DOI 10.70286/ISU-18.02.2026.013

ВПЛИВ НОРМАТИВНО-ПРАВОВИХ ЗАСАД НА РОЗРОБЛЕННЯ ТА ВПРОВАДЖЕННЯ ІНФОРМАЦІЙНИХ СИСТЕМ ПІДТРИМКИ РІШЕНЬ У СФЕРІ ЦИВІЛЬНОЇ БЕЗПЕКИ

Турчак Роман Сергійович
магістр, здобувач наукового ступеня доктора філософії, аспірант
Сумського державного університету, м. Суми, Україна
https://orcid.org/0009-0004-8663-1010

Вступ. Інформаційні системи підтримки рішень (далі – ІСПР) у сфері цивільної безпеки фахівці вважають не лише технічним інструментом оптимізації управлінських процесів. Нині такі системи є елементом публічного управління з підвищеним рівнем правової відповідальності. Особливої актуальності це набуває під час запобігання пожежам та їхньої ліквідації. Помилки аналізу інформації та затримки в ухваленні управлінських рішень щодо реагування на надзвичайні ситуації спричиняють конкретні наслідки, безпосередньо пов’язані з ризиками для життя та здоров’я людей. З огляду на це нормативно-правові засади функціонування ІСПР визначають межі допустимого втручання в технологічні процеси реагування на пожежі та інші надзвичайні ситуації.

Мета дослідження. Мета дослідження – проаналізувати вплив нормативно-правової бази України на формування архітектури ІСПР, зокрема її інформаційну структуру, алгоритми, інтерфейси та протоколи обміну даними. Завдання дослідження полягають у: виокремленні основних нормативно-правових актів України, що регулюють сферу ІСПР; аналізі законодавчих вимог до архітектури та функціонування таких систем; установленні конкретних технічних параметрів (структур даних, алгоритмів, інтерфейсів та протоколів обміну); зіставленні нормативних вимог законодавства з їхньою фактичною реалізацією в наявних системах; виявленні правових прогалин і суперечностей для розроблення пропозицій щодо вдосконалення законодавства.

Літературний огляд. Розроблення та впровадження ІСПР у сфері цивільного захисту потребує суворого дотримання нормативно-правових засад, які визначають функціональні межі систем, а також регламентують процедури обробки та збереження важливих даних. Відсутність чіткої нормативної бази знижує ефективність систем та ускладнює управління надзвичайними ситуаціями. У дослідженні С. П. Садковського [1] проаналізовано особливості нормативно-правового забезпечення інформаційних технологій у контексті інформаційної безпеки України. Автор визначає основні законодавчі акти та стандарти, що регламентують використання цифрових платформ у державному секторі, та обґрунтовує пряму залежність надійності й легітимності ІТ-рішень від

дотримання встановлених норм. Одним з основних напрямів удосконалення цивільної безпеки є впровадження автоматизованих систем моніторингу, які забезпечують своєчасне виявлення загроз та підвищують оперативність ухвалення управлінських рішень. Так, В. Мельник та О. Тесленко у своєму дослідженні аналізують управлінський потенціал цифрових технологій у системі цивільного захисту та виявляють ризики, пов'язані з їхнім використанням, зокрема проблеми інтеграції різнорідних даних та потребу в стандартизації процедур для ефективного прогнозування надзвичайних ситуацій [2]. Динамічний розвиток кіберзагроз і ускладнення інформаційного середовища створюють ризики для національної безпеки, що зумовлює необхідність системного підходу до їхнього визначення та оцінки. У цьому контексті О. Федченко, аналізуючи сучасні впливи на інформаційну сферу держави, визначає основні чинники ефективності управлінських рішень та обґрунтовує необхідність узгодження правових і технічних заходів для запобігання інцидентам [3].

Прогнозування й запобігання надзвичайним подіям у цивільному секторі залежать насамперед від здатності інформаційних систем аналізувати значні обсяги даних і генерувати рекомендації для управлінців. Науковці О. Г. Мельник та Р. П. Мельник [4] розробили комп'ютеризовану систему прогнозування пожеж у житловому секторі, яка інтегрує дані з різних джерел та надає рекомендації щодо мінімізації ризиків, що підтверджує практичну ефективність застосування цифрових рішень у реальному управлінському процесі. У вимірі загальної інформаційної безпеки держави необхідно також враховувати зміни нормативного поля та адаптацію систем до нових викликів. Зокрема, у праці Т. С. Слінько [5] досліджено сучасні загрози інформаційній безпеці України та запропоновано стратегії їхнього подолання. Авторка акцентує на ролі правових механізмів у формуванні комплексного підходу до захисту інформаційної інфраструктури та інтеграції цифрових платформ у межах єдиного безпекового управління. Отже, сучасні дослідження засвідчують, що ефективність інформаційних систем підтримки рішень у сфері цивільної безпеки залежить від поєднання нормативно-правового регулювання, технічних рішень та управлінських процедур, що забезпечує своєчасне реагування на загрози та мінімізує ризики для населення та державних об'єктів.

Результати. Правове регулювання ІСПР у сфері цивільної безпеки має комплексний і міжгалузевий характер. Правовідносини, що виникають у процесі використання цих систем, регулюються нормами законодавства у сфері цивільного захисту, пожежної та інформаційної безпеки, а також публічного управління. Серед основних актів варто виокремити Закон України «Про цивільний захист». Важливими є норми, що регламентують функціонування інформаційних ресурсів та автоматизованих систем.

Функціональні характеристики ІСПР формуються під впливом норм технічного регулювання, державних і галузевих стандартів, будівельних норм та підзаконних актів, що встановлюють вимоги до систем пожежної сигналізації, моніторингу та диспетчеризації. Саме ці нормативні приписи визначають

структуру даних, логіку їхньої обробки та можливості інтеграції ІСПР з іншими інформаційними ресурсами. Водночас чинне регулювання цієї сфери характеризується надмірною формалізацією, що обмежує впровадження адаптивних або інтелектуальних модулів, здатних ураховувати динамічний характер розвитку пожежі. За цих умов необхідним є більш гнучкий правовий підхід до розроблення та впровадження ІСПР у сфері цивільної безпеки, особливо з огляду на темпи технологічного розвитку.

Функціонування ІСПР безпосередньо пов'язане з обробкою значного обсягу інформації, що охоплює технічні параметри об'єктів, оперативні дані про перебіг пожежі та інші відомості, необхідні для аналізу й прогнозування ситуації. З огляду на це доцільно вдосконалювати алгоритми запобігання небезпеці та створювати окремі підсистеми раннього попередження про виникнення пожеж [6, с. 157]. З позицій законодавства це питання має врегульовуватися комплексом норм у сфері інформаційної та кібербезпеки, які встановлюють вимоги щодо перевіреності, цілісності та захищеності відповідних даних, а також визначають юридичну відповідальність за їхнє викривлення або несвоєчасне оновлення. Такий підхід загалом є обґрунтованим, однак у процесі ліквідації пожеж нерідко виникають нештатні ситуації, що потребують оперативного ухвалення рішень. Це актуалізує дискусію щодо допустимих меж автоматизованої обробки інформації в умовах підвищеного ризику та часових обмежень.

Ефективність застосування ІСПР під час ліквідації пожеж істотно залежить від узгодженості норм у сфері цивільної безпеки, інформаційного законодавства та правового режиму кібербезпеки. Це визначає рівень впливу правового регулювання на функціонування ІСПР під час ліквідації пожеж (табл. 1). У реальних умовах такі системи функціонують як складні технічні комплекси, у межах яких алгоритми аналізу пожежної ситуації поєднуються з нормативно визначеними управлінськими процедурами. Це характерно для ІСПР різного виду, зокрема в системі підтримки рішень щодо лісових пожеж, що застосовується в США [7] та інших країнах. За відсутності належної правової координації ІСПР фактично зводяться до ролі допоміжних інформаційних інструментів, що не дає змогу повністю реалізувати їхній потенціал як засобів підтримки ухвалення управлінських рішень.

Законодавство у сфері цивільного захисту детально регламентує повноваження посадових осіб та інших суб'єктів, залучених до ліквідації надзвичайних ситуацій, що свідчить про істотний вплив правового регулювання на практику застосування ІСПР. Однак норми, які визначають порядок обігу даних, функціонування автоматизованих систем та захист інформації, формувалися переважно без урахування специфіки оперативного управління пожежами.

Таблиця 1 Вплив правового регулювання на функціонування ІСПР під час ліквідації пожеж

Сфера правового регулювання	Нормативні обмеження	Наслідки для ІСПР у процесі ліквідації пожеж
Цивільна та пожежна безпека	Процедурне управління без урахування цифрових інструментів	Обмежена інтеграція ІСПР у систему оперативного управління
Інформаційне законодавство	Фрагментарне регулювання збору та обробки даних	Ускладнення комплексного аналізу пожежної ситуації
Кібербезпека	Пріоритет захисту інформації над оперативністю доступу	Зниження оперативності ухвалення рішень у критичних умовах
Правовий режим автоматизованих рішень	Відсутність чіткого статусу рекомендацій ІСПР	Невизначеність відповідальності за управлінські рішення

Джерело: сформовано автором.

Унаслідок цього вимоги до швидкості та повноти обробки інформації, необхідні для ефективної роботи ІСПР, не завжди узгоджуються з обмеженнями щодо доступу, зберігання та використання даних, зокрема тих, що надходять із сенсорних мереж та систем відеомоніторингу. Така ситуація є неприйнятною, оскільки негативно впливає на ефективність функціонування системи ситуаційних центрів [8, с. 41] та інших ІСПР.

Таблиця 2 Нормативно-правові акти та стандарти для ІСПР та їхня технічна реалізація

Нормативний акт / стандарт	Стаття / пункт	Вимога до ІСПР	Приклад реалізації
Закон України «Про цивільний захист»	ст. 32	Інтеграція даних пожежних сповіщувачів у єдину систему, забезпечення обміну інформацією між регіональними центрами	Система «Безпечне місто»: централізований збір сигналів від датчиків, протокол CAP для оповіщення
Закон України «Про пожежну безпеку»	ст. 12	Інтеграція даних автоматичних систем пожежогасіння та сигналізації, алгоритми оповіщення та аналізу ризиків	Регіональні ситуаційні центри ДСНС: інтеграція сповіщувачів, формати даних XML/JSON
Закон України «Про інформацію»	ст. 11	Дотримання стандартів зберігання та передачі даних, забезпечення перевіреності та актуальності	Централізовані бази даних ІСПР з контролем доступу та аудитом змін
Закон України «Про захист персональних даних»	ст. 6	Шифрування персональних даних, контроль доступу, аудит дій користувачів	Системи моніторингу пожежної безпеки об’єктів з анонімізацією персональної інформації
Закон України «Про кібербезпеку»	ст. 18	Захист від несанкціонованого доступу, резервне копіювання, моніторинг мереж	Упровадження багаторівневої автентифікації, шифрування каналів передачі даних

Постанова КМУ № 600 «Про створення ситуаційних центрів»	п. 4	Організаційні вимоги до архітектури та інтеграції підсистем	Централізовані системи управління надзвичайними ситуаціями в областях
Наказ ДСНС № 123	п. 7	Порядок обробки та аналізу даних від датчиків, алгоритми оповіщення	Автоматизовані алгоритми повідомлення відповідальних служб у разі спрацювання сигналізації
ДСТУ 31100:2015	Розд. 5	Стандарти сигналізації та протипожежних мереж	Інтеграція датчиків диму й тепла в централізовані ІСПР
ДБН В.1.1-7:2016	Розд. 3	Протипожежні заходи в будівлях, алгоритми управління інженерними мережами	Використання протоколу BACnet для керування пожежними системами будівель
ISO 22320 / OGC	Розд. 4	Геоінформаційні стандарти для оповіщення та картографії	Використання OGC WMS/WFS для відображення небезпечних зон на інтерактивних картах ІСПР

Джерело: складено автором на основі аналізу [9], [10], [11], [12], [13], [14], [15]

Згідно зі ст. 12 Закону України «Про пожежну безпеку» передбачено, що автоматичні системи пожежогасіння та сигналізації мають охоплювати алгоритми оповіщення та аналізу ризиків, що забезпечують своєчасне інформування відповідальних служб та прогнозування розвитку надзвичайних ситуацій. У регіональних центрах ДСНС ці вимоги реалізуються шляхом централізованої інтеграції сигналів від сповіщувачів, застосування алгоритмів фільтрації подій, пріоритизацію сповіщень за рівнем критичності та автоматичне формування повідомлень для аварійно-рятувальних команд. Проте аналіз засвідчує, що існують розбіжності між нормативними вимогами та фактичними процесами: алгоритми не завжди враховують усі рівні ризиків, пріоритизація сповіщень може бути обмежена, а обробка даних у деяких регіонах не інтегрована з національною системою «Безпечне місто». Це призводить до дублювання інформації та потенційних затримок у реагуванні на надзвичайні події.

Для передачі даних регіональні центри застосовують формати XML/JSON, оскільки вони забезпечують гнучку структуру повідомлень, можливість інтеграції з різними платформами та сумісність із міжнародними стандартами обміну даними. Вибір XML/JSON обґрунтований тим, що традиційні бінарні або пропрієтарні формати ускладнюють міжсистемну інтеграцію та автоматичну обробку сигналів. Водночас такий вибір зумовлює додаткові вимоги до перевірки об’єктивності даних і синхронізації часових міток, і не всі алгоритми регіональних центрів повністю відповідають вимогам ст. 12 щодо комплексного аналізу ризиків. Згідно з даними табл. 2, ст. 6 Закону України «Про захист персональних даних» встановлює обов’язок шифрування даних, контролю

доступу та аудиту дій користувачів в ІСПР, тоді як ст. 18 Закону України «Про кібербезпеку» зосереджується на резервному копіюванні, моніторингу мереж та гарантуванні безперервності функціонування систем. На практиці ці вимоги конфліктують: суворі політики контролю доступу й аудит дій користувачів у режимі реального часу уповільнюють передачу сигналів та обробку даних від датчиків пожежної безпеки, тоді як резервне копіювання та додатковий моніторинг мереж створюють додаткове навантаження на канали передачі та серверні ресурси.

У ст. 32 Закону України «Про цивільний захист» встановлено обов'язок інтеграції даних від пожежних сповіщувачів у єдину систему та забезпечення обміну інформацією між регіональними центрами. Стаття визначає структуру даних, яка має містити ідентифікатори датчиків, часові мітки подій, рівень критичності сигналу, координати місця події та тип небезпечного явища, що дає змогу забезпечити централізовану обробку та автоматичне оповіщення відповідальних служб. Для реалізації цих вимог обрано протокол CAP (Common Alerting Protocol), який підтримує структуровані XML-повідомлення, стандартизовані поля для ідентифікації об'єктів і координат, а також інтеграцію з геоінформаційними системами.

Використання CAP накладає конкретні технічні параметри на ІСПР: повідомлення мають відповідати XML-схемам CAP, забезпечувати сумісність із різними платформами та підтримувати багаторівневу маршрутизацію оповіщень. Водночас ця норма створює певні обмеження: обробка XML-повідомлень є ресурсоємною, потребує синхронізації часових міток і дотримання стандартів кодування, що може спричиняти затримки в передачі даних від сповіщувачів до централізованих систем. Крім того, сувора структура CAP ускладнює інтеграцію нестандартних або застарілих датчиків, що обмежує можливості масштабування та швидкого під'єднання нових пристроїв до ІСПР. Таким чином, для забезпечення повної нормативної відповідності доцільно доповнити регламенти ДСНС чіткими алгоритмами обробки сигналів, стандартизованими процедурами фільтрації подій та інтеграції з централізованими системами оповіщення.

Окремої уваги потребує проблема недосконалості правового регулювання інтеграції даних з різнорідних джерел, до яких належать пожежні сповіщувачі, інженерні системи будівель, геоінформаційні сервіси та моделі поширення пожежі. У чинному законодавстві такі джерела розглянуто ізольовано, без належного визначення їхньої ролі в єдиному циклі ухвалення управлінських рішень. Наслідком цього є недостатність правових підстав для повноцінної міжсистемної інтеграції. Це знижує точність прогнозування та обмежує можливості адаптивного управління під час гасіння пожеж.

Чинна нормативна база розроблення та впровадження ІСПР у сфері цивільного захисту має галузевий характер. За таких умов питання пожежної безпеки, цивільного захисту та інформаційних технологій регулюються відокремлено, а це ускладнює формування комплексних рішень для кризових ситуацій. З огляду на міждисциплінарний характер ІСПР доцільно перейти від

фрагментарного нормативного регулювання до узгодженої моделі, яка поєднувала б положення законодавства про цивільний захист, пожежну безпеку, інформаційні системи та кібербезпеку.

Окремого правового врегулювання потребує сфера використання інформаційних даних, що формуються в процесі функціонування ІСПР (дані сенсорного моніторингу, результати прогнозного моделювання тощо), а також порядок їхнього використання під час ухвалення рішень оперативними штабами. Дискусійним залишається питання щодо можливості делегування окремих управлінських функцій автоматизованим системам. Це вимагає законодавчого закріплення принципу «людського контролю» за критично важливими рішеннями у сфері пожежної безпеки. Крім того, норми законодавства мають охоплювати технічне регулювання, зокрема стандарти сумісності та інтероперабельності ІСПР у будівлях різного функціонального призначення.

Подальший розвиток ІСПР у сфері пожежної безпеки потребує системної уваги та належного контролю. Перспективним напрямом є закріплення на законодавчому рівні вимог щодо обов'язкового застосування ІСПР у будівлях підвищеного ризику, з одночасним запровадженням гнучких моделей публічно-приватного партнерства для їхнього впровадження. Окремої уваги заслуговує створення правових умов для апробації інноваційних цифрових рішень у форматі регуляторних «пісочниць», що дало б змогу тестувати алгоритмічні та прогностичні моделі без порушення вимог безпеки. Запровадження таких заходів сприятиме перетворенню ІСПР на інтегрований інструмент управління процесами аналізу, прогнозування та ліквідації пожеж.

Аналіз чинного законодавства у сфері цивільної безпеки виявив конкретні прогалини, що ускладнюють розроблення та впровадження інформаційних систем підтримки рішень. Зокрема, відсутні норми щодо забезпечення сумісності протоколів CAP і BACnet, що ускладнює інтеграцію систем оповіщення та автоматизації будівель із централізованими платформами. Законодавство не регламентує інтероперабельність між системою «Безпечне місто» та регіональними центрами ДСНС, не визначає уніфіковані формати обміну даними, структуру повідомлень і стандарти захисту інформації, що створює технічні перешкоди для швидкого й безпечного ухвалення рішень у надзвичайних ситуаціях.

Крім того, існують прогалини в Законі України «Про цивільний захист» (ст.ст. 12, 13, 17–19), які не передбачають обов'язкових вимог щодо сертифікації програмного забезпечення, перевірки сумісності протоколів та гарантування інформаційної безпеки під час інтеграції різнорідних систем. Відсутність чітких нормативних положень призводить до дублювання даних, ризиків втрати або несанкціонованого доступу, а також обмежує масштабування та ефективну координацію систем цивільного захисту на національному рівні.

Висновки. Отже, нормативно-правове регулювання розроблення й упровадження ІСПР є важливим у процесах цифрової трансформації цивільної безпеки. Саме правові норми визначають допустимі межі автоматизації управлінських рішень, вимоги до перевіреності та юридичної значущості даних, а

також розподіл відповідальності між суб'єктами. Відкритим залишається питання делегування окремих управлінських функцій автоматизованим системам підтримки рішень. Це актуалізує потребу законодавчого закріплення принципу людського контролю за важливими рішеннями у сфері пожежної безпеки. Крім того, подальший розвиток ІСПР потребує комплексного технічного регулювання, зокрема встановлення стандартів сумісності та інтероперабельності таких систем у будівлях різного функціонального призначення.

Список використаних джерел

1. Садковський С. П. Деякі аспекти нормативно-правового забезпечення інформаційних технологій в контексті інформаційної безпеки України. Юридичний науковий електронний журнал. 2023. № 12. С. 121–123. URL: http://www.lsej.org.ua/12_2023/27.pdf (дата звернення: 15.02.2026).
2. Мельник В., Тесленко О. Автоматизовані системи моніторингу у системі цивільного захисту: управлінський потенціал цифрових технологій та ризики їх використання. Middle European Scientific Bulletin. 2026. Т. 1, № 2. URL: https://www.researchgate.net/publication/400556392 (дата звернення: 15.02.2026).
3. Федченко О. Аналіз факторів та сучасних загроз інформаційній безпеці держави у контексті забезпечення національної безпеки України. Social Development & Security. 2022. Т. 12, № 3. С. 128–134. DOI: 10.33445/sds.2022.12.3.11.
4. Мельник О. Г., Мельник Р. П. Розроблення комп'ютеризованої системи прогнозування пожеж у житловому секторі. Bulletin of Cherkasy State Technological University. 2019. Т. 24, № 1. С. 5–10. URL: https://bulletin-chstu.com.ua/web/uploads/pdf/Bulletin%20of%20Cherkasy%20State%20Technological%20University_2019_Vol_24_No.1_5-10.pdf (дата звернення: 15.02.2026).
5. Слінько Т. С. Сучасні загрози інформаційній безпеці країни та шляхи їх подолання. Український часопис конституційного права. 2021. Вип. 4. С. 77–84. URL: https://www.constjournal.com/pub/4-2021/suchasni-zahrozy-informatsiyniy-bezpetsi-krainy-shliakhy-ikh-podolannia/ (дата звернення: 15.02.2026).
6. Маєвський О. В., Бродський Ю. Б., Хохлов М. О. Інформаційна підсистема забезпечення функції попередження пожежної небезпеки регіонального ситуаційного центру. Технічна інженерія. 2024. № 2 (94). С. 151–159. DOI: 10.26642/ten-2024-2(94)-151-159.
7. Fillmore S. D., Paveglio T. B. Use of the Wildland Fire Decision Support System (WFDSS) for full suppression and managed fires within the Southwestern Region of the US Forest Service. International Journal of Wildland Fire. 2023. No. 32. P. 622–635. DOI: 10.1071/WF22206.
8. Тютюник В. В., Ященко О. А., Рубан І. В., Тютюник О. О. Особливості функціонування системи ситуаційних центрів на різних стадіях розвитку надзвичайних ситуацій. Сучасні інформаційні технології у сфері безпеки та оборони. 2022. Вип. 1 (43). С. 41–52. DOI: 10.33099/2311-7249/2022-43-1-41-52.
9. Про цивільний захист : Закон України від 02.10.2012 р. № 5403-VI. Відомості Верховної Ради України. 2013. № 34–35. Ст. 458. URL: https://zakon.rada.gov.ua/go/5403-17 (дата звернення: 15.02.2026).

10. Про пожежну безпеку: Закон України від 17.12.1993 р. № 3745-XII. URL: https://zakon.rada.gov.ua/laws/show/3745-12#Text (дата звернення: 15.02.2026).
11. Про інформацію: Закон України від 02.10.1992 р. № 2657-XII. Відомості Верховної Ради України. 1992. № 48. Ст. 650. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 15.02.2026).
12. Про захист персональних даних : Закон України від 01.06.2010 р. № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 15.02.2026).
13. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 15.02.2026).
14. Про створення ситуаційних центрів: постанова Кабінету Міністрів України від 18.08.2015 р. № 600. URL: https://zakon.rada.gov.ua/laws/show/600-2015-%D0%BF#Text (дата звернення: 15.02.2026).
15. ISO 22320:2018. Emergency management – Requirements for incident response. [Effective from 2018-11-01]. Geneva: ISO, 2018. URL: https://www.iso.org/standard/67851.html (date of access: 15.02.2026).

THREAT ANALYSIS AND METHODS OF COUNTERING ATTACKS AT THE DATA LINK LAYER LEVEL IN LOCAL NETWORKS

Yuzkov Andrii
Second year cadet
Kamianskyi Yaroslav
Second year cadet
ORCID ID: 0009-0000-5035-6441
Yarema Nikita
Second year cadet
Scientific supervisor:
Kalyakin Serhiy Volodymyrovych
Senior Lecturer
ORCID ID: 0000-0003-3946-0189
Department of Counteracting Cybercrime
Institute No. 4
Kharkiv National University of Internal Affairs, Ukraine

According to data from the research company DataReportal, published in the Digital 2025 report, the number of Internet users in the world as of December 2024 exceeded 5.5 billion people, and in Ukraine this figure was 31.5 million people [1].

Along with the number of authorized users in networks, the number of cybercriminals is also growing. Thus, according to the report of the State Special Communications Service, in 2024 the number of cyberattacks on Ukraine increased by