МАЙБУТНІЙ ПОГЛЯД НА ОРГАНІЗАЦІЮ БЕЗПЕКИ: ФОРСАЙТ БЕЗПЕКИ І ЯК НИМ КОРИСТУВАТИСЯ

ЛИСЕНКО Сергій Олексійович - доктор юридичних наук, професор, ПрАТ «Вищий навчальний заклад «Міжрегіональна Академія управління персоналом», завідувач кафедри правознавства Сєвєродонецького інституту
ORCID ID: https://orcid.org/0000-0002-7050-5536
DOI 10.32782/LAW.2020.3.13

Статья посвящена новому взгляду на современный метод реконструкции модели безопасности организации, который основан на активном использовании форсайта безопасности. Рассмотрены генезис формирования форсайта безопасности и особенности его применения в современных условиях.

Форсайт безопасности рассматривается как инструмент прогнозирования и формирования будущей модели безопасности организации, позволяющий в короткие сроки получить достаточно точные прогнозы возможных рисков и недостатков в развитии организации в долгосрочной перспективе.

Было заявлено, что форсайт безопасности позволяет не только прогнозировать возможные угрозы и положительные последствия, но и выявлять различные сценарии будущего. Определено, что главным преимуществом форсайта, как инструмента безопасности, является способность осознать, что именно нужно делать сейчас, чтобы будущий мир соответствовал самым оптимистичным прогнозам.

Акцент делается на существовании в современной практике безопасности двух форматов форсайта безопасности, различающихся по масштабу. Формат меньшего масштаба, или «локальный форсайт», предполагает отдельную форсайт-сессию для прогнозирования явления. Более крупный формат, предполагающий большое количество специалистов, проводящих серию форсайт-сессий, требует надлежащего административно-правового регулирования, что определяет одно из важных направлений дальнейших исследований в этой области.

Автор анализирует особенности использования форсайта на примере карантинных мер, направленных на противодействие пандемии COVID-19 и прогнозирования угроз, исходящих как от самой эпидемии, так и от мер по борьбе с ней.

Особое внимание уделяется описанию новой профессии – «посредника по безопасности», как лица, работающего в службах безопасности или отдельной фирме, которое вместо основных лиц, находящихся в самоизоляции, будет присутствовать при подписании международных соглашений по вопросам безопасности, связанных, в том числе, с культурными особенностями участников.

Ключевые слова: форсайт; форсайт безопасности; прогнозирование угроз; будущее; экспертная деятельность; административно-правовое регулирование; COVID-19; посредник по безопасности.

Актуальність теми дослідження

Наше уявлення про майбутнє постійно змінюється залежно від прогресу, що обумовлює не лише розвиток технологій, але й еволюцію свідомості та світосприйняття сучасної людини. Стрімкі зміни інформаційно-комп'ютерних систем поєднуються з глобалізаційними процесами, що породжує справжній вир подій, які, на перший погляд, можуть видаватися непередбачуваними. Водночас, разом із цим реально змінюється рівень загроз у дію-

чих організаціях, що обумовлює потребу розробки та впровадження нових методів прогнозування, виявлення та протидії цим загрозам.

Наявний наразі перелік методик для аналізу та виявлення загроз безпеці є доволі різноманітним. Автором неодноразово висвітлювались адміністративно-правові особливості реконструкції як одного із таких заходів. Однак останнім часом методика реконструкції знайшла своє продовження та вдосконалення. Очевидно, що в провідних країнах цю думку розвинули дуже якісно та ґрунтовно, навіть надали цьому заходу оригінальну назву – форсайт безпеки.

Аналіз попередніх досліджень даної тематики

На пострадянському просторі форсайт, як явище та інструмент прогнозування, досліджували І. Баришев, Р. Кравець,- І. Кірнос, С. Кукушкіна, С. Серьогіна, Особливої ж уваги проблематика форсайту набула у працях таких західних дослідників, як A. Clayton, G. Muller, R. Phaal, N. Taleb. Водночас, проблематика форсайту безпеки лишається малодослідженою та потребує уваги науковців, які представляють різні галузі знань.

Метою дослідження є висвітлення нового погляду на сучасну методику реконструкції моделі безпеки організації, яка базується на активному застосуванні форсайту безпеки.

Основний зміст дослідження

Сьогодні для визначення гіпотетичних позитивних і негативних сценаріїв розвитку в організаціях спеціалісти дедалі частіше вдаються до так званого «форсайту безпеки». Форсайт (англ. Foresight – «передбачення») – це технологія і формат комунікації, що дозволяють учасникам домовитися з приводу образів майбутнього, а також, визначивши бажаний образ, узгодити дії в його контексті [1, 2]. Автор у своїх попередніх публікаціях розкривав особливості адміністративно-правових та стратегічних умов використання перспективної реконструкції для забезпечення безпеки організацій [3]. Але в даному випадку мова йде про більш досконалу версію авторської перспективної реконструкції, яку вже зараз активно використовують західні фахівці у галузі безпеки.

Історично, вперше термін «foresight» запропонував відомий письменник-фантаст Герберт Уеллс. Ще у 1930 р., виступаючи на BBC, він запропонував впровадити особливу спеціальність – «професор передбачення», який, подібно до історика, буде аналізувати і знаходити застосування майбутнім технологічним відкриттям [2]. Як і чимало інших передбачень, зроблених письменниками-фантастами початку XX століття, це стало значною мірою пророчим. Якщо говорити про Форсайт безпеки, як про глобальний дослідницький проект закордонних (переважно – західних) фахівців з безпеки, то ця методика сягає своїм корінням у 50-ті роки XX століття. Вперше її прототип було впроваджено в США корпорацією RAND, яка була стратегічним дослідницьким центром, що працював на замовлення уряду і збройних сил США. У подальшому технологія набула поширення у Південній Кореї, Японії та ряді країн НАТО. Спочатку це була важка і досить дорога технологія прогнозування у сфері безпеки, у рамках якої протягом місяців працювала величезна кількість експертів [4].

Наразі можна уявити чимало різних модифікацій форсайту безпеки. Так швидкий Форсайт безпеки (англ. *Rapid Foresight sequrity*) – це інструмент для прогнозування і формування майбутньої моделі безпеки організації, що дозволяє не лише за короткий період часу отримати доволі точні прогнози про можливі ризики та недоліки в розвитку організації, але й об'єднати людей, скоординувавши їх діяльність для реалізації отриманих уявлень про бажаний сценарій розвитку подій [4].

У попередніх дослідженнях, у процесі аналізу інформації в рамках перспективної реконструкції, автором виокремлювалося кілька способів (підходів) до організації мислення, такі як: екстраполяція; моделювання; форсайт; футурологія

тощо [5]. Проте із усіх перелічених саме «форсайт-сесії» із залученням експертів з безпеки часто виявляються незрівнянно більш ефективним інструментом, ніж, наприклад, просте екстраполювання на майбутнє вже наявних даних про минулі загрози та ризики. Отож, форсайт безпеки пов'язаний не стільки з прогнозуванням, скільки з проєктуванням певної моделі безпеки організації. В його основі лежить розуміння того, що майбутня безпека варіативна і безпосередньо залежить від впроваджених заходів. Тому головне завдання, яке варто вирішити суб'єктам безпеки, можна сформулювати як: встановлення певного алгоритму заходів, які спільними зусиллями слід зробити вже зараз для того, щоб прийти до бажаного результату в майбутньому. Автор упевнений у тому, що форсайт безпеки може допомогти підготувати суспільство для безпечного життя прийдешніх поколінь.

Окрім зазначеного, у форсайті безпеки важливу роль відіграє оцінка загроз, що характеризуються низькою ймовірністю виникнення, але при цьому мають великий потенціал негативного впливу на майбутнє досліджуваної організації. Загальносвітова пандемія COVID-19 – яскравий приклад подібної події. Такі загрози називають «чорними лебедями», за визначенням одного з найвідоміших філософів сучасності Нассіма Талеба [6]. «Чорні лебеді» – це точки біфуркації, які є настільки прихованими від поверхневого аналізу, що їх можливо виявити лише на обговореннях на кшталт форсайт-сесій з безпеки, при чому лише за умови залучення до цієї проблеми достатньої уяви.

Про те, що в сучасному світі людям дедалі частіше загрожуватимуть не світові війни, а саме епідемії, свого часу попереджали багато футурологів. Зрозуміло, що вони не говорили саме про 2020 рік і саме про групу «корона вірусів», а тим більш – про COVID-19. Але вони неодноразово підкреслювали, що ми вступаємо в такий світ, у якому інфекції можуть стати більш небезпечною загрозою, ніж раніше. Це видавалося парадоксальним, оскільки в XX столітті впровадженням санітарних заходів, щеплень і антибіотиків нібито вдалося подолати, або принаймні – взяти під контроль більшість небезпечних хвороб. Але водночас, саме на початку XXI століття ми, як ніколи раніше, живемо скупчено, багато подорожуємо. До того ж, наш світ є ще більш неоднорідним, ніж будь-коли, адже поруч з високорозвиненими існують слаборозвинені країни.

Важливо розуміти, що такі події, які можна віднести до категорії «чорних лебедів», дуже рідко відбуваються всупереч наявним глобальним загрозам або ж кардинально змінюють їх. Найчастіше – вони їх посилюють. Наприклад, якщо говорити про тотальний перехід різних сфер діяльності організації в онлайн площину, який набув поширення саме в процесі протиепідемічних ізоляційних заходів протягом 2020 року, то люди так чи інакше до цього йшли і до появи епідемії COVID-19. Поява та поширення нових телекомунікаційних технологій дедалі більше підвищували для організацій загрозу викрадення або пошкодження конфіденційної чи службової інформації, шляхом впливу з мережевого простору. Багато завдань з безпеки відходили на аутсорсинг, фріланс, і дедалі більше організацій віддавали перевагу оренді офісів на короткий час замість облаштування постійного місця для своєї діяльності, що теж негативно позначалося на рівні безпеки таких організацій. Усі перелічені загрози не виникли внаслідок пандемії COVID-19. Але саме завдяки пандемії ці загрози раптово посилилися.

Вже сьогодні зрозуміло, що коли карантин закінчиться, вийдуть з нього не всі. Адже багато людей по всьому світу продовжать працювати з домівок, тому що вони вже налагодили собі повноцінне робоче місце. І якщо бути чесними, то так і зручніше, і дешевше. Це може не подобатися деяким керівникам, для яких притаманний консервативний підхід до організації праці, і прагнення до візуального контролю. Але реальність диктує свої умови, і ті, хто не вміє їх розуміти, програють конкурентну боротьбу. За великим рахунком, саме карантин протидії COVID-19 став своєрідним заходом тотальної сегре-

гації видів діяльності на такі, які можливі в дистанційному режимі, і такі, які потребують фізичної присутності працівників/службовців. І в такому, несподівано новому суспільстві способи та методи роботи суб'єктів з безпеки зміняться докорінно.

Тут важливо розділяти кілька принципово важливих моментів. Говорячи про форсайт безпеки, часто мають на увазі трохи різні речі. Найчастіше під цими словами мають на увазі саме форсайт-сесії фахівців з безпеки. Зазвичай у таких заходах беруть участь експерти, модератор, який веде процес і секретар, який стежить за ходом дискусії і веде всі записи. Оптимальне число учасників – від 7 до 15 осіб, а час на обговорення зазвичай не перевищує кількох днів [7].

Натомість, форсайт безпеки, як глобальний дослідний проєкт, будується складнішими адміністративно-правовими засобами, завдяки яким стає можливо організувати такий складний процес.- У його рамках спочатку, як правило, проводяться попередні дослідження і моніторинги, на основі яких будуються гіпотези, і тільки після цього організовуються обговорення групами експертів з безпеки. Такі фахівці починають вибудовувати на основі попередніх висновків та фактів шлях до майбутньої моделі безпеки, прогнозувати, проєктувати дорожні карти і домовлятися. При цьому однієї форсайт-сесії з безпеки може виявитися недостатньо, і в такому разі планується ряд додаткових. Такі дослідження можуть тривати досить довго і включати в себе участь дуже великого числа фахівців, навіть – з кількох країн [8]. Зрозуміло, що без належного адміністративно-правового регулювання, буде доволі складно забезпечити такий масштабний та тривалий процес. Крім цього, важливу роль у форсайті безпеки відіграє підбір експертів, до яких висуваються певні адміністративно-правові вимоги. У першу чергу, фахівці самі повинні бути зацікавлені в дослідженні і готові до подальших конкретних дій, а головне, в межах конкретної організації повинен підтримуватись режим конфіденційності.

Таким чином, можна вести мову про два формати форсайту безпеки, які відрізняються масштабністю. Але в рамках будь-якого форсайту безпеки проводиться аналіз тенденцій виникнення загроз, технологій їх створення і методів їх запобігання, які можуть розвинутися в даний час у певній галузі. Наприклад – зростає кількість безробітних громадян, усе більше людей працюють з дому або з'являється все більше систем, заснованих на великих базах даних. Усе залежить від того, що конкретно аналізують фахівці. Коли починає вимальовуватися карта змін, група прогнозує, до чого саме може призвести у майбутньому розвиток визначених загроз. Тут завжди і вимальовується найцінніший продукт форсайту: одні й ті самі прогнозовані процеси комусь можуть принести користь, а комусь – саме очікувану загрозу.

Використовуючи попередній приклад, уявімо, що збільшення числа безробітних загрожує роботі торгових підприємств, які завжди розраховують на купівельну спроможність населення. Проте, в той же час, ця ситуація дає нові можливості роботодавцям, здешевлюючи робочу силу. Також це може спричинити за собою появу нових сфер діяльності або популяризації вже наявних, але раніше не настільки затребуваних, які стануть активно освоювати безробітні і власники застарілих професій. Звичайно, це буде також корисним всілякого роду навчальним закладам та бізнес-тренерам. І, таким чином, перебираючи можливі загрози і методики, аналітична група приходить до певного образу майбутнього, де виокремлено як загрози, так і потенціал.

Після цього робляться так звані «ставки» на те, що кожен з учасників готовий почати робити прямо зараз. Це може бути залучення інших фахівців, застосовування запланованих раніше методів боротьби або залучення силових органів влади. Тобто використання будь-яких ресурсів, щоб прийти до потрібного варіанту майбутнього. Наприклад, якщо ми хочемо, щоб у 2030 році всі країни перестали добувати нафту, потрібно вже зараз думати над впровадженням зелених джерел енергії,

тому що їх впровадження потребує значного часу. І якщо цього не почати робити прямо сьогодні, то за кілька років настане вже інший варіант майбутнього.

У кожній сфері людської діяльності, і навіть у кожній окремій організації існує свій спектр прогнозування і життєвий цикл. В індустрії моди, наприклад, він відносно короткий, і будувати перспективну реконструкцію (тобто – форсайт безпеки) далеко вперед просто не має сенсу, тому що все може швидко змінитися. Те ж саме стосується мобільних додатків або ігрової індустрії.

Протилежною виглядає ситуація в атомній енергетиці, де керівники галузі мають мислити поняттями на кшталт «п'ятдесят років і більше». І говорити там в межах річного і навіть десятирічного прогнозу безглуздо, тому що за цей час нічого важливого та нового не відбудеться, а те, що зміниться, швидше за все, вже було раніше сплановано чи спрогнозовано.

Необхідно розуміти, що створений форсайтом безпеки перспективний план не є статичною догмою, до нього потрібно постійно повертатися і робити його корекцію з урахуванням того, що вже сталося. При цьому, ретельно і в точності вгадувати всі загрози, завдання не стоїть [7, 8].

Наприклад, якщо говорити про освіту, то вже кілька років тому під час форсайту безпеки можна було спрогнозувати багато з тих загроз, з якими люди зіткнулися зараз. До таких можна віднести необхідність цифровізації та онлайнізації навчання, важливість якої усвідомили у зв'язку з карантином та ізоляцією населення через загрозу світової пандемії.

У межах адміністративно-правових засад, під час форсайту безпеки не може і не повинно ставитися завдання точно передбачити всі можливі загрози або точно їх описати. Такий абсолютистський підхід є тупиковим. Цілком зрозуміло, що більшість загроз так чи інакше дійсно може виникнути. Звичайно, адміністративно-правові засади повинні бути максимально гнучкими, тому що загрози можуть виникати трохи не в тому вигляді, в якому були б описані під час Форсайту безпеки. Проте вже точно буде відомо, що вони будуть собою представляти, а завдяки прийнятим засадам буде реально перебудувати стратегію захисту та модель безпеки організації для ефективної відсічі цим загрозам та ймовірним агресорам.

Іншим цікавим прикладом може служити поява спеціальності посередника, який може забезпечити безпеку при здійсненні угод немайнового та міжкультурного характеру. Його можна визначити адміністративно-правовими засадами як людину, що працює в штаті служб безпеки та буде, замість основних сторін, які знаходяться на самоізоляції, присутня при підписанні міжнародних договорів для консультування в питаннях безпеки, пов'язаних з культурними особливостями учасників. Відомо, що досі така спеціалізація всередині корпорацій відсутня, але вже з'явилися окремі компанії, які саме цим і займаються. Тобто така задача в основному пішла на аутсорс, або цим займаються фахівці з безпеки, яких, коли необхідно, залучають до окремих переговорів як доповнення до звичайної роботи.

Висновки і перспективи подальших досліджень

Автор поставив перед собою завдання донести до широкого загалу наукової спільноти новий погляд на сучасну методику реконструкції моделі безпеки організації, яка базується на активному застосуванні форсайту безпеки.

Ефективне застосування інструменту, який на заході називають форсайтом безпеки, дозволить уявити світ, яким він буде через десять років, спрогнозувати ризики та позитивний потенціал подій, ймовірність яких сьогодні може видаватися надзвичайно малою. Наглядність варіативності майбутнього, яку демонструє повноцінний форсайт, дає змогу виокремити як вкрай небажані, так і найбільш бажані варіанти розвитку подій. Але головною перевагою форсайту, як інструменту безпеки, є можливість усвідомити, що саме варто робити вже зараз, щоб майбутній світ відповідав найбільш оптимістичному прогнозу.

Особливості форсайту, як інструменту безпеки, проаналізовано на прикладі карантинних заходів, спрямованих на протидію пандемії COVID-19. Уже сьогодні можна спостерігати появу нової професії – безпекового посередника – як особи, що працює в штаті служб безпеки або окремої фірми та буде, замість основних сторін, які знаходяться на самоізоляції, присутня при підписанні міжнародних договорів для консультування в питаннях безпеки, пов'язаних з культурними особливостями учасників

Наголошено на існуванні в сучасній безпековій практиці двох форматів форсайту безпеки, які відрізняються масштабністю. При цьому більш масштабний формат, який передбачає залучення великої кількості фахівців, проведення циклу форсайт-сесій, потребує належного адміністративно-правового регулювання, що обумовлює один з вагомих напрямів подальших досліджень у цій сфері.

Література

1. Road map Report Concerning the Use of Nanomaterials in the Automotive Sector (2006) // *Nanomaterial Roadmap* 2015. URL: http://www.aimme.es/archivosbd/observatorio_oportunidades/nano-roadmap_automotive-industry.pdf

2. Серегина С. Ф., Барышев И. А. Закономерно ли появление форсайта? // Форсайт. 2008. № 2(6). Т. 2 № 2. С. 4–12.

3. Лисенко С. Особливий погляд на інформаційну безпеку. «*Видавництво Людмила*», Київ. 2020. 405с.

4. Phaal R., Muller G. (2009) An Architectural Framework for Road mapping: Toward Visual Strategy // *Technological Force casting and Social Change*. № 76. P. 39-49.

5. Лисенко С. Адміністративно-правові засади інформаційної безпеки підприємництва. «*Видавництво Людмила*», Київ. 2019. 385с.

6. Н. Талеб. Чорний лебідь: Про (не) ймовірне в реальному житті. Київ : *Наш Формат*, 2017. 392 с.

7. Clayton A. (2009) Postroenie dorozhnykh kart dlya razvivayushchikhsya stran [Roadmapping in Developing Countries]. *Foresight-Russia*, vol. 3, no 1, pp. 48-57 (in Russian).

8. Clayton, A. Technology Roadmapping for Developing Countries. Vienna, *UNIDO Publ.*, 2005.

FUTURE VIEW ON SECURITY ORGANIZATION: SECURITY FORESIGHT AND HOW TO USE IT

The article is devoted to a new look at the modern method of reconstruction of the security model of the organization, which is based on the active use of security foresight. The genesis of security foresight formation and peculiarities of its application in modern conditions are considered.

Security foresight is seen as a tool for forecasting and shaping the future security model of the organization, which allows in a short period of time to obtain fairly accurate forecasts of possible risks and shortcomings in the development of the organization in the long run.

It was stated that security foresight allows not only to predict probable threats and positive consequences, but also to identify different future scenarios. It is determined that the main advantage of foresight as a security tool is the ability to realize what exactly should be done now to make the future world meet the most optimistic forecast.

Emphasis is placed on the existence in modern security practice of two formats of security foresight, which differ in scale. A smaller scale format, or "local foresight", involves a separate foresight session to predict a phenomenon. A larger format, which involves a large number of specialists, conducting a series of foresight sessions, requires proper administrative and legal regulation, which determines one of the important areas of further research in this area.

The author analyzes the peculiarities of the use of foresight on the example of quarantine measures aimed at counteracting the COVID-19 pandemic and predicting the threats posed by both the epidemic itself and measures to combat it.

Particular attention is paid to the description of a new profession - "security mediator", as a person working in the security services, or a separate firm and will, instead of the main parties in self-isolation, be present

АНОТАЦІЯ

Статтю присвячено новому погляду на сучасну методику реконструкції моделі безпеки організації, яка базується на активному застосуванні форсайту безпеки. Розглянуто генезу становлення форсайту безпеки та особливості його застосування в сучасних умовах.

Форсайт безпеки розглядається як інструмент для прогнозування і формування майбутньої моделі безпеки організації, що дозволяє за короткий період часу отримати доволі точні прогнози про можливі ризики та недоліки в розвитку організації у довготривалій перспективі.

Констатовано, що форсайт безпеки дозволяє не просто спрогнозувати ймовірні загрози та позитивні наслідки, але й визначити різні сценарії майбутнього. Визначено, що головною перевагою форсайту, як інструменту безпеки, є можливість усвідомити, що саме варто робити вже зараз, щоб майбутній світ відповідав найбільш оптимістичному прогнозу.

Наголошено на існуванні в сучасній безпековій практиці двох форматів форсайту безпеки, які відрізняються масштабністю. Менш масштабний формат, або «локальний форсайт», передбачає проведення окремої форсайт-сесії для прогнозування того чи іншого явища. Більш масштабний формат, який передбачає залучення великої кількості фахівців, проведення циклу форсайт-сесій, потребує належного адміністративно-правового регулювання, що обумовлює один з вагомих напрямів подальших досліджень у цій сфері.

Автор аналізує особливості застосування форсайту на прикладі карантинних заходів, спрямованих на протидію пандемії COVID-19 та прогнозування тих загроз, які несе за собою як сама епідемія, так і заходи протидії їй.

Окрему увагу присвячено опису нової професії – «безпекового посередника», як особи, яка працює в штаті служб безпеки, або окремої організації та буде, замість основних сторін, які знаходяться на самоізоляції, присутня при підписанні міжнародних договорів для консультування з питань безпеки, пов'язаних, серед іншого, з культурними особливостями учасників.

Ключові слова: форсайт; форсайт безпеки; прогнозування загроз; майбутнє; експертна діяльність; адміністративно-правове регулювання; COVID-19; безпековий посередник.

at the signing of international agreements for security advice. related to the cultural characteristics of the participants.

Keywords: *foresight; safety foresight; threat forecasting; future; expert activity; administrative and legal regulation; COVID-19; security broker.*