на своїй стороні. Зазвичай таких каналів створюється декілька, знову ж таки для збереження доступу при викритті.

7) Дії над ціллю – ця фаза символізує повний доступ зловмисника до системи і всіх її аспектів. Тепер порушник має змогу отримати все, що він забажає: облікові дані, персональну інформацію і т.д.

Звісно ця модель є не показовою, бо хоча вона і була оновлена у 2015 році, наразі існує лише невеликі її покращення, а порушники вже багато років

розвиваються. З іншого боку, вона все ще працює і з точки зору практики, порушник все ще не може пропустити хоч один з цих кроків. Розробники моделі стверджують, що достатньо розірвати ланцюг на будь-якому кроці/фазі, щоб зупинити атаку.

Ще однією важливою моделлю для аналізу поведінки порушників є модель Діаманта [11]. Модель описує наступний алгоритм з чотирма основними функціями – зловмисник використовує можливості з використанням деякої інфраструктури проти жертви.

Хто такий зловмисник – зрозуміло. Це особа, що стоїть за кібератакою: хакер, загроза або порушник. Згідно моделі знання порушника є невідомими, і зазвичай такими і залишаються до моменту безпосередньої атаки.

Жертва – є ціллю зловмисника. Жертвою може бути організація, особа, адреса електронної пошти, IP-адреса, домен і т.д. Є два види жертв: персона (організації, люди) та актив (мережа, хост і т.д.). Жертви можуть бути остаточними або прохідними, які лише надають зловмиснику деяку інформацію або можливості для досягнення кінцевої жертви.

Можливість – не є чітким поняттям. До можливостей зловмисника можна відносити його знання і навички, а також інструменти та техніки, які він використовує для досягнення мети. Можливості зазвичай окреслюють тактики, техніки та процедури (TTPs) зловмисника. До таких можливостей відносяться всі техніки, які можуть бути використані порушником, навіть тривіальні, такі як ручний перебір паролів.

Інфраструктура – програмне забезпечення або обладнання. Це також IP-адреси, доменні імена, та навіть шкідливі USB пристрої.

Модель Діаманту будується на подіях. Подія визначає дискретну обмежену в часі діяльність, обмежену певною фазою, коли порушник, потребуючи додаткових ресурсів, використовує можливості та методологію за допомогою певної інфраструктури проти жертви. Зазвичай для побудови події не необхідно знати її особливості, майже в усіх ситуаціях очікується, що всі змінні будуть невідомі до викриття події, та до отримання більшої інформації. Нам відомі основні функції: зловмисник, можливість, інфраструктура та жертва,

але в моделі існують ще мета-функції, які не є необхідними, але надають більше інформації. До таких функцій належать:

- Мітка часу – дата та час події. Кожна подія може бути записана з міткою часу. Може включати в себе час початку і кінця події. Є дуже важливою функцією, адже допомагає знаходити патерни атак і групувати шкідливі події.
- Фаза – до фаз відносяться фази вторгнення, атаки або порушень. Значеннями функції можуть бути фази, які надаються Cyber Kill Chain.
- Результат – дуже важливо фіксувати результати та пост-умови операцій та дій порушника, хоч іноді вони не будуть відомі. Результат може бути прямо пов’язаний з CIA тріадою. Значення функції може містити мітку успішності атаки, а також її вплив на конфіденційність, доступність та цілісність.
- Напрямок – допомагає описати події на основі хоста та мережі, і представляє напрям атаки. Діамантова модель визначає сім потенційних значень для цієї функції: жертва-інфраструктура, інфраструктура-жертва, інфраструктура-інфраструктура, порушник-інфраструктура, інфраструктура-порушник, двонапрямлений або невідомий.
- Методологія – допоможе аналітикам описати загальну класифікацію вторгнення, як фішинг, DDoS, злам, сканування, тощо.
- Ресурс – відповідно до Діамантової моделі, для успіху будь-якої події потрібен один або більше додаткових (зовнішніх) ресурсів. До таких ресурсів відноситься програмне забезпечення, знання, інформація, апаратне забезпечення, гроші, засоби, доступ і т.д.

Розглядаючи цю модель у контексті електронного голосування, варто зазначити соціально-політичний компонент, який пояснює наміри порушника, як-то фінансова вигода, політичні цілі, визнання, шпигунство, тощо. Виходячи з мотивації зловмисника можна зрозуміти його кінцеву мету. Якщо мета політична – то викрадення персональних даних не є основною ціллю, в даному випадку зловмисник буде намагатися виправити результати голосування. Якщо ж фінансова вигода є основною мотивацією – дії зловмисника будуть пов’язані або з викраденням персональних даних, або їх шифруванням для подальшого

вимагання грошей за їх розшифрування. Звісно, варто розуміти, що мотивацію і кінцеву мету зловмисника неможливо знати наперед, і вона буде розкрита або під час самої атаки, залежно від патерну його дій і операцій, або вже під кінець атаки з її результатом і кінцевими шкідливими впливами на систему і державу. Варто також зазначити, що система електронного голосування може бути атакована з ціллю шпіонажу, і в такому разі може будуватись система віддаленого контролю для постійного моніторингу дій на сервері.

4.3 Децентралізація та резервування

Децентралізація – процес розподілення відповідальності за підтримку певних функцій системи [2]. Децентралізована система має багато незалежних учасників, які разом підтримують її функціонування. Децентралізована система має дуже багато переваг, але важливо розуміти різницю між нею та резервуванням. Резервування полягає у забезпеченні додаткових компонентів для підвищення надійності системи. Якщо один компонент відмовляє, він замінюється на резервний. Система, яка передбачає резервування, має надлишкові компоненти, які за необхідності будуть виконувати ті самі функції, що й ті компоненти, які відмовили. Система з резервуванням не обов’язково є децентралізованою. Але децентралізована система обов’язково повинна мати резервування. Робиться це з метою відмовостійкості, коли відмовляє компонент – система повинна працювати далі, навіть, якщо відмовлять усі компоненти окрім одного.

Децентралізація має багато важливих функцій в дуже різних сферах діяльності, чи це соціальні мережі, банки, ігри, файлообмінники або й системи голосування. Децентралізована система голосування може дати наступні переваги:

- Особа, що голосує, може зберегти анонімність;
- Будь-хто може впевнитися у результаті голосування не розкриваючи деталей;
- Може існувати система, яка регулює права голосування і не розкриває особистість виборця.

З цікавих можливостей можна відокремити функцію «токенізації». Токенізація – процес оцифрування фізичного об’єкту, як гроші, акції, ресурси, витвори мистецтва, колекційні предмети та навіть атрибути, що ідентифікують особу. Просто токенізацію можна описати як різновид шифрування інформації. Наразі цей процес активно використовується сервісами Інтернет-розрахунків для зберігання платіжної інформації покупців в онлайн-магазинах, тобто дані їх карти токенізуються і таким чином магазин не буде зберігати дані, а отже їх неможливо викрасти. Для оплати покупки, сервіс направляє створений токен на основі картки онлайн-магазину, і той звіряє його і проводить операцію. Цю функцію можна використовувати безпосередньо у системах голосування, наприклад, шляхом токенізації персональних даних для перевірки особи виборця і його права на голосування.

Одним з можливих варіантів системи голосування можна як раз запропонувати токенізацію. Токенізовані персональні дані, які самі по собі при отримані зловмисником неможливо обернути, можна використовувати як голос. Цей токен-голос можна відправляти на «рахунок» осіб що обираються, тим самим зараховуючи його. При цьому перевірка токену для верифікування його дійсності може бути гарантією того, що голос був зарахований.

Але звісно децентралізація не є локальним інструментом, це є безпосередньо архітектура, за якою будується вся система. Децентралізацію можна використовувати для [2]:

- управління комп’ютерами;
- фізичного зберігання даних;
- фізичної передача даних;
- перевірки даних на відповідність правилам;
- управління протоколом і оновлення правил протоколу;
- управління процесами всередині системи.

Отже, децентралізація, як основа архітектури, допомагає задовольнити необхідні умови відмовостійкості, анонімності та допомагає керувати системою. Основні переваги децентралізованих систем:

- Відмовостійкість, за рахунок організації;

- Незалежність від одноосібного контролю, немає головного центру керування;
- Відсутність потреби у довірі третій стороні;
- Незмінність кінцевих баз даних;
- Гарантується додавання записів без їх зміни;
- Протоколи працюють однаково для усіх, навіть, якщо написані різними мовами програмування.

Звісно важливо пам’ятати, що існують і недоліки:

- Труднощі оновлення протоколу (але в умовах системи голосування це може бути не істотним);
- Проблеми відповідальності;
- Складний процес монетизації розробки (розробка оновлень теж є децентралізованою, важливо цей момент узгоджувати);
- Надмірність, високі вимоги до обладнання, кожен повний вузол зберігає повну копію БД, перевіряє усі транзакції і т.д.;
- Проблема масштабування.

Оскільки система голосування не буде існувати як загальний проект, де кожен користувач буде підтримувати його роботу та ефективність, цим процесом будуть займатися спеціальні вузли підтримки, і вони ж будуть слугувати місцем зберігання повної копії БД. Таким чином з будь-якої точки країни, де є подібний вузол і є необхідність в оновленні протоколу, або якихось програмних рішень проекту, це можливо буде зробити. В такому разі достатньо це зробити на одному вузлі, та верифікувати оновлення на всіх інших. Звісно в такому разі необхідно мати постійний доступ до мережі для кожного вузла, що здебільшого збільшує ризики і загрози, але цю систему можна використовувати у багатьох сферах життя країни, в такому разі це буде лише інструментом для досягнення прозорості державних операцій.

4.4 Блокчейн

Звісно, що будь-яка система голосування повинна зберігати дані про вибори, в деяких ситуаціях і персональні дані користувачів. Будь-яка з цих

інформацій повинна десь зберігатися, а деяка повинна зберігатися в такому вигляді, щоб неможливо було отримати до неї доступ. В цьому питанні доволі важко досягти конфіденційності та цілісності. Але є простий вихід – бази даних, інформацію можна шифрувати та зберігати в одному структурованому вигляді і в одному місці. Але великий об’єм інформації є недоречним, адже такі системи будуть займати багато місця програмного, а згодом і фізичного.

Разом з децентралізованою архітектурою дуже доречним є використання баз даних на основі блокчейн. Блокчейн – спосіб організації БД, коли усі записи додаються окремими блоками і кожен наступний блок має посилання на попередній у вигляді геш-значення [2]. Якщо брати в приклад блокчейн Біткоін – то будь-хто може завантажити собі повну копію бази даних, з найпершою зробленою транзакцією, і пройти увесь ланцюг транзакцій з останньої до самої першої, використовуючи геш-значення. Блокчейн гарантує, що інформація, яку він містить є незмінною, а персональні дані користувачів – закриті.

Можливо побудувати систему електронного голосування, коли результати виборів, а точніше голоси, будуть зберігатися у вигляді ланцюга. Таким чином можна буде забезпечити точність у кількості голосів, їх автентичність та незмінність.

Важливо розуміти, що метою всіх учасників блокчейн системи є мати однакову копію повного ланцюга блоків, навіть, якщо останні блоки можуть бути альтернативними. Отже з точки зору більшої системи, як наприклад, система електронного голосування, для використання блокчейну як бази даних для зберігання результатів голосування, в ній не буде користувачів у звичайній формі. Будуть існувати сервери в різних точках країни, кожен з різною безпековою мережевою та фізичною інфраструктурою, та з резервними серверами, які будуть зберігати всі одну базу даних, завжди однакову. Але звісно не слід забувати про важливий компонент – валідатора. Валідатор – той, хто пише дані від користувачів в ланцюг блоків. Отже, як зазвичай у простому розумінні повинна працювати така система:

1) Користувач, використовуючи деякий алгоритм дій, отримує доступ до системи та голосує;

2) Його голос вбудовується в транзакцію;

3) Згідно консенсусу, валідатор додає транзакцію у блок;

4) Після досягнення деякої кількості транзакцій у блоці, він додається у ланцюг блокчейн.

Відповідно до цього алгоритму, нам необхідно окреслити, що таке консенсус у парадигмі питання систем голосування, та як обрати/затвердити валідаторів, які будуть створювати ланцюг. Отже в нашому випадку створюється децентралізована система на основі блокчейн, де буде вестись обмін голосами. В цьому випадку можна створити умови, при яких він буде відбуватися з автоматизованою системою, яка в обмін на голос буде надавати щось, що буде символізувати гарантію того, що голос був отриманий, оброблений та доданий у блок.

Як вже відомо, право бути валідатором можна отримати двома шляхами [2]:

- за власноручним доказом: на підставі proof-of-stake або proof-of-work;
- за призначенням на посаду: за алгоритмами Byzantine Fault Tolerance (BFT) або Delegated proof-of-stake.

Але нам важливо, щоб валідаторами були конкретні довірені сутності, щоб будь-яка особа не могла отримати право стати валідатором та вирішувати, які транзакції попадуть у блок. Це важливо тому, що система не буде надійна, якщо більше 50% валідаторів є зловмисниками. В такому разі, порушники можуть змінювати систему під свої потреби.

Чи буде існувати консенсус у рамках такої системи – не є важливим. Це залежить безпосередньо від бажаної архітектури. Звісно, що необхідно будувати правила, за якими довірені валідатори будуть перевіряти коректність транзакцій, щоб упевнитись, що в них немає помилок або шкідливих «домішок».

Найважливішим у використанні децентралізованих систем на основі блокчейну є безпека, оскільки зберігатися можуть будь-які дані, в тому числі персональні. В даному випадку велику роль відіграє криптографія. Завдяки криптографії досягається цілісність та автентичність даних, які знаходяться у

блоках. Цілісність досягається алгоритмами гешування, такими як SHA-2, SHA-3, RIPEMD160. В свою чергу автентичність можливо забезпечити за допомогою електронного підпису ECDSA, Schnorr, EDDSA. Решта алгоритмів здебільшого це «non-interactive zero-knowledge proofs'», або ті, які не потребують безпосередньої взаємодії між підтверджувачем та верифікатором.

Питання безпеки конфіденційних даних транзакції, як наприклад, адреса, з якої проводиться транзакція, ідентифікатори і т.д., у блокчейні вирішується заміною даних на деяке число, що відмінне від відкритого ключа користувача, а мережеві адреси плутаються організаційними методами для неможливості відстеження шляху транзакції.

Чи буде існувати загроза з боку квантового комп'ютера або штучного інтелекту? Якщо розглядати кожен з аспектів окремо, то на алгоритми гешування не існує такої загрози, але на алгоритми електронного підпису такі загрози можливі. Алгоритми консенсусу не будуть мати вразливостей для такого роду загроз, а архітектура децентралізованих системи можливо буде.

4.5 Смарт-контракти

Смарт-контракт [20] – контракт, який використовує технологію блокчейн для цифрового забезпечення виконання, перевірки або полегшення виконання або узгодження контракту. Завдяки безпеці децентралізованих систем, смарт-контракти можуть підвищити довіру до транзакцій між договірними сторонами без необхідності участі третіх сторін, як це зазвичай буває у звичайних контрактах.

Для електронного голосування смарт-контракт може виконувати наступні дії:

- Отримувати дані від користувача і перевіряти їх (верифікувати користувача як виборця): цей процес можна пов'язати з токенами користувачів та іншими базами даних, де будуть зберігатися ідентифікатори виборців, таким чином буде проводитися перевірка, що громадянин має право на голосування;

- Відправляти дані у блокчейн у вигляді транзакції для підтвердження реєстрації користувача на голосуванні, та направляти користувачу підтвердження, що він зареєстрований і може голосувати;
- У процесі голосування контракт отримує голос, гешує його з даними користувача, використовуючи його особистий ключ і направляє у блокчейн, користувач отримує підтвердження голосу;
- Підрахунок голосів та обрання переможця, зберігання результатів у блокчейн;
- Розшифрування голосів для верифікації даних, та перевірки коректності підрахованих голосів.

4.6 Рекомендації та пропозиції

Система голосування на основі децентралізації з використанням блокчейн Ефіріум та на смарт-контрактах може створити необхідні умови для створення надійного інструменту волевиявлення. Смарт-контракти будуть виконувати функцію програмного забезпечення, яке скеровує процес у необхідному напрямку. База даних на основі блокчейн буде створювати безпечний простір для зберігання даних і результатів голосування. Токенізація забезпечить гарантію, що конфіденційні дані користувачів залишаються конфіденційними, і, що їх голос можна перевірити та верифікувати.

Важливо розуміти, що системи на смарт-контрактах є доволі цікавими для хакерів, бо це просто код, який нічим не відрізняється від звичайного. Але він виконується у децентралізованій системі і контракти не можна змінити/заблокувати/вилучити з системи. Звісно існують також атаки на блокчейн типа хардфорк-атаки, які виконують примусово для системи, і створюють альтернативну гілку ланцюга, але такі атаки є дуже високовартісними, і хоча такі атаки проводилися з 2014 року на різноманітні системи, в тому числі і на Біткоін, вони не є дуже ефективними для можливої системи електронного голосування, оскільки як вже зазначалось, важливо створити систему, в якій будуть довірені валідатори, щоб не кожний користувач міг стати/бути валідатором.

ВИСНОВКИ

На сьогодні Україна стоїть на шляху розвитку необхідних стандартів, які сама буде розвивати та впроваджувати, використовуючи досвід своєї кібер-війни. Такі стандарти можуть стати початком впровадження необхідних механізмів та заходів захисту персональних даних. Оскільки шлях України у ЄС складається з необхідності впровадження відповідних реформ та законів, важливо розуміти, що висвітлені фреймворки та механізми скоріше за все дуже скоро почнуть впроваджуватися у передові компанії, а вже потім у всі інші галузі.

Вищезазначені механізми захисту та проаналізовані технології показують, що Україна має всі необхідні ресурси для їх впровадження. Цей процес може бути болісним та хаотичним на початку, але у результаті – є шанс отримати єдину інфраструктуру безпеки, яка буде працювати як годинник. Хоч наразі Україна і має регламентні та законодавчі акти, що стосуються КСЗІ, КЗІ і т.д., наразі вони носять скоріше формальний характер, або використовуються лише для отримання необхідних дозволів.

Впровадження механізмів, які використовуються в усьому світі, дозволить побудувати надійні системи захисту інформації для будь-якої галузі держави. Волевиявлення громадян шляхом голосування є одним з ключових конституційних прав кожного громадянина України, саме це робить нашу країну демократичною. Але наразі цей процес є складним та має багато недоліків. При чому конфіденційні дані виборців можна отримати без особливих зусиль шляхом обману або викрадення на дільниці. Електронне голосування забезпечить відкритий та демократичний процес виборів. Використовуючи досвід сусідніх країн та створюючи власні механізми захисту, можна отримати міцну систему, яка буде прикладом для інших. А демократичні вибори дуже допоможуть країні у дипломатичних відносинах.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Будько М. Методика оцінки загроз для інформації автоматизованих систем. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*. 2005. № 10.URL: https://ela.kpi.ua/bitstream/123456789/11427/1/10_p35.pdf (date of access: 23.10.2023).

1. Особистий конспект лекцій з курсу Google Cybersecurity від Coursera (2023)

2. Особистий конспект лекцій з курсу Solidity Smart Contracts від Distributed Lab на платформі Prometheus (2023)

3. Порахувати голоси всього за 2 години замість 2 тижнів: як в Естонії організовані електронні вибори. *Рубрика*. URL: https://rubryka.com/article/e-elections-estonia/ (date of access: 15.09.2023).

4. Про захист персональних даних : Закон України від 01.06.2010 р. № 2297-VI : станом на 27 жовт. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (date of access: 03.10.2023).

5. Тищенко О. І. Запровадження системи електронного голосування в Україні. Київ : 2011.

6. 8 CISSP Domains explained. *Intellipaat Blog*. URL: https://intellipaat.com/blog/cissp-domains-explained/ (date of access: 24.09.2023).

7. Andmekaitsespetsialist | Andmekaitse Inspektsioon. *Avaleht | Andmekaitse Inspektsioon*. URL: https://www.aki.ee/et/eraelu-kaitse/andmekaitsespetsialist (date of access: 08.10.2023).

8. Ben Ayed A. A conceptual secure blockchain based electronic voting system. *International journal of network security & its applications*. 2017. Vol. 9, no. 3. P. 01–09. URL: https://doi.org/10.5121/ijnsa.2017.9301 (date of access: 03.11.2023).

9. Bernstein C. What is PII (personally identifiable information)? | definition from TechTarget. *Security*. URL: https://www.techtarget.com/searchsecurity/definition/personally-identifiable-information-PII (date of access: 18.09.2023).

10. Bidou R. Security operation center concepts & implementation. 2005. URL: https://www.researchgate.net/publication/228587242_Security_Operation_Center_Concepts_Implementation/stats (date of access: 26.09.2023).

11. Caltagirone S., Pendergast A., Betz C. The diamond model of intrusion analysis. 2013. URL: https://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf (date of access: 17.10.2023).

12. Cyber governance regulation |TryHackMe | Cyber Security Training. *TryHackMe*. URL: https://tryhackme.com/room/cybergovernanceregulation (date of access: 20.09.2023).

13. CyberSecurity Malaysia. Guidelines for Secure Software Development Life Cycle. 2020. URL: https://www.oic-cert.org/en/download/MyVAC-3-GUI-2-SSDLC-v1.pdf (date of access: 16.09.2023).

14. Dawson M. Integrating software assurance into the Software Development Life Cycle (SDLC). *Journal of information systems technology and planning*. 2010. Vol. 3, no. 6.

15. Department for Science, Innovation, & Technology. Conducting a STRIDE-based threat analysis. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1155778/Conducting_a_STRIDE-based_threat_analysis.pdf (date of access: 29.10.2023).

16. DREAD threat modeling: an introduction to qualitative risk analysis. *Cybersecurity Exchange*. URL: https://www.eccouncil.org/cybersecurity-exchange/threat-intelligence/dread-threat-modeling-intro/ (date of access: 01.11.2023).

17. Eilam E. Reversing: Secrets of reverse engineering. Indianapolis, IN : Wiley, 2005. 589 p.

18. Elzeiny A. The challenges of usage E-voting. *Academia.edu - Share research.* URL: https://www.academia.edu/4210176/The_challenges_of_usage_E_voting (date of access: 28.10.2023).

19. Encryption. *General Data Protection Regulation (GDPR)*. URL: https://gdpr-info.eu/issues/encryption/ (date of access: 24.09.2023).

20. Ene C. Smart contracts - the new form of the legal agreements. *Proceedings of the international conference on business excellence*. 2020. Vol. 14, no. 1. URL: https://doi.org/10.2478/picbe-2020-0113 (date of access: 04.11.2023).

21. General data protection regulation (GDPR) – official legal text. *General Data Protection Regulation (GDPR)*. URL: https://gdpr-info.eu/ (date of access: 04.10.2023).

22. Incident response playbooks. *Microsoft Learn: Build skills that open doors in your career*. URL: https://learn.microsoft.com/en-us/security/operations/incident-response-playbooks (date of access: 26.10.2023).

23. Is e-voting currently used in any elections with EMB participation? *International IDEA*. URL: https://www.idea.int/data-tools/question-view/742 (date of access: 20.09.2023).

24. Iwasaki M. E-voting in Japan: a developing case?. *4th international conference on electronic voting 2010*, Bregenz, 21 July 2010.

25. KSI Blockchain - e-Estonia. *e-Estonia*. URL: https://e-estonia.com/solutions/cyber-security (date of access: 16.09.2023).

26. LOCKHEED MARTIN. Gaining the advantage | Applying cyber kill chain methodology to network defense. URL: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf (date of access: 10.10.2023).

27. Money makes the cyber-crime world go round - Verizon business 2020 data breach investigations report. *Verizon: Wireless, Internet, TV and Phone Services | Official Site*. URL: https://www.verizon.com/about/news/verizon-2020-data-breach-investigations-report (date of access: 15.10.2023).

28. National Institute of Standards and Technology. Guide for conducting risk assessments. Gaithersburg, 2012. 95 p.

29. OWASP Top Ten | OWASP Foundation. *OWASP Foundation, the*

Open Source Foundation for Application Security | OWASP Foundation. URL: https://owasp.org/www-project-top-ten/ (date of access: 19.10.2023).

30. Personal Data Protection Act : Seadus of 12.12.2018. URL: https://www.riigiteataja.ee/akt/104012019011 (date of access: 11.09.2023).

31. Pomares J., Ovejero T., Lopez Mirau G. The implementation of e-voting in Latin America: The experience of Salta, Argentina from a practitioner´s perspective. 2012.

32. Porup J. Online voting is impossible to secure. So why are some governments using it?. *CSO Online*. URL: https://www.csoonline.com/article/565242/online-voting-is-impossible-to-secure-so-why-are-some-governments-using-it.html (date of access: 19.09.2023).

33. Protection of personal data and privacy | Eesti.ee. *Eesti.ee*. URL: https://www.eesti.ee/en/security-and-defense/safety-and-security/protection-of-personal-data-and-privacy (date of access: 16.09.2023).

34. Reynolds M. Welcome to E-stonia, the world's most digitally advanced society. *WIRED UK*. URL: https://www.wired.co.uk/article/digital-estonia (date of access: 17.09.2023).

35. Risk management | TryHackMe | Cyber Security Training. *TryHackMe*. URL: https://tryhackme.com/room/seriskmanagement (date of access: 17.10.2023).

36. Security principles | TryHackMe | Cyber Security

Training. *TryHackMe*.
URL: https://tryhackme.com/room/securityprinciples (date of access: 18.10.2023).

37. SIEM: a market snapshot. *Dr. Dobb's*.
URL: https://www.drdobbs.com/siem-a-market-snapshot/197002909 (date of access: 21.09.2023).

38. Singh V. MAN IN THE MIDDLE (MITM) ATTACK Man-in-the-Middle Attack Examples. *Academia.edu - Share research*.
URL: https://www.academia.edu/39012612/MAN_IN_THE_MIDDLE_MITM_ATTACK_Man_in_the_Middle_Attack_Examples (date of access: 19.09.2023).

39. The NIST cybersecurity framework 2.0. Official edition. Gaithersburg, 2023. 52 p.
URL: https://doi.org/10.6028/NIST.CSWP.29.ipd (date of access: 21.10.2023).

40. Threat modelling | TryHackMe | Threat Modelling. *TryHackMe*.
URL: https://tryhackme.com/room/threatmodelling (date of access: 22.10.2023).

41. Trüb Baltic AS. Estonian Electronic ID–card application specification. AS Sertifitseerimiskeskus, 2013. 87 p.

42. Voto electrónico - boleta unica electrónica - padrón electoral 2023 dónde voto ?. *Padrón Electoral 2023 Dónde voto ?*.
URL: https://padronelectoral.org/voto-electronico-boleta-unica-electronica/ (date of access: 22.09.2023).