

Інформаційно-довідкове видання

**РАМКОВА ПРОГРАМА ЄВРОПЕЙСЬКОГО СОЮЗУ
З ДОСЛІДЖЕНЬ ТА ІННОВАЦІЙ «ГОРИЗОНТ 2020»**

**Конкурси за тематичним напрямом
«Безпечні суспільства: захист свободи
та безпеки Європи та її громадян»**



Національний університет
«Києво-Могилянська академія»



Національний контактний пункт
програми ЄС з досліджень
та інновацій «Горизонт 2020»

**РАМКОВА ПРОГРАМА ЄВРОПЕЙСЬКОГО СОЮЗУ
З ДОСЛІДЖЕНЬ ТА ІННОВАЦІЙ «ГОРИЗОНТ 2020»**

*Конкурси за тематичним напрямом
«Безпечні суспільства: захист свободи
та безпеки Європи та її громадян»
на 2018 – 2020 рр.*

ІНФОРМАЦІЙНИЙ БЮЛЕТЕНЬ



Київ
2017

РАМКОВА ПРОГРАМА ЄВРОПЕЙСЬКОГО СОЮЗУ З ДОСЛІДЖЕНЬ ТА ІННОВАЦІЙ «ГОРИЗОНТ 2020»

*Актуальні конкурси за тематичним напрямом
«Безпечні суспільства: захист свободи
та безпеки Європи та її громадян»
на 2018 – 2020 рр.*

Horizon 2020

Pillar: Societal Challenges

Work Programme Year: H2020-2018-2020

Work Programme Part: <http://ec.europa.eu/programmes/horizon2020/en/h2020-section/secure-societies---protecting-freedom-and-security-europe-and-its-citizens>

Характеристика тематичного напрямку

Основними завданнями тематичного напрямку «Безпечні суспільства» є:

- підвищення стійкості суспільства до природних і техногенних катастроф, починаючи від розробки нових інструментів управління в умовах кризи – до комунікаційної сумісності, а також розробка нових рішень для захисту критичної інфраструктури;
- боротьба зі злочинністю та тероризмом, починаючи від нових судово-медичних інструментів – до захисту від вибухових пристроїв;
- підвищення безпеки кордонів, починаючи від поліпшення охорони морського кордону – до зовнішньої безпеки Євросоюзу, в тому числі запобігання конфліктам і підтримка мирних ініціатив;
- забезпечення підвищеної кібербезпеки, починаючи від безпечного обміну інформацією – до нових моделей захисту.

Захист суспільства від стихійних лих є одним з центральних елементів його функціонування.

Боротьба зі злочинністю і тероризмом потребують нових технологій і можливостей для боротьби і запобігання злочинності (в тому числі кіберзлочинності), контрабанді і тероризму (в тому числі кібертероризму), включаючи розуміння і виявлення терористичних ідей і вірувань з метою уникнення повітряних загроз.

Захист європейських кордонів вимагає розробки систем, обладнання, інструментів, процесів і методів для швидкої ідентифікації.

Конкурси за цим тематичним напрямком мають об'єднати всі сторони, зацікавлені в дотриманні безпеки: промисловість – в тому числі малі і середні підприємства, науково-дослідні організації, університети, а також державні органи, неурядові організації та державні і приватні організації зі сфери безпеки. Активна участь кінцевих споживачів також має велике значення.

Захист інфраструктури Європи і людей в європейських розумних містах

Загрози для місць великого скупчення людей та перебої в роботі інфраструктури наших країн можуть обмежити свободи наших громадян та загрожувати функціонуванню наших суспільств та їхньої економіки. Необхідно забезпечити безпеку та стійкість критично важливої інфраструктури Європи, оскільки перебої у її роботі можуть спричинити крах великих секторів нашої діяльності. Загрози для «м'яких» цілей, таких як місця скупчення людей, натовпи, можуть мати менш довгостроковий фізичний вплив, але спричиняють серйозну шкоду через потенційно велику кількість жертв та наступні психологічні та соціологічні наслідки.

Мета цього конкурсу – захистити та покращити стійкість критичної інфраструктури Європи та «м'яких» цілей.

ТЕМА: SU-INFRA01-2018-2019-2020:
**Попередження, виявлення, реагування та пом'якшення
комбінованих фізичних та кібер-загроз
для критичної інфраструктури в Європі**

Ідентифікатор теми:	SU-INFRA01-2018-2019-2020	
Типи діяльності:	IA Інноваційна діяльність	
Модель подачі:	одноетапна	
Дата відкриття:	15 березня 2018 р.	14 березня 2019 р.
Реченець:	23 серпня 2018 р.	22 серпня 2019 р.

**Специфічна проблема,
на вирішення якої спрямований конкурс**

Порушення у функціонуванні важливих елементів інфраструктури наших країн можуть стати результатом багатьох видів небезпек, зокрема фізичних та / або кібер-атак на ключові компоненти та пов'язані з ними системи. Події останніх років свідчать про збільшення кількості об'єднаних фізичних та кібер-атак. Для забезпечення наявних або майбутніх, державних або приватних програм, необхідний комплексний, однак водночас, й індивідуальний підхід. Бюджетні обмеження як у державному, так і в приватному секторах означають, що нові рішення безпеки повинні бути більш точними, ефективними, економічно релевантними та, можливо, більш автоматизованими, ніж ті, які доступні нині.

Очікувані результати: Пропозиції повинні включати: прогнози, оцінку фізичних та кібер-ризиків, запобігання, виявлення, реагування, а також, у разі невдачі, пом'якшення наслідків (включаючи нові проекти інсталяції) та швидке відновлення після інцидентів протягом усього терміну експлуатації інфраструктури; досягнення безпеки та стійкості всіх функцій. У 2018 та 2019 роках проекти повинні зосередити увагу на тих програмах, що належать до найголовніших компонентів інфраструктури: водні системи, енергетична інфраструктура (електростанції та розподільчі мережі, нафтові установки, офшорні платформи), транспортна інфраструктура (аеропорти, порти, залізниці, міські мультимодальні вузли), інфраструктури комунікації та наземних сегментів космічних систем, медичних послуг, електронної комерції та поштової інфраструктури, важливих промислових майданчиків, заводів та фінансових послуг.

Детальніше про конкурс:

<http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/su-infra01-2018-2019-2020.html>

ТЕМА: SU-INFRA02-2019:
**Безпека для розумних міст,
включно з громадськими місцями**

Ідентифікатор теми:	SU-INFRA02-2019
Типи діяльності:	IA Інноваційна діяльність
Модель подачі:	одноетапна
Дата відкриття:	14 березня 2019 р.
Реченець:	22 серпня 2019 р.

**Специфічна проблема,
на вирішення якої спрямований конкурс**

У містах такі громадські місця як: торговельні центри, відкриті зони для подій з великою кількістю учасників, а також небезпечні райони транспортної інфраструктури, є «м'якими цілями», тобто потенційними цілями для нападів та терористичних актів. Генерування, обробка та обмін великими обсягами даних в розумних містах робить міські системи та служби потенційно більш чутливими та здатними до реагування в реальному часі. З одного боку, розумні міста забезпечують покращення безпеки відкритих і багатолюдних територій від загроз (включаючи терористичні загрози) та ризиків, використовуючи широкі мережі можливостей виявлення та попередження, які можуть бути об'єднані з пошуком адекватних відповідей на кризу для посилення першої реакції. З іншого боку, інтелектуальні технологічні та комунікаційні середовища (міська, транспортна інфраструктура, компанії, промисловість) в розумному місті вимагають спільного підходу до управління кібербезпекою.

Очікувані результати: Захист та належна робота розумного та безпечного міста спираються на взаємопов'язані, складні та взаємозалежні мережі та системи: мережі громадського транспорту, енергетики, зв'язку, транзакційної інфраструктури, цивільної безпеки та повноцінної роботи правоохоронних органів, підтримка дорожнього руху, мережі та послуг громадського інтересу. Пропозиції повинні експериментально розробляти та інтегрувати компоненти відкритої платформи для обміну та управління інформацією між операторами державної служби та суб'єктами безпеки великого, розумного міста, зокрема: методи виявлення зброї, вибухових речовин, токсичних речовин, системи відео спостереження, методи, що дозволяють ідентифікувати та нейтралізувати злочинців, мінімізуючи вторгнення в місця великого скупчення людей.

Детальніше про конкурс:

<http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/su-infra02-2019.html>

Цифрова безпека

Трансформації, що відбуваються завдяки сучасним інформаційно-комп'ютерним технологіям, привносять нові можливості в багатьох важливих секторах, але разом з тим, вони вразливі щодо критичної інфраструктури та цифрових послуг, які можуть мати вагомні наслідки для функціонування суспільства, економічного зростання і технологічного інноваційного потенціалу Європи. Ці проблеми вирішуються за допомогою новаторських підходів, які перетинають кордони окремих тематичним напрямів програми Горизонт 2020.

Цей конкурс має справу з дослідженнями та інноваціями у сфері підвищення цифрової безпеки. У пропозиціях слід враховувати відповідний людський чинник та соціальні аспекти при розробці інноваційних рішень. У відповідних випадках пропозиції також повинні описувати, як враховувати гендерний аспект у їх змісті.

ТЕМА: SU-DS01-2018:
**Кібербезпекова готовність –
кібер-діапазон, моделювання і економіка**

Ідентифікатор теми:	SU-DS01-2018
Типи діяльності:	IA Інноваційна діяльність
Модель подачі:	одноетапна
Дата відкриття:	15 березня 2018 р.
Реченець:	23 серпня 2018 р.

**Специфічна проблема,
на вирішення якої спрямований конкурс**

Цифрова інфраструктура, від якої залежать як бізнес так і суспільство, має бути стійкою та надійною, і повинна залишатися безпечною, незважаючи на зростаючу кількість кібер-загроз. Нові технології та їх нові комбінації вимагають інноваційних способів впровадження заходів безпеки, а також створення нових пов'язаних із безпекою, механізмів, прогнозування нових загроз, управління кібер-ризиками. Багато організацій не в змозі прогнозувати та / або оцінити вплив кібер-ризиків. Цей результат часто виникає внаслідок недостатніх та / або невідповідних інвестицій для забезпечення більш захищеного середовища в Інтернеті. Крім того, фахівці з кібербезпеки повинні щоразу адаптувати свої знання відповідно до віртуального ландшафту, який постійно розвивається і потенційно містить в собі все більш складні кібер-атаки, та послуг у сфері комунікаційних технологій, набору змінених законодавчих актів. В ЄС існує нагальна потреба у висококваліфікованих професіоналах у галузі кібербезпеки, що повинні перебувати в постійному навчальному процесі, аби вміти гідно відповідати швидким темпам еволюції кібер-загроз.

Очікувані результати: У пропозиціях необхідно розглянути, протестувати та перевірити динамічні симулятори, що служать платформами для знань, що супроводжуються механізмами взаємодії в режимі реального часу та обміну інформацією, циклів зворотного зв'язку. Ці імітаційні платформи допоможуть професіоналам, відповідальним за кібербезпеку в організаціях, спільно вдосконалити їх здатність обробляти та прогнозувати інциденти в сфері безпеки, складні атаки на основі цілеспрямованих сценаріїв та дій. Пропозиції повинні запропонувати спільні підходи задля перетворення користувацьких потреб у фактичні експерименти та комп'ютерні вправи, а також розробляти / інтегрувати відповідні інструменти та методи підтримки поточних і майбутніх сценаріїв моделювання. Пропозиції також повинні містити (але не обмежуватись) віднайденням рішень, що здатні швидко адаптуватися до еволюції кібер-хакерів або навіть перевершувати їх.

Детальніше про конкурс:

<http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/su-ds01-2018.html>

ТЕМА: SU-DS03-2019-2020:
**Цифрова безпека і конфіденційність для громадян,
малих, середніх та мікро- підприємств**

Ідентифікатор теми:	SU-DS03-2019-2020
Типи діяльності:	IA Інноваційна діяльність
Модель подачі:	одноетапна
Дата відкриття:	14 березня 2019 р.
Реченець:	22 серпня 2019 р.

**Специфічна проблема,
на вирішення якої спрямований конкурс**

Деякі члени цифрового суспільства в ЄС є більш вразливими, оскільки вони менш готові протистояти кібератакам. Масштаби, значення та вразливість персональних даних у кіберпросторі суттєво зростають, і громадяни, як правило, не знають, хто контролює, отримує доступ та модифікує їхні особисті дані. Порушення особистих даних може призвести до таких небезпек як: кібер-загрози, примус, шантаж, корупція тощо. З метою захисту свободи, безпеки та конфіденційності, а також з метою забезпечення захисту персональних даних мешканців ЄС громадянам слід надавати можливість оцінювати ризики, пов'язані з їх цифровими діями, та налаштувати власні параметри безпеки та збереження конфіденційності та захисту персональних даних. Громадяни повинні повністю усвідомлювати, що їх згода необхідна у багатьох ситуаціях і потребує надання доступу до їх особистих даних / пристроїв / терміналів з підвищеним рівнем деталізації. Крім того, існує потреба у підвищенні спроможності громадян покращувати рівень та точність інструментів моніторингу, які використовуються службами (наприклад, через файли cookie, позиціонування, tokens).

Очікувані результати: Більшість підприємств малого та середнього бізнесу не мають достатньої обізнаності та можуть виділяти обмежені ресурси - як технічні, так і людські - для боротьби з кібер-ризиками, отже вони є першочерговими цілями у порівнянні з великими організаціями. Спеціалісти з безпеки та експерти, що працюють у сфері МСП та МП, повинні мати доступ до постійного навчального процесу, оскільки кібербезпека є сферою знань, що швидко розвивається. Беручи до уваги значну економічну роль МСП та МС в ЄС, спеціальні дослідження для інновацій повинні підтримувати кібербезпеку.

Детальніше про конкурс:

<http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/su-ds03-2019-2020.html>

ТЕМА: SU-DS04-2018-2020:
**Кібербезпека в електроенергетичній
та енергетичній системах: броня проти кібератак
та загроз конфіденційності і витік даних**

Ідентифікатор теми:	SU-DS04-2018-2020
Типи діяльності:	IA Інноваційна діяльність
Модель подачі:	одноетапна
Дата відкриття:	15 березня 2018 р.
Реченець:	23 серпня 2018 р.

**Специфічна проблема,
на вирішення якої спрямований конкурс**

Електрична енергетика та енергосистема (EPES) має ключове значення для економіки, оскільки всі інші сфери залежать від наявності електроенергії, отже, відключення електроенергії може безпосередньо впливати на доступність інших послуг (наприклад, транспорт, фінанси, зв'язок, водопостачання), де резервна потужність недоступна або час відновлення енергії виходить за межі резервної автономії. З переходом до децентралізованої енергетичної системи цифрові технології відіграють все більш важливу роль в EPES: вони сприяють зниженню споживання енергії та розбудові енергоефективної системи. У той же час, з посиленням використання цифрових пристроїв та більш розвинутих комунікацій та взаємопов'язаних систем, EPES все більше піддається зовнішнім загрозам, таким як віруси, хакери та порушення конфіденційності даних.

Для того, аби продовжувати інтегрувати відновлювані джерела енергії в рамках наявної EPES та забезпечити, щоб воно мало користь від переваг сучасної цифрової електромережі, існує потреба в нових підходах до безпеки, що дозволяють виявляти та запобігти новим загрозам. Без адекватної стратегії та заходів для захисту енергетичної системи від кібератак постачання енергії буде більш ризикованим, дорожчим і, можливо, більш небезпечним.

Очікувані результати: Пропозиції повинні продемонструвати, яким чином реальні EPES можуть бути стійкішими до зростаючих і більш складних кібер-нападів, конфіденційності та порушень даних (включаючи порушення персональних даних), беручи до уваги розвиток мережі у бік децентралізованої архітектури та залучення всіх зацікавлених сторін. Ці пропозиції повинні продемонструвати стійкість EPES шляхом розробки та впровадження адекватних заходів. Необхідно передбачити різні сценарії атак із очікуваним потенційним руйнівним впливом на EPES.

Детальніше про конкурс:

<http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/su-ds04-2018-2020.html>

ТЕМА: SU-DS05-2018-2019:
**Цифрова безпека, конфіденційність, захист даних
і звітність в критичних секторах**

Ідентифікатор теми:	SU-DS05-2018-2019	
Типи діяльності:	IA Інноваційна діяльність	
Модель подачі:	одноетапна	
Дата відкриття:	15 березня 2018 р.	14 березня 2019 р.
Реченець:	23 серпня 2018 р.	22 серпня 2019 р.

**Специфічна проблема,
на вирішення якої спрямований конкурс**

У критичних вертикальних секторах технології кібербезпеки повинні бути узгоджені з конкретними потребами домену, поєднавши попит та пропозицію для таких кібер-технологій. У контексті посилення оцифрування та зростаючої складності кібер-атак існують окремі сектори / підсектори, визнані критичними з точки зору потреб в кібербезпеці, а саме: енергія (електрика, нафта, газ), транспорт (повітряний транспорт, залізничний транспорт, водний транспорт, автомобільний транспорт), банківська справа, інфраструктура фінансового ринку, сектор охорони здоров'я (медичні установи, включаючи державні лікарні та приватні клініки), постачання та розподілення питної води та цифрова інфраструктура. Повинні бути чітко визначені принципи та стандарти, щоб захистити критичну інфраструктуру в цих секторах та забезпечити цілісність та конфіденційність персональних даних.

Очікувані результати: Серед вищезгаданих критичних секторів, пропозиції повинні розглядати загальні аспекти принаймні двох з них, шляхом виявлення загальних загроз та нападів та розробки доказів концепцій управління ризиками кібербезпеки та конфіденційності. Крім того, пропозиції повинні розглядати конкретні аспекти для одного з трьох критичних секторів, згаданих як підтеми, тобто транспорт, охорона здоров'я та фінанси, шляхом виявлення конкретних вразливостей, ефектів поширення та контрзаходів шляхом розробки та тестування кібербезпекових рішень. Під час розробки концепції слід враховувати особливості критичних секторів, таких як складність інфраструктури та великий обсяг. Пропозиції також повинні містити (але не обмежуватись) розробкою конкретних соціальних аспектів цифрової безпеки, пов'язаної з практичним навчанням, включаючи: підвищення динаміки методів навчання та обізнаності, щоб відповідати / перевищувати ті ж темпи еволюції кібер-атакуючих; нові методи поінформованості, які пропонують більш ефективну інтеграцію працівників з питань ІКТ та роботодавців на європейський ринок електронних навичок.

Детальніше про конкурс:

<http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/su-ds05-2018-2019.html>

Безпека

Цей конкурс присвячений дослідженням та інноваціям у створенні суспільств, стійких до катастроф (лих), боротьби з злочинністю та тероризмом, а також вдосконалення прикордонної та зовнішньої безпеки.

Суспільства, стійкі до лих. Мета цього розділу полягає в тому, щоб просувати інновації в суспільстві в цілому, щоб зменшити втрати людських життів та зменшити екологічні, економічні та матеріальні збитки від природних та техногенних катастроф, у тому числі від кліматичних погодних явищ, землетрусів та вулканічних подій, космічних подій, промислових катастроф, злочинності та терористичних загроз.

Амбітні заходи в рамках "Боротьби з злочинністю та тероризмом" - це пом'якшення можливих наслідків злочинів та / або пов'язаних з тероризмом інцидентів або їх уникнення. Для цього потрібні нові технології та можливості. Вони повинні вирішувати питання боротьби та попередження злочинів (включаючи кіберзлочинність), незаконного обігу та тероризму (включаючи кібер-тероризм та напади CBRN), а також розуміння та подолання терористичних ідей та переконань. Людські чинники та соціальний контекст повинні враховуватися при дотриманні основних прав, включаючи приватність, захист персональних даних та вільне пересування людей.

Безпека кордонів. Метою цього розділу є розробка технологій та можливостей, необхідних для посилення систем та їх сумісності, обладнання, інструментів, процесів та методів швидкої ідентифікації, щоб покращити безпеку кордонів, поважаючи основні права, включаючи свободу пересування людей, захист персональних даних та конфіденційність. Необхідні нові технології, можливості та рішення також необхідні для підтримки політики зовнішньої безпеки Союзу в цивільних завданнях, починаючи від цивільного захисту до гуманітарної допомоги, управління кордонами, правоохоронних органів або миротворчих операцій та посткризової стабілізації, включаючи запобігання конфліктам, будівництво та посередництво. Це також вимагатиме проведення досліджень з вирішення конфліктів та відновлення миру та правосуддя, раннього виявлення факторів, що ведуть до конфліктів, та наслідки процесів відновного правосуддя.

ТЕМА: SU-BES01-2018-2019-2020:
**Людські фактори, соціальні та організаційні аспекти
безпеки кордонів та зовнішньої безпеки**

Ідентифікатор теми:	SU-BES01-2018-2019-2020	
Типи діяльності:	RIA Дослідницька та інноваційна діяльність	
Модель подачі:	одноетапна	
Дата відкриття:	15 березня 2018 р.	14 березня 2019 р.
Реченець:	23 серпня 2018 р.	22 серпня 2019 р.

**Специфічна проблема,
на вирішення якої спрямований конкурс**

Прикордонна та зовнішня безпека можуть залежати від різних людських чинників, а також соціальних аспектів, включно з гендерним. Необхідне прийняття відповідних організаційних рішень та глибшого розуміння того, як нові технології та соціальні мережі мають вплив на прикордонний контроль. Одне з головних завдань - керувати потоком подорожуючих людей та товарів на зовнішніх кордонах, одночасно вирішуючи проблему нелегальної міграції та посилення нашої внутрішньої безпеки.

Очікувані результати: Пропозиції (які повинні враховувати вже наявні інструменти) мають запропонувати інноваційні рішення за наступними підтемами: [2018] Виявлення загроз для безпеки, спричиненого певними сприйняттями за кордоном, які відрізняються від реальності ЄС; [2019] Моделювання, прогнозування та керування міграційними потоками задля уникнення напруженості та насильства. [2020] Розробка індикаторів загроз на зовнішніх кордонах ЄС на основі методологій оцінки ризику та вразливості.

Детальніше про конкурс:

<http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/su-bes01-2018-2019-2020.html>

ТЕМА: SU-BES02-2018-2019-2020:
**Технології покращення безпеки кордонів
та зовнішньої безпеки**

Ідентифікатор теми:	SU-BES02-2018-2019-2020	
Типи діяльності:	RIA Дослідницька та інноваційна діяльність	
Модель подачі:	одноетапна	
Дата відкриття:	15 березня 2018 р.	14 березня 2019 р.
Реченець:	23 серпня 2018 р.	22 серпня 2019 р.

**Специфічна проблема,
на вирішення якої спрямований конкурс**

Інновації для прикордонної та зовнішньої безпеки можуть бути спрямовані, зокрема, на нові технології, за умови, що вони доступні для громадян, а також адаптовані та впроваджені для потреб працівників із забезпечення безпеки.

Очікувані результати: Пропозиції повинні бути сформовані у руслі наступних підтем:

Підтема 1: [2018] Забезпечення комплексної ситуативної обізнаності та застосування віртуальної реальності до безпеки кордонів. Сьогодні інформація доступна для прикордонних та прибережних охоронців у кількох форматах та на різноманітних дисплеях, які практично не сумісні. Крім того, прикордонні та прибережна охорона часто працюють в малонаселених і віддалених районах, де наявність телекомунікаційних мереж може бути проблемою. Дослідження мають створити хмарні інтегровані системи з простими, але високо стандартизованими інтерфейсами, які показують інформацію в режимі реального часу зручним способом, що може допомогти прикордонникам у прийнятті рішень.

Підтема 2: [2018] Виявлення шахрайства, перевірка справжності документів та альтернативні технології для ідентифікації людей. Нові заходи необхідні для подолання потенційних шахрайств, зокрема для виявлення синтезованих зображень. Використання біометричних методів, що без зусиль зможуть ідентифікувати особу без зупинки потоку людей є сферою для подальшого розвитку, тестування та перевірки.

Підтема 3: [2019] Безпека бортових пасажирських суден. Для забезпечення безпеки протягом «життєвого циклу» плавання можуть бути впроваджені нові технології (з їх інтеграцією в суднобудівні системи).

Підтема 4: [2019] Виявлення загроз у потоці комерції без порушення бізнесу. Особливе значення мають: покращення можливостей виявлення контрабанди (головним чином цигарок), прихованих у вантажах високої щільності (вугілля, залізна руда), зокрема, для перевезення вантажів залізничним транспортом, а також боротьби з незаконним обігом радіоактивних матеріалів.

Підтема 5: [2020] Розумні технології сенсорів для відеоспостереження на кордонах.

Детальніше про конкурс:

<http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/su-bes02-2018-2019-2020.html>

ТЕМА: SU-BES03-2018-2019-2020:
**Демонстрація прикладних рішень для покращення
прикордонної та зовнішньої безпеки**

Ідентифікатор теми:	SU-BES03-2018-2019-2020	
Типи діяльності:	IA Інноваційна діяльність	
Модель подачі:	одноетапна	
Дата відкриття:	15 березня 2018 р.	14 березня 2019 р.
Реченець:	23 серпня 2018 р.	22 серпня 2019 р.

**Специфічна проблема,
на вирішення якої спрямований конкурс**

Рішення з високим ступенем технологічної готовності (TRL) необхідні, щоб покращити прикордонну і зовнішню безпеку, що повинні бути продемонстровані в контексті фактичних операцій або навчань для перевірки практичними працівниками.

Очікувані результати: Пропозиції повинні бути сформовані у руслі наступних підтем:

Підтема 1: [2018] Дистанційно пілотовані літальні апарати та підводні автономні платформи, які будуть використовуватися з бортових офшорних патрульних суден. Дистанційно пілотовані автономні платформи всіх видів повинні демонструвати інноваційні можливості для сухопутного та прибережного спостереження. Підвищення ефективності витрат, надійності та наявності таких платформ шляхом збільшення ефективності наявних технологій або розробки інноваційних концепцій експлуатації суттєво сприятиме покращенню ситуативної обізнаності на тактичному рівні за межами прибережних вод (до 200 морських миль), одночасно зменшуючи ризики під час пошуково-рятувальних місій.

Підтема 2: [2019] Нові концепції для підтримки прийняття рішень та інформаційних систем. Інформаційні системи для підтримки прикордонної та зовнішньої безпеки можуть поєднувати широкий спектр даних з дуже різних джерел, включаючи персональні дані. Необхідні інноваційні рішення для забезпечення взаємозв'язку систем спостереження та наявності інформації для моніторингу морського кордону, яка надходить з району операцій в стандартизованих форматах. Це дозволить швидше реагувати на інциденти в морській сфері та зменшити кількість жертв на морі.

Підтема 3: [2020] Поліпшені системи для виявлення, ідентифікації та відстеження малих човнів.

Детальніше про конкурс:

<http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/su-bes03-2018-2019-2020.html>

ТЕМА: SU-DRS01-2018-2019-2020:
**Людські фактори, соціальні та організаційні аспекти
суспільств, стійких до загроз**

Ідентифікатор теми:	SU-DRS01-2018-2019-2020	
Типи діяльності:	RIA Дослідницька та інноваційна діяльність	
Модель подачі:	одноетапна	
Дата відкриття:	15 березня 2018 р.	14 березня 2019 р.
Реченець:	23 серпня 2018 р.	22 серпня 2019 р.

**Специфічна проблема,
на вирішення якої спрямований конкурс**

Вплив суспільства залежить від того, як громадяни поведуться індивідуально чи колективно, і як уряди та організації громадянського суспільства розробляють та впроваджують політику щодо пом'якшення ризиків, підготовки, реагування на них, подолання наслідків стихійних лих та навчання. Поширення нових технологій та засобів масової інформації викликає суттєві зміни в поведінці людей та громад.

Очікувані результати: Пропозиції мають вирішити наступні проблеми:

Недавні стихійні лиха, пов'язані або з природними причинами (включаючи небезпеку, пов'язану з кліматом), або з терористичними нападами, виявили прогалини у рівні готовності європейського суспільства до стихійних лих, і тому підкреслив важливість підвищення рівня поінформованості про ризики та, отже, стійкості людей та організацій в Європі. Існує багато чого, що можна дізнатись у деяких країнах з високим ступенем ризику стихійних лих (наприклад, Японія з високим рівнем ризику землетрусів, вулканічних подій та цунамі). Необхідні дослідження того, як культурні зміни можуть створити еластичне суспільство в Європі відповідно до Сендайської програми зменшення ризиків від стихійних лих.

Дослідження має проаналізувати як позитивні, так і негативні ролі засобів масової інформації у кризових ситуаціях. Наприклад, внаслідок теракту або стихійного лиха вони пропонують швидкий та простий спосіб поширення інформації про постраждалі райони в перші моменти після катастрофи; вони були використані для поширення ранніх попереджень та важливої інформації про безпеку. Однак соціальні медіа також можуть використовуватися для розповсюдження фальшивих висловлювань та перевищення загроз, тому слід також вирішувати проблеми перевірки інформації. Сама соціальна мережа також залежить від функціонування критичної інфраструктури, такої як телефонні мережі, і може не завжди бути доступною.

Детальніше про конкурс:

<http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/su-drs01-2018-2019-2020.html>

ТЕМА: SU-DRS02-2018-2019-2020: *Технології першого реагування*

Ідентифікатор теми:	SU-DRS02-2018-2019-2020	
Типи діяльності:	RIA Дослідницька та інноваційна діяльність	
Модель подачі:	одноетапна	
Дата відкриття:	15 березня 2018 р.	14 березня 2019 р.
Реченець:	23 серпня 2018 р.	22 серпня 2019 р.

Специфічна проблема, на вирішення якої спрямований конкурс

Вирішальне значення має здатність влади приймати належні заходи у відповідь на серйозні катастрофи, як природні (включаючи екстремальні події, пов'язані з кліматом) так і техногенні. Інновації для суспільств, що постраждали внаслідок стихійних лих, можуть спиратися на нові технології, за умови, що вони доступні, прийняті громадянами, а також адаптовані та впроваджені для (міжгалузевих) потреб першої допомоги.

Очікувані результати: Пропозиції повинні запропонувати нові рішення, які покращують захист першої реакції від багатьох непередбачених небезпек або збільшують їхні можливості шляхом вирішення пов'язаних із дослідженням та інновацій питань, зокрема:

Підтема 1: [2018] Технології виявлення жертв. Швидке виявлення жертв, які потенційно потрапили в небезпеку внаслідок будь-яких катастроф природного, аварійного, техногенного чи терористичного походження, є головною проблемою для рятувальників. Нові технології повинні дозволяти їм заощаджувати час, необхідний для виявлення невидимих жертв, що дає можливість більш ефективного та швидкого рятування, що збільшує шанси збереження життя та зменшення кількості травм.

Підтема 2: [2019] Інновації для швидкого та точного визначення патогенних мікроорганізмів. Перші реабілітологи вимагають нових технологій для швидкого та точного виявлення патогенних мікроорганізмів, а також інструментів спільної епідеміологічної та кримінальної оцінки ризику та оцінки загроз та розслідування.

Підтема 3: [2020] Методи та рекомендації щодо перед-лікарняного догляду та піклування.

Детальніше про конкурс:

<http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/su-drs02-2018-2019-2020.html>

ТЕМА: SU-DRS03-2018-2019-2020:
**Перед-нормативні дослідження та демонстрація
для суспільств, стійких до лих**

Ідентифікатор теми:	SU-DRS03-2018-2019-2020	
Типи діяльності:	IA Інноваційна діяльність	
Модель подачі:	одноетапна	
Дата відкриття:	15 березня 2018 р.	14 березня 2019 р.
Реченець:	23 серпня 2018 р.	22 серпня 2019 р.

**Специфічна проблема,
на вирішення якої спрямований конкурс**

Причиною складної взаємодії між практиками, а також низьким рівнем взаємодії обладнання та процедур, реалізованих першими, є недостатня гармонізація та стандартизація, які попередньо-нормативні дослідження та демонстрації можуть ефективно вирішувати. Ринок безпеки в Європі - дуже роздроблений (через відсутність стандартизації та гармонізованої сертифікації), а також має значний суспільний вимір (це багато в чому безпосередньо впливає на громадян). Необхідні заходи щодо врегулювання криз та стандартизації громадянського захисту, щоб полегшити реакцію, ефективність та співпрацю як найважливіші пріоритети, особливо в тому, що стосується надзвичайних ситуацій, пов'язаних із природними катаклізмами.

Очікувані результати: Пропозиціям пропонується розглянути питання, пов'язані з попередньою стандартизацією, зокрема:

Підтема 1: [2018] Перед-стандартизація для забезпечення водопостачання. Тестові об'єкти повинні з'єднувати мережі безпеки датчиків, що розгортаються в мережах водопостачання та розподілу. Основна увага повинна полягати у створенні об'єктів тестування мереж, розроблених водопровідними підприємствами, для демонстрації використання сучасних технологій датчиків з метою безпеки води, включаючи методи моніторингу резервуарів та рівня моря або річки для раннього попередження.

Підтема 2: [2019] Попередня стандартизація при врегулюванні кризових ситуацій (включаючи природні небезпеки та надзвичайні ситуації з CBRN). Розробка стандартів цивільного захисту в сферах управління кризовими ситуаціями, підвищить взаємозв'язок устаткування та процедур.

Підтема 3: [2020] Перша допомога - розгортання транспортних засобів, навчання, технічне обслуговування, матеріально-технічне забезпечення та засоби дистанційної централізованої координації.

Детальніше про конкурс:

<http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/su-drs03-2018-2019-2020.html>

ТЕМА: SU-DRS04-2019-2020:
**Хімічний, біологічний, радіологічний
та ядерний (CBRN) кластер**

Ідентифікатор теми:	SU-DRS04-2019-2020
Типи діяльності:	RIA Дослідницька та інноваційна діяльність
Модель подачі:	одноетапна
Дата відкриття:	14 березня 2019 р.
Реченець:	22 серпня 2019 р.

**Специфічна проблема,
на вирішення якої спрямований конкурс**

Технології та інновації в галузі CBRN розробляються компаніями, які часто стикаються з труднощами при виході на ринки. Можна визначити принаймні три причини: вони звертаються до місцевих, дрібних нішевих ринків; ці компанії не мають ані можливостей, ані стратегічних цілей виходити на зовнішні ринки; окремі технології, які вони розробляють, можуть вийти на ринок лише в тому випадку, якщо вони інтегровані та поєднуються з іншими інструментами інших компаній, які мають можливості та стратегію щодо продажу продуктів за кордоном, і, можливо, на світовому ринку.

У цьому контексті була створена платформа SEC-05-DRS-2016-2017 в 2016 році. На цю платформу необхідно додати більше інноваційних технологій, пристроїв та послуг.

Очікувані результати: У 2019 та 2020 роках Комісія буде вибирати кілька проектів, спрямованих на дослідження та розробку нових технологій CBRN та інновацій, виявлених у каталозі, який регулярно оновлюється проектом ENCIRCLE. Кожна з цих дій буде очолювана МСП. Кожен консорціум, який реалізує такий проект, повинен не лише створити консорціумний договір між своїми членами, а також укласти угоду з учасниками проекту ENCIRCLE, який повинен визначити, як будуть використані результати інтеграції до платформи, керованої ENCIRCLE.

Детальніше про конкурс:

<http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/su-drs04-2019-2020.html>

ТЕМА: SU-DRS05-2019:
**Демонстрація нових концептів управління
пандемічними кризами**

Ідентифікатор теми:	SU-DRS05-2019
Типи діяльності:	IA Інноваційна діяльність
Модель подачі:	одноетапна
Дата відкриття:	14 березня 2019 р.
Реченець:	22 серпня 2019 р.

**Специфічна проблема,
на вирішення якої спрямований конкурс**

Великі пандемії становлять постійно зростаючу загрозу в сучасному глобалізованому суспільстві, враховуючи зростаючі потоки товарів і людей між континентами. Ця проблема повинна бути вирішена на міжнародному рівні, а також за участі великої кількості практиків та зацікавлених сторін, від плановиків у національних системах охорони здоров'я до надання першої допомоги. Робоча програма Horizon 2020 окремо включає премію EIC Horizon за «Раннє попередження про епідемію», що має відношення до готовності та реагування на випадки спалахів захворювань.

Очікувані результати: Необхідні демонстрації для оцінки нових концепцій реагування у випадку транскордонних надзвичайних ситуацій (етап 2), для посилення готовності та реагування на пандемії (включаючи виявлення спалахів хвороб, які можуть призвести до пандемії).

Результатом проектів мають стати: нові концепції охорони здоров'я та безпеки у випадку масштабних пандемій, затверджені міжнародними організаціями та великою кількістю держав-членів ЄС, включаючи зобов'язання поділитися цими новими концепціями.

Прототип ІТ-системи, що інтегрує інноваційні інструменти та підтримує наявні системи.

Операційна стратегія для реалізації концепцій та ІТ-системи, що підтримують транскордонну готовність та управління кризовими ситуаціями, і продемонстровані на місці.

Детальніше про конкурс:

<http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/su-drs05-2019.html>

ТЕМА: SU-FCT01-2018-2019-2020:
**Людські фактори, соціальні та організаційні аспекти
вирішення проблем у боротьбі зі злочинністю
та тероризмом**

Ідентифікатор теми:	SU-FCT01-2018-2019-2020	
Типи діяльності:	RIA Дослідницька та інноваційна діяльність	
Модель подачі:	одноетапна	
Дата відкриття:	15 березня 2018 р.	14 березня 2019 р.
Реченець:	23 серпня 2018 р.	22 серпня 2019 р.

**Специфічна проблема,
на вирішення якої спрямований конкурс**

Вільне та демократичне суспільство ЄС, засноване на верховенстві права, мобільності через національні кордони, глобалізованої інфраструктури зв'язку та фінансування, надає багато можливостей своїм громадянам. Однак переваги пов'язані з ризиками злочинності та тероризмом, значна частина яких має транскордонний вплив в рамках ЄС. Безпека є ключовим фактором забезпечення високої якості життя та захисту нашої інфраструктури шляхом запобігання та подолання загальних загроз. ЄС має зіграти свою роль, щоб сприяти запобіганню, розслідуванню та / або пом'якшенню наслідків злочинних дій, одночасно захищаючи основні права.

Очікувані результати: Запропоновані підходи повинні спиратися на наявні знання та підходи. Соціальне вимірювання боротьби з злочинністю та тероризмом має бути основою запропонованої діяльності. Пропозиції мають подаватися відповідно до наступних підтем:

Підтема 1: [2018] Нові методи попередження, розслідування та пом'якшення наслідків торгівлі людьми та сексуальної експлуатації дітей, захист жертв. Глобалізація та розвиток технологій сприяють торгівлі людьми та сексуальній експлуатації дітей. Потрібні різні запобіжні заходи, а також заходи щодо забезпечення адекватного захисту та допомоги жертвам, які спираються на досягнення в галузі соціальних та гуманітарних наук.

Підтема 2: [2019] Розуміння чинників кіберзлочинності та нових методів запобігання, розслідування та пом'якшення кібер-кримінальної поведінки. Інтернет речей, все більша кількість пристроїв, які постачаються в Інтернеті, може створювати серйозні загрози для кібербезпеки, оскільки Інтернет став об'єктом для кіберзлочинців. Головним завданням у цьому питанні є визначення того, що є причиною нових форм кібернетичної злочинності та як їх можна запобігти та пом'якшити.

Підтема 3: [2020] Розробка комплексних міждисциплінарних та багатоагентних підходів до запобігання та протидії радикалізації та тероризму в країнах ЄС.

Детальніше про конкурс:

<http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/su-fct01-2018-2019-2020.html>

ТЕМА: SU-FCT02-2018-2019-2020:
**Технології для посилення боротьби з злочинністю
та тероризмом**

Ідентифікатор теми:	SU-FCT02-2018-2019-2020	
Типи діяльності:	RIA Дослідницька та інноваційна діяльність	
Модель подачі:	одноетапна	
Дата відкриття:	15 березня 2018 р.	14 березня 2019 р.
Реченець:	23 серпня 2018 р.	22 серпня 2019 р.

**Специфічна проблема,
на вирішення якої спрямований конкурс**

Організована злочинність і терористичні організації часто користуються новітніми технологічними інноваціями у плануванні, виконанні та приховуванні своєї злочинної діяльності та доходів, що впливають з них. Правоохоронні органи натомість часто відстають в освоєнні прогресивних технологій.

Очікувані результати: Існує нагальна потреба зосередити увагу на нових технологічних можливостях. З цією метою необхідно визначити нові знання та цільові технології для боротьби зі старими та новими формами кримінальної та терористичної поведінки, підтримуваними прогресивними технологіями. Наслідком зростаючої діджиталізації суспільства є те, що практично будь-який вид злочину має цифровий компонент. Відстеження грошових потоків є ще однією проблемою. Питання про місцезнаходження та юрисдикцію необхідно розглянути, беручи до уваги високий імовірний транскордонний характер таких злочинів.

Підтема 1: [2019] Відстеження кваліфікації. Криміналістичний аналіз матеріалу сліду може бути надзвичайно корисним на початковому етапі дослідження, якщо відповіді є швидкими (в реальному часі) та відповідають кримінальному правосуддю. Необхідно розробити нові роботизовані або автоматизовані засоби для криміналістичного аналізу.

Підтема 2: [2018] Цифрова криміналістика в контексті кримінальних розслідувань. Необхідні нові криміналістичні інструменти, методи та методика, засновані на загальних практиках, стандартах, протоколах та / або вимогах сумісності, які дозволяють швидко вилучати, зберігати, аналізувати та перевіряти цифрові докази (в тому числі і ті, що зберігаються в хмарі), які захищаються в суді, і дає змогу проводити розслідування для виявлення злочинців, а також жертв.

Підтема 3: [2020] Відстеження грошових потоків.

Детальніше про конкурс:

<http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/su-fct02-2018-2019-2020.html>

ТЕМА: SU-FCT03-2018-2019-2020:
**Управління інформацією та потоками даних
для боротьби з кіберзлочинністю та тероризмом**

Ідентифікатор теми:	SU-FCT03-2018-2019-2020	
Типи діяльності:	ІА Інноваційна діяльність	
Модель подачі:	одноетапна	
Дата відкриття:	15 березня 2018 р.	14 березня 2019 р.
Реченець:	23 серпня 2018 р.	22 серпня 2019 р.

**Специфічна проблема,
на вирішення якої спрямований конкурс**

Великі обсяги даних та інформації з різних джерел стали доступними для практиків, які займаються боротьбою з злочинністю та тероризмом. Але сьогодні не використовуються найсучасніші методи аналізу великих даних та штучного інтелекту.

Очікувані результати: Кількість даних, створених та зібраних в рамках досліджень кіберзлочинів, збільшується експоненціально, тим самим створюючи значну проблему для правоохоронних органів. Ефективність правоохоронних дій залежить від можливостей покращення якості даних, а також перетворення об'ємних та неоднорідних наборів даних (зображень, відео, геопросторової розвідки, даних зв'язку, даних про рух, дат фінансових операцій тощо) до оперативного інтелекту. Ці можливості можуть бути значно покращені завдяки використанню спеціальних інструментів домену, тобто додатків для аналізу великих даних, розроблених для потреб дослідників злочинів (попередня обробка, обробка та аналіз, візуалізація тощо). Крім того, прогнозована аналітика значною мірою сприятиме збору даних з відкритим кодом, аналізу соціальної мережі та «темних» даних, а також дозволить забезпечити ресурсозберігаючу, ефективну та активну діяльність у сфері правопорядку.

Приклади тенденцій в галузі кіберзлочинності численні. Інтернет речей потенційно може з'єднувати практично все, тому потенційно робить все більш уразливим. Носильні пристрої роблять нас відстежуваними, 3D-принтери можуть випускати зброю, автономні автомобілі надають можливості для викрадення людей, телеробот відкриває двері для кібер-шпигунства тощо. Правоохоронні органи отримали б вигоду від нових засобів запобігання та протидії новим видам злочинності, спираючись на комплексний аналіз тенденцій розвитку видів діяльності, пов'язаної з кіберзлочинністю на основі попередніх кіберзлочинної діяльності, технологічного розвитку та тенденцій в суспільстві.

Детальніше про конкурс:

<http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/su-fct03-2018-2019-2020.html>

ТЕМА: SU-GM01-2018-2019-2020:
**Пан-європейські мережі практиків
та інших акторів у сфері безпеки**

Ідентифікатор теми:	SU-GM01-2018-2019-2020	
Типи діяльності:	CSA Дії з координації та підтримки	
Модель подачі:	одноетапна	
Дата відкриття:	15 березня 2018 р.	14 березня 2019 р.
Реченець:	23 серпня 2018 р.	22 серпня 2019 р.

**Специфічна проблема,
на вирішення якої спрямований конкурс**

Організації, що відповідають за безпеку в Європі не мають достатньо можливостей, часу і ресурсів для моніторингу інновацій та досліджень, які можуть бути корисними для них. У них є небагато можливостей взаємодіяти з науковими установами з таких питань. Всі зацікавлені сторони - державні служби, промисловість, наукові організації, включаючи тих, хто бере участь у Консультативній групі з питань безпеки, визнають це як проблему.

Очікувані результати: Практики запрошуються до співпраці в 4 різних категоріях мереж у галузі безпеки:

а. [2019-2020] Практики (кінцеві користувачі) з усієї Європи запрошуються об'єднатись для того, щоб:
1) проводити моніторинг дослідницьких та інноваційних проектів з метою рекомендації щодо індустріалізації результатів; 2) висловлювати загальні вимоги стосовно інновацій, які могли б задовольнити можливості та інші прогалини та покращити майбутню продуктивність; 3) вказати пріоритети щодо сфер, що потребують більшої стандартизації. У 2019 році пропозиції приймаються у двох специфічних сферах спеціалізації: захист громадських діячів; обробка гібридних загроз.

б. [2018] Кластерні інновації з усієї Європи (створені на національному, регіональному або місцевому рівнях), що управляють демонстраційними майданчиками, тестові майданчики та навчальні центри (у тому числі ті, що забезпечують симулятори).

с. [2018] Органи закупівель або відділи, що займаються питаннями бюджетування та реалізацією придбання рішень з безпеки на європейському, національному, регіональному або місцевому рівні, можуть об'єднатися задля: 1) обміном інвестиційними планами, 2) порівняння методів та правил закупівель та 3) планування загальних закупівель науково-дослідних послуг, а також інноваційних продуктів.

д. [2019] Прикордонні та берегові охоронні організації, органи закупівель, промисловість та дослідники запрошуються об'єднати зусилля та розробляти дорожні карти, необхідні для надання інноваційних, майбутніх рішень для спостереження за кордоном та береговим наглядом.

Детальніше про конкурс:

<http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/su-gm01-2018-2019-2020.html>

ТЕМА: SU-GM02-2018-2020 :
**Стратегічні попередні комерційні закупівлі
інноваційних, сучасних систем підтримки безпеки**

Ідентифікатор теми:	SU-GM02-2018-2020
Типи діяльності:	CSA Дії з координації та підтримки
Модель подачі:	одноетапна
Дата відкриття:	15 березня 2018 р.
Реченець:	23 серпня 2018 р.

**Специфічна проблема,
на вирішення якої спрямований конкурс**

Необхідні інноваційні рішення для посилення безпеки, в умовах, коли ресурси з різних країн вимагають більш тісної співпраці. Такі рішення повинні підтримувати розвиток Союзу безпеки ЄС.

Очікувані результати: Підтема 1: [2018] Специфікації спільних вимог для інноваційних, сучасних систем підтримки безпеки.

Практики з кількох країн запрошуються працювати над загальними вимогами будь-якої системи, якої вони можуть потребувати в майбутньому, для посилення прикордонної та зовнішньої безпеки, для боротьби зі злочинністю та тероризмом, для захисту інфраструктури або для створення більш стійких суспільств та залучати їх відповідні органи закупівель для підготовки до майбутніх придбань. Практикуючі організації можуть бути приватними чи державними організаціями.

Підтема 2: [2020] Закупівля прототипів серед тих, що зазначені у підтемі 1.

Загальні вимоги до інноваційних прототипів узгоджені серед організацій-практиків, які беруть участь в акції. Технічні тендерні документи, готові до використання в подальших заходах до комерційних закупівель.

Детальніше про конкурс:

<http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/su-gm02-2018-2020.html>

ТЕМА: SU-GM03-2018-2019-2020:
**Передкомерційні розробки інноваційних рішень
для посилення безпеки**

Ідентифікатор теми:	SU-GM03-2018-2019-2020	
Типи діяльності:	PCP Передкомерційні закупівлі	
Модель подачі:	одноетапна	
Дата відкриття:	15 березня 2018 р.	14 березня 2019 р.
Реченець:	23 серпня 2018 р.	22 серпня 2019 р.

**Специфічна проблема,
на вирішення якої спрямований конкурс**

Необхідні інноваційні рішення для посилення безпеки, в умовах, коли ресурси з різних країн вимагають більш тісної співпраці. Такі рішення повинні підтримувати розвиток Союзу безпеки ЄС.

Очікувані результати: Практики з кількох країн запрошуються до закупівлі інноваційних рішень для підвищення їх операційної спроможності. Практикуючі організації можуть бути приватними чи державними. Проекти передбачають декілька фаз:

Етап 0: розробляти спільні вимоги до інноваційних прототипів, узгоджених між організаціями-практиками, що беруть участь у акції, і підготувати технічні тендерні документи, готові до використання на наступному етапі дії;

Етап 1: Підготовка пакету повного тендеру для проведення тендерних пропозицій щодо створення прототипів, що мають відношення до безпеки, на основі технічного вкладу, отриманого в результаті етапу 0; готуватися до перевірки майбутніх прототипів;

Етап 2: реалізувати запрошення на тендери для створення 2 прототипів із 2 різних джерел;

Етап 3: тестування та перевірка 2-х прототипів проти методу, розробленого під час етапу 1;

Етап 4: Розробити навчальний план загальноєвропейського навчання з використанням прототипів.

Детальніше про конкурс:

<http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/su-gm03-2018-2019-2020.html>

ЗМІСТ

Конкурс «Захист інфраструктури Європи і людей в європейських розумних містах»	3
ТЕМА: Попередження, виявлення, реагування та пом'якшення комбінованих фізичних та кібер- загроз для критичної інфраструктури в Європі	4
ТЕМА: Безпека для розумних міст, включно з громадськими місцями	5
Конкурс «Цифрова безпека»	6
ТЕМА: Кібербезпекова готовність – кібер-діапазон, моделювання і економіка.....	7
ТЕМА: Цифрова безпека і конфіденційність для громадян, малих, середніх та мікро- підприємств	8
ТЕМА: Кібербезпека в електроенергетичній та енергетичній системах: броня проти кібератак та загроз конфіденційності і витік даних.....	9
ТЕМА: Цифрова безпека, конфіденційність, захист даних і звітність в критичних секторах.....	10
Конкурс «Безпека»	11
ТЕМА: Людські фактори, соціальні та організаційні аспекти безпеки кордонів та зовнішньої безпеки	12
ТЕМА: Технології покращення безпеки кордонів та зовнішньої безпеки.....	13
ТЕМА: Демонстрація прикладних рішень для покращення прикордонної та зовнішньої безпеки	14
ТЕМА: Людські фактори, соціальні та організаційні аспекти суспільств, стійких до загроз	15
ТЕМА: Технології першого реагування.....	16
ТЕМА: Перед-нормативні дослідження та демонстрація для суспільств, стійких до лих	17
ТЕМА: Хімічний, біологічний, радіологічний та ядерний (CBRN) кластер.....	18
ТЕМА: Демонстрація нових концептів управління пандемічними кризами	19
ТЕМА: Людські фактори, соціальні та організаційні аспекти вирішення проблем у боротьбі зі злочинністю та тероризмом	20
ТЕМА: Технології для посилення боротьби з злочинністю та тероризмом	21
ТЕМА: Управління інформацією та потоками даних для боротьби з кіберзлочинністю та тероризмом	22
ТЕМА: Пан-європейські мережі практиків та інших акторів у сфері безпеки	23
ТЕМА: Стратегічні попередні комерційні закупівлі інноваційних, сучасних систем підтримки безпеки	24
ТЕМА: Передкомерційні розробки інноваційних рішень для посилення безпеки.....	25

Інформаційно-довідкове видання

Рамкова програма Європейського Союзу з досліджень та інновацій «Горизонт 2020». Конкурси за тематичним напрямом «Безпечні суспільства: захист свободи та безпеки Європи та її громадян» на 2018 – 2020 рр.

Інформація підготовлена національним контактним пунктом Національного університету «Кієво-Могилянська академія» на основі робочої програми за тематичним напрямом «Безпечні суспільства: захист свободи та безпеки Європи та її громадян» на 2018 – 2020 рр.

Адреса НКП в НаУКМА:
вул. Волоська, 8/5, Київ, 04655
корпус 5, к. 307-308

www.h2020.ukma.edu.ua
<https://www.facebook.com/H2020NaUKMA/>

