СТЕНОГРАМА
засідання Комітету Верховної Ради України
з питань цифрової трансформації
28 квітня 2026 року

Веде засідання голова комітету КРЯЧКО М.В.

ГОЛОВУЮЧИЙ. Шановні народні депутати, присутні, ми починаємо наш комітет. Я хотів би звернутися до Антона Швачка, що поки немає Сергія Ларіна, то підрахунок голосів...

ШВАЧКО А.О. Добре.

ГОЛОВУЮЧИЙ. Дякую.

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. 5 – за.

ГОЛОВУЮЧИЙ. Перше 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 на 2025 рік.

Колеги на виконання статті 15 Закону України «Про основні засади забезпечення кібербезпеки України» комітет розглядає на своєму засіданні звіти основних суб'єктів національної кібербезпеки. На засіданні комітету присутні представники основних суб'єктів національної кібербезпеки. Пропоную заслухати виступи та зазначити про проблеми, пропозиції та зауваження.

Шановні доповідачі та колеги, перед розглядом цього питання хочу вам нагадати, що засідання у нас відкрите, ведеться відеозапис та стенограма, які будуть опубліковані на сайті комітету. Тому прошу доповідачів та колег, які будуть задавати питання, озвучувати тільки відкриту інформацію. Дякую.

Я хотів би тоді почати. І почнемо ми, надамо слово для доповіді представнику Генерального штабу Збройних Сил України. Прошу.

_____. ... почати з Міноборони, тому що ми узагальнюємо інформацію.

ГОЛОВУЮЧИЙ. Давайте так.

_____. Шановний голово комітету, шановні народні депутати, на ваш розгляд вноситься звіт системи Міністерства оборони України про стан забезпечення кібербезпеки держави у відповідності до вимог Закону України «Про основні засади забезпечення кібербезпеки України».

Міністерством оборони України та Збройними Силами заходи кібербезпеки виконувалися відповідно до вимог Закону України «Про основні засади забезпечення кібербезпеки України», Закону України «Про захист інформації в інформаційно-комунікаційних системах», Розпорядження Кабінету Міністрів «Про затвердження плану заходив на 2025 рік з реалізації Стратегії кібербезпеки» та інших нормативно-правових актів Кабінету Міністрів України.

Заходи, які були виконані в повному обсязі. За напрямком створення кібервійськ в системі Міноборони. На виконання наказу Верховного Головнокомандувача Збройних Сил, розроблено цільову модель функціонування Кіберсил Збройних Сил України. Також на виконання зазначеного введено в дію штат командування Кіберсил Збройних Сил України.

За напрямком стандартизації та управління інформаційною безпекою. Протягом звітного періоду в підрозділах Міністерства оборони, які безпосередньо займаються впровадженням та підтримкою інформаційно-комунікаційних систем, побудована система управління інформаційною безпекою. Міністерством оборони України пройшла сертифікацію система управління інформаційною безпекою на відповідність національному стандарту ДСТУ ISO/IEC 27001 2023 року. Забезпечено безперервний моніторинг подій кібербезпеки та виявлення аномалій у ключових інформаційно-комунікаційних системах оборонного відомства. Організовано постійну взаємодію команд реагування на кіберінциденти Міністерства оборони та Збройних Сил з основними суб’єктами національної системи кібербезпеки України. Обмін інформацією та про кіберінциденти здійснюються на постійній основі через визначені канали взаємодії в межах об’єднаних груп реагування на кіберінциденти і кібератаки. Також затверджено галузевий профіль безпеки. Розроблено стратегію кібербезпеки в системі Міністерства оборони.

За напрямком міжнародного співробітництва. Забезпечено технічну інтеграцію структурних підрозділів Міністерства оборони та Збройних Сил до платформи обміну інформацією про кіберзагрози і напад. Відомча команда реагування на кіберінциденти стала повноправним членом міжнародної організації «FIRST» – це форум команд реагування на кіберінциденти. Налагоджено постійний обмін інформацією про кіберзагрози з кіберкомандуванням Сполучених Штатів Америки, Франції, Естонії, Польщі та регіональним центром кібербезпеки Міністерства оборони Литви.

Протягом року представники Міністерства оборони Збройних Сил взяли участь у національних навчаннях Locked Shields, Cyber Coalition, CWIX та Defence Cyber Marvel. За напрямком військової освіти та кадрового забезпечення, до програми базової загальновійськової підготовки включено обов'язкову навчальну дисципліну, основи кібербезпеки для осіб, призваних за мобілізацією та військовослужбовців за контрактом.

Заходи, які були частково та такі, що перебувають на стадії завершення. З метою законодавчого визначення статусу та засад діяльності Кіберсил Збройних Сил України, Міністерством оборони та Збройними Силами, приймали активну участь в розробленні проєкта Закону України про Кіберсили Збройних Сил України (реєстраційний номер 12349), який було прийнято за основу та на цей він очікує розгляд на пленарному засіданні.

З метою взаємодії суб'єктів національної системи кібербезпеки в межах військових заходів кібероборони, було здійснено заходи у відповідності до плану кібероборони, в тому числі шляхом забезпечення роботи міжвідомчими групами кіберборотьби на пункті управління Генерального штабу Збройних Сил України.

Заходи, які не потребували виконання в звітному періоді. Уточнення плану кібероборони України в 2025 році не проводилося. Відповідні коригування, зумовлені зміною воєнної політичної та оперативної обстановки, були ініційовані та проведені заздалегідь у 2023 та 2024 роках.

Шановні народні депутати, реалізація зазначених заходів дозволила створити організаційну, технічну та кадрову основу для функціонування Кіберсил Збройних Сил України та основу для подальшого розвитку кібербезпеки в системі Міністерства оборони України. Для завершення процесу інституалізації нового роду сил Збройних Сил України прошу підтримати проєкт Закону 12349 в другому читанні.

Доповідь закінчив. Дякую за увагу.

ГОЛОВУЮЧИЙ. Дякую.

Я хотів би надати слово представнику Генерального штабу.

_____. Пане голово, панове народні депутати, колеги, я хотів би додати стосовно цього звіту, що ми приділяємо велику увагу прийняттю закону, проєкту Закону про Кіберсили Збройних Сил України, тому що він дуже необхідний і важливий для того, щоби ми могли в рамках реалізації заходів з відбиття воєнної агресії в кіберпросторі побудувати ефективну систему і нормативно узгодити всі ці питання.

В іншому представники міністерства відповідно по звіту, який надали, з всіма пунктами… ми також підтримуємо і додати більше нічого.

Дуже дякую.

ГОЛОВУЮЧИЙ. Дякую.

Я тоді прошу надати слово представнику Держспецзв'язку.

_____. Шановний головуючий, шановні народні депутати, присутні, до вашої уваги коротке представлення звіту Держспецзв'язку про стан виконання завдань із забезпечення кібербезпеки держави у 25-му році. Як основний суб'єкт національної системи кібербезпеки, на який покладено реалізацію найбільшої кількості завдань, в 25-му році служба була зосереджена на виконанні комплексних заходів, серед яких пріоритетом стала розробка нового удосконалення законодавства у зв'язку з прийняттям Закону 4336, який був прийнятий у березні 25-го року. Згідно плану уряду Адміністрацією Держспецзв'язку було розроблено та супроводжено прийняття 16 актів Кабінету Міністрів, 15 наказів Адміністрації Держспецзв'язку. На даному слайді якраз показані всі напрямки, по яких було внесено зміни до законодавства, і ті питання, які були реалізовані через Закон 4336, а саме методики, накази про застосування, авторизацію і інші напрямки, які були реалізовані в даному законі.

Наступний слайд. В умовах повномасштабної збройної агресії спостерігається стала тенденція до збільшення кількості кіберінцидентів. Протягом 25-го року Національною командою реагування на кіберінциденти, кібератаки та кіберзагрози CERT-UA зафіксовано 5 тисяч 927 кіберінцидентів. Переважна кількість даних інцидентів стосувалася поширення шкідливого програмного забезпечення. Об'єкти, на які були здійснені атаки, це органи державної влади, критична інфраструктура, зокрема енергетичний сектор, ІТ-компанії і ІТ-компанії з ІТ-комунікаціями. Ці інциденти були відпрацьовані разом з нашими колегами, була надана, в деяких випадках надана практична допомога, в деяких ми просто їх зафіксували, заблокували.

Наступний, будь ласка. Щодо координації діяльності суб'єктів забезпечення кібербезпеки та кіберзахисту. З метою переходу від формального виконання норм до практичної стійкості у 25-му році було акцентовано увагу на практичній підготовці та взаємодії. Результатами такої діяльності було проведено два масштабних командно-штабних навчання (ТТХ) з питань захисту критичної інфраструктури. Спільно з НАДС та міжнародними партнерами реалізовано проєкти навчання підвищення кваліфікації для керівників підрозділу з кіберзахисту. Платформа «CISO Campus» стала центром обміну практичним досвідом щодо побудови системи кіберзахисту та реагування на кіберінциденти, відпрацювання такої взаємодії і прийняття рішення в умовах кібербезпеки. Було проведено загалом більше 19 тренінгів та семінарів. Загальна кількість людей, які прийняли участь у цих тренінгах – десь біля 12 тисяч фахівців.

Для операторів критичної інфраструктури проведено 16 цільових заходів, в межах ініціативи з кібергігієни проведено 60 занять, які охопили понад 4,5 тисячі осіб.

Подальші напрямки... Наступний, будь ласка. Подальші напрямки удосконалення. Для подальшого зміцнення кібербезпеки держави у 2026 році визначено наступні стратегічні цілі. Завершення розробки та затвердження нормативно-правових актів на виконання Закону 4336. Тому що зараз ми фактично завершили всі зміни... всі прийняття нормативних актів на рівні Кабінету Міністрів, зараз більше уже іде робота над нашими наказами, методиками і методологіями. До кінця цього року плануємо повністю завершити все це нормативне навантаження.

Масштабування та розвиток платформи «CISO Campus». Ми розглядаємо «CISO Campus» не просто як навчальний майданчик, а як центр експертизи та формування професійної спільноти.

Масштабування та розвиток сервісів кіберзахисту. Впровадження концепції активного кіберзахисту, надання державним органам та операторам критичної інфраструктури доступу до високотехнологічних інструментів захисту. Розробка професійних стандартів, уніфікація вимог до фахівців на ринку праці, що дозволить чітко визначити кваліфікаційні рівні та створити прозору систему сертифікації спеціалістів. На сьогоднішній день необхідність у фахівцях CISO приблизно 70 тисяч людей. Тому ми плідно працюємо із деякими вищими навчальними закладами, щоб там відкривати центри по підготовці даних фахівців і також пропонуємо їм відкривати центри сертифікації, які перші у нас уже є на базі ДержНДІ, ми вже проводимо і навчання, і приймаємо іспити, видаємо відповідні сертифікати, але хочемо це масштабувати на рівні України, щоб воно не було, скажемо

так, монополізоване. Тому що велика кількість фахівців і розглядали навіть співпрацю з приватними структурами, які взяли напрямок по таким фахівцям. Це якраз уже демобілізованих, інвалідів, які мають профільну освіту, вони через Міністерство соціальної політики включають їх в ці навчання і потихеньку формується кількість таких фахівців.

Створення та розвиток мережі регіональних центрів кібербезпеки Держспецзв'язку. Ми масштабуємо присутність у регіонах, на сьогоднішній день фактично вже завершений досить потужний кіберцентр на Західній Україні, після його завершення будемо раді бачити вас і дамо офіційне запрошення.

Тому що це вже як би нового рівня кіберцентр, який буде закривати декілька областей і декілька галузей. І таких кіберцентрів ми плануємо, в найближчі 2-3 роки, зробити 9 по всій Україні.

Акредитація. І останнє – акредитація органу сертифікації продуктів, процесів та послуг, створення акредитованого органу сертифікації – це є кроком до створення внутрішнього ринку, перевірених та безпечних ІТ-продуктів. Тобто в цьому напрямку ми також здійснюємо розвиток як нормативної бази, так і практичного входу, в тому числі входу на ринок надання таких послуг.

Дякую за увагу.

ГОЛОВУЮЧИЙ. Дякую.

Я хотів би надати слово представнику Національної поліції України.

_____. Дякую.

За 2025 рік підрозділами Національної поліції зареєстровано 26 тисяч 900 кіберзлочинів. Повідомлено про підозру 3,5 тисячі особам у вчиненні 9 тисяч кримінальних правопорушень. І до суду з обвинувальним актом направлено 9 тисяч 100 кримінальних правопорушень. В цілому по результатах роботи відшкодування по злочинах понад 784 мільйони гривень, що встановило 102 відсотки по відшкодуванню, це через вартість майна, на яке було накладено арешт.

Також було б доцільно відмітити, що 583 скерованих до суду обвинувальних актів відносно організованих груп та злочинних організацій, які були виявлені працівниками Національної поліції, 72 з яких було пов'язано з інформаційно-комунікаційними технологіями. Питома вага злочинів – це онлайн-шахрайства. По онлайн-шахрайствах у нас 1 тисяча осіб отримали підозри, ще 96 осіб отримали обвинувальні акти у вчиненні

кримінальних правопорушень. В цілому було припинено діяльність 21 організованої злочинної групи та організації.

Національно поліцією з травня 25-го року було ініційовано проєкт Antifraud. Наразі в цьому проєкті залучено 12 регіональний підрозділів ГУНП. І цей проєкт було ініційовано спільно з Національним банком, з банківськими установами України та міжбанківською асоціацією. Що результат цієї роботи – це перші 6 годин після вчинення шахрайства, наші співробітники мають змогу в банківській установі встановити безпосередньо інституцію, платіжні засоби якої було використано для цього злочину, і за першої години заморозити кошти, які належать нашим громадянам. Так по результатах роботи цього проєкту за рік у нас у перші години було заморожено майже 145 мільйонів гривень, які було, потім може бути відшкодовано, які безпосередньо злочинці не отримали. Протягом року опрацьовано вже більше ніж 5 тисяч запитів по таких злочинах.

Протягом цього року планується, що вся Україна буде долучена, всі ГУНП будуть долучені до цієї системи і буде можливість отримувати інформацію безпосередньо і блокувати кошти наших громадян в перші години, як вони були отримані злочинцями.

Також хотілось би звернути увагу на те, що безпосередньо Національною поліцією проведено протягом року 22 спільні міжнародні поліцейські операції, частина з яких – це боротьба з онлайн-шахрайством та кол-центрами, а частина яких є великі транснаціональні злочинні угруповання по роботі так званого Ransomware – це шкідливе програмне забезпечення і програми-вимагачі.

Також необхідно зазначити, що 12 міжнародних операцій було ініційовано безпосередньо співробітниками Національної поліції, і у нас є окремий KPI для наших підрозділів, коли Національна поліція має бути ініціатором проведення міжнародної операції, а не долучатися до тої операції, яка проводиться нашими міжнародними партнерами.

Також необхідно сказати, що в структурі департаменту кіберполіції створено кіберцентр, безпосередньо це Security Operation Center, це SOC, який відповідає і за наказом міністра має відповідати безпосередньо за всю структуру Міністерства внутрішніх справ. Наразі проводиться інтеграція всіх *(нерозбірливо)* Міністерства внутрішніх справ до цього кіберцентру. Вже розгорнуто MISP і у нас є інтеграція як і з CERT-UA, так і з СБУ, і з MISP іншими, національними і міжнародними, для обміну інформацією про події та кіберінциденти.

Також необхідно наголосити на тому, що Національною поліцією проводиться декілька ініціатив, такі як «Кібербезпека фінансів» або

«Шахрай, good bay» за іншими учасниками ринку і за фінансовими установами, які направлені на те, щоб провести превенції, заходити превенції, та проінформувати наших громадян про найбільш актуальні та сучасні схеми шахрайські, які злочинці використовують, як не стати жертвою цього шахрайства, як не попастися на гачок.

Доповідь закінчив. Якщо є питання… Дякую.

ГОЛОВУЮЧИЙ. Дякую.

Да, прошу.

_____. Можна питання? Вчора просто вийшла доповідь такої організації «Global initiative». Вони якраз у кол-центр написали, там велика доповідь 50 сторінок. У вас є …

_____. Неготовий сказати, якщо можна…

_____. Да, якщо ви дасте контакт, я вам просто перекину.

_____. Да.

_____. Тому що там все детально.

_____. Дякую.

ГОЛОВУЮЧИЙ. Дякую за доповідь.

Я хотів би надати слово представнику Служби безпеки України.

_____. Шановний пане голово, шановні народні депутати, шановні колеги, ми розуміємо, що кіберпростір зараз є одним з головних фронтів, на якому вирішується стійкість нашої держави і обороноздатність та безпека наших громадян. І кібератаки на паливно-енергетичний, фінансовий, логістичний, інформаційний сектор і сектор безпеки та оборони – це невід’ємна частина практично всього періоду повномасштабного вторгнення. За 2025 рік кіберфахівцями Служби безпеки України було локалізовано більш ніж три тисячі кібератак і критичних кіберінцидентів, якщо точніше, то три тисячі десять кібератак і критичних кіберінцидентів, і стратегічними цілями ворожої атаки є підтримка їх військового вторгнення, деструктивний вплив на процеси всередині України, створення хаосу шляхом руйнування,

блокування роботи критичних сервісів, маніпуляція суспільною думкою та залякування.

Водночас сформовані Службою безпеки структури і напрацьовані механізми дозволяють нам своєчасно і ефективно, і невідкладно, у першу чергу, реагувати на виявлення кіберзагрози. І суттєво зменшити час і підвищити ефективність вжитих заходів.

Що стосується контррозвідувального захисту кібербезпеки суб'єктів сектору безпеки і оборони, то над пріоритетом Служби безпеки України є разом спільна, разом з нашими колегами з Міністерства оборони, з Генерального штабу Збройних Сил блокування витоку відомостей з інформаційно-комунікаційних систем підрозділів Сил оборони України, ми вживаємо спільних заходів з колегами щодо опрацювання і блокування витоків компроментації з акаунтів військовослужбовців Сил оборони України, зокрема, ми провели роботу з розробниками системи «Віраж» щодо якого виявлено та усунуто недоліки в реалізації алгоритмів шифрування паролів, що могло призвести до його розкриття.

Також ми провели масштабні ініціативні заходи з виявлення та блокування організованим підконтрольними російським спецслужбам хакерського угруповання каналу витоку даних з інформаційно-комунікаційних систем військових формувань.

Що стосується контррозвідувального захисту вітчизняного оборонно-промислового комплексу та виробництва. Кібербезпека підприємств оборонно-промислового комплексу та постачальників ЗСУ в умовах повномасштабного вторгнення набуває критично важливого значення. І протягом 2025 року кіберфахівцями Служби безпеки проведені проактивні заходи на ряді підприємств, що задіяні в реалізації державних оборонних замовлень. На жаль, в деяких інформаційно-комунікаційних системах були виявлені фактичні дані, що підтверджують проникнення ворога до інформаційно-комунікаційних систем зазначених підприємств, наразі вжитими вичерпними заходами Служби безпеки України ці витоки і відомості були блоковані і вживаються заходи щодо посилення кібербезпеки об'єктів військово-промислового комплексу.

Контррозвідувальний захист кібербезпеки органів державної влади та управління. Ви всі пам'ятаєте як наприкінці 2024 та початку 2025 року головна увага кіберфахівців Служби безпеки України була прикута до локалізації та нейтралізації однієї з масштабніших, наймасштабніших, мабуть, кібератак щодо державних реєстрів, які адмініструються ДП «НАІС» і які підпорядковані Міністерству юстиції. І завдяки оперативному реагуванню ми забезпечили, я маю на увазі кіберфахівців Служби безпеки

України, також нам допомагали, дякую вам, колеги з Держспецзв'язку, щодо швидкого відновлення критичних інформаційних державних сервісів. Тому що реально була, ну, загроза щодо, ну, втрати такого великого масиву інформації, але спільними заходами все відновили. І наразі забезпечення кібербезпеки набагато... безпека набагато суттєво підвищена на цьому об'єкті завдяки прийнятим ними заходам самостійно.

Фіксуємо активні акти кібершпигунства щодо систем відеоспостереження та відеоаналітики. І, зокрема, тільки в 2025 році ми локалізували і відпрацювали більше 30 тисяч доступних з мережі Інтернет камер відеоспостереження, що функціонують або з базами – заводськими налаштуваннями і авторизаційними даними, використовують слабкі паролі або такі, що мають відомі вразливості, які створюють ризики несанкціонованого підключення та отримання ворогом потоку відеоданих.

Контррозвідувальний захист кібербезпеки об'єктів критичної інфраструктури та їх життєзабезпечення. Тенденція до інтеграції кібершпигунства, кібертероризму та кібердиверсії з військовими та політичними цілями РФ слід розглядати не як реально епізодичний набір інструментів, це системна стратегія ворога для досягнення власних імперських геополітичних амбіцій.

У березні 25-го року Україна зазнала одну з найбільших скоординованих та масштабних кібератак, це кібератака на Укрзалізницю, акціонерне товариство «Укрзалізниця». Вона мала, я маю на увазі кібератака, чітко виражений деструктивний характер. Але завдяки оперативному реагуванню СБУ вдалось запобігти колосальним наслідкам, які могли б призвести до зупинки транспортного сполучення, економічних втрат та загроз для безпеки пасажирів.

У 25-му році ми також фіксуємо цілеспрямовані кібератаки на ряд об'єктів теплоенергетичної інфраструктури, що поєднані з кінетичними ударами могли мати додатковий вплив на населення і забезпечення населення теплом та енергетикою відповідно. І нам вчасно вдалося зреагувати на потужні хвилі кібератак і запобігти суттєвим негативним наслідкам саме в цифровій віртуальній сфері.

В 25-му році діяльність СБУ України посіла ключове місце в формуванні національної системи протидії кіберзагрозам. І дякую вам, що в минулому році ви прийняли зміни до Закону «Про основні засади забезпечення кібербезпеки», вони дали і визначили нам реальне передбачене законодавством повноваження щодо реагування на кіберінцидент у сфері держбезпеки. І це дуже важливо для нас. Ще раз вам дякую. І ми отримали

додаткові повноваження щодо координації дій суб'єктів забезпечення кібербезпеки, протидії кібершпигунству, кібертероризму та кібердиверсіям.

У 25-му році... він став у тому числі завдяки цьому нормативно-правовому акту, цього закону він став переломним у переході від переважно реактивних дій до проактивної моделі роботи, і був налагоджений контррозвідувальний пошук потенційних та реальних кіберзагроз для державних інформаційних ресурсів, інформаційно-комунікаційних систем об'єктів критичної інфраструктури та суб'єктів сектору безпеки та оборони. Завершено розбудову по нашій системі мережі регіональний центр забезпечення кібербезпеки регіональних органів СБУ. Тобто в кожній області є регіональний РЦСК – регіональний центр забезпечення кібербезпеки, який є найближче до об'єктів посягань ворога і може невідкладно надати відповідну допомогу щодо відбиття або локалізації ворожої кібератаки.

В межах наукового забезпечення діяльності Служби безпеки сформовано три територіально-методологічного та прикладну основу для організації негласних перевірок готовності об'єктів критичної інфраструктури до протидії кібератакам і кіберінцидентам. Впроваджено та забезпечено функціональний повний цикл розвитку кіберзагроз, так званий Cyber Threat Intelligence, тобто CTI, що передбачає безперервний процес збору, обробки та аналітичного узагальнення даних щодо потенційних та актуальних кібератак, з метою проактивного захисту інформаційно-комунікаційних систем.

За узагальненими результатами ми поінформували Прем'єр-міністра України, Секретаря Ради національної безпеки і оборони, керівника Офісу Президента України. Відповідно надіслали належні звіти до Верховної Ради України.

Розвиток державно-приватної взаємодії. В 25-му році провели черговий 5 та 6 практичні семінари з питань підвищення кіберстійкості для представників центральних органів виконавчої влади, і там були присутні більше 133 різних відомств, підприємств та установ. 24 жовтня 25-го року ми провели вперше в історії України форум: кібертероризм, саме як кібертероризм як виклик державі в умовах війни, і командно-штабні навчання «Оберіг-2025». І це стало першим в Україні масштабним заходом, спрямованим на практичне відпрацювання алгоритму реагування на прояви кібертероризму та загрози терористичного характеру. І ми цей захід, він поєднав моделювання практичної сфери, моделювання реальних сценаріїв вчинення терористичних актів та кібератак і напрацювання рішень щодо спільної їх ефективної нейтралізації, саме всіх суб'єктів загроз.

У минулому році ми провели з урахуванням, що фіксуються системні проникнення кібератаки щодо вітчизняних медіа та особистого акаунту в українських журналістів ми провели у 2025 році для представників масмедіа низки занять з підвищення рівня кіберграмотності і безпеки в Інтернеті в рамках семінару організованої програми підтримки України ОБСЄ. Це були такі, наприклад, брошури, який чіткий алгоритм прописаний, як забезпечити, наприклад, кібербезпеку як персональних гаджетів, комп'ютерів, так і інформаційно-комунікаційних ресурсів.

У 2025 році Служба безпеки України спільно з Українською радою збройрів проведено онлайн-семінар «Сучасні виклики для оборони ІТ-систем» і в цих заходах брали більш ніж 30 підприємств обронно-промислового сектору України.

І мета цього заходу була підвищення рівня технічних бізнесів фахівців ОПК щодо сучасних кіберзагроз. Я не буду перелічувати ці нормативно-правові акти, але ми спільно з Держспецзв'язком приймаємо участь у розробці відповідних підзаконних нормативно-правових актів на виконання закону, про який я раніше зазначив щодо внесення змін до Закону України «Про основні засади забезпечення кібербезпеки».

У 2025 році власними силами відповідно до міжнародного стандарту ДСТУ ISO 27001 була створена система управління інформаційною безпекою, яка забезпечує комплексний і безперервний захист інформаційних активів СБУ, підвищує стійкість до кіберзагроз, забезпечує відповідність міжнародним вимогам.

Як висновок можна констатувати, що Служба безпеки України перебуває у процесі постійного розвитку та адаптації до зростаючих викликів у кіберпросторі послідовно нарощується аналітичні, технічні та організаційні спроможності, що дозволяє адекватно реагувати на сучасні загрози та діяти на випередження. І на моє особисте переконання, робота СБУ у звітному періоді дозволить посилити спроможність у сфері забезпечення кібербезпеки та створила необхідні умови для подальшого розвитку в 2026 році. Велике дякую вам за увагу.

ГОЛОВУЮЧИЙ. Дякую.

Я хотів би надати слово представнику Служби зовнішньої розвідки.

_____. Шановний пане голово комітету, шановні народні депутати, шановні колеги, Служба зовнішньої розвідки у звітному періоді прикладала зусиль на забезпечення споживачів розвідувальною інформацією про загрози нацбезпеці в кіберпросторі. Така інформація, як аналітична, так і

технічна, надавалась основним суб'єктом забезпечення кібербезпеки відповідно до їх компетенції на постійній основі. Технічна інформація також передавалася національними системами обміну такої інформації для швидкого реагування. Також заходи виконувалися в рамках протокольних рішень Національного координаційного центру при РНБО, а також участі в оперативній директиві з кібероперацій. Спільно з міністерством... ми давали сприяння Міністерству закордонних справ у захисті інформаційних систем закордонних дипломатичних установ.

З публічної доповіді все. Звіт повний був направлений на вашу адресу в січні. Якщо є питання, готовий відповісти.

ГОЛОВУЮЧИЙ. Дякую.

Колеги, якщо будуть зараз питання, ви можете по ходу задавати до виступаючих.

Я хотів би надати слово представнику Національного банку України. Прошу.

_____. Шановний голово, шановні народні депутати, Національний банк у 25-му році забезпечив виконання завдань і реалізацію повноважень основного суб'єкта національної системи кібербезпеки України, визначений Законом «Про основні засади забезпечення кібербезпеки України». В умовах правового режиму воєнного стану Національний банк продовжив працювати над забезпеченням кіберстійкості банківської системи та забезпечення сталої роботи фінансового сектору України в цілому. В 25-му році Центр кіберзахисту Національного банку та його команда реагування CSIRT-NBU продовжувала працювати в посиленому режимі та режимі посиленого моніторингу кіберзагроз, оперативного вжиття необхідних заходів реагування та протидії у сфері своєї відповідальності.

В межах компетенції Національний банк забезпечив реалізацію заходів стратегії кібербезпеки України відповідно до рішення Ради національної безпеки і оборони від 30 грудня 21-го року та про план реалізації Стратегії кібербезпеки України. Забезпечено участь Національного банку в роботі Національного координаційного центру, НКЦК при Раді національної безпеки та оборони і виконання прийнятих НКЦК при РНБО рішень... забезпечено керівництвом та відповідними структурними підрозділами Національного банку.

В 25-му році зберігалась тенденція попередніх років щодо кількості кібератак, спрямованих на об'єкти критичної інфраструктури, банківської системи України, а також щодо зростання проявів кібершахрайства та

кіберзлочинності. Впродовж 25-го року командою CSIRT виявлено та проведено аналіз близько 2 тисяч зразків шкідливого програмного забезпечення та своєчасно проінформовані банки України про виявлені інциденти кібербезпеки і зафіксовані спроби вчинення кібератак.

На платформі обміну інформацією MISP-NBU, до якої підключено 60 банків та ключові небанківські фінансові установи, було надіслано 340 повідомлень про кіберінциденти та індикатори кіберзагроз.

За результатами аналізу подій впродовж 2025 року встановлені кіберзагрози для фінансової системи мали стійкий та системний характер і були зосередженні переважно на фішингових і таргетованих компаніях.

Протягом 2025 року CSIRT-NBU було виявлено та опрацьовано понад 15 тисяч фішингових електронних повідомлень, значна частина яких містила шкідливі посилання, що використовувались зловмисниками для отримання несанкціонованого доступу до облікових даних користувачів або ініціювання поширення шкідливого програмного забезпечення. Командою CSIRT-NBU виявлено та ініційовано блокування 72 тисяч фішингових ресурсів, пов'язаних із фінансовим шахрайством і стилізованих під урядові, публічні та популярні портали. Це такі як портал Кабінету Міністрів України, Дія, Допомога, Зимова єПідтримка, єВідновлення, єПільга, єВиплата, портал гуманітарної допомоги, Укрпошта, OLX, Нова пошта тощо, портал українських банків і платіжні сервіси. За результатами аналізу трендових шахрайських компаніях на порталі центру кіберзахисту опубліковано 39 матеріалів, що описують відповідні схеми.

В 2025 році з використанням системи фільтрації фішингових доменів убезпечено від доступу на шахрайські ресурси близько 2,3 мільйона запитів громадян України.

Міжнародна співпраця залишається пріоритетом роботи команди CSIRT, команда реагування на кіберінциденти продовжила виконувати свої обов'язки і умови для підтримання статусу accredited в TF-CSIRT в міжнародній спільноті команд реагування на кіберінциденти.

У звітному періоді Національний банк провів виїзні перевірки за напрямком інформаційна безпека та кіберзахист п'яти банків, також проведено ризик-орієнтоване планування таких заходів на наступний період.

З метою приведення нормативно-правових актів Національного банку відповідно до Закону «Про основні засади забезпечення кібербезпеки України» та Закону «Про Національний банк України» унормовано питання встановлення вимог щодо організації заходів забезпечення інформаційної безпеки та кіберзахисту надавачами фінансових послуг, страховиками, кредитними спілками, фінансовими компаніями, ломбардами. Це Положення

про організацію заходів забезпечення інформаційної безпеки та кіберзахисту надавачам фінансових послуг затверджене Постановою Правління Національного банку № 143.

На виконання вимог Закону «Про хмарні послуги» унормовано питання визначення порядку застосування технологій хмарних обчислень банками надавачами фінансових послуг, операторами платіжних систем, учасниками платіжних систем, технологічними операторами платіжних систем. Це Положення про порядок застосування технологій хмарних обчислень затверджене Постановою Правління Національного банку № 99.

Реалізовано додаткові заходи спрямовані на розвиток і посилення спроможності функціонування системи кіберзахисту Національного банку. В 2025 році проведено аудит інформаційної безпеки Національного банку, за результатами аудиту визначено та сплановано заходи щодо усунення потенційних вразливостей інформаційної інфраструктури НБУ.

Крім цього в 2025 році Національний банк, за результатами первинного сертифікаційного аудиту системи управління інформаційної безпеки ISO 27001*(нерозбірливо)*отримав сертифікат відповідності, який засвідчує, що Національним банком впроваджена та згідно з сучасним світовим досвідом ефективно функціонує система управління інформаційної безпеки.

Доповідь закінчив.

ГОЛОВУЮЧИЙ. Дякую.

Я хотів би надати слово представнику Міністерства закордонних справ України.

_____. Дякую.

Шановний пане голово, шановні народні депутати члени комітету, дорогі колеги, Законом України №4336-IX від 27 березня 2025 року Міністерство закордонних справ України було додане до основних суб'єктів національної системи кібербезпеки України. Цим законом перед міністерством було поставлено декілька основних завдань. Якщо стисло підсумувати результати 2025 року, то робота МЗС на цьому напрямі була зосереджена на трьох ключових блоках.

Перше. Поглиблення європейської та міжнародної координації для посилення кіберстійкості України.

Друге. Просування українських інтересів в міжнародних організаціях та формування правил поведінки у кіберпросторі.

Третє. Синхронізація з партнерами у питаннях атрибуції, санкцій і спільної відповіді на деструктивну кіберактивність.

Насамперед, у 2025 році МЗС забезпечено суттєве просування євроінтеграційного треку у сфері кібербезпеки. Ключовою подією стало проведення у жовтні минулого року четвертого раунду кібердіалогу Україна – ЄС. Цей формат дав змогу узгодити підходи до подальшої інтеграції України у європейську кібербезпекову екосистему, до зміцнення кіберспроможностей, до розвитку державно-приватної взаємодії, а також до координації санкційного реагування на деструктивну діяльність у кіберпросторі.

Другий важливий елемент – «Талліннський механізм», який у 2025 році залишався центральним інструментом координації міжнародної технічної допомоги для посилення цивільної кіберстійкості України. Упродовж року механізм розширився, до нього приєдналися нові донори, а партнерами було задекларовано 60,9 мільйона євро додаткового фінансування. Міжнародна підтримка України вийшла далеко за межі політичних декларацій і вже працює практично інструмент підвищення стійкості державних органів, і критичних цивільних сервісів.

У листопаді 2025 року було проведено перший раунд кібердіалогу Україна-Нідерланди, який заклав основу для регулярного двостороннього механізму координації дій по питаннях реагування на кібератаки, захист критичної інфраструктури та обміну інформацією про загрози. Паралельно розвивалася регіональна співпраця з Румунією та Молдовою, результатом якої стала інституалізація тристороннього Cyber Alliance з метою предметності праці для протидії кібер та гібридним загрозам. Також розвивалася взаємодія з профільними міжнародними інституціями, зокрема, з Європейським центром передового досвіду з протидії гібридним загрозам та Об’єднаним центром передового досвіду НАТО з кібероборони.

Другий великий блок – це участь України у міжнародних організаціях для вироблення норм відповідальної поведінки у кіберпросторі.

У 2025-му році українська делегація активно працювала в рамках ООН та ОБСЄ. У межах робочої групи складу ООН з питань безпеки ІКТ, Україні вдалося відстояти підходи, які відповідають нашим національним інтересам, і не допустити включення до підсумкових документів неприйнятних положень.

ОБСЄ Україна в рамках діяльності неформальної робочої групи з питань зміцнення довіри у сфері використання ІКТ системно доводила до партнерів факти зловмисної кібердіяльності РФ та просувала необхідність дотримання відповідальної поведінки у кіберпросторі.

Крім цього, МЗС сприяло проведенню спільних з ЄС заходів, спрямованих на підвищення стійкості у кіберпросторі та спроможності

реагувати на кіберзагрози. Йдеться і про участь у відповідних робочих групах Ради ЄС і про залучення українських представників до профільних конференцій, тренінгів, навчань та семінарів. Це було важливо для посилення професійної підготовки наших фахівців, наближення українських практик до європейських та розвитку спільних механізмів реагування.

Третій блок – це координація санкційної політики та спільних дипломатичних дій у відповідь на деструктивну кіберактивність.

У 2025 році МЗС продовжувало системно інформувати міжнародних партнерів про необхідність посилення тиску на Російську Федерацію за її зловмисну діяльність у кіберпросторі. Україна синхронізувала підходи з євроатлантичними партнерами, підтримувала відповідні санкційні рішення та приєднувалась до актів і заяв Європейського Союзу. Важливо, що впродовж року партнери запровадили нові санкційні обмеження проти підрозділів ГРУ, офіцерів розвідки та російської інфраструктури задіяної в кібератаках. МЗС оприлюднило відповідні заяви на підтримку таких рішень.

Окремо хочу підкреслити, що у 2025 році МЗС не лише виконувало зовнішньополітичні та координаційні функції, а і посилювало власну інституційну спроможність як суб'єкт національної системи кібербезпеки.

Було виокремлено відділ кіберзахисту МЗС в окремий структурний підрозділ, одночасно фахівцями міністерства забезпечувався комплексний кіберзахист органів дипломатичної служби. Також була розроблена і впроваджена навчальна програма з кібербезпеки для працівників дипломатичної служби.

Отже, за підсумками 2025 року можемо констатувати, що МЗС України забезпечувало посилення координації з ЄС і ключовими партнерами, сприяла залученню міжнародної допомоги для підвищення кіберстійкості України, відстоювала національні інтереси в міжнародних організаціях, а також працювала над формуванням узгоджених санкційних і дипломатичних механізмів реагування на деструктивну кіберактивність.

Доповідь закінчено. Дякую за увагу.

ГОЛОВУЮЧИЙ. Дякую.

Всі виступи завершено, якщо у колег є... Прошу.

_____ . Доброго дня, хотів би поставити питання Держспецзв’язку щодо однієї з попередніх доповідей. Там було, якщо не помиляюсь приблизно 6 тисяч кіберінцидентів, які були проранжовані по ступеню їх критичності. Я побачив, що там 5 тисяч 800 – це medium критичності, 70 – low, якщо не помиляюсь, 11 – high і одна прямо critical.

Якщо можна, поясніть, трошки, в межах того, що ми можемо казати публічно, що це була за єдина кіберзагроза статусу «critical», що це було за кіберзагроза статусу «high», яких було так порівняно небагато, ну, в порівнянні з «medium».

_____. Да, дозвольте відповісти? Директор департаменту кіберзахисту адміністрації Держспецзв'язку. У нас дійсно в країні вже усталеною є система категоригування кіберінцидентів, кібератак і вона відповідає постанові Кабінету Міністрів України, дійсно командою CERT-UA було зафіксовано та пропрацьовано 12 кіберінцидентів високого та критичного рівня. В принципі, не для гласності ми можемо передати вам цю інформацію стосовно цих операторів або державних органів, де сталися ці кіберінциденти. Тому що просто нагадаю, у нас відповідно до постанови 1533, у нас є критерії визначення, що інформація, деяка технічна інформація про кіберінциденти, кібератаки є інформацією з обмеженим доступом. Тому або, можливо, після засідання, можливо, скажімо, особисто що це за організація. Якщо необхідна інформація – залюбки ми поділимося.

_____. Дякую. Достатньо.

ГОЛОВУЮЧИЙ. Так, прошу, Володимире.

АР'ЄВ В.І. В мене питання до Держспецзв'язку і Міністерства оборони щодо месенжерів, які заборонені до використання на лінії бойового зіткнення або в районі лінії бойового зіткнення. Чи оновлювався цей список? І причини блокування тих чи інших месенжерів, наприклад, вайбер, про найпопулярніший, на превеликий жаль, меседжер? Я хочу почути інформацію: чи відповідає дійсності те, що вайбер ключі доступу, зокрема, в тій частині, де вони працюють у Російській Федерації, на вимогу їхнього законодавства віддав для контролю федеральній службі безпеки, їхнім органам? Це перше питання. Будь ласка.

_____. Я думаю, що більше навіть до Генерального штабу. Начальник управління кібербезпеки Головного управління зв'язку. Значить, відповідно до Наказу №165 Головнокомандувача Збройних Сил в 2024 році Збройні Сили дозволили використання визначених месенжерів, в тому числі і на лінії бойового зіткнення. Це пов'язано з тим, що, ну, стало зрозуміло, що на відміну від мирного часу, де у нас всі месенджери були заборонені, а використання мобільних пристроїв було обмежено, на жаль, в условиях

бойових дій це неможливо. Тому ми врегулювали це питання, дозволили використання відповідно трьох месенджерів: Signal, Threema і WhatsApp, але ввели чіткі правила їх використання, зокрема регуляцію поведінки в групах месенджерів, призначення адміністраторів з виключною функцією додавання членів в ці групи з обов'язком ідентифікації їх щомісячно і так далі.

Крім того, зараз практично фіналізуються роботи по створенню військового месенджера, з одним із операторів відповідно українських уже проводиться його тестування і далі після його впровадження, в принципі, решта месенджерів будуть заборонені взагалі. Решта месенджерів, такі як Telegram і згаданий Viber, вони обмежуються технічними засобами, тобто блокуються на рівні військових мереж і дозволяються лише тим, кому відповідно до рішення командира письмового дозволено використовувати ті месенджери відповідно до службових обов'язків. Тобто розвідники, інформаційно-психологічні операції і так далі. Доповідь закінчив.

АР'ЄВ В.І. Тоді уточнення, все ж таки хто може зараз, тому що це все ж таки у нас публічна інформація надається, пояснити небезпеку використання Viber і Telegram для того, щоб люди нарешті зрозуміли, в чому є небезпека? От якщо військовим заборонено використовувати без, як ви сказали, без спеціального дозволу ці месенджери, то назвіть, будь ласка, причини цього.

_____. Причини заборони месенджера Telegram, тому що на рівні Ради національної безпеки і оборони було прийнято відповідне рішення, доведено до всіх органів державної влади, державних установ про заборону використання месенджера Telegram, що було реалізовано в Збройних Силах без додаткових запитань.

Стосовно Viber, так же як і решти месенджерів, ми вирішили, що буде доцільніше дозволити обмежену кількість, яка необхідна суто для виконання бойових завдань, які проще контролювати, держать під контролем групи і так далі. Ми не аналізували питання детально, чи можливий доступ до ключів, серверів і так далі, але ми провели консультації з Держспецзв'язку зі Службою безпеки України і за результатами були визначені саме ці месенджери.

АР'ЄВ В.І. Ну і тоді ще питання, напевно, до Держспецзв'язку чи проводяться роботи з уніфікації баз даних, самих структур баз даних? Бо одною з причин, зокрема, дірявої такої структури в серверах, в реєстрах Мін'юсту ця вразливість стала причиною великої атаки, яка вивела з ладу ці

сервери. Тобто вони там, скажімо так, база даних була, існувала із різних різного формату файлів такий-то собі конструктор «Лего» від старого до більш сучасного, що поставило питання про те, щоб уніфікувати ці бази даних і покращити захист взагалі серверів, реєстрів, які зберігаються на цих серверах. Скажіть, будь ласка, чи були зроблені відповідні кроки для того, щоб привести це все до єдиного знаменника.

_____. Да. Технічно після атаки на Мін'юст не будемо углублятися в саму причину, там не зовсім так, як доносилось, там декілька є факторів, чому це відбулося. Да, один. У нас були внесені зміни в 303 Постанову, що дало нам можливість проводити перевірки під час військового стану Департаментом державного контролю плюс було відповідне рішення ставки про проведення всіх перевірок по нашому напрямку.

Перше. Це ДІР (державні інформаційні реєстри) і далі якби йдемо поетапно перевіряємо зараз всіх суб'єктів, які використовують ІКС, особливо там, де вони, там де є критичними.

Крім того, ми надаємо сервіс по зберіганню бекапів, є платформа реєстрів, яка є, це обов'язок всіх органів, які мають реєстри, бекапи зберігати у нас на захищених локаціях і це також уже, робота ця, проводиться постійно. Тому напрямки в цьому, вони системно йдуть і багато де вже покращено, десь ще є, там, де ми заходимо на контрольні перевірки, які не усунуті, там уже іде адміністративний вплив на суб'єктів, але в цілому це системна робота проводиться, вона проводилася завжди, але після цього інциденту, який був в НАІС, потім в Укрзалізниці, планово, системно у нас працюють всі 25 областей в цьому напрямку, наші підрозділи, там третій відділ, і центральний апарат.

_____. Доброго дня. У мене, можна сказати так, загальне питання. Ми з вами бачили ситуацію, коли жодна досконала система кібербезпеки не працює, якщо немає так званої кібергігієни. Це приклад Пентагона, це приклад месенджера Signal, це додавання туди незрозумілих людей і так далі, і тому подібне. У мене питання. А чи працює у нас система, яка здійснює контроль за оцією кібергігієною усіх відомств узагальнено і хто її, якщо ця інформація може бути озвучена, хто її здійснює?

_____. Дозвольте відповісти? Директор Департаменту кіберзахисту Адміністрації Держспецзв'язку. У нас, дійсно, в тому числі Законом 4336, який був прийнятий в березні минулого року, введена нова норма, що тренінги та інструктажі з кібергігієни тепер є обов'язковими що

для народних депутатів України, що для органів місцевого самоврядування, що для центральних органів виконавчої влади, військових формувань, органів державної влади, територіальних громад.

Тобто ця норма була введена. Окремо до нього постановою Кабінету Міністрів України було затверджено Порядок проведення інструктажів та тренінгів з кібергігієни, де вказано строки, коли, як саме, хто може проводити, який термін, яка періодичність і яке саме звітування. Окремо наказом Адміністрації Держспецзв'язку було затверджено Методичні рекомендації щодо проведення інструктажів та тренінгів з кібергігієни.

Наразі органи державної влади включаються в цю роботу. Дещо деякі своїми силами для своїх представників, для своїх держслужбовців проводять заходи з кібергігієни, деякі залучають основних суб'єктів нацсистеми кібербезпеки. Активну роль в цьому проводить Держспецзв'язку, ми постійно проводимо заходи з кібергігієни для великих міністерств, органів державної влади, місцевих органів виконавчої влади, Служби безпеки України, Національної поліції України і так Міністерства оборони та Генеральний штаб Збройних Сил України для своїх представників, для своїх військовослужбовців постійно проводять заходи з кібергігієни. Як тільки військовослужбовець вступає на свою посаду, або як тільки держслужбовець приходить на свою посаду, впродовж місяця повинен бути обов'язково проведений. Це питання також включене до переліку заходів державного контролю у сфері кіберзахисту.

Тобто в подальшому саме контролюючий орган Держспецзв'язку повинен буде по переліку питань перевірити, чи дійсно проводилися заходи з кібергігієни, оскільки дійсно ви праві: 80 відсотків реалізованих атак – це дійсно через людський фактор. Тому це питання важливе.

_____. Якщо дозволите, я б додав, що в Збройних Силах України вже чотири роки відповідно до розпорядження Головнокомандувача діє вимога, що щорічно військовослужбовці всі мають пройти курс кібергігієни, який спеціально розроблений, таргетований і саме на питання військової служби. Тобто там немає безпеки банківських карток, таке, а суто військові питання. Відповідно цей курс в цьому році благодаря Міністерству оборони мігрував з вебплатформи військового інституту в Армію+. Тобто зараз він доступний взагалі військовослужбовцям на мобільних телефонах будь-де. Відповідно за результатами проходження курсу формується сертифікат, і лише на підставі діючого сертифіката, який діє 1 рік відповідно до наступного проходження курсу, військовослужбовець командиром має право бути допущений до роботи з обчислювальною технікою. А для всіх

військовослужбовців там є окремий модуль, який стосується від солдата до генерала по безпеці особистих пристроїв і користування соцмережами, меседжерами і так далі.

ГОЛОВУЮЧИЙ. Якщо… Так, прошу.

_____. Можна додати ще від Нацполу? Що стосується гібергігієни, це, як колеги дуже слушно зазначили, це низка за хотів, які безпосередньо в організаціях відпрацьовується. І це не проєкт, це процес.

Зі свого боку ми дотримуємося цих усіх моментів, але що стосується безпосередньо безпеки наших громадян та обізнаності наших громадян, ми також ставимося до цього, як до процесу, але у нас є проєкт такий як спільно з волонтерами, «Кібер Брама». Так за допомогою донорів з Євросоюзу було по факту відбудовано систему, в якій... це вона розміщена на домені *(нерозбірливо).*gov.ua і там є низка матеріалів, які постійно оновлюються. І безпосередньо через цю платформу доноситься інформація, як не стати жертвою або фішингового... що таке безпосередньо базова гігієна, що таке фішинг, що таке кібератака, які мають бути по складності паролі, як використовується другий фактор і таке інше. І там є декілька категорій, безпосередньо інформація по направленості для різної категорії по населенню, починаючи від школярів і закінчуючи військовослужбовцями, держслужбовцями і людьми, які звичайними онлайн-сервісами користуються, як не стати жертвами і підвищити рівень безпосередньо обізнаності по кібергігієні.

Дякую.

_____. Можна питання тоді?

_____. Так, звичайно.

_____. Наскільки часто перевіряється просто фізично, скільки стікерів із логінами і паролями наклеєні на екрани комп’ютерів у службовців в кабінетах?

_____. Я можу відповісти за Національну поліцію, то у нас під час перевірок, у нас є перевірки, коли перевіряється, в принципі, що знаходиться у наших співробітників в кабінетах. Це є внутрішня структура всіх перевірок. І це я думаю, що стікер не є проблемою, обізнаність є

проблемою. І якщо технічна команда досить фахова, то вона має межі, декілька контурів безпеки, які навіть стікери будуть захищені.

Дякую.

ГОЛОВУЮЧИЙ. Я хотів би подякувати всім виступаючим за доповіді, також подякувати за вашу роботу. Ми маємо ухвалити відповідне рішення нашого комітету щодо наших слухань і інформацію, викладену у звітах суб'єктів національної кібербезпеки, визначених частиною другої статті 8 Закону України «Про основні засади забезпечення кібербезпеки України», взяти до відома.

Також хочу ще зазначити, що з метою недопущення можливих ризиків розголошення інформації, шкода від оприлюднення якої може переважати суспільний інтерес в її отриманні, відзначити про існування перешкод для її оприлюднення на офіційному вебсайті Верховної Ради України у період воєнного стану в Україні. Тому прошу проголосувати.

За? Проти? Утримався?

Дякую. Рішення прийнято.

Я хотів би подякувати. І можете йти, да, а ми зараз ще продовжимо.

Ладно, колеги, нам ще потрібно два коротеньких питання затвердити: це про затвердження розкладу, нам треба щось запланувати, це на 12 і 26 травня о 10-й годині. Якщо ніхто не проти, давайте проголосуємо.

Хто – за? Проти? Утримався?

І ще у нас одне питання, це проведення круглого столу на тему: «Про вдосконалення механізмів забезпечення доступності універсальних електронних комунікаційних послуг» на травень 26-го. Є пропозиція внести круглий стіл 28-го о 15-й під моїм головуванням. Якщо хто захоче, може приєднуватися. Тому прошу проголосувати.

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

Все. Всі питання розглянуті. Дякую.