ЗАТВЕРДЖУЮ
Проректор з наукової роботи
доктор фізико-математичних наук, професор
_____ В.О. Катрич
«15» 12 2021 р.

М.П.

АНОТОВАНИЙ ЗВІТ
про виконану роботу в рамках реалізації проєкту
із виконання наукових досліджень і розробок
Аналіз, дослідження, розробка та впровадження сучасних технологій інформаційної безпеки для глобального моніторингу кібернетичного простору України в умовах кризових та надзвичайних ситуацій
(назва Проєкту)

Назва конкурсу: Наука для безпеки людини та суспільства
Реєстраційний номер Проєкту: 2020.01/0351

Підстава для реалізації Проєкту з виконання наукових досліджень і розробок (реєстраційний номер та назва Проєкту) 2020.01/0351 Аналіз, дослідження, розробка та впровадження сучасних технологій інформаційної безпеки для глобального моніторингу кібернетичного простору України в умовах кризових та надзвичайних ситуацій

Рішення наукової ради Національного фонду досліджень України щодо визначення переможця конкурсу Наука для безпеки людини та суспільства (назва конкурсу)
протокол від 16-17 вересня 2020 року № 21

1. ЗАГАЛЬНА ІНФОРМАЦІЯ ПРО ПРОЄКТ

Загальна тривалість виконання проєкту 2020 рік – 2021 рік
Тривалість виконання Проєкту у 2021 році
Початок – 18.05.2021
(дата укладання Договору про виконання наукового дослідження і розробки)
Закінчення – 15.12.2021

Загальна вартість Проєкту, грн. 6 851 400

Вартість Проєкту по роках, грн.:
1-й рік 2 106 000
2-й рік 4 745 400

2. ІНФОРМАЦІЯ ПРО ВИКОНАВЦІВ ПРОЄКТУ

до виконання Проєкту залучено 15 виконавців, з них:
доктори наук 7;
кандидати наук 5;
інші працівники 3.

3. ІНФОРМАЦІЯ ПРО ГРАНТООТРИМУВАЧА ТА ОРГАНІЗАЦІЮ(Ї) СУБВИКОНАВЦЯ(ІВ) ПРОЄКТУ

Харківський національний університет імені В.Н. Каразіна.

Субвиконавці відсутні.

4. ОПИС ПРОЄКТУ

4.1. Мета Проєкту (до 200 знаків)

Дослідження загроз інформаційної безпеки, розробка ефективних технологій захисту інформації для глобального моніторингу кібернетичного простору України в умовах кризових та надзвичайних ситуацій.

4.2. Основні завдання Проєкту (до 400 знаків)

Аналіз та дослідження сучасних вимог та загроз національної безпеки в інформаційній сфері; обґрунтування, розробка та впровадження ефективних технологій захисту інформації для глобального моніторингу кібернетичного простору України в умовах кризових та надзвичайних ситуацій.

4.3. Детальний зміст Проєкту:

- Сучасний стан проблеми (до 400 знаків)

Проєкт прикладного дослідження спрямований на попередження та подолання наслідків кризових та надзвичайних ситуацій, викликаних за природними та/або техногенними обставинами в енергетиці, транспорті, військовій сфері, банківському секторі, промисловості, екології, порушеннями медико-санітарних вимог, поширенням особливо небезпечних інфекцій, тощо.

- Новизна Проєкту (до 400 знаків)

Полягає в обґрунтуванні, розробці та впровадженні ефективних технологій захисту інформації (децентралізованої приватної бази даних без наявності будь-якої довіреної сторони, безпечних протоколів взаємодії та засобів криптографічного перетворення, відмовостійкої маршрутизації, тощо) для глобального моніторингу кібернетичного простору України в умовах кризових та надзвичайних ситуацій.

- Методологія дослідження (до 400 знаків)

Полягає у комплексному застосуванні методів теорії захисту інформації, криптології, сучасних протоколів та технологій комп'ютерних мереж та систем, теорії систем та системного аналізу, комп’ютерного та імітаційного моделювання, сучасних методів побудови децентралізованих криптографічних протоколів з нульовим розголошенням, в тому числі неінтерактивних, кільцевих підписів тощо.

5. ОТРИМАНІ НАУКОВІ АБО НАУКОВО-ТЕХНІЧНІ РЕЗУЛЬТАТИ (до 2 сторінок) в поточному році/ в рамках реалізації Проєкту, зокрема:

5.1. Опис наукових або науково-технічних результатів, отриманих в рамках виконання Проєкту (із зазначенням їх якісних та кількісних (технічних) характеристик)

Комплекс криптографічних протоколів для побудови децентралізованої приватної бази даних, які надають можливість виконувати задану обробку виключно у зашифрованому вигляді з гарантією конфіденційності інформації та доступністю відповідного фрагменту оригінальних та/або перетворених даних виключно учаснику, який є власником відповідного фрагменту даних і при цьому не має довіри до решти учасників. Протоколи взаємодії для побудови системи моніторингу та інформування населення щодо епідеміологічної ситуації з гарантованою анонімністю користувача та можливістю з боку закладів охорони здоров’я досліджувати контакти хворого для більш ефективного виявлення та запобігання розповсюдження інфекційних

захворювань. Результати з обґрунтування створення дублюючої системи оповіщення населення про надзвичайні події у регіоні та небезпеки в зоні перебування людини.

Методи моніторингу та аналізу мультифрактальних та рекурентних характеристик мережного трафіка з формуванням та рейтингуванням бази сигнатур. Методи виявлення вторгнень на підставі аналізу сигнатур та аномалій в поведінці (зміні стану) мережі. Для їх розробки залучаються засоби машинного навчання та методи фрактального аналізу. Реалізація запропонованих методів сприятиме підвищенню швидкості та точності виявлення вторгнень в широкому діапазоні атак на мережу. Рекомендації для реалізації різних протоколів автентифікації та розподілення таємниці з точки зору програмної імплементації та побудови систем моніторингу та інформування населення щодо епідеміологічної ситуації. Методи управління трафіком і управління системами виявлення вторгнень для об'єднання в концепцію універсалізації та централізації аналізу трафіка і стану мережі при використанні систем виявлення вторгнень шляхом розвитку засобів глибокого аналізу пакетів. Методи аналізу протоколів з відстеженням стану, при роботі яких відстежуються і аналізуються всі події в з'єднанні або сеансі, що дозволяє датчику знаходити кореляції між різними подіями протягом сеансу, ідентифікуючи атаки з кількома компонентами, які інакше не можуть бути виявлені. Методи безпечної маршрутизації для фрагментованої передачі конфіденційних повідомлень в інфокомунікаційній мережі. Новизною методів є використання оптимізаційної моделі розрахунку максимальної кількості найбільш безпечних маршрутів та можливість використання шляхів, які можуть перетинатись. Це дозволяє більш повно використати наявний в мережі ресурс щодо пропускної здатності та кіберресурс, знизивши ймовірність компрометації конфіденційних повідомлень.

Протоколи взаємодії для системи моніторингу та інформування населення щодо епідеміологічної ситуації з гарантованою анонімністю користувача, що засновані на кільцевих підписах та алгоритмах Безпосередньої Анонімної Атестації. Новий алгоритм кільцевого підпису з використанням операції спарювання, який є більш швидким та вимагає меншої кількості відкритих ключів, ніж існуючий. Механізми економічного стимулювання підключення до системи й протоколи активної взаємодії як звичайних громадян, так і повних вузлів, що забезпечують функціонування децентралізованої кореневої інфраструктури.

Метод моніторингу та аналізу мультифрактальних та рекурентних характеристик мережного трафіка з формуванням та рейтингуванням бази сигнатур. Комплексний метод виявлення вторгнень, який базується на використанні методів аналізу сигнатур, аналізу аномалій поведінки мережі та ентропійному аналізі протоколів з урахуванням ймовірності виявлення вторгнень. Структура підсистеми моніторингу, виявлення вторгнень та ідентифікації мережних атак що базується на хмарному підході машинного навчання яка є складовою дублюючої системи оповіщення населення про надзвичайні події у регіоні.

Комплекс науково-методичних рекомендації щодо практичної реалізації результатів проєкту. За результатами виконання проєкту складено науковий звіт (про заключні результати реалізації проєкту); опубліковано низку наукових праць, зокрема, у провідному міжнародному видавництві Springer видано 33 монографій (розділів монографій); опубліковано 11 публікації у виданнях що входять до науково-метричних баз даних WoS та/або Scopus; опубликовано 60 статей у наукових фахових журналах України, що відносяться до категорії «Б», статті у закордонних наукових виданнях, а також англомовні тези доповідей у матеріалах міжнародних конференцій, що індексуються науково-метричними базами даних WoS або Scopus; подано до публікації ще 10 наукових робіт; оформлено 4 патенту України; опубліковано 9 навчальних посібників; захищено 2 дисертації доктора філософії (кандидата наук), ще одну заплановано до захисту у грудні 2021 року; захищено 1 дисертацію доктора наук, ще одну заплановано до захисту 28 грудня 2021 року.

5.2. За наявності науково-технічної продукції обґрунтування її переваг у порівнянні з існуючими аналогами

Використання запропонованих криптографічних примітивів дозволить виконувати ефективний моніторинг та, разом з тим, забезпечити достатній рівень анонімності. Рівень стійкості криптографічного примітиву визначався індивідуально, відповідно до загальноприйнятого визначення, що дає можливість гарантувати загальну стійкість комплексу всіх криптографічних примітивів, що плануються до використання. Метод моніторингу трафіка в системах виявлення

вторгнень, на відміну від існуючих, враховує мультифрактальні характеристики трафіка та ймовірність виявлення вторгнень. Методи безпечної маршрутизації конфіденційних повідомлень більш повно враховують особливості нерегулярної топології сучасних інфокомунікаційних мереж; забезпечують розрахунок множини найбільш безпечних шляхів різних типів. Новий алгоритм кільцевого підпису має суттєво меншу довжину підпису та час роботи алгоритму і суттєво вищу стійкість у порівнянні з алгоритмами на основі RSA.

5.3. Практична цінність отриманих результатів реалізації Проєкту для економіки та суспільства (стосується проєктів, що передбачають проведення прикладних наукових досліджень і науково-технічних розробок)

Обґрунтована необхідність застосування кожного з алгоритмів гешування, цифрового підпису, гібридного шифрування та інкапсуляції ключа у моніторингових системах. Практичне застосування математичних моделей криптографічного захисту дозволяє забезпечити фундаментальні властивості криптографічних примітивів, які в свою чергу використовуються для розробки більш складних об'єктів (криптосистем та криптографічних протоколів) і які гарантують одне або декілька властивостей безпеки високого рівня. Застосування на практиці запропонованих моделей та методів моніторингу трафіка підвищує як рівень якості обслуговування за показниками мережної продуктивності, так і рівень мережної безпеки. Застосування технологій машинного навчання призведе до підвищення захищеності інформаційних ресурсів шляхом підвищення точності, швидкості та своєчасності виявлення вторгнень та ідентифікації атак. Практичне вВикористання моделей та методів безпечної маршрутизації дозволяє знизити ймовірність компрометації конфіденційних повідомлень в залежності від сценаріїв та рівнів кіберзагроз. Запропоновані методи є основою математичного та алгоритмічно-програмного забезпечення існуючих та перспективних маршрутизаторів IP/MPLS-мереж, серверів маршрутів та контролерів програмно-конфігурованих мереж. Протоколи взаємодії для системи моніторингу та інформування населення надають можливість з боку закладів охорони здоров'я досліджувати контакти хворого для більш ефективного виявлення та запобігання розповсюдження інфекційних захворювань. Протоколи взаємодії забезпечують максимальну децентралізацію системи, а механізми економічного стимулювання мають виключно добровільний характер з відсутністю будь-якої каральної складової.

5.4. Опис шляхів та способів подальшого використання результатів виконання Проєкту в суспільній практиці.

Отримані математичні моделі та методи безпечної маршрутизації а також їх програмні прототипи доцільно використовувати при управлінні конфіденційним трафіком в умовах можливих загроз, вторгнень та реалізації вразливостей апаратно-програмного забезпечення комутаційного та серверного обладнання інфокомунікаційних мереж загального та спеціального призначення. Особливо це стосується мереж, які розгорнуті для забезпечення функціонування об'єктів критичної інфраструктури України, та мереж військового призначення. Представлені математичні моделі криптографічного захисту в подальшому можуть бути застосовані як при проведенні пошукових досліджень з обґрунтування нових технологій криптографічного перетворення, механізмів та протоколів забезпечення безпеки персональних та інших даних, захист яких передбачено нормативно-правовими актами, так і для розробки навчально-методичних праць з викладення основних положень сучасної криптології. Розроблені та запропоновані методи збору, аналізу та систематизації статистичних даних щодо стану мережі, характеристик трафіку, поведінки користувачів у різних режимах функціонування інформаційної системи. Представлені методи безпечної маршрутизації конфіденційних повідомлень отримали програмну реалізацію та представлені програмними прототипами протоколів безпечної маршрутизації у середовищі MATLAB та Python. Використовуючи наведені механізми кільцевих підписів та БАА, можна побудувати відповідні протоколи моніторингу епідеміологічної ситуації з максимальним забезпеченням анонімності. Запропоновано протоколи взаємодії для використання у системах зберігання та поширення інформації у децентралізованих середовищах із застосуванням механізмів економічного стимулювання підключення до системи. Розроблені та запропоновані

методи моніторингу, виявлення вторгнень та ідентифікації атак, як частина дублюючої системи оповіщення населення про надзвичайні події у регіоні та небезпеки в зоні перебування людини.

Примітка: Анотований звіт не містить відомостей, заборонених до відкритого опублікування

Науковий керівник Проєкту
Науковий керівник/Головний науковий співробітник
(посада)

Роман Олійников
(Власне ім'я та ПРІЗВИЩЕ)

(підпис)