**СТЕНОГРАМА**

засідання Комітету з питань цифрової трансформації

20 березня 2024 року

Веде засідання голова Комітету КРЯЧКО М.В.

ГОЛОВУЮЧИЙ. Шановні народні депутати України, запрошені, вітаю вас у нас на комітеті! Ми починаємо наше засідання. У зв'язку з тим, що секретар комітету сьогодні поки що не підійшов, на час відсутності прошу підрахунок результатів під час голосування здійснювати Антона Швачка.

Прошу Антоне.

ШВАЧКО А.О. Добре.

ГОЛОВУЮЧИЙ. Для роботи комітету необхідно затвердити порядок денний. Він був надісланий вам раніше, тому прошу проголосувати.

Хто – за? Проти? Утримався? Дякую. Рішення прийнято.

ШВАЧКО А.О. 4 – за. 0 – проти.

ГОЛОВУЮЧИЙ. Перше питання порядку денного – проект Закону про внесення змін до деяких Законів України щодо врегулювання повноважень центральних органів виконавчої влади у сфері забезпечення енергетичної ефективності (реєстраційний номер 10393), поданий Кабінетом Міністрів України. Запрошую до доповіді Юрія Васькова, заступник міністра розвитку громад, територій та інфраструктури.

Прошу Юрій.

ВАСЬКОВ Ю.Ю. Доброго дня, шановні народні депутати, шановні присутні! До розгляду пропонується зміни до Закону України щодо

врегулювання повноважень центральних органів виконавчої влади у сфері забезпечення енергетичної ефективності.

По суті закон розроблено у зв'язку з реорганізацією Мінрозвитку громад, територій України та приєднання до Міністерства інфраструктури України. Із основних новел, додаткових новел, крім реорганізації додали термін декарбонізація, який вже використовується у законодавстві України і в інших нормативно-правових актах. І також додали необхідність о наявності місцевого енергетичного плану, під яким розуміється документ стратегічного планування, що затверджується органом місцевого самоврядування і має відповідні цілі. Без зауваження законопроект - погодження Міндовкілля. Зауваження, які були враховані, – Мінфін, Мінекономіки, Мінцифри, Мінюст, Міненерго, Держенергоефективності, Урядовий офіс в координації європейської та євроатлантичної інтеграції. Тобто зауваження всі враховані. Прошу підтримати.

Дякую.

ГОЛОВУЮЧИЙ. Дякую.

Питання є у наших колег до доповідача? Тому прошу Антон Швачко.

ШВАЧКО А.О. Доброго дня, шановні колеги! Щодо запропонованих законопроектом 10393 законодавчих змін у межах предметів відання комітету зазначаю наступне: Міністерство цифрових трансформацій у своєму висновку до законопроекту зауважує, що пункт 9 проекту Закону потребує доопрацювання з метою приведення його до вимог у відповідність до частини другої статті 26 Закону "Про публічні електронні реєстри". В частині питань щодо реєстру суб'єктів господарювання, що отримали сертифікати системи енергетичного менеджменту та/або екологічного менеджменту, а також у відповідність до частини другої статті 27 Закону щодо припинення реєстру органів державної влади та органів місцевого самоврядування, в яких впроваджено систему енергетичного менеджменту.

Підтримуючи ідею законодавчих ініціатив Кабінету Міністрів України, які покликані врегулювати повноваження центральних органів виконавчої влади у сфері забезпечення енергетичної ефективності, слід звернути увагу на пропозиції Міністерства цифрової трансформації України, викладені у висновку.

Пропоную прийняти наступний висновок комітету та ухвалити таке рішення. Рекомендувати Комітету з питань енергетики та житлово-комунальних послуг врахувати висловлені зауваження та пропозиції під час підготовки та розгляду проекту Закону про внесення змін до деяких законів України щодо врегулювання повноважень центральних органів виконавчої влади у сфері забезпечення енергетичної ефективності (реєстраційний номер 10393).

Висновок комітету про розгляд зазначеного законопроекту направити до Комітету з питань енергетики, житлових та комунальних послуг.

Дякую, колеги. Прошу підтримати.

ГОЛОВУЮЧИЙ. Дякую, Антон.

Є пропозиція підтримати рішення, що було озвучено та проголосувати. Хто – за?

ШВАЧКО А.О. 4 – за. 0 – проти.

ГОЛОВУЮЧИЙ. Проти? Утримався? Дякую. Рішення прийнято.

Переходимо до другого питання.

Юрію, дякую вам за доповідь.

ВАСЬКОВ Ю.Ю. Я вам дякую за підтримку.

ГОЛОВУЮЧИЙ. Ми переходимо до другого питання денного проект Закону про внесення змін до Кримінального процесуального кодексу України

щодо оптимізації досудового розслідування та судового розгляду кримінальних повноважень (реєстраційний номер 10206).

Прошу до доповіді Вікторію Подгорну.

ПОДГОРНА В.В. Проектом Закону (реєстраційний номер 10206) пропонується внести зміни до Кримінального процесуального кодексу України, яким передбачити, що під час розслідування кримінальних корупційних правопорушень допускається створення і використання спеціальної несправжньої (імітаційної) інформації у вигляді вигаданих відомостей, які вносяться до автоматизованих інформаційних довідкових систем, реєстрів та банків даних, держателями (адміністраторами), яких є державні органи, органи місцевого самоврядування, підприємства, установи та організації.

Водночас стосовно запропонованої законодавчої ініціативи необхідно зазначити, що Законом України "Про публічні електронні реєстри" встановлені правові, організаційні фінансові засади створення та функціонування публічних електронних реєстрів з метою захисту прав і інтересів фізичних і юридичних осіб, під час створення, зберігання, оброблення і використання інформації в публічних електронних реєстрах.

Діяльність у сфері публічних електронних реєстрів базується на принципах гарантування державою та держателями об'єктивності, актуальності, достовірності, повноти і захищеності реєстрових даних та реєстрової інформації від несанкціонованих змін, презумпції достовірності реєстрових даних і інформації. Від себе додам: це є міжнародним стандартом.

Законом також передбачено, що інформація про об'єкти реєстрів, яка внесена до відповідного реєстру, вважається достовірною і може використовуватися державними органами, органами місцевого самоврядування, їх посадовими особами, при здійсненні ними повноважень,

зазначених законом, а також фізичними і юридичними особами, при вчиненні правочинів.

Міністерство цифрової трансформації України також у своєму експертному висновку до законопроекту наголошує на тому, що засадами для створення реєстрів є використання актуальної і достовірної інформації з реєстрів, що свою чергу ставить під сумнів запропоновані проектом закону зміни до статті 273 Кримінального процесуального кодексу.

Стосовно запропонованих проектом закону змін до статті 571 КПК, вважаємо доцільними слова "в письмовій та електронній формах" замінити словами "паперову та електронну форму", відповідно до Закону України "Про електронні документи та електронний документообіг".

Пропоную ухвалити висновок до законопроекту та рішення комітету.

Перше. Рекомендувати Комітету з питань правоохоронної діяльності врахувати зауваження і пропозиції під час підготовки, розгляду і опрацювання проекту Закону про внесення змін до Кримінального процесуального кодексу України щодо оптимізації досудового розслідування, досудового розгляду кримінальних проваджень (реєстраційний номер 10296).

Друге. Направити цей висновок до Комітету з питань правоохоронної діяльності.

Дякую. Прошу підтримати рішення комітету.

ГОЛОВУЮЧИЙ. Дякую, Вікторія.

Є пропозиція підтримати рішення, що було озвучено та проголосувати.

Хто – за?

ШВАЧКО А.О. 4 – за, 0 – проти. Рішення прийнято.

ГОЛОВУЮЧИЙ. Дякую. Рішення прийнято.

Ми переходимо до третього питання порядку денного, проект Закону про внесення змін до Закону України "Про адвокатуру та адвокатську діяльність" щодо врегулювання питання своєчасності отримання відповіді на адвокатський запит (реєстраційний номер 10445).

Прошу до доповіді Сергія Штепу.

ШТЕПА С.С. Доброго дня, шановні колеги. Законопроект номер 10445 розроблений з метою врегулювання питання своєчасності отримання відповіді на адвокатський запит шляхом закріплення на законодавчому рівні положення, яке встановлює необхідність повідомлення адвоката про направлення йому відповіді на адвокатський запит, в межах строку встановленого частиною другою статті 24 Закону України "Про адвокатуру та адвокатську діяльність".

Зокрема частину другу статті 24 зазначеного закону пропонується доповнити словами: "та за прохання адвоката направити таку інформацію, копію документів засобами електронного зв'язку з накладанням електронного кваліфікаційного підпису".

Слід зазначити, що в Законі України "Про електронну ідентифікацію та електронні довірчі послуги" використовується трохи інший термін, а саме кваліфікований електронний підпис.

Враховуючи наведене, пропонується в проекті закону слова "з накладанням електронного кваліфікаційного підпису" замінити словами "з накладанням кваліфікованого електронного підпису".

Міністерство цифрової трансформації України та Міністерство юстиції України у висновках до законопроекту також наголошує на необхідності його приведення у відповідність до Закону України "Про електронну ідентифікацію та електронні довірчі послуги".

Враховуючи викладене, прошу ухвалити наступний висновок і рішення комітету. Перше – рекомендувати Комітету з питань правової політики врахувати зауваження під час підготовки до розгляду проекту

Закону про внесення змін до Закону України "Про адвокатуру та адвокатську діяльність" щодо врегулювання питання своєчасності отримання відповіді на адвокатський запит (реєстраційний номер 10445). І друге – направити цей висновок до Комітету з питань правової політики.

Дякую. Прошу підтримати.

ГОЛОВУЮЧИЙ. Дякую, Сергію. Я прошу підтримати рішення та проголосувати.

Хто – за? Проти? Утримався? Дякую. Рішення прийнято.

ШВАЧКО А.О. *(Не чути)*

ГОЛОВУЮЧИЙ. Ми переходимо до четвертого питання порядку денного – проект Закону про внесення змін до чинного законодавства щодо удосконалення корпоративного управління в товариствах (реєстраційний номер 10304). Якщо є на зв'язку Іван Калаур, прошу.

КАЛАУР І.Р. Добрий день, шановні колеги. Я є на зв'язку, заступник голови з питань правової політики. Тут у вас на розгляді вашого комітету два законопроекти: 10304 і 10305. Це паралельні два законопроекти. Особливість їх полягає в тому, що в результаті наукових напрацювань багатьма науковцями в сфері корпоративного права було запропоновано внесення змін в закони України "Про товариства з обмеженою та додатковою відповідальністю" та Закон України "Про акціонерні товариства" і відповідно в Цивільний кодекс України, де ці норми, які запропоновані, вони сприятимуть кращому управлінню корпоративними правами і порівняно з тими, які передбачені сьогодні чинним законодавством. Прошу членів комітету підтримати ці законопроекти для того, щоб в подальшому ми з ними працювали.

ГОЛОВУЮЧИЙ. Дякую, Іване. Але я так розумію, по наступному питанню немає сенсу, так, виступати вам?

КАЛАУР І.Р. Да, теж два... Вони ідуть паралельно.

ГОЛОВУЮЧИЙ. Да, зрозумів, зрозумів. Дякую вам.

Я прошу до співдоповіді Антона Швачка.

ШВАЧКО А.О. Шановні колеги, метою законопроекту (реєстраційний номер 10304) є деталізація положень щодо принципу юридичної визначеності та впливу норм законодавства на регламентацію корпоративних відносин у підприємницьких юридичних особах приватного права. В межах предметів відання комітету щодо запропонованих задач і змін визначаємо наступне.

Міністерство цифрової трансформації України у своєму висновку пропонує привести законопроект у відповідність до Закону України "Про державну реєстрацію юридичних осіб, фізичних осіб-підприємців та громадських формувань". А саме в запропонованій редакції пункту 2 частини першої статті 17 проекту закону словосполучення "державного реєстру" замінити словосполученням "єдиного державного реєстру". Також у разі застосування у проекті закону терміну "державний реєстр" в іншому значені з метою правильного його трактування пропонується надати відповідне визначення такого реєстру.

Підтримуючи ідею законодавчих ініціатив, які покликані, між іншим, внести відповідні зміни, що мають доповнювати відомості про юридичних осіб у Єдиному державному реєстрі юридичних осіб, фізичних осіб-підприємців та громадських формувань. Слід звернути увагу на зауваження та пропозиції Міністерства цифрової трансформації, викладені у висновку. Пропоную прийняти висновок до законопроекту та ухвалити наступне рішення.

Рекомендувати Комітету з питань економічного розвитку врахувати висловлені зауваження та пропозиції під час підготовки та розгляду проекту Закону про внесення змін до чинного законодавства щодо удосконалення корпоративного управління в товариствах (реєстраційний номер 10304). Висновок комітету про розгляд зазначеного проекту закону направити до Комітету з питань економічного розвитку.

Дякую. Колеги, прошу підтримати.

ГОЛОВУЮЧИЙ. Дякую, Антон.

Є пропозиція підтримати рішення, що було озвучено, та проголосувати.

Хто – за? Проти? Утримався? Дякую. Рішення прийнято.

Я хотів би, Антон, попросити по наступному питанню зачитати рішення, тому що сенсу виступати Івану знову немає.

ШВАЧКО А.О. Добре. Шановні колеги...

ГОЛОВУЮЧИЙ. Стоп, стоп, ми переходимо до п'ятого питання порядку денного – проект Закону про внесення змін до Цивільного кодексу України (реєстраційний номер 10305), він пов'язаний з 10304. Тому, Антон, прошу.

ШВАЧКО А.О. Шановні колеги, законопроектом №10305 пропонується внести до Цивільного кодексу України зміни, якими вдосконалюються положення щодо корпоративних прав учасників юридичної особи. Розглянувши законопроект в межах предметів відання, пропоную виключити норму, передбачену пунктом 2 розділу I проекту закону – відомості про місцезнаходження юридичної особи включаються до Єдиного державного реєстру, оскільки вона дублює чинну норму, передбачену частиною четвертою статті 89 Цивільного кодексу України.

Пропоную також звернути увагу на зауваження та пропозиції Міністерства юстиції до законопроекту та потребу їх опрацювати.

Пропоную прийняти висновок до законопроекту та наступне рішення комітету. Рекомендувати Комітету з питань правової політики врахувати висловлені зауваження та пропозиції під час підготовки та розгляду проекту Закону про внесення змін до Цивільного кодексу України (реєстраційний номер 10305), направити висновок комітету про розгляд зазначеного законопроекту до Комітету з питань правової політики.

Дякую, колеги. Прошу підтримати рішення комітету.

ГОЛОВУЮЧИЙ. Дякую, Антоне.

Є пропозиція підтримати рішення та проголосувати. Хто – за? Проти? Утримався? Дякую. Рішення прийнято.

Ми переходимо до… Іване, дякую вам за виступ.

КАЛАУР І.Р. Я дякую вам за підтримку моїх законопроектів.

ГОЛОВУЮЧИЙ. Ми переходимо до шостого питання порядку денного про розгляд звітів основних суб'єктів національної кібербезпеки, визначених частиною другою статті 8 Закону України "Про основні засади забезпечення кібербезпеки України", щодо стану виконання заходів з питань забезпечення кібербезпеки держави за 2023 рік.

Колеги, до комітету надійшли звіти основних суб'єктів національної кібербезпеки щодо стану виконання заходів з питань забезпечення кібербезпеки. Їх було опрацьовано. На засіданні комітету присутні представники основних суб'єктів національної кібербезпеки. Пропоную виступити бажаючим та зазначити про проблеми, пропозиції та зауваження.

Шановні доповідачі та колеги, звертаю вашу увагу про озвучення лише відкритої інформації, інформацію з обмеженим доступом ми отримали на

руки, ми з нею ознайомилися, тому я хочу передати слово представнику Держспецзв'язку. Прошу.

_____. Добрий день, шановний пане голово, шановні народні депутати, запрошені. До вашої уваги пропонується звіт Держспецзв'язку за виконану роботу за законом України за 23-й рік.

Держспецзв'язку виконує завдання за декількома напрямками і основні результати складаються з того, що в напрямку формування реалізації державної політики щодо захисту державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури. Держспецзв'язку впроваджено, сформовано нарешті перелік об'єктів критичної інформаційної інфраструктури, який схвалений урядом у минулому році, впроваджено механізм застосування процедури Bug Bounty – пошуку, виявлення вразливостей в інформаційно-комунікаційних системах. Підготовлено і рішенням уряду затверджено етапи реагування на різні види подій у кіберпросторі, а також перелік заходів за кожним етапом реагування на такі події.

За напрямком координації діяльності суб'єктів забезпечення кібербезпеки, ми брали участь у виконанні плану оборони України, завдання, поставлені Генеральним штабом, виконані в повному обсязі. Проведено чотири командно-штабних навчання, які мають бренд *(нерозбірливо)* CIREX, які відбулися в енергетичному секторі, кроссекторальні з місцевими органами виконавчої влади та територіальними громадами. За напрямком впровадження авіаційно-технічної моделі ми врегулювали питання функціонування системи захищеного доступу державних органів до мережі Інтернет. Забезпечено функціонування, розвиток та збільшення переліку послуг кіберзахисту, що надаються Національним центром резервування державних інформаційних ресурсів. Автоматизована система експертної оцінки, ведення звітності та обліку стану кіберзахисту інформаційно-комунікаційних систем та об'єктів критичної інформаційної інфраструктури.

За напрямками організаційно-технічних заходів і запобігання та виявлення, та реагування на кіберінциденти, кібератаки. Забезпечення функціонування та розвиток урядової команди реагування на комп'ютерні звичайні події CERT-UA, опрацьовано майже більше ніж 2,5 тисячі кіберінцидентів, забезпечено проведення більше сотні сканувань на предмет виявлення вразливості та оцінювання стану захищеності державних інформаційних ресурсів об'єктів критичної інформаційної інфраструктури. Функціонує система, функціональна система антивірусного захисту, виявлення вразливості, реагування на кіберінциденти та кібератаки захищеного доступу державних органів до Інтернету.

За напрямком інформування про кіберзагрози та відповідні методи захисту від них ми запровадили ще пів року, публікуємо звіти, аналітичні звіти з питань кіберзахисту, де надаємо відповідні рекомендації. За напрямком державного контролю у сфері кіберзахисту затверджена нарешті Кабінетом Міністрів Постанова про Порядок здійснення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури і ця система зараз впроваджується.

За напрямком реалізації Стратегії кібербезпеки ми забезпечили вдосконалення організації, координації та моніторинг виконання плану заходів з виконання Стратегії кібербезпеки України. Ми сформували, уточнили, змістили відповідно до того, що в нас почалася війна і деякі питання були пролонговані у виконанні, і ми це затвердили в плані заходів уряду на 2023-2024 роки з реалізації Стратегії кібербезпеки.

За напрямком науково-методичного управління підготовкою фахівців. Ми за минулий рік затвердили 14 професійних стандартів у сфері кібербезпеки та захисту інформації. Разом кількість цих професійних стандартів складає 21 і був акредитований Національним агентством кваліфікацій вперше в Україні Кваліфікаційний центр інформаційних технологій та кібербезпеки ДержНДІ і технологій кібербезпеки Держспецзв'язку. За напрямками міжнародного співробітництва ми

співпрацюємо з державами-членами Європейського Союзу і Організацією Північноатлантичного договору в рамках відповідних договорів і меморандумів. Забезпечуємо реалізацію, де підписано меморандум з агентством кібербезпеки та безпеки інфраструктури Департаменту національної безпеки Сполучених Штатів Америки (CISA). Сформовано план та вживаються заходи і виконуються щодо укладеного (action plan) укладеного меморандуму з Іспанським національним інститутом кібербезпеки (INCIBE) та Національним криптологічним центром Іспанії (CCN).

Підготовлено та впроваджені низка меморандумів з нашими країнами-партнерами з їх відповідальними за кіберзахист державними органами.

Дякую за увагу. Доповідь закінчено.

ГОЛОВУЮЧИЙ. Дякую.

Є питання у колег? Да, прошу.

ШТЕПА С.С. Доброго дня. Я на початку вашого виступу почув одну фразу. Можливо, я не так і зрозумів. Хотілось би від вас почути все-таки тлумачення або пояснення. Я правильно зрозумів, що Держспецзв'язку разом з урядом лише нещодавно затвердили перелік об'єктів критичної інфраструктури так чи не так?

_____. Так, саме в минулому році був сформований і затверджений національний перелік об'єктів критичної інформаційної інфраструктури як підмножина об'єктів критичної інфраструктури.

ШТЕПА С.С. Тобто цей перелік був створений, коли минуло вже десь півтора, майже 2 роки війни, так? Повномасштабної.

_____. Від початку  війни ця робота була розпочата і вона була зосереджена на формуванні переліку об'єктів критичної інфраструктури. Одразу після того, як це перелік був сформований, буквально через 3 місяці, був затверджений Національний перелік об'єктів критичної інформаційної інфраструктури.

ШТЕПА С.С. Дякую. Почув.

ГОЛОВУЮЧИЙ. Дякую за доповідь.

Я прошу до слова представника  Міністерства оборони України.

_____. Міністерством  оборони, протягом 2023 року, в рамках робочої групи при Комітеті Верховної Ради України з питань національної  безпеки, оборони та розвідки, підготовлено законопроект про кіберсили Збройних Сил України, опрацьована четверта версія. Визначено формувача MILT CERT-UA, як основу підрозділу команди швидкого реагування на кіберінциденти  у військовій сфері. Сформовано та здійснено реагування на кіберінциденти  операційним центром кібербезпеки Міноборони. Ситуаційним центром Міністерства  оборони організовано на постійній основі централізовану агрегацію даних щодо подій кібербезпеки за уніфікованою формою та надається  структурним підрозділам для аналізу та прогнозування.

На базі вищих військових навчальних закладів готуються фахівці тактичного рівня за військово-обліковими спеціальностями кіберрозвідки, кіберзахисту  та кібервпливу. Імплементовано три військових стандарти НАТО щодо криптографії та порядку  доступу, а також один військовий стандарт з кіберборотьби.

На базі Національного університету оборони України розпочато виконання науково-дослідної роботи щодо визначення обрису системи кібероборони України.

Центральним науково-дослідним інститутом Збройних Сил України розпочато виконання наукових досліджень щодо перспективного кіберозброєння. Прийнято участь в низці міжнародних заходів за напрямом кібербезпеки, а також здійснено візит представників до засідання робочої групи України при військовому комітеті НАТО.

На інформаційних телекомунікаційних системах Державної служби спеціальної служби транспорту проводяться заходи штатної служби захисту щодо забезпечення кібербезпеки.

Доповідь закінчив.

ГОЛОВУЮЧИЙ. Дякую.

Є питання у доповідача, у колег? Якщо немає, дякую за доповідь.

Я хотів би надати слово представнику Національної поліції України.

_____. Шановний головуючий, шановні колеги, розглядаючи практичну площину діяльності Національної поліції. Необхідно відзначити, що робота у протидії кіберзлочинності відмічається своєю наступальністю та комплексністю. Всього у звітному періоді підрозділами Національної поліції зареєстровано близько 61,5 тисячі кіберзлочинів, повідомлено про підозру 3,5 тисяч особам, закінчено розслідування та скеровано до суду за обвинувальними актами понад 13,5 тисяч кримінальних проваджень. Відшкодовано понад 286 мільйонів гривень, що становить 86 відсотків від завданих збитків.

У 23-му році поліцейські активно протидіяли різним формам онлайн-шахрайству, запобіганню, виявленню, припиненню та розкриттю кіберінцидентів. Так у період дії воєнного стану набула поширення заволодіння коштами громадян під виглядом надання послуг з оформлення документів для чоловіків призивного віку, продаж військової амуніції, спорядження, оренди квартири для внутрішньо переміщених осіб, їх перевезень в безпечні регіони та волонтерська допомога. Загалом у

зазначеній сфері повідомлено про підозру понад 1,3 тисячі особам, пред'явлено обвинувальні акти понад 900 особам. Протягом звітного періоду особлива увага приділяється також протидії найбільш поширеним різновидам афер, так званим дзвінкам з банку та фішингу.

В результаті співпраці поліції з фахівцями Національного банку України та Національного центру оперативно-технічного управління мережами телекомунікацій, Адміністрації Держспецзв'язку вжито заходів для обмеження доступу до майже 45 тисяч доменних імен, які масово використовувались шахраями для створення фішингових посилань. Крім того, у рамках співпраці з міжнародними партнерами ініційовано та забезпечено активну участь у проведенні 18 міжнародних поліцейських операцій, у ході яких задокументовано протиправну діяльність ряду учасників хакерських угруповань.

З початку військової агресії Російської Федерації проти України поліція приймає активну участь у протидії державі-терористу у кіберпросторі, працівники якої залучені до забезпечення кібероборони України та виконання завдань з кіберборотьби. Зокрема, забезпечена участь у розбудові та реалізації проекту MRIYA, яка наразі перейменована у BRAMA. Екосистема BRAMA створена спільно із волонтерами для протидії ворогу на інформаційному фронті. Діяльність із забезпечення кібербезпеки тісно пов'язана із особами ІТ-осередку, які в свою чергу в наших реаліях готові до активних наступальних дій. На постійній основі здійснюється залучення волонтерів, фрілансерів, спеціалістів ІТ-осередку до співпраці щодо протидії агресії та дезінформації, якими здійснено вже 16,5 мільйонів заходів щодо висвітлення інформації в медіапросторі. Так, з початку збройної агресії держави-терориста підготовлено 86 тисяч 250 досьє на військовослужбовців Російської Федерації, колаборантів та так званих "рупорів Кремля".

З метою протидії російському військовому вторгненню, а також підтримці порядку на території України забезпечено обмеження доступу до 12 тисяч ресурсів Республіки Білорусь та Російської Федерації з переліку

важливих для економічної та політичної інфраструктури урядових сайтів, банківської та медійної сфери.

Дякую за увагу.

ГОЛОВУЮЧИЙ. Колеги, є питання до доповідача?

_____. Є питання.

ГОЛОВУЮЧИЙ. Прошу.

_____. Скільки фактично за 2023 рік було закрито вами кол-центрів, які працюють у банківській сфері шахрайство? І скільки людей було затримано?

_____. Нами було проведено, ну, наразі у мене такої статистики немає, але близько 500 обшуків на території України проводилося взагалі Національною поліцією та кількість підозр значна, але я зараз не можу вам повідомити, можемо надіслати у письмовому вигляді, якщо це потрібно.

_____. Добре. Дякую.

ГОЛОВУЮЧИЙ. Дякую, колеги. Дякую за виступ.

Ми переходимо далі. Я хотів би надати слово представнику Служби безпеки України.

_____. Дякую.

Службою безпеки України за 2023 було зосереджено зусилля як на забезпеченні кібербезпеки. Характерною особливістю є те, що абсолютна більшість, якщо не всі, кібератаки та наступальні кібероперації ворога були

здійснені спецслужбами Російської Федерації, зокрема, Федеральною службою безпеки головного управління Генштабу (колишнє ГРУ) та Службою зовнішньої розвідки, здебільшого саме ГРУ і ФСБ.

Службою безпеки України опрацьовано за 2023 рік понад чотири тисячі 400 кібератак та кіберінцидентів. Безпосередньо технічними працівниками служби здійснено реагування на наймасштабніші кібератаки, в принципі, наймасштабніші в історії України, це, зокрема, і Київстар, низка атак деструктивних на об'єкти енергетики, телекомунікаційні об'єкти, зокрема інтернет-провайдери, хостинг-провайдери, а також органи державної влади, зокрема Кабінет Міністрів, Міністерство фінансів, Антимонопольний комітет, Міністерство інфраструктури, Міністерство агрополітики тощо.

Безпосередньо технічними працівниками служби в рамках існуючої вже, створеної раніше платформи MISP-UA Malware Information Sharing Platform, до якої сьогодні підключено понад 1750 користувачів, розповсюджено понад 30 тисяч індикаторів компрометації. Також Служба безпеки під'єднана до MISP-NATO, єдина в Україні організація, яка під'єднана. Там нами створено 96 подій безпеки та завантажено понад тисячу індикаторів компрометації. З зазначеного приводу також були неодноразові візити до НАТО, власне, на яких наші працівники розповідали детальніше, що саме відбувається в країні та про роботу системи. Наповнення системи MISP-NATO сьогодні в більшій мірі здійснюється саме Україною.

Також здійснено заходи щодо підключення і розширення технічними пристроями об'єктів критичної інфраструктури з метою кращого розуміння і реагування на критичні події. Це, зокрема, встановлення так званих EDR, XDR рішень. Сьогодні в нас такими рішеннями безпосередньо службою покрито понад 40 об'єктів критичної інфраструктури. А до систем управління безпеки, так званих СМ-системам, підключено понад 30 об'єктів критичної інформаційної інфраструктури. Це по технічній протидії спецслужбам РФ, зокрема кіберагресії.

Важливо сьогодні сказати, що основним об'єктом сьогодні є саме сили оборони, зокрема Збройні Сили України. Тут Службою безпеки України здійснено низку кібероборонних операцій, які були визнані експертами по всіх стандартах НАТО. Зокрема, це кібероборонна операція по захисту системи ситуаційної обізнаності "Кропива", в рамках якої загалом службою за 2023 рік було проаналізовано і проактивно вивчено 6 військових систем ситуаційної обізнаності, це і Delta, "Кропива", Griselda тощо. Але саме в "Кропиві" нами було вчасно заблоковано 1700 скомпрометованих акаунтів та 800 пристроїв. Могли бути трагічні наслідки, тому що одне із шкідливих програмних забезпечень із семи, яке було віднайдемо в зазначеній системі. Атака була здійснена ГРУ ГШ так званою ПТ групою Sendworm Російською Федерацією могли завдяки шкідливому програмному забезпеченню бачити навіть конфігурації Starlink, і таким чином встановлювати по цим конфігураціям місця зосередження акаунтів, і таким чином коригувати в подальшому артилерійські та ракетні удари. Вказаною операцією повністю був зазначений доступ блоковано. Загалом в рамках забезпечення кібербезпеки саме Збройних Сил за 2023 рік було організовано перевірки: низку військових об'єктів органів управління абсолютно в усіх точках України. Було винайдено понад 400 скомпрометованих пристроїв, блоковано понад 200 каналів витоку інформації. Загалом перевірено понад 21 тисячу пристроїв всього. Це без розкриття, щоб не входити в інформацію з обмеженим доступом, вкрай системно діє ворог, як по ІКС Збройних Сил так і Міноборони, так і по спробам компрометації окремих пристроїв Telegram-акаунтів, Signal-акаунтів, тощо. І діють абсолютно всі і ГРУ ГШ, і ФСБ активно в зазначеному напрямку.

Крім того, за 2023 рік кібердепартаментом, тут уже як правоохоронним органом здійснено, було відкрито низку кримінальних проваджень, а також оголошено підозри, як за зловживання у сфері діджиталізації, тобто при розтраті, здебільшого це в статті 191, та інші службові злочини при розтраті коштів, які йдуть на цифровізацію та забезпечення функціонування ІТ-

інфраструктури. Також було припинено низку інтернет-провайдерів, які одночасно функціонували як на території України так і на тимчасово окупованих територіях України, і об'єктивно підозрювалися у передачі інформації агресору, також було блоковано низку доступів до об'єктів критичної інфраструктури з тимчасово окупованих територій. Знову ж таки це були оператори інтернет-провайдери, а також оператори систем документообігу тощо, щоб не розкривати далі деталей.

Загалом різних протиправних діянь, які пов'язані з державною зрадою, колабораціоністською діяльністю та діяльністю у сфері інформаційних технологій Службою безпеки за 2023 рік було, зокрема, по державній зраді, оголошено 130 підозр, для порівняння у 2022 році – 100. Інформаційних там в статті 109, 110, 436-2 тощо було оголошено понад 500 підозр, також позитивний період порівняно з 2023 роком. Загалом був надісланий широкий звіт, я думаю, що достатньо для…

ГОЛОВУЮЧИЙ. Дякую.

Є питання у колег?

_____. Я маю декілька запитань. Перше запитання. Ви знаєте, що у нас на території, так сказати, прикордонних областей функціонує  російське телебачення, беремо зону там 30-50 кілометрів. Як це фіксує СБУ, куди вона направляє свої висновки щодо цієї фіксації? Як на це дивиться Кабмін? Які взагалі заходи розробляються для припинення цього? Тому що не мені треба вам пояснювати, що відбувається, коли наші люди дивляться тільки російське телебачення, наше там не функціонує. Я кажу на прикладі Сумщини, але я впевнений, що Харківська область, також і інші прикордонні області мають цю проблематику.

Дякую.

_____. Звичайно, ми займалися цим питанням спільно з іншими органами, була відповідна робоча група під егідою Офісу Президента, ми… а також потім в Кабінеті Міністрів і наприкінці в цьому вже році буквально декілька тижнів назад вже вийшло розпорядження Кабінету Міністрів, воно гласне, на якому були нарешті виділені кошти на побудову системи блокування російського сигналу саме в прикордонних територіях.

Це відкрита інформація, є це розпорядження, там, якщо я не помиляюся, 160 чи 180 мільйонів гривень виділено на це. Будуть закуплені відповідні передатчики, які будуть встановлені на вежах Концерну РРТ по всіх прикордонних областях. В минулому році працювала робоча група, здійснювалися відповідні розрахунки, прорахунки, яким чином це зробити.

Хочу одразу сказати, що є як технічні певні проблеми стосовно того, тому що все одно, щоб закрити певні сліпі зони, треба забагато обладнання, так і те, що ці передавачі, вони знаходяться близько від лінії бойового зіткнення і, можливо, ви вже знаєте, буквально на минулому тижні і перед цим була масштабна атака "шахедами" саме по вежам КРРТ. Це було зокрема в Сумській  і Харківській області. До цього були спроби атак FPV-дронами веж в Чернігівській області. Сьогодні знову ж таки з цього питання є відповідна робоча група і вже сьогодні розроблений комплексний план захисту обладнання, який буде поступово впроваджуватися. Тому цим питанням займалися, в принципі, весь минулий рік, служба відповідним чином надсилала інформування, приймала участь в розробці, власне, рішення і в складі робочих груп. І нарешті вже рішення, воно є і є вже і фінансування. Тепер справа за впровадженням і подальшому ефективному захисту цих відповідних передавачів і веж для того, щоб вони могли безперебійно працювати.

_____. Дякую за відповідь.

ГОЛОВУЮЧИЙ. Прошу, Вікторія.

ПОДГОРНА В.В. У мене може трошки незручне запитання. Скажіть, будь ласка, а ви проводите якісь операції на руйнування кіберінфраструктури нашого ворога?

_____. Проводимо операції. Але у зв'язку з тим, що у нас тут більш відкрита інформація циркулює. Я можу сказати, що Службою безпеки проводяться як кіберооборонні так і кібернаступальні операції. Їх проведено десятки за минулий рік. Основний пріоритет у нас, звичайно, це отримання розвідувальної інформації. Нами підготовлено сотні, реально сотні інформувань на Головне управління розвідки, Генштаб, головнокомандуючим, МЗС, вище політичне керівництво держави по тій інформації, яку ми отримуємо з наших доступів з систем Російської Федерації. Зокрема, ну це таке, що вже відомо там і публічно, ми також працюємо над припиненням ланцюжків поставки складових частин до озброєння Російської Федерації, а також складових частин різних в напрямку, як правило, це електронники яким чином росіяни обходять санкції. І знову ж таки, це є комплектуючі здебільшого до озброєння – *(нерозбірливо)* плати, чипи тощо, тощо. Цією інформацією ми ділимось з партнерами. Завдяки партнерам нам вдалося в минулому році припинити поставку понад 400 тисяч чипів до крилатих ракет, які виробляються в Російській Федерації, а також сервомоторів, приблизно можна було виготовити понад 1600 БПЛА Shahed. Це як такий гласний приклад, про що можна говорити. А також ініційовано низку санкційних моментів тощо, тощо. Також були проведені звичайно і деструктивні операції. Але ми тут не будемо про це говорити, відкрито брати на себе відповідальність, про те така діяльність також здійснюється. Ви про неї багато про що могли чути там з Telegram-каналів тощо без прив'язки до Служби безпеки.

ПОДГОРНА В.В. Скажіть, будь ласка, а… *(Не чути)*

_____. Що саме? Дата-центри. Дивіться, є дата-центри на кшталт.. Дивіться, є дата-центри на кшталт "Парковий", умовно, як у нас, таких є три: Парковий, GigaCloud і DeNovo. Це такий комерційний дата-центр, де можуть там будь-хто, ви можете там викупити, наприклад, собі місце. А не комерційний, дивіться, умовно, у нас є дати-центри податкової, у нас є дати-центри митниці, у нас є дати-центри… в принципі, будь-де, де є інформаційні ресурси якісь значні, є дати-центри. Як правило, повинен бути свій один основний, ще резервний, можливо, тобто їх дуже багато питань. Але, звичайно, коли ми здійснюємо відповідні атакуючі дії свого роду, можна сказати так, що і треба дібратися до ядра інфраструктури і понищити те, що є на відповідних… Те, що ви називаєте дата-центрами або ЦОД (Центр обробки даних) тощо, звичайно, але це їх сотні.

Якщо ви прямо про такі комерційні говорите, як наші версії Amazon, то і в такі дата-центри у нас мали місце проникнення. Але здебільшого в тому випадку, якщо ми розуміємо, що якісь державні органи важливі там орендують інфраструктуру і можна отримати якусь важливу розвідувальну інформацію чи здійснити деструктивні акції, які будуть важливі для оборони нашої держави.

_____. Я ще маю одне невелике запитання. А мені цікаво, чи проводиться у вас якась навчальна програма для військових щодо кібербезпеки, кібергігієни, я маю на увазі не фактично з Генштабом? З вашої доповіді я зрозумів, що у вас в принципі високий рівень кібербезпеки, який ви пропонуєте і провадите у нас в країні. Але чи є співпраця безпосередньо з військовими, які знаходяться на нулі і, ми знаємо, що не всі люди там розуміють, що таке кібербезпека і як нею правильно користуватися. Чи є у вас якась програма спеціально для військових щодо цього, якщо це не таємниця?

_____. Насправді це величезна проблема. Тому що у нас сотні тисяч військовослужбовців і дійсно рівень кібергігієни, він залишає бажати кращого. Втім ви ж розумієте, що Служба безпеки України – це не інструкторський підрозділ, який об'їде...

_____. Я розумію.

_____. У нас трошечки інші задачі. В той же час тільки за 23-й рік, а і за попередні роки постійно, ми регулярно про всі перевірки, які ми здійснюємо, виявляємо, як я вже сказав, що там сотні скомпрометованих пристроїв. До речі, на жаль, має місце те, що військові передають відкритим способом, тобто через месенджери – Telegram, Signal, пошту – незахищені, інформацію, яка є з обмеженим доступом, а інколи може бути і визнана державною таємницею, через нерозуміння, через те, що треба там швидко все зробити і так далі. І, дійсно, сьогодні ворог цим користується. Мало того, ворог сьогодні вже вибудував систему аналітичної обробки даних, тих, які вони крадуть через свої проникнення. Нами було один із прикладів зафіксовано. Від часу як вони викрали дані в нас, бо тут був контрольований витік інформації, ми контролювали в нас цей канал, до того, як це дійшло до їх груп, де вони розповсюджують і повідомляють вже своїм військовим певні координати, тощо, пройшло чотири години. Це надзвичайно швидко. Тобто працюють цілі центри обробки, залучають і штучний інтелект, і так далі. Це з проблематики. Так ось нами по кожній такій перевірці, по виявленим проблемам і загально, я навіть не буду просто говорити скільки разів, надіслані відповідні листи, рекомендації, вимоги з глибокими інструкціями того, яким чином... починаючи від того, як двохфакторку встановлювати в телефоні, елементарні речі, до побудови безпеки вже окремих ІКС. Тому така робота як роз'яснює... А також ми працюємо спільно з ДВКР (Департамент військової контррозвідки) наш, в яких є представники відповідні на місцях.

Ходимо, говоримо, розповідаємо і так далі, і так далі. Проте, дійсно, проблеми є. Я впевнений, що якщо зараз тут у вас і у Верховній Раді депутатів перевірити, тут також будуть проблеми з кібергігієною. Так це декілька сотень чоловік. Так, постійно служба веде цю роботу в межах своїх повноважень, компетенції, всі надсилаються інформування, рекомендації, тощо. А також сьогодні є низка вже і кримінальних проваджень по недбалості військовослужбовців, за недотримання от цих відповідних норм.

Дякую.

ГОЛОВУЮЧИЙ. Дякую за доповідь.

Ми йдемо далі, прошу висловитись Службу зовнішньої розвідки України. Прошу до доповіді.

_____. Шановний пане голово, шановні народні депутати, шановні колеги. Служба зовнішньої розвідки здійснює розвідувальну діяльність щодо загроз національній безпеці України у кіберпросторі, інших подій і обставин, що стосуються сфери кібербезпеки.

У звітному періоді основні завдання – це було здобування та своєчасне забезпечення розвідувальною інформацією споживачів. Відповідно до їх компетенції, з національної системи забезпечення кібербезпеки, нами зосереджені зусилля обміну інформацією з Державною службою спеціального зв'язку та захисту інформації, Службою безпеки України, з Генеральним штабом, в рамках оперативних директив працюємо, плану оборони.

Обмінюємося як аналітичними даними так і технічною інформацією, технічними каналами з Національним координаційним центром кібербезпеки Ради національної безпеки і оборони і з CERT Держспецзв'язку, там достатньо великий обсяг інформації було надіслано.

За звітний період підготовлено план, який відповідно до чинного законодавства направлено на комітет у терміни.

Доповідь закінчив, якщо є конкретні питання, *...(Не чути)*.

ГОЛОВУЮЧИЙ. Дякую.

Колеги, є питання?

_____. Ну більшість діяльності – це, звісно, не публічна.

ГОЛОВУЮЧИЙ. Ми розуміємо. Дякуємо вам.

Якщо немає питань, я прошу представника Генерального штабу Збройних Сил України.

_____. Пане голово, панове народні депутати, колеги. З метою протидії кібервпливу противника Генеральний штаб Збройних Сил України спільно з іншими службами сил оборони в 2023 році продовжив здійснювати заходи з кіберзахисту інформаційно-комунікаційних систем Збройних Сил України та інших складових сил оборони, а також продовження заходів з кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури.

Для виконання вказаних завдань були залучені суб'єкти, підрозділи кібербезпеки та кіберзахисту від таких сил оборони і інших – це Збройні Сили України, Головне управління розвідки Міністерства оборони України, Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, Національної поліції України, Державної прикордонної служби України, Національної гвардії України і Служби зовнішньої розвідки України.

Значить, основні зусилля щодо впровадження заходів з кіберзахисту державних інформаційних ресурсів об'єктів критичної інформаційної інфраструктури та інформаційно-комунікаційних систем сил оборони в 2023 році були зосереджені на виконанні заходів з кіберзахисту інформаційно-комунікаційних систем сил оборони. Далі, проведення інформаційно-

аналітичної діяльності в частині виконання заходів з кіберзахисту державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури, роботі щодо посилення взаємодії між суб'єктами забезпечення національної системи кібербезпеки CERT-UA та органи державної влади стосовно своєчасного виявлення та негайного реагування на події кібербезпеки, кіберінциденти, кібератаки, роботи щодо провадження заходів забезпечення кіберзахисту критичної інформаційної інфраструктури в умовах надзвичайного, воєнного стану. А також брали участь в роботі щодо ідентифікації, індифікації та категоризації об'єктів критичної інфраструктури та об'єктів та об'єктів критичної інформаційної інфраструктури, формування відповідних національних перелік.

Далі, в рамках виконання плану реалізації Стратегії кібербезпеки України, значить, на виконання пункту 2 Генеральний штаб Збройних Сил України брав участь в розробці законопроекту про кіберсили разом з Міністерством оборони, а також проводив наради з погодження відповідного законопроекту з іншими зацікавленими суб'єктами.

Далі, значить, на виконання пункту 4 щодо розробки і забезпечення виконання плану кібероборони як складова частина Плану оборони України, значить, наступна інформація, що даний план розроблений і він постійно уточнюється, відповідно від задач, які надходять або зміни ситуації.

Значить, інші заходи, які виконуються в розрізі плану кібероборони, в принципі, частково вже колегами була зроблена доповідь, більш детальна інформація надана у звіті.

Дякую за увагу.

ГОЛОВУЮЧИЙ. Дякую вам.

Колеги, є питання до доповідача? Якщо ні, ми йдемо далі. Я даю слово представнику Національного банку України.

_____. Доброго дня, колеги. В умовах збройної агресії РФ проти України, оголошення військового стану Національний банк зосередив свої зусилля на забезпеченні сталої роботи банківської системи України, захист критичної інфраструктури, а також посилення кібербезпеки та кіберзахисту. Ключовим елементом забезпечення кіберзахисту стала робота в посиленому режимі Центру кіберзахисту Національного банку та команди реагування на кіберінциденти в банківській системі CSIRT-NBU, яка здійснювала постійний моніторинг ризиків та кіберзагроз інформаційним ресурсам Національного банку та банківської системи, також забезпечувала вжиття своєчасних та адекватних заходів реагування протидії. В посиленому режимі також працювали підрозділи інформаційної та кібербезпеки банків України.

Суттєвим результатом роботи в минулому році була протидія зростаючим проявам кібершахрайству та кіберзлочинності, здебільшого пов'язаним з програмами надання державної та міжнародної фінансової допомоги громадянам України. Завдяки безперервному моніторингу кіберпростору в 23-му році CSIRT-NBU виявив, ініціював блокування понад 41 тисячі фішингових ресурсів. Для порівняння, в 22-му – 5 тисяч 710. Все пов'язано з фінансовим шахрайством. В 23-му році система фільтрації фішингових доменів проектів DNS, яка працює в складі національного сервісу доменних імен зафіксувала майже 18,5 мільйонів переходів на фішингові посилання та забезпечила переведення на безпечну лендінгову сторінку близько 2 мільйонів запитів громадян на вказані шахрайські ресурси, які були.

Розширюючи коло та обсяг міжнародного співробітництва також був в 23-му році у Національного банку план, Меморандум про взаємодію у сфері забезпечення кібербезпеки та кіберзахисту з Фондом цивільних досліджень та розвитку Сполучених Штатів Америки (CRDF Global). Належну увагу Національний банк також приділив захисту об'єктів критичної інформаційної інфраструктури в банківській системі. Об'єкти критичної інформаційної

інфраструктури в банківській системі визначено, сформовано та підтримується в актуальному стані Реєстр об'єктів критичної інформаційної інфраструктури. В 23-му році також банк продовжує сприяти розвитку систем дистанційного обслуговування клієнтів банків, зокрема, поширюючи електронні довірчі послуги банківської системи *(Не чути)* Протягом 2023 року довірчих послуг на підставі рішення *(Не чути)* центру набули Ощад та Приватбанк. З метою подальшого розвитку вітчизняного ринку фінансових послуг системи дистанційного обслуговування клієнтів банків Національний банк унормував використання електронних підписів та електронних печаток у банківській системі, а також на ринку небанківських фінансових послуг державного регулювання, нагляд за діяльністю яких здійснює Національний банк. З метою підвищення рівня захисту власних інформаційних комунікаційних ресурсів Національний банк унормував питання порядку виявлення та розкриття вразливості інформаційних ресурсів Національного банку.

Також у 23-му році відбувся зовнішній аудит щодо відповідності процедури SWIFT положенням Концепції забезпечення безпеки користувачів *(Не чути)* засвідчив, що Національний банк забезпечив надійний захист даних та інформації в локальному середовищі SWIFT, а також мінімізовані кіберризики при використанні сучасних інформаційних технологій та підвищення контролю за безпекою інформації Національного банку. У мене все, колеги.

ГОЛОВУЮЧИЙ. Дякую.

Колеги, є питання до доповідача? Прошу.

_____. Я не знаю, колеги, чи може це відноситися до сьогоднішнього порядку денного, але я думаю, що якимось чином відноситься.

Я раптово з'ясував, що моя дружина рахується на ресурсах наших "Миротворець", на сервісах МВС як... і фінмон Нацбанку там заблоковував мені певні дії наші державні банки, тому що моя дружина, виявляється, є суддею Верховного Суду ДНР. Моя дружина, яка проживає тут, яка сплачує податки, яка пенсіонер і так далі. Дуже багато я доклав зусиль для того, щоб викреслити її з ресурсів: з "Миротворця", з *(Нерозбірливо)*, ще й на сервісі МВС.

Я, користуючись нагодою, вам задаю питання. Яким чином взагалі працюють у цій сфері наші фінмони і так далі, і так далі? Як взагалі ця інформація, яка... у нас є Дія, є всі інші сервіси, які об'єднуються, як взагалі таке може відбуватися, коли надаєш банку всі документи і все це в просторі, а тут таке от взагалі може відбуватись. І при чому, коли я до банку звернувся, вони кажуть, ні, нічого не маємо, ми нічого не можемо зробити, у нас червоне виходить, що ваша дружина, прізвище, ім'я і по батькові співпадає І вони записали і так далі, і воно, я познімав це в ручному, але це ж взагалі, про яку ми кібербезпеку можемо говорити, якщо взагалі у нас речі такі коїться в наших державних установах.

Дякую.

_____. Ну от дивіться, скажемо, банки у нас проводять оцінку ризиків клієнтів самостійно, у нас є ряд нормативних документів, які встановлює Національний банк. В цих нормативних документах не прописано банкам, що вони там мають брати ресурсі з *...(Нерозірливо)* або з "Миротворця", бо ще з якихось цих джерел, ну це взагалі не коректно, там навіть такого близько нема.

Є, скажемо, ну це більш стосується сторони фінансового моніторингу, ну я трошки більш по кібербезпеці, а то фінансовий моніторинг. Але, дивіться, є дуже, сотні таких випадків, різного плану, для цього у Національного банку створено ціле управління, воно називається Управління захисту прав споживачів. І туди кожний громадянин пише на любий банк, по

любій, по відмовам, по зняттю коштів, свої скажемо претензії і це обов'язково розглядається і обов'язково направляються запити на ці банки і обов'язково інформується людина, яка, скажемо, постраждала від цих дій, або як вона вважає, постраждала.

Ну такого абсурду, що банк не може, десь в красні лінії неї, ну ви розумієте – це якийсь абсурд. Це банк, програмно-технічний комплекс якийсь, в який вони ввели цю інформацію і на підставі цього, своїми документами це закріпили і вони не можуть зняти і придумують якусь цю, поки це десь так виглядає.

_____. *...(Не чути)* ресурсами, які взагалі, державні банки користуються ресурсами, які взагалі громадські організації?

_____. Да, да.

_____. А це повинно бути, до речі *... (Не чути)*

Тому три запитання, *... (Не чути)*

Коли ми кажемо про кібербезпеку, а взагалі виходить, що завтра вас можуть записати ім'я по батькові,*... (Не чути)*

*(Загальна дискусія)*

ГОЛОВУЮЧИЙ. Дякую, колеги.

Є ще питання у когось? Якщо ні, ми ознайомились зі звітами та заслухали доповіді, і я пропоную прийняти таке рішення, що інформацію, викладену у звітах суб'єктів національної кібербезпеки, визначених частиною другою статті 8 Закону України "Про основні засади забезпечення кібербезпеки України", взяти до відома та ухвалити це рішення.

Прошу проголосувати. Хто – за? Проти? Утримався? Дякую. Рішення прийнято.

Я хотів би подякувати всім доповідачам сьогодні. Я хотів би подякувати за вашу роботу і побажати вам удачі, далі ефективно працювати. У нас ще є питання, ми не будемо вас затримувати, так що…

_____. Дякую.

ГОЛОВУЮЧИЙ. Колеги, у нас є ще два питання. Перше – це про затвердження розкладу засідань комітету на 24-й рік. Є пропозиція провести… На квітень, на квітень, так. Є пропозиція провести засідання 3-го та 17 квітня. Прошу підтримати, проголосувати.

Хто – за? Проти? Утримався? Дякую.

Так, і є у нас ще питання у "Різному" про перегляд рішення комітету від 3 серпня 2022 року щодо подання від комітету кандидатури для включення до складу конкурсної комісії з добору кандидатів на посаду члена Національного регулятора. Відповідно до норм Закону про національного регулятора наш комітет має подати кандидатуру, одного представника до складу конкурсної комісії з добору кандидатів на посаду члена регуляторного органу. Конкурсну комісію в подальшому затверджує Кабінет Міністрів України.

На виконання норм закону комітет ще 3 серпня 2022 року подав до складу комісії кандидатуру Федієнка Олександра Павловича. На той час він був заступником голови Комітету з питань цифрової трансформації. За цей час, що пройшов, комісію не було утворено.

Станом на зараз Штепа Сергій Сергійович є заступником голови комітету, відповідним за предмети відання цифрової індустрії та електронних комунікацій радіочастотного ресурсу.

Тому пропоную переглянути уже зазначене рішення комітету та подати на розгляд Кабінету Міністрів України кандидатуру Сергія Штепи для затвердження членом конкурсної комісії з добору кандидатів на посаду членів регуляторного органу. Прошу голосувати.

Хто – за? Проти? Утримався? Дякую. Рішення прийнято.

Дякую. Всі питання вичерпані. Дякую за роботу.