DHS/DOJ Fusion Process Technical Assistance Program and Services

Міркування щодо координації роботи Об'єднаного центру та Центру надзвичайних ситуацій

Посібник з комплексної готовності (CPG) 502

Травень 2010

Передмова

Об'єднані центри та центри з надзвичайних ситуацій (EOC) повинні бути ознайомлені з ролями і можливостями один одного, щоб полегшити успішну взаємодію і співпрацю між ними. Крім того, вкрай важливо, щоб вони налагодили міцні стосунки для ефективної спільної роботи над досягненням своїх цілей. Відносини, встановлені між цими двома структурами, дозволять їм мати постійні, змістовні контакти, що посилить їхню здатність обмінюватися інформацією і розвідданими незалежно від статусу активації EOC. Взаємна довіра і повага повинні лежати в основі політик і протоколів міжвідомчої взаємодії, що забезпечить ефективну і послідовну співпрацю як в умовах сталого стану, так і під час надзвичайних ситуацій.

На додаток до визначення взаємовідносин у концепції операцій (CONOPS) і стандартних операційних процедурах (SOP), слід створити, переглянути і оновити меморандуми про взаєморозуміння (MOU) для визначення ролей як у період активації, так і в період неактивації. SOP і меморандуми про взаєморозуміння також визначають, як буде здійснюватися обмін інформацією між двома суб'єктами. Посібник з комплексного планування (CPG) 502 зосереджує увагу на цьому важливому партнерстві та обміні інформацією між цими суб'єктами.

Партнерства

Ефективність зусиль із запобігання, захисту, реагування та відновлення залежить від здатності всіх рівнів і секторів влади, а також приватного сектору збирати, аналізувати, поширювати і використовувати інформацію та розвідувальні дані, пов'язані з національною безпекою та злочинністю. На підтримку цього, Національна стратегія обміну інформацією закликає до створення національної спроможності обміну інформацією шляхом створення національної інтегрованої мережі центрів злиття інформації. З метою сприяння розвитку потенціалу національних центрів злиття даних, Управління національної готовності (NPD) Федерального агентства з надзвичайних ситуацій (FEMA) Міністерства внутрішньої безпеки США (DHS) і Бюро сприяння правосуддю (BJA) Міністерства юстиції США (DOJ) об'єднали свої зусилля для розробки Програми технічної допомоги в процесі злиття даних (Fusion Process Technical Assistance Program). Ця програма була розроблена за підтримки Управління розвідки та аналізу (I&A) DHS США та в координації з Офісом директора національної розвідки (ODNI); Офісом керівника програми з питань обміну інформацією (PM-ISE); Федеральним бюро розслідувань (ФБР) та експертами з державного та місцевого рівнів, включаючи Глобальну ініціативу з обміну інформацією у сфері правосуддя (Global), Координаційну раду з питань кримінальної розвідки (CICC) та Глобальну робочу групу з питань розвідки (GIWG). Програма технічної допомоги процесу злиття також була розроблена для безпосередньої підтримки впровадження Керівництва для центрів злиття та Базових можливостей для центрів злиття на рівні штатів і великих міських районів.

При розробці Посібника для Центрів злиття Global залучив різноманітних представників державного і приватного секторів, об'єднавши досвід управління в надзвичайних ситуаціях і правоохоронних органів. Партнери з виконавчої влади, такі як ODNI та PM-ISE, роз'яснили політику і процедури, які керують обміном інформацією.

Процес створення керівництва для роботи центрів злиття розвивався через розробку Базових можливостей для центрів злиття на рівні штатів і великих міських районів. Цей документ визначає базові можливості центрів злиття та операційні стандарти, необхідні для досягнення кожної з них. Стале федеральне партнерство зі штатами та великими міськими центрами злиття має вирішальне значення для безпеки нації. Базові спроможності рекомендують розвивати процеси, які регулюють офіційну роботу з лідерами і політиками, державним сектором, ЗМІ та громадянами. Також рекомендується розробити план підвищення обізнаності про мету, місію

та функції об'єднаного центру (що, своєю чергою, посилює партнерство з EOC), а також забезпечити спільне розуміння ролей та обов'язків.

Подяки

Робоча група, до складу якої входили менеджери з надзвичайних ситуацій, представники правоохоронних органів, представники центрів злиття, а також дослідники в галузі управління надзвичайними ситуаціями та розвідки, розробила CPG 502 спільно з DHS/FEMA та спільною Програмою технічної допомоги DHS/DOJ щодо процесу злиття. До складу групи та наступних оглядових сесій входили представники:

Національні та федеральні органи влади

- Робоча група CPG
- Управління розвідки та аналізу DHS
- Управління національної готовності DHS FEMA
- Група управління Центром злиття
- Координаційна рада кримінальної розвідки
- Національна асоціація центрів злиття

Промисловість, дослідницькі організації та університети

- Аргонська національна лабораторія: Центр інтегрованої готовності до надзвичайних ситуацій
- Буз Аллен Гамільтон
- Community Research Associates, Inc.
- IEM, Inc.
- Lafayette Group

Зміст

Вступ та огляд

Процес злиття є наріжним каменем для ефективного запобігання загрозам, в тому числі тероризму та іншим злочинам, з боку штатних, місцевих, племінних і територіальних органів влади. Термін "злиття" означає всеохоплюючий процес управління потоками інформації і розвідувальних даних на всіх рівнях і в усіх секторах державного управління і в приватному секторі. Він виходить за рамки створення інформаційно-розвідувального центру або комп'ютерної мережі. Багато об'єднаних центрів застосовують підхід, що охоплює всі види злочинів і/або всі види загроз, а також залучають до своїх процесів міждисциплінарних і неправоохоронних партнерів.
Зрештою, процес злиття підтримує реалізацію програм запобігання, захисту, реагування і відновлення, що ґрунтуються на оцінці ризиків і керуються інформацією. Водночас він підтримує зусилля, спрямовані на вирішення негайних або нових обставин і подій, пов'язаних із загрозами.

Загальна мета процесу злиття - перетворити необроблену інформацію та розвіддані на практичні знання. Об'єднані центри є ефективними механізмами для управління цим процесом. Крім того, національна мережа об'єднаних центрів працює з федеральними агентствами і розвідувальним співтовариством над реалізацією національних пріоритетів розширеного регіонального співробітництва, обміну інформацією і співпраці, як це визначено в Керівництві з національної готовності Міністерства національної безпеки США. Керівні принципи національної готовності передбачають процес і доктрину готовності, що ґрунтуються на силах і засобах, з прикладними програмами планування. У настановах є посилання на Перелік цільових сил і засобів (Target Capabilities List, TCL) як на всеосяжний каталог сил і засобів, які можуть бути використані для виконання місій з національної безпеки, в тому числі для управління та розвідки під час EOC. TCL допомагає оперативним планувальникам і керівникам програм по всій країні використовувати загальні інструменти і процеси при плануванні, навчанні, оснащенні та інших інвестиціях і досягати вимірюваних результатів.

Міжвідомча координація (MAC)/Управління EOC: Здатність активувати та підтримувати операції EOC/MAC, координувати дії з іншими установами та зацікавленими сторонами, розробляти пріоритети та стратегії для підтримки управління інцидентами та операцій з безперервності, управляти ресурсами та підтримувати зв'язок з іншими організаціями для координації ресурсів, а також підтримувати прийняття управлінських рішень та координувати інформацію.

EOC та центри спостереження/попередження, а також інші органи громадської безпеки, служби швидкого реагування та організації приватного сектору є важливими постачальниками первинної інформації, оперативної інформації з управління надзвичайними ситуаціями, розвідданих про всі види небезпек та інших спеціальних знань. Крім того, вони є користувачами оперативної інформації і розвідданих і, отже, також "клієнтами" об'єднаних центрів.

Координація роботи EOC та об'єднаних центрів має вирішальне значення для підвищення безпеки населення. Об'єднані центри, EOC та інші органи внутрішньої безпеки повинні розвивати позитивні відносини і встановлювати політику і протоколи для обміну відповідною інформацією і розвідданими під час повсякденних операцій і під час інцидентів. У багатьох випадках минулі спроби досягти такого рівня координації наштовхувалися на занепокоєння з приводу того, як обмінюватися інформацією з огляду на її рівень секретності. І навпаки, співробітники об'єднаних центрів часто не знають, яка саме інформація потрібна співробітникам EOC на щоденній основі або під час інцидентів.

Центр оперативного реагування на надзвичайні ситуації: Фізичне місце, де зазвичай відбувається координація інформації та ресурсів для підтримки заходів з управління інцидентом (операцій на місці події). EOC може бути тимчасовим об'єктом або розташовуватися в більш центральному чи постійно діючому об'єкті, можливо, на вищому рівні організації в межах юрисдикції.

EOC можуть бути організовані за основними функціональними дисциплінами (наприклад, пожежні служби, правоохоронні органи, медичні служби), за юрисдикцією (наприклад, федеральна, штатна, регіональна, племінна, міська, окружна) або за певною комбінацією цих дисциплін.

Успішна реалізація цих інформаційних вимог вимагає наявності зацікавлених партнерів (які розуміють потреби і занепокоєння один одного, а також правові обмеження, які можуть обмежувати поширення правоохоронної, медичної або іншої конфіденційної інформації) і створення відповідних каналів зв'язку. Зрештою, ці покращені відносини сприятимуть більш скоординованому, своєчасному та ефективному реагуванню на нові інциденти або загрози, а також інтеграції превентивних заходів, спрямованих на правоохоронні органи, із заходами, спрямованими на управління надзвичайними ситуаціями.

Мета

Цей документ надає посадовим особам об’єднаних центрів штатів і великих міських агломерацій та посадовим особам EOC рекомендації щодо координації дій між об'єднаними центрами та EOC. У ньому окреслено ролі центрів та EOC в процесі об'єднання і запропоновано кроки, за допомогою яких ці організації можуть працювати разом для постійного обміну інформацією та розвідданими. Цей посібник підтримує впровадження Базових спроможностей для об'єднаних центрів штатів і великих міських районів, а також допомагає EOC виконувати свої завдання як в умовах сталого стану, так і під час активних операцій з ліквідації наслідків надзвичайних ситуацій, як це передбачено в CPG 601: Створення та управління центрами управління в надзвичайних ситуаціях. Ця CPG містить вказівки щодо широких вимог до спроможностей EOC.

Застосування та сфера використання

Цей посібник призначений для керівників, відповідальних за громадську безпеку, в тому числі для персоналу центрів управління в надзвичайних ситуаціях та об’єднаних центрів. Посібник визнає, що багато юрисдикцій по всій країні вже розробили робочі відносини і протоколи обміну, і тому не встановлює жодних негайних вимог. Скоріше, цей посібник пропонує, щоб майбутні зусилля з координації брали до уваги цю настанову.

Органи влади

Наступне федеральне законодавство, плани та стратегії мали вирішальне значення для розвитку процесів обміну інформацією:

- Державний закон 110-53, Імплементація рекомендацій Акту Комісії 9/11 від 2007 року
- Національна структура реагування (NRF)
- Національна система управління інцидентами (NIMS)
- Національний план обміну кримінальною розвідкою
- Національна стратегія обміну інформацією
- Посібник для Об'єднаного центру
- Базові можливості для об'єднаних центрів штатів і великих міських районів
- Можливості захисту критичної інфраструктури та ключових ресурсів (CIKR) для об'єднаних центрів
- План впровадження середовища обміну інформацією (ISE)
- Вказівка 2 щодо ISE
- Керівні принципи національної готовності

- CPG 601: Проектування та управління центрами надзвичайних ситуацій

Державний закон 110-53 (також відомий як "Імплементація рекомендацій Акту Комісії 9/11 від 2007 року"). Цим законом було засновано Ініціативу з безпеки міських територій (UASI) для надання грантів на допомогу мегаполісам з високим рівнем ризику у запобіганні, підготовці, захисті від терористичних актів та реагуванні на них. Цей закон також заснував Державну грантову програму з національної безпеки (HSGP) і закликав до фінансування правоохоронної діяльності та заходів із запобігання тероризму, включаючи обмін інформацією та її аналіз, посилення цільової аудиторії, розпізнавання загроз і припинення терористичних актів.

NRF, Функція підтримки в надзвичайних ситуаціях (ESF) 5 (Управління в надзвичайних ситуаціях). ESF-5 координує зусилля з управління та реагування на надзвичайні ситуації. Вона сприяє обміну інформацією на етапі, що передує інциденту, і координує міжурядове планування, навчання і тренування з метою підготовки сил і засобів до розгортання. Діяльність ESF-5 включає критично важливі функції, які підтримують і полегшують міжвідомче планування і координацію операцій, пов'язаних з інцидентами, що потребують федеральної координації, в тому числі такі функції, як збір, аналіз і управління інформацією.

NRF, ESF-13 (Громадська безпека). ESF-13 сприяє координації громадської безпеки між федеральними, штатними, місцевими, племінними та територіальними органами, щоб забезпечити відповідність процесів комунікації та координації заявленим місіям і цілям управління інцидентами. ESF-13, як правило, активується, коли необхідна широка допомога через неадекватність або перевантаженість штатних, місцевих, племінних і територіальних ресурсів, або коли потрібні захисні рішення або можливості, унікальні для федерального уряду, особливо в ситуаціях до або після інциденту. При активації ESF-13 може надавати ресурси захисту і безпеки, допомогу в плануванні, технологічну підтримку та іншу технічну допомогу для підтримки операцій з ліквідації наслідків інциденту.

NIMS. NIMS - це набір принципів, який забезпечує систематичний, проактивний підхід, що орієнтує державні установи на всіх рівнях, неурядові організації та приватний сектор на безперебійну роботу із запобігання, захисту, реагування, відновлення та пом'якшення наслідків інцидентів, незалежно від причини, розміру, місцезнаходження або складності, з метою зменшення людських і матеріальних втрат, а також шкоди навколишньому середовищу.

Національний план обміну кримінальною розвідкою. Національний план обміну кримінальною розвідкою був вперше опублікований у жовтні 2003 року і переглянутий у липні 2005 року. Метою плану є налагодження зв'язків між федеральними, штатними, місцевими, племінними і територіальними правоохоронними органами, що дозволить їм обмінюватися розвідувальною інформацією для запобігання тероризму і злочинності. План окреслює політику, стандарти і керівні принципи розвитку розвідувальної функції місцевих правоохоронних органів, а також містить рекомендації щодо ключових проблем і перешкод на шляху його реалізації. Він також наголошує на кращих методах розробки та обміну критично важливими даними. CICC був створений з метою розробки політики на національному рівні для реалізації плану та моніторингу його виконання на штатному та місцевому рівнях. CICC співпрацює з Ініціативою інформаційної стратегії правоохоронних органів Міністерства юстиції та Координаційною радою з питань судової розвідки з метою покращення обміну розвідданими та інформацією між усіма рівнями правоохоронних органів.

Національна стратегія обміну інформацією. Ця стратегія відповідає Стратегії національної безпеки і тісно пов'язана з Національною стратегією боротьби з тероризмом, Національною стратегією розвідки і Національною стратегією внутрішньої безпеки. Стратегія описує план Адміністрації щодо створення більш інтегрованої системи обміну інформацією, покращення міжвідомчого обміну інформацією на федеральному рівні та налагодження обміну інформацією між федеральним урядом і партнерами, що не входять до складу федерального уряду.
Стратегія ґрунтується на таких керівних принципах:

- Ефективний обмін інформацією досягається завдяки міцному партнерству між федеральними, штатними, місцевими, племінними та територіальними органами влади, організаціями приватного сектору та іноземними партнерами і союзниками.

- Необхідно розвивати культурну обізнаність, щоб використовувати інформацію і знання з усіх джерел для підтримки антитерористичних зусиль.
- Обмін інформацією має бути інтегрований в усі аспекти антитерористичної діяльності.
- Процедури, процеси і системи обміну інформацією повинні спиратися на існуючі технічні можливості та інтегрувати їх, а також поважати встановлені повноваження і обов'язки.
- Об'єднані центри штатів і великих міст повинні бути включені в національну систему обміну інформацією.

Керівництво для об'єднаних центрів - DOJ у співпраці з DHS та FBI розробило ці настанови для правоохоронних органів, розвідки, громадської безпеки та приватного сектору з метою ефективного впровадження шляхів розвитку та функціонування об'єднаних центрів по всій країні. Настанови містять конкретні рекомендації щодо ролі правоохоронних органів, управління, потреб в інформаційних технологіях (IT) та інформаційної безпеки для кращого захисту нашої батьківщини та максимізації зусиль у боротьбі зі злочинністю.

Базові можливості для об'єднаних центрів штатів і великих міських районів. Цей документ є доповненням до Керівних принципів для об'єднаних центрів і визначає базові можливості та операційні стандарти, необхідні для досягнення об'єднаними центрами своїх цілей. Базові можливості позначені в розділах "Можливості процесу злиття" та "Управлінські та адміністративні можливості".

Можливості захисту CIKR для термоядерних центрів. Як додаток до Базових можливостей Global для штатних і великих міських центрів, цей документ визначає можливості, необхідні для штатних і великих міських центрів злиття для створення аналітичного потенціалу захисту CIKR, який підтримує діяльність з безпеки інфраструктури на штатному та місцевому рівнях.

ISE План впровадження. Ухвалений відповідно до Закону про реформування розвідки і запобігання тероризму від 2004 року, план визначає і просуває процедури обміну інформацією для сприяння антитерористичним зусиллям між федеральним урядом, урядами штатів, місцевими, племінними і територіальними урядами та іншими партнерами по ISE.

ISE Настанова 2. Ухвалена відповідно до Закону про реформування розвідки і запобігання тероризму від 2004 року, настанова розробляє загальну структуру для обміну інформацією між федеральними департаментами і відомствами, а також органами влади штатів, місцевими, племінними і територіальними органами, правоохоронними органами і приватним сектором. Він вимагає розробки і впровадження цієї системи для "інформації з питань внутрішньої безпеки", "інформації про тероризм" і "інформації для правоохоронних органів."

Керівні принципи національної готовності. Ці керівні принципи, що впроваджуються відповідно до президентської директиви з питань внутрішньої безпеки (HSPD) 8, замінюють Національну мету з готовності і визначають, як підготуватися до всіх небезпек. Вони організовують і синхронізують зусилля по всій країні, спрямовані на посилення готовності нації, зміцнюючи концепцію, що готовність є спільною відповідальністю.

CPG 601: Проектування та управління центрами надзвичайних ситуацій (дата випуску не визначена). CPG 601 - це новий федеральний керівний документ, розроблений для задоволення широких вимог до спроможностей EOC. Він замінює Посібник з цивільної готовності 1-20, Посібник для центрів управління в надзвичайних ситуаціях, який був написаний у 1984 році і переглянутий у 1989 році. Посібник з цивільної готовності 1-20 втратив чинність.

Як користуватися цим посібником

Цей документ є частиною спільної Програми технічної допомоги DHS/DOJ щодо процесу злиття та ширшої програми FEMA CPG і покликаний допомогти як початківцям, так і досвідченим планувальникам орієнтуватися в процесі планування. У першому розділі розглядається застосовність, повноваження, мета та сфера застосування цього CPG. Наступний розділ описує ролі та ініціативи федеральних відомств. У третьому і четвертому розділах детально описано, як функціонують об'єднані центри і EOC в більш широкому контексті середовища обміну інформацією. У п'ятому розділі описано, як об'єднані центри та EOC можуть координувати свою діяльність з метою обміну розвідданими та інформацією, а в останньому розділі наведені конкретні приклади такої координації. Додатки до цього посібника є наступними:

- Додаток A: Глосарій та абревіатури
- Додаток B: Проект Меморандуму про взаєморозуміння
- Додаток C: Інтерфейс між об'єднаним Центром та EOC: Аналіз найкращих практик координації та інтеграції
- Додаток D: Розробка процесів отримання та використання геопросторової інформації для підтримки планування та реагування на всі види небезпек
- Додаток E: Державно-приватне партнерство: Посібник з Кодексу поведінки Партнерства "Сейфгард Айова" для зв'язкових, які працюють у центрах реагування на надзвичайні ситуації

NIMS Дотримання вимог та інтеграція

NIMS надає рекомендації щодо використання та інтеграції функції розвідки/розслідування. Функція розвідки/розслідування в системі управління інцидентом (ICS) забезпечує гнучку і масштабовану структуру, яка дозволяє інтегрувати розвідувальну і слідчу діяльність та інформацію. На рисунку 1 показано місця, де функція інформації і розвідки може бути знайдена в структурі командування інцидентом, і де оперативний відділ може отримати підтримку від персоналу об'єднаного центру.

Залежно від потреб інциденту, функція інформації та розвідки може бути активована як п'ята секція, як елемент у складі оперативної секції або секції планування, або як частина командного штабу.

Додаткову інформацію див. в NIMS.

Рисунок 1: Можливе розміщення інформаційно-розвідувального підрозділу в структурі командування

Хоча система управління надзвичайними ситуаціями і мережа центрів злиття можуть використовувати різні методи і інструменти, обидві вони мають спільну місію - забезпечення громадської безпеки. Інтеграція концепцій NIMS та ISE може сприяти ефективній співпраці у спільному просторі місії.

Рекомендовані тренінги

Див. розділ "Координація роботи EOC та об'єднаного Центру ": Крок четвертий: Тренінги, семінари та вправи.

Процес перегляду

DHS переглядатиме цей CPG за необхідності та публікуватиме змінені сторінки через систему публікацій та розповсюдження, а також в Інтернеті через різні джерела (наприклад, Disaster Assistance [http://www.disasterassistance.gov] та DHS Lessons Learned Information Sharing (LLIS) [http://www.llis.dhs.gov]).

DHS вітає рекомендації щодо покращення цього посібника, щоб він краще відповідав потребам спільнот, які займаються питаннями національної безпеки, правоохоронних органів та управління надзвичайними ситуаціями. Рекомендації щодо покращення цього посібника можна надсилати на адресу NPD-Planning@dhs.gov, ATTN: PAB - CPG Initiative - 502.

Ініціативи, ролі та керівні принципи федеральних департаментів

Федеральні ініціативи та ролі

Група управління об’єднаним центром

Групу з управління об'єднаними центрами очолюють Управління розвідки та аналізу Міністерства оборони США (I&A) і Офіс керівника програми "Середовище обміну інформацією" (PM-ISE). Місія цієї групи полягає в забезпеченні керівництва, координації і керівництва в розвитку - і підтримки з боку федерального уряду - національної інтегрованої мережі об'єднаних центрів, що функціонують на визначеному базовому рівні спроможностей. Перед групою стоять наступні завдання:

- Слугувати основним форумом для координації федеральної підтримки у розвитку, підтримці та підтримці національної інтегрованої мережі центрів злиття штатів та великих міських територій, що працюють на визначеному базовому рівні спроможності;
- Сприяти підвищенню обізнаності внутрішніх і зовнішніх зацікавлених сторін про місію, мету та цінність центрів злиття; і
- Розробити скоординовану стратегію для підтримки центрів злиття.

Міністерство національної безпеки

Міністр національної безпеки визначив I&A виконавчим органом DHS, який координує діяльність Департаменту з об'єднавчими центрами. Як член розвідувального співтовариства і DHS, I&A забезпечує життєво важливий зв'язок між розвідувальним співтовариством і федеральними, штатними, місцевими, племінними, територіальними та приватними структурами. Воно тісно співпрацює з 16 федеральними розвідувальними організаціями та відомствами, а також місцевими, племінними, територіальними та приватними структурами для забезпечення збору, об'єднання, аналізу та розповсюдження інформації і розвідувальних даних серед усіх пов'язаних партнерів у міру необхідності і доцільності, щоб забезпечити повну оцінку загроз по всій країні. Воно співпрацює з об'єднаними центрами по всій країні для протидії загрозам і небезпекам, пов'язаним з різними питаннями і ситуаціями, включаючи безпеку кордонів, радикалізацію і екстремізм, окремі групи, що в'їжджають до США, захист CIKR і зброю масового знищення (WMD). DHS також створило програмний офіс в рамках I&A для вирішення проблем штатних і місцевих чиновників і управління розгортанням персоналу та інших ресурсів в центрах злиття.

FEMA надає підтримку Департаменту внутрішнього аудиту та аудиту DHS з метою сприяння розробці, впровадженню та функціонуванню об'єднаних центрів у рамках спільної Програми технічної допомоги DHS/DOJ з питань об'єднаного процесу. Ці зусилля включають координацію роботи відповідних центрів злиття з конкретними підрозділами DHS, включаючи Управління захисту інфраструктури DHS (IP), Управління охорони здоров'я DHS (OHA), Пожежну адміністрацію США (USFA) та інші.

FEMA також підтримує розробку та функціонування EOC з метою покращення можливостей управління надзвичайними ситуаціями та готовності до них на федеральному рівні, рівні штатів, місцевому, племінному, територіальному та приватному рівнях шляхом надання підтримки через службу технічної допомоги з проектування та управління EOC, а також шляхом підтримки відповідності вимогам NIMS. NIC забезпечує стратегічне керівництво і національну програму з навчання та інформування про NIMS по всій країні.

Департамент юстиції, Бюро сприяння правосуддю

BJA є компонентом програм Міністерства юстиції США і підтримує правоохоронні, виправні, технологічні та інші пов'язані з ними превентивні ініціативи, які зміцнюють національну систему кримінального правосуддя. BJA складається з трьох основних компонентів: політика, програми та планування. Політичний відділ забезпечує національне лідерство в політиці кримінального правосуддя, навчанні та технічній допомозі з метою подальшого вдосконалення відправлення правосуддя. Воно також виступає в ролі зв'язкового з національними організаціями, які співпрацюють з BJA у формуванні політики і допомагають поширювати інформацію про найкращі та перспективні практики. Управління програм координує та адмініструє всі штатні та місцеві грантові програми, а також виступає прямою лінією зв'язку BJA з штатними, місцевими, племінними та територіальними органами влади, надаючи допомогу та координуючи ресурси. Офіс планування координує планування, комунікації, формування та виконання бюджету; забезпечує загальну координацію в рамках BJA та підтримує зусилля з оптимізації. BJA також підтримує управління спільною Програмою технічної допомоги DHS/DOJ Fusion Process Technical Assistance Program, яка підтримує розробку, впровадження та функціонування центрів злиття.

Глобальна ініціатива з обміну інформацією у сфері правосуддя та Координаційна рада з питань кримінальної розвідки

Створений у травні 2004 року, CICC Global складається з представників правоохоронних органів усіх рівнів влади. Члени CICC є важливим голосом і захисниками штатних, місцевих, племінних і територіальних правоохоронних органів і об’єднаних центрів, підтримуючи їхні зусилля з розвитку та обміну кримінальною розвідкою. Зважаючи на незамінну роль, яку відіграють штатні, місцеві, племінні та територіальні правоохоронні органи у забезпеченні внутрішньої безпеки, вкрай важливо, щоб вони мали право голосу в розробці політики та систем обміну інформацією та розвідданими. CICC має унікальну можливість забезпечити, щоб ці голоси були почуті, і консультує Генерального прокурора США щодо найкращого використання кримінальної розвідки для забезпечення безпеки Сполучених Штатів.

Роль об’єднаних центрів

Згідно з визначенням, наведеним у Посібнику з питань діяльності об'єднаних центрів, об'єднаний центр - це "спільні зусилля двох або більше відомств, які надають ресурси, досвід та інформацію центру з метою максимізації їхньої здатності виявляти, запобігати, розслідувати та реагувати на злочинну та терористичну діяльність". Основними продуктами об'єднаного центру є ситуаційна обізнаність і попередження, підкріплені розвідданими правоохоронних органів, отриманими в результаті застосування розвідувального процесу, в якому формуються вимоги до інформації, необхідної для вжиття заходів, а інформація збирається, інтегрується, оцінюється, аналізується і поширюється.”

Процес розвідки

Основною функцією об’єднаного центру є процес розвідки. Простіше кажучи, процес (або цикл) розвідки - це організований процес, за допомогою якого інформація збирається, оцінюється і розподіляється. На рисунку 2 зображені наступні етапи цього процесу: планування і керівництво, збір, обробка і зіставлення інформації, аналіз і виробництво, поширення і переоцінка (зворотний зв'язок). Об’єднані центри беруть участь у цьому процесі незалежно від їхньої місії (всі злочини, тероризм або всі загрози), дисциплін або зацікавлених сторін, яких вони підтримують (правоохоронні органи, пожежні служби, громадська охорона здоров'я тощо), або типів інформації, яку вони отримують. Цей процес є засобом, за допомогою якого необроблена інформація стає готовим розвідувальним продуктом для використання при прийнятті рішень і формулюванні політики/дій.

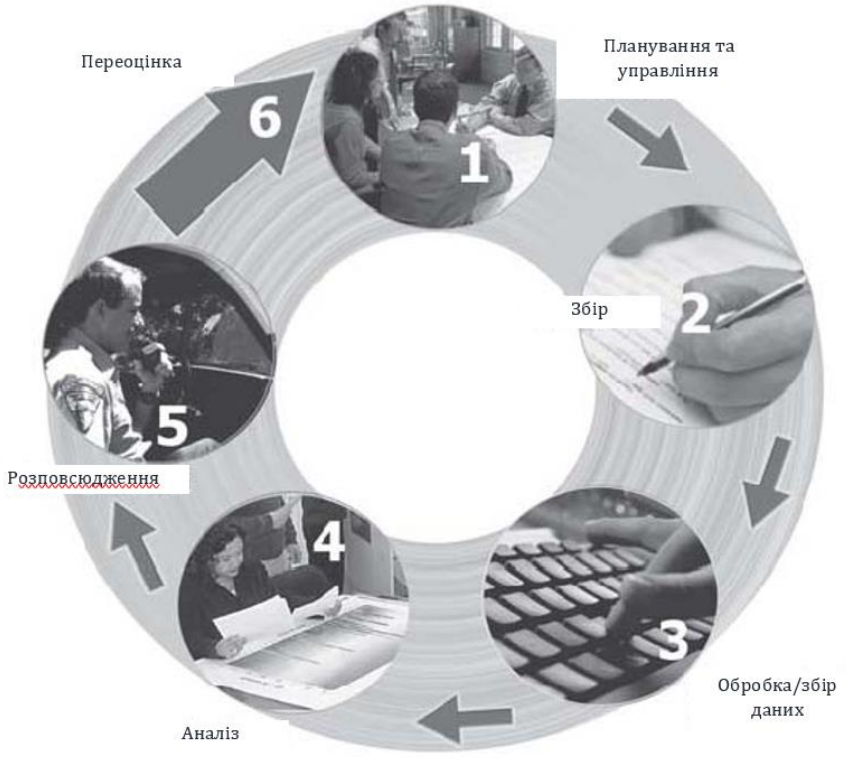


Рисунок 2: Процес розвідки

Процес синтезу: Перетворення інформації та інтелекту на практичні знання

Термін "злиття" означає управління потоками інформації і розвідданих між рівнями і секторами уряду і приватного сектору. Він виходить за рамки створення розвідувального центру або комп'ютерної мережі. Злиття підтримує реалізацію програм запобігання, реагування і подолання наслідків, що ґрунтуються на оцінці ризиків і керуються інформацією. Водночас процес злиття підтримує зусилля з реагування на негайні або нові обставини і події, пов'язані із загрозами. Злиття даних передбачає обмін федеральною і нефедеральною інформацією з різних джерел, в тому числі правоохоронних органів, громадської безпеки і приватного сектору. У поєднанні з відповідним аналізом злиття даних призводить до отримання змістовних і дієвих розвідданих та інформації. Таким чином, процес злиття перетворює інформацію і розвіддані на знання.

Інформація та розвіддані

- **Інформація:** Фрагменти необроблених, неаналізованих даних або повідомлень з різних джерел про подію, злочинну діяльність або суб'єкта, що становить інтерес.
- **Розвіддані:** Результат збору, оцінки та аналізу первинної інформації щодо особи або групи осіб, яку можна ідентифікувати, з метою передбачення, запобігання або моніторингу можливих загроз (наприклад, кримінальної, терористичної або природної діяльності), які можуть виникнути в майбутньому).

"Розвіддані - це інформація, яка була проаналізована для визначення її значення та актуальності."

Процес синтезу також:

- Дозволяє штатним, місцевим, племінним та територіальним органам влади краще прогнозувати та виявляти нові тенденції у сфері злочинності, громадської безпеки та охорони здоров'я;
- Підтримує міждисциплінарне, проактивне, ризик-орієнтоване та орієнтоване на громаду вирішення проблем;
- Забезпечує безперервний потік розвідувальної інформації для посадових осіб, щоб допомогти в розробці картини загроз або небезпек, що розвиваються; і
- Покращує надання екстрених і неекстрених послуг.

Дієва розвідка

Розвідка повинна:

- Намалювати картину;
- Розкажіть історію;
- Скеровувати реагування; і
- Надавати знання, на основі яких можна розробити/рекомендувати план дій для вирішення проблеми.

Керівництво для ф'южн-центру (об’єднаного центру)

Кожен центр адаптує свою сферу діяльності та місію до конкретних потреб юрисдикції, але в Настановах для центрів злиття (ф’южн, об’єднаних) підкреслюється, що всі центри злиття повинні працювати за єдиними принципами. Існує 18 настанов, і в кожній з них обговорюються очікування щодо діяльності таких центрів. Наприклад, усім об'єднаним центрам рекомендується використовувати існуючі системи, бази даних і мережі (такі як Глобальна модель даних розширюваної мови розмітки Міністерства юстиції США (DOJ) і стандарти Національної моделі обміну інформацією (NIEM)). Очікується, що центри злиття також дотримуватимуться Національного плану обміну кримінальною розвідкою, розроблять заяву про місію для визначення цілей і сприятимуть поширенню спільної термінології для всіх залучених зацікавлених сторін.

Базові можливості для центрів злиття штатів і великих міських районів

Керівні принципи для центрів злиття містять додаток під назвою "Базові можливості для центрів злиття штатів і великих міських районів", який містить низку рекомендованих базових можливостей і стандартів або завдань, необхідних для виконання їхньої місії. Базові можливості поділяються на два розділи:

1. Можливості процесу синтезу; та
2. Управлінські та адміністративні можливості.

Розділ "Можливості процесу злиття" присвячений процесу розвідки в об'єднаному центрі, а розділ "Управлінські та адміністративні можливості" - належному управлінню та функціонуванню об'єднаного центру. Вони також надають загальні принципи інтеграції процесів обміну інформацією між об'єднаними центрами і ЕОС, які будуть більш детально розглянуті в розділі "Координація роботи ЕОС і об'єднаних центрів" цього посібника.

Можливості процесу злиття

Сили і засоби процесу злиття стосуються процесу розвідки в центрі злиття, включаючи збір, аналіз і поширення розвідувальних даних (див. Рисунок 2). Процес розвідки є основою процесу злиття і необхідний для функціонування центрів злиття. Процес розвідки розглядається в кожній з наступних сфер:

1. Планування та розробка вимог;
2. Збір інформації та розпізнавання індикаторів і попереджень;
3. Обробка та узагальнення інформації;
4. Аналіз та виробництво розвідувальної інформації;
5. Поширення розвідданих/інформації; та
6. Переоцінка.

Управлінські та адміністративні можливості

Управлінські та адміністративні можливості зосереджені на належному управлінні та функціонуванні центрів злиття. Ці можливості створюють середовище, в якому центри можуть працювати, призначати завдання, розподіляти ресурси та управляти ними, а також розробляти та впроваджувати політику. Управлінські та адміністративні можливості, як правило, включають наступні функції:

1. Менеджмент/управління;
2. Захист конфіденційності інформації;
3. Безпека;
4. Персонал та навчання;
5. IT/комунікаційна інфраструктура, системи, обладнання, приміщення та фізична інфраструктура; та
6. Фінансування.

Функції об’єднаних центрів

Ф'южн-центри збирають, аналізують і поширюють кримінальну, внутрішньо безпекову і терористичну інформацію та розвіддані, а також інформацію про громадську безпеку, правоохоронну діяльність, пожежну безпеку, охорону здоров'я, соціальні послуги, громадські роботи і т.д. Ці розвідувальні дані та інформація є як стратегічними (тобто призначеними для надання рекомендацій щодо загальних тенденцій), так і тактичними (тобто призначеними для конкретної події) і збираються на постійній основі. Національна стратегія обміну інформацією визнає суверенітет суб'єктів, які володіють та/або розглядають можливість управління об'єднаним центром. Місії об'єднаних центрів різняться залежно від середовища, в якому працює центр - деякі з них застосовують підхід, що охоплює всі види злочинів, тоді як інші також включають підхід, що охоплює всі види небезпек. Стратегія підтримує і заохочує ці підходи, поважаючи при цьому принцип, згідно з яким місія об'єднаного центру повинна визначатися на основі потреб юрисдикції.

Штатні, місцеві, племінні та територіальні органи влади, а також суб'єкти приватного сектору заохочуються до співпраці з регіонами штату і UASI для участі в об'єднанні зусиль. Громадськість також слід залучати через програми громадської освіти, які описують попереджувальні знаки і дії, яких слід вжити в разі виявлення підозрілої активності.

Для успішної координації між EOC та об'єднаними центрами дуже важливо, щоб сфера діяльності об'єднаних центрів виходила за рамки правоохоронних органів. У багатьох штатах об'єднані центри включають в свою діяльність або в рамках зв'язку чи інформаційно-просвітницької роботи менеджерів з надзвичайних ситуацій, пожежників, фахівців з небезпечних матеріалів, громадського здоров'я та інших дисциплін. Як правило, ці зусилля, спрямовані на включення потреб і персоналу інших відомств, були надзвичайно успішними і сприяли інтеграції об'єднаних центрів у всі сфери запобігання, захисту, реагування і відновлення. Ця інтеграція також допомагає закріпити довгострокову цінність і життєздатність об'єднаних центрів для підтримки управління надзвичайними ситуаціями і реагування на них.

Базовий потенціал об'єднаного центру: Комплексний підхід до небезпек

Підхід, що враховує всі загрози, стосується готовності до терористичних атак, великих катастроф та інших надзвичайних ситуацій у Сполучених Штатах. В контексті процесу злиття деякі центри злиття визначили свою місію як таку, що включає в себе підхід на випадок усіх небезпек. Хоча застосування підходу, що враховує всі загрози, варіюється, він, як правило, означає, що об'єднаний центр визначив пріоритетні типи великих катастроф і надзвичайних ситуацій, окрім тероризму і злочинів, які можуть статися в межах його юрисдикції. За такого підходу об'єднані центри також збирають, аналізують і поширюють інформацію, яка допоможе відповідним органам (наприклад, правоохоронним органам, пожежним службам, органам охорони здоров'я, управління в надзвичайних ситуаціях, об'єктам критичної інфраструктури тощо) у запобіганні, захисті, реагуванні або відновленні після таких інцидентів. Центр злиття може використовувати підхід, що враховує не всі можливі небезпеки у своїй діяльності. Частиною щорічної оцінки ризиків, яку розробляє (або підтримує розробку) об'єднаний центр, має бути визначення того, яким загрозам штат, територія, плем'я або регіон повинні надавати пріоритет у процесі планування внутрішньої безпеки. Оцінка ризиків може бути використана об'єднаними центрами для формулювання своїх постійних інформаційних потреб (SIN). SIN, в свою чергу, використовуються для керівництва учасниками процесу злиття і їхніми зусиллями зі збору інформації.

Ця сторінка навмисно залишена порожньою.

Роль Центру оперативного реагування на надзвичайні ситуації

ЕОС - це фізичне місце, де відбувається міжвідомча координація реагування. Більшість штатів мають штатні ЕОС, які можуть розширюватися за необхідності для управління подіями, що потребують допомоги на державному рівні. ЕОС допомагають сформувати загальну оперативну картину інциденту, звільняють командування на місці події від тягаря зовнішньої координації і забезпечують додаткові ресурси. Основні функції ЕОС включають координацію, комунікацію, розподіл і відстеження ресурсів, а також збір, аналіз і розповсюдження інформації.

Загальна оперативна картина: Огляд інциденту всіма відповідними сторонами, який надає інформацію про інцидент, що дозволяє Командувачу інцидентом/Об'єднаному командуванню та будь-яким допоміжним установам і організаціям приймати ефективні, послідовні та своєчасні рішення.

ЕОС Організація та структура

Посібник з цивільної готовності 1-20 був останнім федеральним посібником, написаним у 1984 році, в якому розглядалися широкі вимоги до спроможностей ЕОС. Незважаючи на те, що він був переглянутий у 1989 році, з того часу сфера управління надзвичайними ситуаціями зазнала значних змін. Посібник з цивільної готовності 1-20 втратив чинність і був замінений на CPG 601: Проектування та управління центрами управління в надзвичайних ситуаціях. Цей новий федеральний посібник з планування надає інформацію для створення нового ЕОС або модернізації існуючого на основі оцінки та аналізу потреб.

ЕОС можуть бути постійними організаціями та установами, які працюють повний робочий день, або ж вони можуть бути створені для задоволення короткострокових потреб. Постійно діючі ЕОС (або ті, що активуються для підтримки більших і складніших інцидентів), як правило, створюються в центральному або постійно діючому приміщенні. Такі постійні об'єкти в штаті або більшій громаді, як правило, керуються штатним керівником з питань надзвичайних ситуацій. ЕОС можуть бути організовані за основною дисципліною (пожежна охорона, правоохоронні органи, медичні служби тощо), за юрисдикцією (місто, округ, регіон тощо), за ESF (комунікації, громадські роботи, інженерія, транспорт, ресурсне забезпечення тощо) або, що більш ймовірно, за певною комбінацією цих дисциплін.

ЕОС також можуть бути укомплектовані персоналом - з різним рівнем підготовки, а іноді і з додатковими обов'язками, - який представляє різні юрисдикції та функціональні дисципліни, а також має широкий спектр ресурсів. Наприклад, до складу ЕОС, створеної у відповідь на інцидент біологічного тероризму, можуть входити представники правоохоронних органів, управління надзвичайними ситуаціями, громадського здоров'я та медичного персоналу (наприклад, місцеві, штатні або федеральні посадові особи з питань громадського здоров'я і, можливо, представники медичних установ, служб екстреної медичної допомоги тощо).

Фізичний розмір, штат і оснащення ЕОС залежать від розміру юрисдикції, наявних ресурсів і очікуваного обсягу робіт з управління інцидентом. ЕОС можуть бути організовані та укомплектовані різними способами. Незалежно від конкретної організаційної структури, ЕОС повинен виконувати такі основні функції: координація; зв'язок; розподіл і відстеження ресурсів, а також збір, аналіз і розповсюдження інформації; збір, аналіз і розповсюдження інформації.

Функція EOC

У той час як місцева структура управління інцидентом керує діяльністю з ліквідації інциденту на місці події та здійснює командування і контроль над операціями на місці інциденту, EOC активуються за необхідності для підтримки цих місцевих зусиль. Таким чином, EOC є центральним пунктом, з якого координується діяльність за межами місця інциденту. Крім того, деякі штати можуть створювати і використовувати регіональні оперативні центри між місцевим командуванням з ліквідації інциденту і EOC на рівні штату. Головні виборні та призначені посадові особи, а також персонал, який підтримує основні функції, можуть знаходитися в EOC залежно від обов'язків, які вони виконують на своїх посадах. Ці посадові особи часто є членами політичної групи і можуть нести основну відповідальність за прийняття політичних рішень. Основна функція персоналу EOC полягає в тому, щоб гарантувати наявність ресурсів (наприклад, персоналу, інформації, інструментів та обладнання), необхідних для реагування, а також для управління інформацією для громадськості. Крім того, урядові департаменти (або агентства, бюро тощо) чи приватні організації можуть мати відомчі операційні центри (DOC), які слугують сполучною ланкою між поточними операціями цієї організації та операціями з ліквідації наслідків надзвичайних ситуацій, які вона підтримує. DOC може безпосередньо підтримувати інцидент і отримувати інформацію, пов'язану з його операціями. У більшості випадків, DOC фізично представлені в об'єднаному відомчому EOC уповноваженими агентами департаменту або відомства.

Після активації EOC необхідно встановити зв'язок і координацію між командуванням інцидентом і EOC. Крім того, EOC на всіх рівнях влади і в різних функціональних відомствах повинні мати можливість належного зв'язку з іншими EOC, у тому числі з тими, що утримуються приватними організаціями. Системи зв'язку між EOC повинні бути надійними і містити вбудовані резерви. Ефективне функціонування EOC часто залежить від наявності угод про взаємодопомогу та спільних комунікаційних протоколів між відомствами-учасниками.

ЕОС активується для підтримки реагування на місці події під час ескалації інциденту. Активація ЕОС звільняє командувача інцидентом від тягаря зовнішньої координації та забезпечення додаткових ресурсів.

- ЕОС –це:
  - Фізичне місцезнаходження;
  - Укомплектований персоналом, який пройшов підготовку та уповноважений представляти відомство/дисципліну;
  - Оснащений механізмами для зв'язку з місцем інциденту та отримання ресурсів;
  - Управляється за допомогою протоколів; і
  - Використовується на всіх рівнях влади.
- До складу ЕОС входить персонал та обладнання, що відповідає рівню інциденту.
- ЕОС використовується:
  - Різними способами на всіх рівнях влади та в приватному секторі; і
  - Забезпечення координації, керівництва та підтримки під час надзвичайних ситуацій.
- ЕОС повинен:
  - Сприяти функціонуванню системи міжвідомчої координації (MACS) і може знадобитися для підтримки територіального командування, командування інцидентом або об'єднаного командування, коли потреби в ресурсах перевищують місцеві можливості;
  - Забезпечити перехід до відновлення; і
  - Активуватися в очікуванні події.
- ЕОС не командує на тактичному рівні інцидентом на місці події.

ЕОС повинні бути гнучкими та масштабованими. Під час інциденту вони, як правило, виконують загальні функції; однак, не всі функції системи будуть виконуватися під час кожного інциденту, і функції можуть виникати не в певному порядку. Первинні функції можуть включати наступне:

- Оцінка ситуації;
- Визначення пріоритету інциденту;
- Отримання та розподіл критично важливих ресурсів;
- Політичне керівництво відповідним управлінням інцидентами та міжвідомчою діяльністю;
- Координація з Регіональними центрами координації реагування FEMA (RRCC);
- Координація з іншими елементами MACS;
- Координація з обраними та призначеними посадовими особами;
- Координація зведеної інформації; і
- Інформування громадськості.

Міжвідомча координаційна система: Основна функція MACS - координувати діяльність вище польового рівня і визначати пріоритетність потреб інциденту в критично важливих або конкуруючих ресурсах, тим самим сприяючи координації операцій на місцях. MACS складається з комбінації елементів, таких як персонал, процедури, протоколи, бізнес-практики та комунікації, інтегровані в загальну систему.

Операційний обмін інформацією

Основна увага центрів реагування на надзвичайні ситуації зосереджена на реагуванні та відновленні після природних і техногенних інцидентів. Хоча цілі ЕОС та об'єднаного центру суттєво відрізняються, важливо, щоб ці дві організації працювали разом і розуміли цілі та пріоритети одна одної, а також те, в чому їхні місії можуть бути схожими або перетинатися. Як мінімум, ЕОС повинні налагодити тісний зв'язок з об'єднаними центрами для обміну практичною інформацією. Плани і процедури об'єднаних центрів повинні включати інформацію про те, як центр буде підтримувати ЕОС до, під час і після події або інциденту.

Процеси обміну інформацією повинні починатися на ранніх стадіях планування (тобто, до інциденту, з визначення ролі об'єднаного центру на стадіях розробки планів реагування та аналізу небезпек). Під час аналізу небезпек юрисдикція вивчає небезпеки, які можуть вплинути на громаду, а потім кількісно оцінює ризики, пов'язані з кожною небезпекою. Після завершення аналіз небезпек, проведений громадою, має стати основою для всього процесу планування на випадок надзвичайних ситуацій та розробки планів реагування на надзвичайні ситуації (EOP). EOP визначає загальні повноваження, ролі та функції, що виконуються під час надзвичайних ситуацій, активується для керівництва заходами з реагування на надзвичайні ситуації та відновлення, а також визначає об'єкт, який буде виконувати функції ЕОС під час надзвичайних ситуацій.

Залежно від юрисдикційних повноважень, об'єднані центри можуть відігравати важливу роль у наданні інформації та розвідувальних даних для підтримки завершення або оновлення аналізу небезпек і відповідного плану дій під час НС. Крім того, будь-яка інформація про конкретні інциденти або події, що можуть вплинути на юрисдикцію - або дозволять юрисдикції бути краще підготовленою - повинна передаватися керівнику з питань надзвичайних ситуацій і, можливо, всьому персоналу ЕОС. ЕОС можуть забезпечити об'єднаний центр ситуаційною обізнаністю про події, що відбуваються, і слугувати пунктом оповіщення під час активації.

Що таке аналіз небезпек?

Аналіз небезпек передбачає вивчення ймовірних загроз, які можуть вплинути на громаду, та кількісну оцінку ризику, пов'язаного з кожною з них. Небезпеки - це умови або ситуації, які потенційно можуть завдати шкоди людям, майну або навколишньому середовищу. Небезпеки можна поділити на три категорії:

- Природні (наприклад, торнадо та землетруси);
- навмисні (наприклад, тероризм або громадські заворушення); і
- Технологічні (наприклад, збій в електромережі або розлив небезпечних матеріалів)).

Сам аналіз небезпек складається з трьох етапів:

Крок 1: Ідентифікувати небезпеки. Складіть перелік небезпек, які можуть виникнути в громаді. Цей перелік зазвичай базується на історичних даних про минулі події. Джерелами інформації про минулі події можуть бути газетні підшивки, записи про погоду, страхові записи, звіти про нещасні випадки, записи ЕОС, результати перевірок пожежної служби та невигадана інформація від мешканців, які живуть у громаді тривалий час.

Крок 2: Розробка профілів небезпек. Розробити профіль кожної ідентифікованої небезпеки відповідно до наступних характеристик:

- Передбачуваність (наприклад, частота та/або ймовірність виникнення, сезонність тощо);
- Масштаб або серйозність впливу на громаду (наприклад, обсяг очікуваної шкоди, типи пошкоджень, які можна очікувати для інфраструктури тощо);
- Швидкість настання (наприклад, урагани зазвичай мають певний час на підготовку перед тим, як завдати удару, тоді як землетруси або вибухи можуть статися без попередження); і
- Потенціал каскадних ефектів (наприклад, повені після урагану або пожежі після землетрусу через розриви газопроводів).

Крок 3: Визначення ризику за допомогою аналізу небезпек. Після збору інформації про кожну загрозу, до якої вразлива громада, необхідно оцінити ризики, пов'язані з кожною загрозою, щоб група планування могла передбачити і підготуватися до тих, що мають найбільший потенційний вплив на людей, служби, об'єкти та споруди. Оцінюючи ризики, важливо пам'ятати про таку ієрархію пріоритетів реагування:

1. Безпека життєдіяльності. Умови, які можуть вплинути на здоров'я та/або безпеку населення;
2. Об'єкти життєзабезпечення. Об'єкти, такі як пожежні депо, поліцейські дільниці або очисні споруди, які в разі ураження небезпекою можуть серйозно і негативно вплинути на здатність громади до реагування; і
3. CIKR. Дороги, інженерні комунікації та інші компоненти інфраструктури, пошкодження яких може серйозно і негативно вплинути на безпеку життя або можливості реагування.

Сталий стан: Сталий стан - це позиція для рутинних, нормальних, повсякденних операцій і ситуаційної обізнаності, на відміну від тимчасових періодів підвищеної бойової готовності або реагування в режимі реального часу на загрози чи інциденти.

Оскільки багато ЕОС мають обмежені кадрові ресурси, аналітики розвідки з штатних або міських об'єднаних центрів можуть бути залучені для посилення взаємодії між об'єднаними центрами та ЕОС (фізично або віртуально), а також для забезпечення зв'язку під час інциденту. Деталі доповнення штату ЕОС персоналом об'єднаних центрів повинні бути включені в Меморандум про взаєморозуміння між двома центрами і включати як стаціонарний, так і активний стан операцій ЕОС. У багатьох випадках центри злиття розташовуються в одному приміщенні або в безпосередній близькості від ЕОС. ЕОС також може розглянути можливість створення робочої групи з персоналу, призначеного для зв'язку з об'єднаним центром, коли ЕОС не активований, щоб персонал міг ознайомитися з діяльністю та операціями об'єднаного центру. В юрисдикціях, де програма зв'язку з об'єднаними центрами є офіційно затвердженою, може вже існувати штат кваліфікованого персоналу.

ЕОС повинні планувати можливість доступу до інформації та обміну нею з об'єднаними центрами, а також з іншими організаціями, і використовувати для цього такі системи, як Регіональна система обміну інформацією (RISS), Правоохоронні органи онлайн (LEO) та Інформаційна мережа національної безпеки (HSIN).
Крім того, ЕОС повинні забезпечити вжиття заходів безпеки при передачі інформації з об'єднаного центру. Ці запобіжні заходи можуть включати обмеження поширення інформації відповідним персоналом, призначеним в ЕОС, підписання угод про нерозголошення і забезпечення того, щоб члени, які мають доступ до цієї інформації, пройшли перевірку на наявність громадянства США і були зобов'язані знати.

Координаторам з ліквідації наслідків надзвичайних ситуацій також потрібна інша інформація, зокрема, дані про погоду, геопросторові знімки і знімки дистанційного зондування, оцінки збитків, повідомлення ЗМІ, фінансові наслідки і соціальні наслідки. Їм може знадобитися допомога в зборі цієї інформації про подію або інцидент для цілей планування, реагування і/або відновлення. Персонал об'єднаного центру також може бути корисним у зборі інформації від джерел НС, особливо коли НС перебуває в активному стані і має більшу потребу в інформації для прийняття рішень.

Управління інформацією та розвідкою: Важливо, щоб організація з управління інцидентами встановила процес збору, обміну та управління інформацією та розвідданими, пов'язаними з інцидентом. Нижче наведено приклади інформації та розвідувальних даних, що використовуються для управління інцидентом:

- Оцінка ризиків;
- Медична розвідка (тобто спостереження);
- Інформація про погоду;
- Геопросторові дані;
- Структурні проекти;
- рівні токсичних забруднювачів; і
- дані про комунальні та громадські роботи.

Низка об'єднаних центрів перебуває на різних етапах розробки формалізованих процесів і процедур запиту, доступу та використання геопросторових даних для підтримки планування та реагування на всі види небезпек. Корисні геопросторові дані можуть охоплювати діапазон від аерофотозйомки до/після, супутникових знімків до точного розташування водозаборів у заплаві до місць розташування активів CIKR. Центри злиття повинні займатися ретельним плануванням, щоб бути готовими запитувати, отримувати доступ і ефективно використовувати геопросторові ресурси.

Див. додаток D: Розробка процесів отримання і використання геопросторової інформації для підтримки планування і реагування на всі види небезпек для отримання додаткової інформації.

Координація роботи EOC та об’єднаного центру

Координація та/або інтеграція роботи EOC і центрів злиття вимагає ретельного планування і координації. Для цього процесу рекомендуються наступні кроки. В рамках кожного кроку розглядаються відповідні базові можливості об'єднаного центру злиття.

Як центр злиття, так і EOC залучають до обговорення ресурси, можливості, продукти/звіти і проблеми, що викликають занепокоєння. Для розбудови довгострокових робочих відносин, які включають навчання і тренування, необхідне ретельне планування. Відкритий діалог із самого початку дозволить обом сторонам вирішити проблеми і розробити механізм управління для підтримки процесу.

Базові можливості об’єднаного центру:

I. Можливості процесу злиття:

A. Планування та розробка вимог

8. **Координація з посадовими особами, відповідальними за реагування та відновлення.** Об'єднані центри повинні визначати та координувати з керівниками аварійних ситуацій, відповідним персоналом з реагування та відновлення і оперативними центрами розробку, впровадження та підтримку плану та процедур для забезпечення спільного розуміння ролей та обов'язків, а також для забезпечення можливості використання можливостей розвідки та аналізу для підтримки оперативних заходів з управління надзвичайними ситуаціями, у разі необхідності, коли події вимагають такого реагування.

Крок перший: Ознайомлення з можливостями, потребами та вимогами

Перш ніж укладати угоди або розробляти політику, керівники EOC і центру злиття повинні зустрітися, щоб обговорити свої можливості та потреби/вимоги.

Кожен центр повинен підготувати для іншого перелік своїх можливостей, продуктів, оцінок і звітів, які вони виробляють, а також своїх інформаційних потреб/вимог, постійних інформаційних потреб (SIN) і/або основних елементів інформації (EEI). Особливо важливо, щоб EOC точно визначив, яка саме інформація або розвідувальні дані йому потрібні (тобто, його EEI), навіщо вони йому потрібні і коли вони йому потрібні. Це може варіюватися між нормальним робочим часом (стабільний стан) і часом, коли інцидент накопичується, відбувається (активний стан) і, врешті-решт, повертається до стабільного стану. Якщо існують певні графіки, встановлені для продуктів EOC, таких як брифінги або звіти про ситуацію, EOC повинен забезпечити, щоб об'єднаний центр був про них поінформований. Крім того, EOC повинен мати можливість описати звіти і продукти, які він може розробити і надати об'єднаному центру, особливо ті, що стосуються інцидентів, пов'язаних з усіма видами небезпек або природними катастрофами.

Елементи даних Національного центру координації реагування FEMA (NRCC)

FEMA визначило 26 IOI. Крім того, були розроблені Плани збору інформації для конкретних інцидентів (ICP), щоб перетворити EEI на конкретні інформаційні вимоги.

Основні елементи інформації

- Межі зони стихійного лиха/пункти доступу
- Юрисдикційні межі
- Соціальні/економічні/політичні наслідки
- Стан транспортної системи
- Стан системи зв'язку
- Стан ключових федеральних/штатних об'єктів
- Інформація про конкретну небезпеку
- Важливі погодні умови
- Сейсмічні або інші геофізичні дані
- Статус критично важливого об'єкта
- Статус повітряної розвідки
- Ключовий офіційний статус
- Статус активації/деактивації ESF
- Статус оголошення стихійного лиха/надзвичайної ситуації
- Основні проблеми/заходи у ESF
- Дефіцит ресурсів
- Обмежуючі фактори
- Пріоритети реагування
- Заплановані або майбутні заходи
- Пожертви

Плани збору інформації

- Землетрус
- Епідемія-Пандемія
- Повінь
- Загальні
- Небезпечні матеріали
- Ураган
- Атомна станція
- Відключення електроенергії
- Терорист
- Торнадо
- Цунамі
- Вулкан
- Зимовий шторм

Відвертий діалог про потреби кожного центру забезпечить краще розуміння потенційних обмежень, які необхідно подолати, щоб задовольнити ці потреби. Без такого діалогу було б легко передавати непотрібні або непридатні для використання продукти чи інформацію в надії поділитися достатньою кількістю потрібної інформації. Забезпечення обміну своєчасною, точною і придатною для використання інформацією є ключем до такої успішної взаємодії.

Стандартні політики та процедури

Розуміння CONOPS і SOP один одного допоможе об'єднаним центрам і EOC сформулювати план спільної роботи. Багато об'єднаних центрів розробили CONOPS і SOP, які включають в себе Настанови для об'єднаних центрів і Базові можливості. Цими документами слід поділитися з EOC, і можна розробити нові SOP для врегулювання робочих взаємовідносин між ними. SOP є особливо важливими для нового персоналу, який призначається на роботу в будь-яку структуру під час кризи або катастрофи. Під час сесій планування слід переглядати SOP, щоб переконатися, що вони є актуальними. Персонал повинен бути навчений цим SOP, а самі SOP повинні застосовуватися та оцінюватися, щоб переконатися, що вони є точними та застосовними.

Комунікаційні інструменти

Здатність обмінюватися інформацією та спілкуватися за допомогою різних засобів до, під час та після інциденту має важливе значення. Тому ЕОС та об'єднані центри повинні переглянути поточні процеси, щоб визначити, як ця комунікація відбуватиметься на всіх необхідних рівнях класифікації.

- Які інструменти доступні для ЕОС та центрів злиття для надсилання, отримання та управління інформацією?
  - Чи сумісні інструменти між собою?
  - Чи мають інструменти обмежені права доступу?
  - Чи використовувалися інструменти?
- Які інструменти реального часу використовуються під час інциденту?
- Чи має центр злиття або ЕОС потенціал для створення порталів для обміну інформацією в Інтернеті? Як щодо електронної пошти та списків розсилки?
  - Чи може ЕОС отримувати, зберігати та обробляти секретну інформацію?
  - Чи має ЕОС та центр злиття можливості захищеного зв'язку?

Базові можливості об’єднаного центру:

II. Управлінські та адміністративні можливості:

E. Інформаційні технології / комунікаційна інфраструктура, системи, обладнання, приміщення та фізична інфраструктура

3. План комунікацій - ф'южн-центри повинні мати план забезпечення безпечного, захищеного та надійного зв'язку, включаючи політику та можливості аудиту. (Вказівка 18, Настанова для центрів злиття)

a. Визначити, як партнери об'єднаного центру будуть спілкуватися під час інциденту або надзвичайної ситуації. Переконайтеся, що існуючі засоби зв'язку сумісні між собою.

b. Включити поточні комунікаційні плани, що використовуються правоохоронними органами та службами екстреної допомоги.

Бази даних

Які програмні додатки та бази даних використовують або до яких мають доступ об’єднані центри та ЕОС? Чи сумісне програмне забезпечення? Якщо так, то як воно буде пов'язане і для яких цілей? Якщо ні, чи потрібно внести зміни, щоб зробити його сумісним?

- CIKR бази даних
  - Автоматизована система управління критично важливими активами (ACAMS)
- Можливості географічних інформаційних систем (GIS)
- LEO
- RISS
- HSIN

- Мережа даних національної безпеки (HSDN)
- Віртуальний EOC або інші програмні додатки для управління надзвичайними ситуаціями
- Системи оповіщення та обміну інформацією в галузі охорони здоров'я, такі як Мережа оповіщення про стан здоров'я (HAN), Обмін епідемічною інформацією (Epi-X), Інформаційна мережа громадського здоров'я (PHIN) та Національна електронна система нагляду за захворюваннями (NEDSS)
- Ситуаційна обізнаність або системи спостереження/попередження
- Інші засекречені і незасекречені IT-платформи та платформи для обміну розвідданими

Кадрове забезпечення

До складу персоналу об'єднаних центрів входять співробітники правоохоронних органів, а також аналітики з питань розвідки, боротьби зі злочинністю та/або CIKP. Крім того, як і в EOC, в об'єднаних центрах часто працюють фахівці зі спеціалізованими знаннями, зокрема, з пожежної охорони, охорони здоров'я та/або управління і реагування на надзвичайні ситуації. При обговоренні можливостей та потреб/вимог до персоналу об'єднані центри та EOC повинні обговорити спеціалізовані знання та досвід, якими володіє їхній центр, а також вивчити додаткові можливості для взаємодії. Крім того, листи про згоду (LOA) або меморандуми про взаєморозуміння можуть допомогти у формалізації та виконанні узгоджених обов'язків. (Див. Крок другий)

Керівники також повинні вирішити, чи потрібні співробітникам допуски до секретної інформації на випадок необхідності обміну секретною інформацією між центром злиття і EOC. Керівники повинні визначити співробітників, які потребують допуску до секретної інформації, і через об'єднаний центр звернутися до DHS з проханням надати їм такий допуск.

Навчальні ресурси

- Які навчальні інструменти/програми наразі використовуються в EOC та об’єднаному центрі?
- Що можна зробити для сприяння перехресному навчанню персоналу?
  - Персонал об'єднаного центру повинен пройти навчання з питань NIMS, ICS та оперативних процедур EOC.
  - Персонал EOC або відповідний персонал з управління в надзвичайних ситуаціях повинен пройти навчання з питань роботи об'єднаного центру, а також протоколів обміну розвідданими та інформацією, таких як:
    - Політика конфіденційності та безпеки;
    - Отримання/обробка секретної та несекретної інформації;
    - Отримання/обробка інформації кримінальної розвідки відповідно до Розділу 28 Кодексу федеральних нормативних актів (CFR), частина 23;
    - Захист конфіденційності інформації та інших законних прав у контексті середовища обміну інформацією1; та
    - Отримання/обробка інформації, пов'язаної з CIKR, такої як захищена інформація про критичну інфраструктуру (PCII), чутлива інформація з питань безпеки (SSI), інформація про вразливість до хімічного тероризму (CVI) та/або інформація про гарантії (SGI).

[1] Додаткові ресурси та тренінги з питань недоторканності приватного життя та громадянських свобод у середовищі обміну інформацією доступні за посиланням http://www.it.ojp.gov/PrivacyLiberty and http://www.ise.gov/pages/privacy-overview.aspx.

- Які тренінги необхідно розробити, щоб заповнити прогалини?
- Чи проводяться вправи між центрами для налагодження відносин і взаємодії? (Див. Крок четвертий)
- Чи переглядається державний календар навчань на предмет можливості перевірити очікувану взаємодію?

Наявна та доступна інформація

Перш ніж визначати, якою інформацією можна буде обмінюватися і як саме, важливо, щоб ЕОС описали, яку інформацію вони хотіли б отримувати від центру злиття і навпаки. Щоб визначити ці потреби/вимоги, центр злиття і ЕОС повинні описати свої поточні процеси, можливості і продукти, які вони розробляють і якими вони обмінюються. Описавши поточний ландшафт, відповідні центри можуть визначити, яку інформацію вони хотіли б отримувати і як вони хотіли б її отримувати.
Крім того, знання потреб/вимог замовника допоможе сформувати продукти, що виробляються, або виявити прогалини в інформації, які центр злиття або ЕОС можуть заповнити, створюючи нові продукти або звіти.

ЕОС та всі, хто отримує інформацію від центру злиття, повинні дотримуватися політики конфіденційності центру злиття та політики розповсюдження інформації, залежно від обставин. Крім того, перед отриманням інформації від правоохоронних органів або розвідки, ЕОС повинні розробити і дотримуватися політики захисту, щоб забезпечити належне поводження з цією інформацією, не передавати її ЗМІ або громадськості і знищувати належним чином. ЕОС повинні вирішити це питання шляхом розробки власної політики або плану, прийняття політики або плану безпеки центрів злиття або шляхом підписання меморандуму про взаєморозуміння з центром злиття.

Базові можливості об’єднаного центру:

I. Можливості процесу злиття:

D. Аналіз та виробництво розвідувальних даних

1. ***Аналітичні продукти.*** *Центри злиття повинні розробити, впровадити та підтримувати виробничий план, який описує типи аналізів та продуктів, які вони мають намір надавати своїм клієнтам та партнерам, як часто або за яких обставин продукт буде вироблятися, а також як кожен тип продукту буде розповсюджуватися.*

   c. *Визначте зацікавлені сторони та клієнтську базу для конкретних лінійок продуктів і запросіть зворотній зв'язок від клієнтів, щоб керувати майбутніми продуктами.*

   d. *Забезпечити виробництво розвідувальних продуктів з доданою вартістю, які підтримують розробку програм запобігання, захисту, реагування та подолання наслідків, що базуються на результатах діяльності та враховують ризики.*

Центри злиття виробляють різноманітні продукти для своїх клієнтів, включаючи щоденні, щотижневі та/або щомісячні розвідувальні звіти, спеціальні бюлетені, що описують загрози або проблеми зі злочинністю, звіти про тенденції злочинності, бюлетені про безпеку офіцерів, повідомлення про необхідність бути напоготові, тактичні аналітичні звіти та відповіді на запити про надання інформації (RFI).
Несекретні звіти, що стосуються діяльності та обов'язків ЕОС, повинні надаватися ЕОС для покращення його обізнаності щодо ситуації та створення загальної картини роботи. Періодичність надання звітів має бути взаємно узгоджена з розумінням того, що обидві сторони повинні брати участь в обміні інформацією. Ці домовленості можуть стосуватися того, як юрисдикції, правоохоронні органи і спільнота громадської безпеки спілкуються з об'єднаними центрами і ЕОС, а також як об'єднані центри спілкуються з розвідувальним співтовариством. Питання, які впливають на обмін інформацією між центром злиття і ЕОС, мають кілька складових - першою з них є рівень секретності інформації і рівні секретності, якими володіють учасники ЕОС.

Як правило, більшість співробітників ЕОС не мають допуску до секретної інформації, тому інформація, яку вони отримують, може бути обмежена грифом "ДЛЯ ОФІЦІЙНОГО ВИКОРИСТАННЯ" (UNCLASSIFIED) або "ТІЛЬКИ ДЛЯ ОФІЦІЙНОГО ВИКОРИСТАННЯ" (FOUO). Надання початкових відомостей про засекреченість зменшить занепокоєння персоналу ЕОС щодо типів інформації, яку вони можуть або не можуть отримати. Друга ситуація може бути пов'язана з кримінальним розслідуванням, яке може бути скомпрометоване широким розповсюдженням або несанкціонованим чи ненавмисним розголошенням інформації.

Critical Infrastructure represent assets, systems andnetworks, whether physical or virtual, so vital to a community and/or the United States that the incapacityor destruction of such assets, systems or networks would have a debilitating impact on the community's orthe country's security, continuity of government, continuity of operations, public health, public consciousness or a combination of these effects.

Key Resources represent publicly or privately controlled resources essential to the minimal operationsof the economy and government.

Крім того, будь-який персонал, у тому числі з ЕОС, якому може знадобитися інформація з баз даних правоохоронних органів або доступ до них, повинен бути належним чином перевірений, щоб забезпечити дотримання обмежень доступу або 28 CFR, частина 23. 28 CFR, частина 23 - це інструкція для правоохоронних органів. Цей нормативний акт містить стандарти впровадження систем кримінальної розвідки, що фінансуються з федерального бюджету та знаходяться в різних юрисдикціях. Він також містить вказівки щодо подання та введення інформації кримінальної розвідки, безпеки, розслідування, розповсюдження, а також процесу перегляду та очищення.

Зрештою, об'єднаний центр повинен буде визначити, чи поширювати цей тип інформації, а також оцінити вплив будь-яких потенційних штатних, місцевих або федеральних законів і нормативних актів, таких як обмеження 28 CFR, частина 23.

Крім того, об'єднаний центр може бути сховищем інформації CIKR, якою можна ділитися з ЕОС під час інциденту, а також використовувати її для надання допомоги в проведенні відповідних заходів з реагування та відновлення. З ростом і розвитком програм аналізу розвідданих і захисту інфраструктури вони, ймовірно, будуть розміщені в об'єднаних центрах. Такий зв'язок посилює можливості обміну інформацією.

Безперервність діяльності

Планування та можливості забезпечення безперервності операцій (COOP) можуть бути додатковою сферою спільного інтересу. Більшість ЕОС обладнані резервними джерелами живлення, мають альтернативні робочі майданчики і покладаються на добре розроблені плани. Керівники аварійних служб можуть допомогти об'єднаним центрам у розробці відповідних планів COOP, включаючи визначення або спільне використання альтернативних майданчиків і засобів зв'язку для продовження виконання основних функцій об'єднаних центрів. Така координація між об'єднаним центром і ЕОС може також забезпечити спільне використання будь-яких резервних ресурсів, а також надання взаємодопомоги у разі виникнення інциденту або збою.

Базові можливості об’єднаного центру:

II. Управлінські та адміністративні можливості:

E. Інформаційні технології/комунікаційна інфраструктура, системи, обладнання, приміщення та фізична інфраструктура

4. *Плани на випадок надзвичайних ситуацій та забезпечення безперервності роботи - Центри злиття повинні мати плани на випадок надзвичайних ситуацій та забезпечення безперервності роботи для забезпечення безперервного виконання критично важливих для місії процесів та інформаційно-технологічних систем під час події, що призводить до виходу цих систем з ладу, а також, за необхідності, для забезпечення виконання основних функцій в альтернативному місці під час надзвичайної ситуації. (Вказівки 9, 10 і 18, Посібник для Центру злиття).*

   b. *Розробка планів у координації з керівниками аварійних служб та іншими відповідними посадовими особами з питань реагування та відновлення.*

   c. *Чітко визначте ролі та обов'язки персоналу під час надзвичайних ситуацій.*

Крок другий: встановлення партнерських відносин

Після того, як керівники EOC та об'єднаного центру зрозуміють можливості один одного, вони повинні працювати разом над встановленням партнерських відносин між установами. Важливою є підтримка на рівні виконавчої влади для координації або інтеграції між EOC та об'єднаними центрами. Деякі держави вважають корисним проведення зустрічей з керівниками об'єднаних центрів, правоохоронних органів та агентств з управління надзвичайними ситуаціями для розробки єдиного, узгодженого плану реагування (включаючи протоколи обміну інформацією під час реагування на інцидент). Об'єднані центри, ймовірно, залучатимуть до цього процесу свої керівні органи. Регулярна взаємодія і налагодження відносин допомагає створити середовище співпраці для обміну інформацією. Ця концепція особливо актуальна для штатів або юрисдикцій з новостворених або менш потужними об'єднаними центрами.

EOC та центр злиття повинні інформувати один одного про політику, процедури та протоколи. Зустрічі між керівниками EOC та центрів злиття повинні проводитися через регулярні проміжки часу, щоб сприяти постійному розумінню та оцінці ролей, обов'язків та поточної діяльності кожного з центрів.
Крім того, управління персоналом має розглянути можливість перехресного навчання персоналу для забезпечення міжвідомчого ознайомлення з відповідними процесами та процедурами (наприклад, співробітники EOC повинні знати, як поводитися з чутливою або секретною інформацією). Така регулярна та рутинна взаємодія допоможе навчати обидві установи та сприятиме співпраці і є найважливішим елементом у розвитку відносин співробітництва.

Базові можливості об’єднаних центрів:

II. Управлінські та адміністративні можливості:

A. Менеджмент/управління

1.b. До складу керівного органу центру мають увійти представники штатних і місцевих правоохоронних органів та органів громадської безпеки. Це посилить спроможність центру виконувати ключові базові функції, зокрема:

i.b. Підтримка заходів з управління надзвичайними ситуаціями, реагування та планування відновлення на основі ймовірних сценаріїв загроз та об'єктів, що перебувають у зоні ризику.

Обмін персоналом, участь у програмах офіцерів зв'язку (або створення таких програм) і створення робочих груп можуть сприяти зміцненню комунікації. Співробітники об’єднаного центру, які також працювали в ЕОС, будуть краще підготовлені до налагодження відносин з персоналом ЕОС і передбачення інформаційних потреб ЕОС.

Після встановлення партнерства необхідно формалізувати меморандуми про взаєморозуміння, SOP та/або CONOPS, щоб задокументувати ролі та обов'язки. Меморандуми про взаєморозуміння повинні бути розроблені між центром злиття і координуючим агентством ЕОС. Метою такого документа є уточнення ролей кожного суб'єкта під час активації ЕОС.

Партнерство "Сейфгард Айова" розробило посібник з кодексу поведінки для своїх зв'язкових, які працюють в ЕОС. Посібник з кодексу поведінки допомагає гарантувати, що всі координатори розуміють свої ролі та обов'язки під час перебування в ЕОС.

Додаток E: Державно-приватне партнерство: Посібник з Кодексу поведінки для зв'язкових, які працюють в операційних центрах з ліквідації наслідків надзвичайних ситуацій Партнерства "Сейфгард Айова" для отримання додаткової інформації.

На додаток до цієї переваги, меморандуми про взаєморозуміння можуть також використовуватися для вирішення політичних конфліктів між сторонами. Однак юрисдикціям слід пам'ятати, що отримання відповідних підписів під меморандумом про взаєморозуміння може бути трудомістким і складним процесом, частково через велику кількість сторін, які мають розглянути та затвердити документ. Конкуруючі інтереси, штатні чи місцеві закони або правила організації, а також непорозуміння можуть сповільнити або зупинити цей процес. Меморандуми про взаєморозуміння можна використовувати як засіб вирішення політичних конфліктів між сторонами.

Оскільки Меморандум про взаєморозуміння може бути об'ємним і визначати загальні взаємовідносини, а також деякі деталі операції, в ньому можуть бути прописані всі операційні можливості, ролі та вимоги. Приклад меморандуму про взаєморозуміння наведено в Додатку B.

Крок третій: Визначте процес

Процедури обміну інформацією

Необхідно розробити угоди, що описують, якою інформацією та розвідувальними даними будуть обмінюватися між ЕОС та об'єднаним центром, а також яким чином буде здійснюватися обмін цими даними. Коли об'єднаний центр передає інформацію до ЕОС, необхідно чітко вказати одержувачів інформації (беручи до уваги рівень допуску до неї), а також цільове призначення цієї інформації. Як обговорювалося на першому етапі, ЕОС повинні надати об'єднаним центрам список персоналу, до якого можна звертатися з приводу чутливої та секретної інформації. У свою чергу, об'єднані центри повинні бути готові ділитися відповідною інформацією з ЕОС з таких питань, як розвіддані про катастрофи або злочинну діяльність (у форматі, який не створює конфлікту для співробітників ЕОС, які не мають допуску до секретної інформації), а також з питань, що стосуються).

Процедури обміну інформацією між EOC та об'єднаним центром повинні також враховувати існуючі процедури обміну інформацією між EOC, DHS та правоохоронними органами. Наприклад, якщо у керівників служб з надзвичайних ситуацій вже є процедури для безпосереднього спілкування з поліцією, пожежною службою та управлінням шерифа, як це може вплинути на процес обміну інформацією між EOC та об'єднаними центрами?

Оскільки об'єднані центри можуть мати пряме представництво в EOC - або через представника об'єднаного центру, або через ESF-13 - EOC повинен використовувати об'єднаний центр як канал зв'язку та обміну інформацією з розвідувальним співтовариством. Розвіддані і інформація повинні проходити через об'єднаний центр, а потім надсилатися до EOC. І навпаки, інформаційні і розвідувальні продукти, такі як звіти про ситуацію, плани дій на випадок інцидентів і довгострокові плани, повинні розповсюджуватися серед персоналу об'єднаного центру, щоб показати поточні і майбутні пріоритети і проблеми, які турбують EOC. Таким чином, аналітики об'єднаного центру можуть бути обізнані з інформаційними потребами або вимогами, які можуть мати відношення до EOC.

Базові можливості об’єднаних центрів:

II. Управлінські та адміністративні можливості

A. Менеджмент/управління

3. Середовище для співпраці - Центри злиття повинні визначити організації, які представляють їхні основні (постійні) та спеціальні зацікавлені сторони, а також ролі та обов'язки кожної із зацікавлених сторін, і розробити механізми та процеси, що сприятимуть створенню середовища для співпраці з цими зацікавленими сторонами. (Керівні принципи 4 і 5, Посібник для ф'южн-центрів)

b. Включити визначення організацій та осіб, відповідальних за планування, розробку та реалізацію заходів із запобігання, захисту, реагування та ліквідації наслідків на штатному, місцевому та племінному рівнях.

f. Розробити та впровадити Меморандум про взаєморозуміння (MOU) або Угоду (MOA) та, за необхідності, угоди про нерозголошення (NDA) між центром та кожною зацікавленою стороною, яка має намір брати участь у роботі або співпрацювати з центром злиття.

Програма офіцерів зв'язку (FLO) - це координація мережі офіцерів зв'язку центрів злиття, які є представниками правоохоронних органів, пожежної служби, охорони здоров'я та інших відомств (включаючи громадські роботи, виправні установи та управління з надзвичайних ситуацій). Ця програма була створена в декількох штатах для полегшення комунікації із зацікавленими сторонами центрів злиття, включаючи правоохоронні органи та управління з надзвичайних ситуацій. FLO координують діяльність з обміну інформацією між приватним сектором і партнерами CIKR, такими як електричні компанії, нафтопереробні заводи, банки і розважальні заклади. За допомогою цієї мережі центри злиття отримують інформацію про національну безпеку і злочинність для оцінки і аналізу. Розвіддані також надходять з національного рівня і з об'єднаних центрів до польового персоналу через мережу. Потік інформації, що надходить до персоналу на місцях, забезпечує місцеві органи влади інформацією про ситуацію, необхідною для запобігання, захисту або реагування на події, що впливають на їхню громаду.

Однією з переваг об'єднаного центру є його здатність інтегрувати інформацію та розвідувальні дані від різних правоохоронних органів та органів національної безпеки, а також штатних і федеральних структур, аналізуючи та поширюючи відповідну інформацію в юрисдикції. Щоб уникнути дублювання або непорозумінь, EOC повинен також направляти будь-яку зібрану інформацію до об'єднаного центру, як це доречно і визначено об'єднаним центром і EOC.

Об'єднані центри повинні забезпечувати регулярне проведення брифінгів на відповідному рівні засекреченості для ЕОС, а також для їхніх клієнтів та зацікавлених сторін. Об'єднані центри можуть розміщувати інформацію з відкритих джерел про комп'ютеризоване програмне забезпечення для управління надзвичайними ситуаціями, і між ЕОС та об'єднаними центрами має бути чітке розуміння того, як часто ця інформація буде розміщуватися та оновлюватися. Оновлення можна публікувати після того, як вони будуть перевірені персоналом об'єднаного центру, щоб переконатися, що до інформації з відкритих джерел не було додано конфіденційної інформації і вона не була скомпрометована. Використання таких порталів допоможе ЕОС у координації та плануванні зусиль.

Базові можливості об’єднаних центрів:

I. Можливості процесу злиття

A. Планування та розробка вимог

8. ***8. Координуйте дії з посадовими особами, відповідальними за реагування та відновлення.*** *Об'єднані центри повинні визначати та координувати з керівниками аварійних ситуацій та відповідним персоналом з реагування та відновлення і оперативними центрами розробку, впровадження та підтримку плану та процедур для забезпечення спільного розуміння ролей та обов'язків, а також для забезпечення можливості використання розвідувальних та аналітичних можливостей для підтримки оперативних заходів з управління надзвичайними ситуаціями, у разі необхідності, коли події вимагають такого реагування.*

    a. *Переконатися, що центр визначив свої розвідувальні та аналітичні функції та обов'язки відповідно до NIMS та ICS.*

Стаціонарний стан проти активного стану

Координатори ЕОС (а також представники правоохоронних органів та інших органів національної безпеки) повинні бути ознайомлені з роботою центрів злиття. Плани і протоколи ЕОС повинні включати тригер для активації (або часткової активації) ЕОС на основі розвідданих, отриманих від центру злиття.

Різні інформаційні потреби пов'язані з тим, що об'єднаний центр знаходиться в стаціональному стані та в активному стані. На щоденній основі об'єднані центри повинні бути готові надавати інформацію про потенційні події координаторам НС. Це часто робиться шляхом включення керівника з питань надзвичайних ситуацій у рутинні зведення розвідки (які іноді бувають довгими і містять невелику кількість відповідної інформації). Однак об'єднані центри повинні бути готові надсилати інформацію, яка може мати безпосереднє відношення до юрисдикції, і не розраховувати на те, що інші матимуть час, щоб переварити і розпізнати потенційну загрозу для юрисдикції. Ця діяльність включатиме повідомлення про будь-яку активацію об'єднаного центру на вищий рівень, що, в свою чергу, спонукатиме керівника аварійного реагування уважніше стежити за ситуацією і бути готовим активувати (або частково активувати) ЕОС у передовому положенні або у відповідь на інцидент.

Стаціонарний стан - це позиція для рутинних, нормальних, повсякденних операцій і ситуаційної обізнаності, на відміну від тимчасових періодів підвищеної бойової готовності або реагування в режимі реального часу на загрози чи інциденти.

Під час активації ЕОС об'єднані центри можуть виконувати допоміжну функцію для ЕОС і повинні планувати надання ЕОС розвідувальних брифінгів через узгоджені проміжки часу або за необхідності, а також надавати додаткову інформацію директору ЕОС, якщо така потреба виникне між брифінгами. Секретна інформація може надаватися директору ЕОС (якщо вона має допуск), але зазвичай інформація може надаватися ЕОС у незасекреченому вигляді для розповсюдження серед загального персоналу ЕОС.

Дієва розвідка

Після встановлення партнерських відносин на рівні відомств керівництву об'єднаного центру та CCC важливо визначити, кому і за яких обставин можна надавати розвідувальну інформацію, яка може бути використана в практичних цілях. Якщо заздалегідь узгодити чіткі умови, обмін відповідною інформацією може відбуватися своєчасно.

Дієва розвідка

Розвідка повинна:

- Намалювати картину;
- Розкажзати історію;
- Скеровувати реагування; і
- Надавати знання, на основі яких можна розробити/рекомендувати план дій для вирішення проблеми.

Кадрове забезпечення

Процес злиття може допомогти співробітникам EOC та планувальникам з управління надзвичайними ситуаціями, посилюючи процес збору інформації у відділі планування EOC. Хоча EOC та об'єднаний центр використовують зібрану інформацію, основна відповідальність об'єднаного центру полягає в аналізі інформації та поширенні розвідувальних даних до EOC.

Персонал центрів злиття широко варіюється від юрисдикції до юрисдикції і може включати в себе:

- Управління центрами злиття;
- Штатні, місцеві, племінні та/або територіальні правоохоронні органи;
- Аналітики розвідки, кримінальні аналітики, аналітики/планувальники GIS, аналітики CIKR і т.д.;
- Оперативні планувальники;
- IT-підтримка (може також підтримувати IT-службу EOC);
- Директори або зв'язківці EOC;
- Федеральні зв'язківці;
- Штатні або місцеві координатори зв'язку з тероризмом;
- Пожежні служби;
- служби екстреної медичної допомоги (EMS);
- Громадська охорона здоров'я; і
- Персонал, що працює з небезпечними матеріалами.

Наступні кроки можуть покращити інтеграцію та/або координацію роботи центрів злиття та EOC, а також обмін інформацією, але вони можуть бути застосовні не в кожній юрисдикції.

- **Визначення контактних осіб/представників:** Між центром злиття і EOC має бути визначена особа/представник, основним обов'язком якого є забезпечення координації між двома організаціями. Це може бути неповний робочий день або додаткова робота. Ролі цієї особи/представника повинні бути чітко задокументовані та визначені.
  - **ESF-13 (Громадська безпека):** Слід розглянути можливість використання персоналу об’єднаного центру для виконання функції ESF-13 під час активації EOC. Це підвищить здатність об'єднаного центру надавати аналітичну підтримку EOC і забезпечить можливість зворотного зв'язку з федеральними, штатними і місцевими розвідувальними ресурсами.

- **Призначення штатних аналітиків/персоналу:** Виходячи з наявних ресурсів, ЕОС або відповідальний орган з управління надзвичайними ситуаціями повинен розглянути питання про призначення штатного аналітика в об'єднаному центрі або деталізувати його роботу. Цей аналітик повинен мати глибокі знання про операції з управління надзвичайними ситуаціями і виступати в якості експерта з питань управління/реагування на надзвичайні ситуації (SME). До обов'язків аналітика входило б надання експертної підтримки операціям і аналізу об'єднаного центру, а також забезпечення своєчасного і точного обміну інформацією між об'єднаним центром і ЕОС до, під час і після інцидентів. Крім того, об'єднаний центр повинен розглянути можливість призначення або розміщення офіцера розвідки з відповідним допуском в штабі ЕОС під час активації. Це забезпечить безперервний і життєво важливий потік інформації та розвідувальних даних до ЕОС, а також зворотний зв'язок для отримання підтримки від об'єднаного центру.
- **- Об'єднання або віртуальне з'єднання вахтових офісів/чергових:** Вартові офіси або чергові служби як об'єднаного центру, так і ЕОС повинні розглянути можливість віртуального об'єднання, щоб забезпечити найбільш своєчасний і точний обмін повідомленнями. Це дозволить своєчасно обмінюватися інформацією, координувати і/або усунути конфліктні ситуації, а також слугуватиме механізмом офіційної інтеграції превентивних заходів об'єднаного центру з заходами реагування, що вживаються ЕОС. Такий механізм також дозволить ефективно використовувати обмежені ресурси/персонал.
- **Розширення програм FLO:** Існуючі програми FLO слід розглядати як механізм для покращення комунікації між центром злиття та ЕОС, особливо якщо не було визначено спеціальних аналітиків або зв'язкових, відповідальних за цю взаємодію. Слід розглянути можливість включення до програми персоналу з управління надзвичайними ситуаціями, якщо він ще не бере в ній участі. Якщо програма FLO ще не існує, об'єднаний центр повинен розглянути можливість її впровадження з метою налагодження відносин з ЕОС через мультидисциплінарний та малий і середній персонал (наприклад, пожежні служби, служби екстреної медичної допомоги, управління в надзвичайних ситуаціях та заклади охорони здоров'я).

Якщо центри злиття розташовані в одному приміщенні з ЕОС, то, якщо цього вимагає ситуація, їхній персонал може бути залучений до роботи в секторі довгострокового планування ЕОС. Крім того, центри злиття можуть надавати ресурси і підтримку ЕОС, в тому числі ділитися новими технологіями, коли вони стають доступними, наприклад, інструментами розпізнавання облич.

Виклики

Досягнення спільного розуміння того, якою інформацією ділитися і як ділитися, іноді стоїть на заваді розвитку координації між об'єднаними центрами і ЕОС. Традиційні моделі не враховують центри злиття і їхню зростаючу здатність надавати інформацію і розвіддані для ЕОС. Одним із способів вирішення цієї проблеми є постійні зусилля з ознайомлення цих двох структур один з одним. Розуміння ланцюгів підпорядкування, рівня залучення ресурсів і можливостей можна досягти лише шляхом спільних навчань і тренувань. Розробка спільних CONOPS і SOP також сприятиме координації і комунікації навіть у разі неминучих кадрових змін.

Крок четвертий: Тренінги, семінари та вправи

Одним із найкращих способів познайомити співробітників відомств один з одним є спільне відвідування тренінгів та навчань. У наступних розділах ви знайдете ресурси для тренінгів та семінарів.

Тренування

Необхідно провести тренінг для ознайомлення членів EOC з правилами та положеннями, що стосуються секретної інформації, а також з типом інформації, яку вони можуть отримати під час брифінгів, що проводяться центром злиття. Членам EOC можна запропонувати короткий опис типів секретної інформації, її походження та використання, щоб покращити їхнє розуміння того, яку інформацію вони можуть або не можуть отримати. Можна зробити акцент на тому, який обсяг інформації можна отримати з відкритих і незасекречених джерел.
Навчальні курси, які можуть бути застосовані для персоналу EOC/управління в надзвичайних ситуаціях та об'єднаних центрів, включають в себе наступне:

- Національна система реагування: IS-800.b. Цей курс знайомить з керівними принципами, які необхідні всім партнерам з реагування на надзвичайні ситуації, щоб підготуватися і забезпечити уніфіковане реагування на всі види небезпек. NRF "встановлює комплексний, національний підхід до реагування на всі види небезпек для реагування на внутрішні інциденти". http://training.fema.gov/EMIWeb/IS/IS800b.asp.
- Національна система управління інцидентами: IS-700.a. Цей курс знайомить з NIMS, пояснюючи її мету, принципи, ключові компоненти та переваги. http://training.fema.gov/EMIWeb/IS/is700A.asp.
- Система управління інцидентами з використанням єдиних ресурсів та першочергових заходів: IS-200.a. Цей курс призначений для того, щоб навчити персонал ефективно діяти під час інциденту або події в рамках ICS, а також надає навчання та ресурси для персоналу, який, ймовірно, обійматиме керівну посаду в ICS. http://training.fema.gov/EMIWeb/IS/IS200A.asp.
- - Міжвідомча координаційна система NIMS (MACS): IS-701a. Цей курс розповідає учасникам про компоненти MACS і про те, як встановити взаємозв'язок між усіма елементами системи. http://training.fema.gov/EMIWeb/IS/is701a.asp.
- - Національний план захисту інфраструктури (NIPP): IS-860a. Цей курс знайомить з NIPP, визначає відповідні органи влади для захисту CIKR та пов'язані з цим процеси обміну інформацією. http://training.fema.gov/EMIWeb/IS/IS860a.asp.
- - Додаток з підтримки критичної інфраструктури та ключових ресурсів: IS-821. Цей курс надає вступ до Додатку з підтримки CIKR до NRF. http://training.fema.gov/EMIWeb/IS/IS821.asp.
- - Вступ до системи управління інцидентами: IS-100.a. Цей курс знайомить з ICS та забезпечує основу для навчання з ICS на більш високому рівні. Курс описує історію, особливості, принципи та організаційну структуру ICS. Він також пояснює взаємозв'язок між ICS та NIMS. http://training.fema.gov/EMIWeb/IS/IS100A.asp.
- - Вступ до ICS для правоохоронних органів: IS-100.LEa. Цей курс знайомить з ICS та забезпечує основу для навчання з питань ICS на більш високому рівні. Курс описує історію, особливості, принципи та організаційну структуру ICS. Він також пояснює взаємозв'язок між ICS та NIMS. Цей курс використовує ті ж цілі та зміст, що й інші курси ICS 100, з прикладами та вправами з правоохоронної діяльності. http://training.fema.gov/EMIWeb/IS/IS100LEA.asp.
- - Громадська безпека та охорона Додаток: IS-813. Цей курс знайомить з Додатком ESF-13 (Громадська безпека і захист). http://training.fema.gov/EMIWeb/IS/IS813.asp.
- - Управління та операції КНП: IS-775. Цей курс описує роль, структуру та функції КНС та їх взаємозв'язок як компонентів системи MACS. Курс містить приклади, пов'язані з катастрофами, діяльність та тематичні дослідження, які стосуються EOC та MACS на місцевому, державному та федеральному рівнях управління. http://training.fema.gov/EMIWeb/IS/IS775.asp.

- - Інтегрований курс з управління в надзвичайних ситуаціях (IEMC) FEMA. IEMC - це чотири південні навчальні курси на основі вправ, які підвищують обізнаність та навички, необхідні для розробки та впровадження політик, планів та процедур в умовах НС. http://training.fema.gov/EMIWeb/IEMC/.
- - IEMC: Інтерфейс між командою з управління аварійними ситуаціями та командою з управління інцидентами: E947.
- http://www.training.fema.gov/EMICourses/crsdetail.asp?cid=E947&ctype=R.
- - Федеральний навчальний центр правоохоронних органів (FLETC) - Навчальна програма з антитерористичної розвідки (AIATP). Цей курс є вступною ознайомчою програмою, покликаною надати слухачам практичні знання про процес кримінальної розвідки та відповідні закони, керівні принципи, політику, інструменти і методи. http://www.fletc.gov/state-and-local/tuition-free-training- programs/anti-terrorism-intelligence-awareness-training-program-aiatp.
- - FLETC - Вступна програма підготовки аналітиків розвідки (IIATP). Цей курс забезпечує історичну, правову та етичну основу для діяльності правоохоронних органів зі збору, збереження та поширення розвідувальної інформації відповідно до розвідувального циклу. http://www.fletc.gov/state-and- local/tuition-free-training-programs/introductory-intelligence-analyst-training-program-iiatp.
- - Навчальні ресурси для штатних, місцевих і племінних центрів злиття з питань конфіденційності та громадянських свобод в умовах обміну інформацією. Тренінги та ресурси, в тому числі шаблони політики конфіденційності, для захисту конфіденційності інформації та інших законних прав і громадянських свобод в контексті ISE доступні на http://www.it.ojp.gov/PrivacyLiberty та http://www.ise.gov/pages/privacy- overview.aspx.
- - Тренінг по 28 CFR Part 23. 28 CFR Part 23 був виданий з метою забезпечення конфіденційності та конституційних прав громадян під час збору та обміну інформацією кримінальної розвідки. Вона є важливою частиною розвідувального ландшафту. Цей тренінг покликаний допомогти представникам штатних і місцевих органів влади зрозуміти керівні принципи, які регулюють розробку і впровадження політики і систем, що сприяють обміну розвідувальною інформацією. Тренінг включає огляд нормативно-правових актів; вимоги дотримання; вимоги до зберігання; вимоги до запитів і розповсюдження інформації, а також вимоги до перегляду і очищення. Доступ до онлайн-тренінгу можна отримати на захищеному веб-сайті Національного ресурсного центру кримінальної розвідки (NCIRC), який доступний через HSIN, LEO і RISS. http://www.iir.com/28cfr/Overview.htm.
- - Тренінг для авторизованих користувачів з вивчення інформації про вразливість до хімічного тероризму доступний онлайн за посиланням http://www.dhs.gov/files/programs/gc_1181835547413.shtm.
- - Програма підготовки авторизованих користувачів з питань захисту інформації про критично важливу інфраструктуру (Protected Critical Infrastructure Information Program) доступна в Інтернеті за адресою: https://pciims.dhs.gov/pciims.

Базові можливості об’єднаних центрів:

II. Управлінські та адміністративні можливості:

D. Персонал та навчання

3. ***План тренінгу.*** *Центри злиття повинні розробити та задокументувати навчальний план, щоб забезпечити розуміння персоналом та партнерами процесу розвідки та місії, функцій, планів і процедур центру злиття. План повинен визначати потреби в базовій підготовці всього персоналу центру, а також спеціалізовану підготовку, необхідну для виконання місії центру і задоволення поточних інформаційних потреб. (Керівні принципи 12 і 13, Керівні принципи для об'єднаних центрів)*

b. Як мінімум, весь персонал центру повинен пройти навчання з наступних питань:

ii. Ролі та обов'язки розвідувальних та аналітичних функцій відповідно до NIMS та ICS.

- Програми FLO. Як уже згадувалося раніше, програми FLO сприяють розвитку і координації мережі FLO, які є членами місцевих або штатних правоохоронних органів, пожежних служб, органів охорони здоров'я та інших установ, таких як громадські роботи, виправні заклади та управління з надзвичайних ситуацій. Мережа FLO забезпечує участь життєво важливих дисциплін у процесі об'єднання і слугує каналом, через який інформація з питань внутрішньої безпеки та боротьби зі злочинністю надходить до об'єднаного центру для оцінки та аналізу. Технічна допомога Програми FLO також пропонується в рамках спільної Програми технічної допомоги DHS/DOJ щодо процесу злиття, щоб допомогти в розробці та впровадженні цієї програми. Зацікавлені сторони з управління надзвичайними ситуаціями перераховані як потенційні партнери програми і заохочуються до участі в ній.

Додаткову інформацію про програми FLO можна отримати за допомогою програми "Створення офісу зв'язку з питань синтезу" (Establishing a Fusion Liaison Officer Program): Посібник та робочий зошит з питань планування та розвитку, розміщеному в Системі LLIS за адресою www.llis.dhs.gov та NCIRC за адресою www.ncirc.gov.

Майстер-класи

Необхідно провести семінари для персоналу центрів злиття та EOC (особливо для персоналу з планування), щоб ознайомити персонал EOC з можливостями центрів злиття і навпаки. На семінарах має бути окреслена концепція роботи, яка визначає, яким чином EOC та об'єднаний центр отримають доступ до можливостей один одного. Зокрема, семінари повинні включати обговорення баз даних і того, як вони будуть використовуватися і з'єднуватися під час активації EOC. Семінари можна також регулярно планувати для ознайомлення персоналу об'єднаних центрів і EOC та надання оновленої інформації про інструменти, можливості та інші ресурси, що використовуються у відповідних центрах.

В рамках Програми технічної допомоги DHS/DOJ у процесі злиття Програма обміну між центрами злиття підтримує обмін персоналом центрів злиття і пов'язаний з цим обмін передовим досвідом роботи та отриманими уроками. Програма технічної допомоги DHS/DOJ Fusion Process сприяє взаємодії, обміну інформацією та операціям між директорами та ключовими співробітниками з розвідки та планування з метою зміцнення національної мережі центрів злиття.

Програма технічної допомоги Fusion Process також сприяє проведенню семінарів прямої взаємодії Fusion Center, що дозволяє SME забезпечити ефективний та дієвий обмін передовим досвідом та отриманими уроками.

Вправи

Об'єднані центри та EOC повинні розглянути можливість регулярної координації та/або проведення спільних навчань на основі сценаріїв та реальних тренувань для оцінки своїх комунікаційних можливостей та обміну оперативною інформацією, визначеною в їхніх SOP і меморандумах про взаєморозуміння. Ці навчання також мають бути спрямовані на оцінку та усунення конфліктів між ролями та обов'язками персоналу, відповідального за координацію та/або інтеграцію цих зусиль. Використання посібників з оцінки вправ також забезпечує інструмент вимірювання для виявлення прогалин у підготовці або ролях і обов'язках, а також додатково забезпечує рівень відповідності вимогам NIMS.

Базові можливості об’єднаних центрів:

I. Можливості процесу злиття:

A. Планування та розробка вимог

10. ***Вправи.*** *Центри злиття повинні проводити або брати участь в теоретичних і практичних навчаннях на основі сценаріїв інших відомств, щоб регулярно оцінювати свої можливості.*

b. Навчання повинні залучати весь відповідний персонал центру та його учасників і сприяти розумінню цінності загальноштатного процесу об'єднання, плану збору даних центру, процесу SAR, аналітичних продуктів, ролі центру в середовищі обміну інформацією та ролі центру в заходах з реагування та відновлення відповідно до NIMS та ICS.

Навчання повинні відповідати Програмі навчань та оцінки національної безпеки (HSEEP).

Програма навчань із запобігання тероризму (TPEP) проводить навчання і підтримує діяльність, спрямовану на підвищення обізнаності, координації та обміну інформацією між співробітниками служб внутрішньої безпеки і правоохоронних органів на всіх рівнях влади. Під час навчань оцінюються можливості запобігання тероризму, включаючи аналіз розвідувальних даних, обмін інформацією та розпізнавання індикаторів і попереджень.

Тематичні дослідження та приклади

Об'єднані центри відіграють важливу роль у забезпеченні планування та розвідувальної підтримки операцій під час спеціальних подій різного масштабу. Як центральне сховище стратегічної і тактичної інформації, об'єднані центри надають правоохоронним органам, органам громадської безпеки, управління надзвичайними ситуаціями та іншим партнерам інформацію і розвідувальні дані для керівництва підготовкою і підтримки прийняття тактичних рішень під час спеціальної події. Планування, організаційна структура і процеси збору, аналізу, усунення конфліктів і поширення інформації можуть бути масштабовані відповідно до оперативних потреб і ресурсних обмежень.

При плануванні спеціальних подій, а також національних подій спеціальної безпеки (NSSE), юрисдикції повинні враховувати всі чотири напрямки місії (запобігання, захист, реагування і відновлення) в процесі планування. У міру того, як об'єднані центри зростають і стають більш надійними, вони здатні збирати інформацію з широкого кола джерел і надавати готові аналітичні продукти, які допоможуть сформувати рішення про розподіл ресурсів, необхідних для ліквідації наслідків події.

Під час планування запобігання різні збирачі інформації, залучені до процесу злиття (до яких належать федеральні, місцеві, племінні, територіальні та приватні органи влади), повинні підготувати план збору інформації, який зосереджується на питаннях, пов'язаних з подією. Інформація може надходити від Федерального розвідувального співтовариства, правоохоронних органів штатів і місцевих органів влади, інших організацій державного сектору, служб швидкого реагування та громадськості. Планування заходів із запобігання забезпечить інформацією зацікавлені сторони заходу напередодні події та оперативні центри під час події.

Планування Республіканського та Демократичного з'їздів, а також інавгурації Президента є прикладом того, як концепції та процеси запобігання можуть бути інтегровані в загальний процес планування. Юрисдикція, в якій відбудеться захід, починає процес планування запобігання за багато місяців до його проведення. Об'єднаний центр, до складу якого входять різні штатні, місцеві, племінні, територіальні та федеральні учасники, може розпочати процес збору, аналізу та розповсюдження інформації та розвідувальних даних. Секретна служба США (USSS) є провідним федеральним агентством для NSSE і розробляє плани щодо захисту кандидатів, Президента та Віце-президента під час подій. Вони є невід'ємною частиною процесу планування, оскільки першочерговим завданням є запобігання нападу на осіб, яких вони мають захищати.

Аналітики об'єднаного центру можуть використовувати методи збору інформації з відкритих джерел для оцінки загрози події. Наприклад, вони можуть збирати інформацію про групи, які планують прямі дії проти заходу, і оцінювати ступінь загрози. Ця інформація може бути передана командному складу поліції, FBI, USSS та іншим посадовим особам, які можуть приймати рішення про використання ресурсів. Це також дозволяє їм приймати рішення про те, де розгортати ресурси для посилення захисту цілей, які раніше не розглядалися.

Важливу роль у плануванні превентивних заходів відіграє також внесок радників з питань захисної безпеки DHS, які взаємодіють з власниками об'єктів критичної інфраструктури та ключових ресурсів, що можуть постраждати під час події. Власники CIKR можуть надавати дані про загрози, а також отримувати належним чином перевірені матеріали для захисту своєї власності.

У юрисдикціях, де центр злиття і EOC розташовані спільно, успішні відносини будуються на низці кроків, які визначають ролі та обов'язки учасників. Необхідними компонентами є відповідне законодавство, Меморандум про взаєморозуміння між головними відомствами, SOP і щире бажання обмінюватися інформацією. Вахтові офіси в EOC і об’єднаному центрі розробили протокол обміну інформацією, який заохочує відкриту комунікацію.

Об'єднаний центр і EOC обмінюються аналітиками, щоб гарантувати, що до інформації застосовується належна класифікація, яка дозволяє її належним чином поширювати.

Програма FLO може бути використана для посилення зв'язку між об'єднаним центром і EOC. Штати підготували фахівців з управління надзвичайними ситуаціями, служби швидкого реагування та інших працівників державного сектору, які не є співробітниками правоохоронних органів, до виконання функцій офіцерів зв'язку. Перевага цієї програми полягає в тому, що між об'єднаним центром і головним відомством офіцера зв'язку існує потужний канал зв'язку. Оскільки більш підготовлені офіцери зв'язку призначаються до EOC під час активації, зв'язок між об'єднаним центром і EOC зміцнюється.

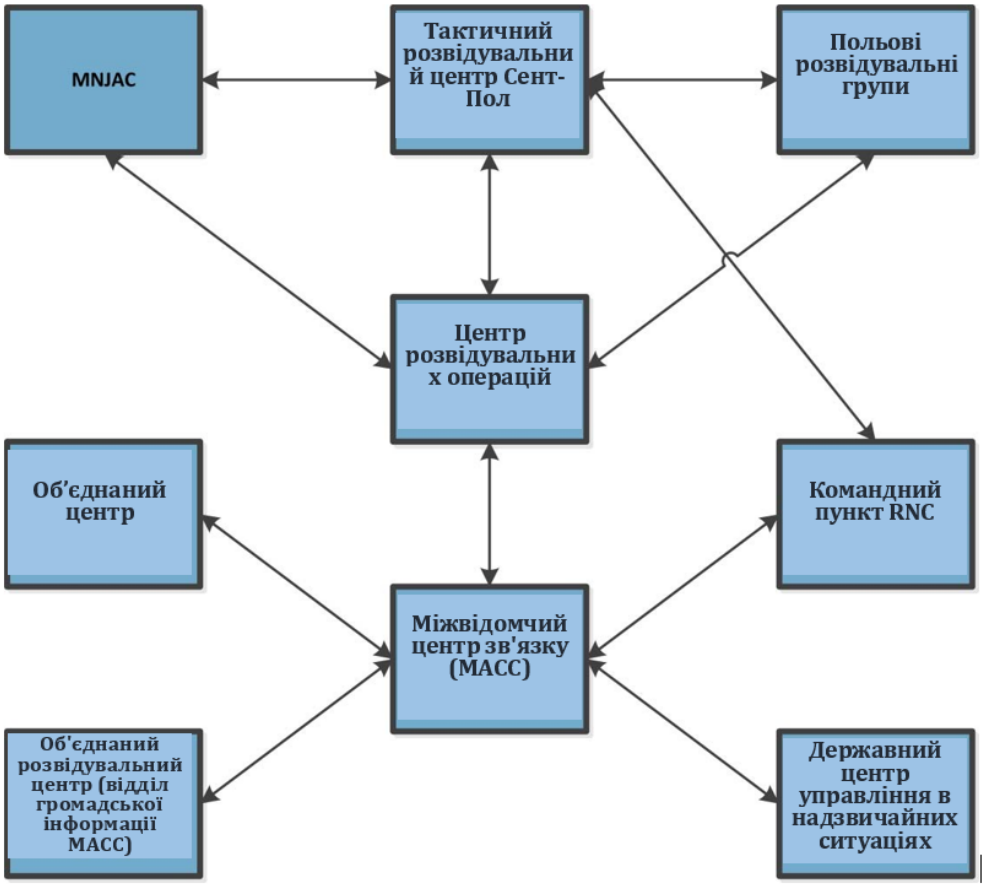
Об'єднаний аналітичний центр Міннесоти та Республіканський національний з'їзд

Об'єднаний аналітичний центр штату Міннесота (MNJAC), який є центром злиття даних штату, надав критично важливу інформацію та розвідувальну підтримку під час Республіканської національної конвенції (RNC), що проходила в Міннеаполісі-Сент-Полі, штат Міннесота, з 1 по 4 вересня 2008 року. Через класифікацію NSSE, USSS була провідним агентством, в той час як FBI, Департамент поліції Сент-Пола і MNJAC розділили відповідальність за збір, злиття, аналіз і розповсюдження всієї інформації на підтримку операцій з безпеки RNC. Інші відомства, які допомагали у забезпеченні безпеки заходу, включали FEMA, Берегову охорону США, Митну і прикордонну службу, Адміністрацію транспортної безпеки, Управління з контролю і аудиту Міністерства національної безпеки, Управління з виявлення ядерних матеріалів, Імміграційну і митну службу США, Управління громадських робіт Сент-Пола і Приймаючий комітет RNC.

Приблизно 45 000 делегатів, заступників делегатів, волонтерів, представників ЗМІ та інших гостей приїхали на з'їзд. Під час проведення RNC також зібралася велика кількість протестувальників, що призвело до загрози громадській безпеці та проблеми контролю над натовпом (правоохоронці заарештували 818 осіб). Під час RNC співробітники MNJAC працювали в Центрі тактичної розвідки (TIC) та Центрі розвідувальних операцій (IOC), що забезпечило ефективний потік інформації до та з цих центрів. Персонал MNJAC також допомагав підтримувати поточну оперативну картину в рамках IOC.

MNJAC зміг використати мережу Intelligence Communications Enterprise for Information Sharing and Exchange (ICEFISHX) (яка використовується для збору інформації про підозрілу активність, пов'язану зі злочинною діяльністю та захистом інфраструктури в Міннесоті) для швидкої передачі інформації через кордони штату до інших об'єднаних центрів та федеральних агентств. Це дозволило MNJAC отримати довідкову інформацію та дані про судимості щодо осіб і груп, які беруть участь у протестній діяльності.

На наступній діаграмі 2 показано, як відбувався обмін інформацією між численними зацікавленими сторонами:



Співпраця і спільне розміщення федеральних, штатних і місцевих органів, а також приватного сектору впродовж усього періоду проведення RNC і всіх супутніх заходів забезпечили сприятливе середовище, що сприяло своєчасному обміну інформацією та успішному управлінню численними видами діяльності. Зокрема, здатність MNJAC зв'язуватися з сусідніми штатами, розвідувальним підрозділом поліції Сент-Пола, розвідувальним підрозділом поліції Міннеаполіса та іншими федеральними відомствами забезпечила значну стратегічну підтримку на етапах планування заходу, а також під час проведення заходу.

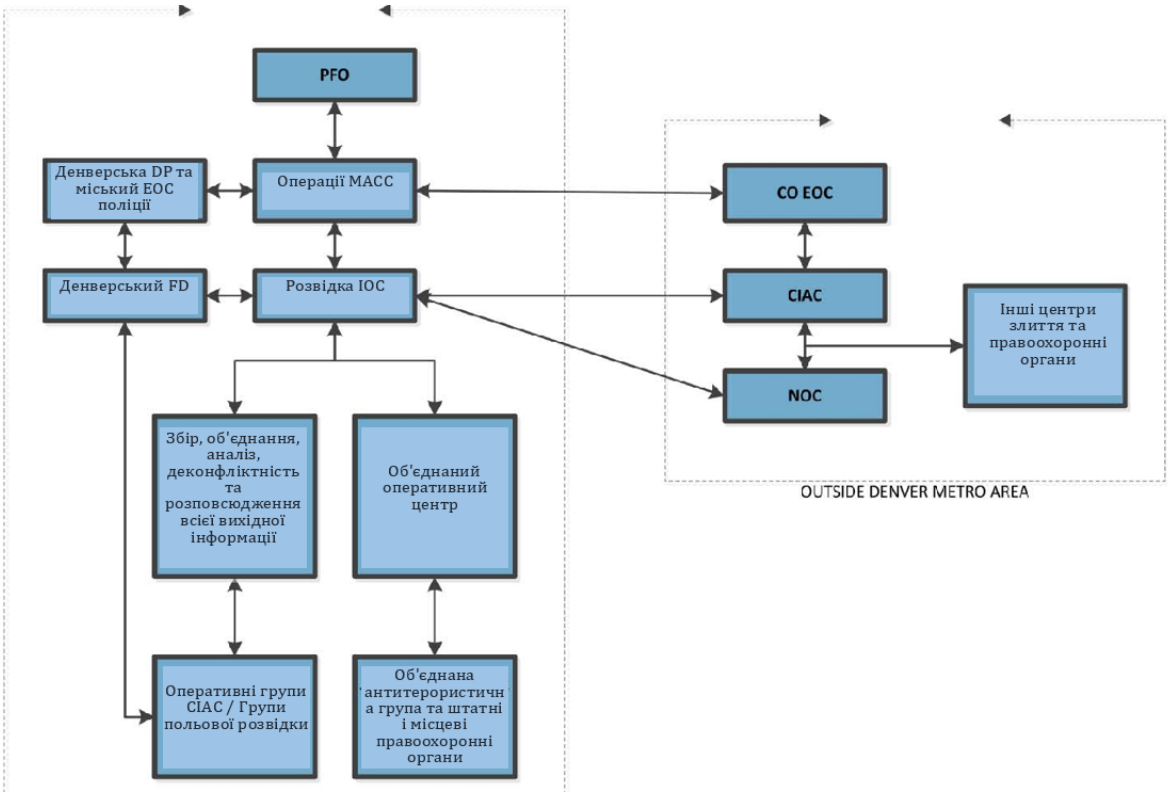
Колорадський розвідувально-аналітичний центр і Національний з'їзд Демократичної партії 2008 року

Колорадський розвідувально-аналітичний центр (CIAC) надав критично важливу інформацію та розвідувальну підтримку під час Національного з'їзду Демократичної партії (DNC), що проходив у Денвері, штат Колорадо, з 25 по 28 серпня 2008 року. CIAC є штатним об'єднаним центром, розташованим у передмісті Денвера і підпорядкованим Патрулю штату Колорадо, який знаходиться в одній будівлі з Центром розвідки штату Колорадо. CIAC і FBI розділили між собою рівну відповідальність за управління IOC, який відповідав за збір, злиття, аналіз, деконфліктність і поширення всієї інформації на підтримку операцій з безпеки DNC.

[2] Джерело: Центр злиття в центрі уваги, Програма та послуги з технічної підтримки процесу злиття DHS/DOJ, 2008 р..

До DNC регулярні тренування між об'єднаним центром і EOC не проводилися. Під час підготовки до DNC CIAC підготував понад 200 TLO з різних дисциплін, які або були призначені до різних командних центрів і центрів управління під час активації, або заповнювали місця в CIAC. За взаємною домовленістю Департамент поліції Денвера був основним EOC, хоча Державний EOC також був активований, але перебував у режимі очікування під час заходу. Командир CIAC був призначений до штабу і забезпечував керівництво штабу ситуаційною обізнаністю. Командир CIAC також здійснював моніторинг інформації, що надходила до EOC, щоб переконатися, що секретна інформація не була скомпрометована.
Під час змін CIAC інформував персонал EOC про розслідування та потенційні загрози, що було дуже корисно для персоналу EOC і дозволяло підтримувати канали зв'язку відкритими.

Інформація, що стосувалася операцій з безпеки DNC в районі Денвера, координувалася IOC. CIAC разом з Національним оперативним центром (NOC) Міністерства внутрішньої безпеки США у Вашингтоні, округ Колумбія, координував інформацію з об'єднаними центрами по всій країні та іншими державними і місцевими правоохоронними органами. CIAC також діяв як канал передачі розвідувальної та іншої інформації до EOC штату Колорадо. На наступній схемі3 показано інформаційний потік між різними зацікавленими сторонами:



[3] Source: Fusion Center Spotlight, DHS/DOJ Fusion Process Technical Assistance Program and Services 2008.

CIAC головним чином відповідав за діяльність за межами зони діяльності DNC, включаючи координацію з NOC та іншими центрами термоядерного синтезу. Він підтримував деякі види діяльності IOC. Щоб забезпечити IOC можливостями для збору розвідувальної інформації, CIAC наклав концепцію польової розвідувальної групи (FIT) на існуючу програму TLO. Складаючись з команди міжвідомчих оперативних груп, ГПР відповідали за надання розвідувальних даних у режимі реального часу та інформації про кримінальні злочини та інциденти, пов'язані з громадською безпекою.

DNC наводить багато прикладів того, як державний або місцевий об'єднаний центр може підтримати планування і виконання планів безпеки заходів. Співпраця і спільне розташування федеральних, державних і місцевих установ забезпечили сприятливе середовище, що призвело до своєчасного обміну інформацією та успішного управління численними заходами. Співпраця між CIAC і FBI під час проведення IOC слугує моделлю для майбутніх NSSE та інших спеціальних заходів.

Для отримання додаткової інформації

Будь ласка, зверніться до розділу "Центр "Ф'южн" - підтримка спеціальних заходів": Колорадський розвідувально-аналітичний центр і Національний з'їзд Демократичної партії 2008 року, що проходив у Fusion Center, а також семінар з інтеграції та координації EOC: Комплект довідкових документів для отримання додаткової інформації про діяльність та взаємодію CIAC під час DNC. Цей документ також розміщений в системі LLIS за адресою www.llis.dhs.gov і NCIRC за адресою www.ncirc.gov.

This page intentionally left blank.

Додаток A: Глосарій та абревіатури

Глосарій

Підхід за всіма злочинами

Підхід, який включає тероризм та інші загрози високого ризику в існуючу систему боротьби зі злочинністю, щоб забезпечити перевірку та аналіз можливих злочинів-прекурсорів на предмет їх зв'язку з більш масштабними терористичними або іншими злочинами. Цей підхід визнає, що існує взаємозв'язок між видами злочинної діяльності (наприклад, незаконними операціями з наркотиками, бандитизмом, відмиванням грошей, шахрайством, крадіжкою особистих даних і тероризмом). Використання підходу, що охоплює всі види злочинів, не означає, що центр злиття повинен займатися кожним окремим злочином, який трапляється в зоні його відповідальності. Скоріше, рутинна оцінка ризиків, яку розробляє або підтримує розробку об'єднаний центр, повинна допомогти у визначенні пріоритетів щодо злочинів та/або загроз, на які штат або регіон повинні звернути увагу, а при розробці плану збору даних - визначити, які інші джерела інформації можуть бути корисними для вивчення можливих зв'язків з іншими злочинами.

Підхід за всіма небезпеками

Підхід, який стосується готовності до терористичних атак, великих катастроф та інших надзвичайних ситуацій у Сполучених Штатах. (Джерело: HSPD-8, 17 грудня 2003 р.) В контексті процесу об'єднання деякі об'єднані центри визначили свою місію як таку, що включає в себе підхід до всіх небезпек. Хоча застосування цього підходу варіюється, загалом це означає, що об'єднаний центр визначив пріоритетні типи великих катастроф і надзвичайних ситуацій, окрім тероризму і злочинності, які можуть статися в межах його юрисдикції. Об'єднаний центр також збирає, аналізує і поширює інформацію, яка допоможе відповідним відповідальним органам (наприклад, правоохоронним органам, пожежним службам, органам охорони здоров'я, управління в надзвичайних ситуаціях, об'єктам критичної інфраструктури тощо) у запобіганні, захисті, реагуванні або відновленні після таких інцидентів. Центр злиття може використовувати підхід, що охоплює всі небезпеки, але не враховувати у своїй діяльності всі можливі небезпеки. Частиною щорічної оцінки ризиків, яку розробляє або підтримує розробку об'єднаний центр, має бути визначення того, яким загрозам штат або регіон повинні надавати пріоритет у процесі планування національної безпеки, а також надання об'єднаному центру пріоритетів, необхідних для розробки відповідних SINs.

Аналіз

Діяльність, за допомогою якої значення, фактичне або передбачуване, виводиться шляхом організації та систематичного вивчення різноманітної інформації та застосування індуктивної або дедуктивної логіки для цілей кримінального розслідування або оцінки.

Базова спроможність

Спроможність забезпечує засоби для виконання місії або функції в результаті виконання одного або декількох критично важливих завдань, за визначених умов, до цільових рівнів ефективності. Спроможність може бути реалізована за допомогою будь-якої комбінації належним чином спланованого, організованого, оснащеного, підготовленого і навченого особового складу, що дозволяє досягти бажаного результату (Джерело: Керівництво з національної готовності, с. 40). У контексті цього документа базова спроможність об'єднаного центру - це спроможність, необхідна для виконання об'єднаним центром своїх основних функцій зі збору, обробки, аналізу та розповсюдження інформації про тероризм, національну безпеку та правоохоронну діяльність.

Закрита інформація/розвіддані

Єдина система засекречування, захисту та розсекречування інформації з питань національної безпеки, включаючи інформацію, що стосується захисту від транснаціонального тероризму, для забезпечення збереження конфіденційності певної інформації з метою захисту громадян, демократичних інститутів США, внутрішньої безпеки США та взаємодії США з іноземними державами та організаціями.

Зведення (інформації)

Огляд зібраної та оціненої інформації з метою визначення її суттєвої застосовності до справи або проблеми, що розглядається, та розміщення корисної інформації у формі або системі, яка дозволяє легкий та швидкий доступ до неї та її пошук.

Збір (інформації)

Ідентифікація, визначення місцезнаходження та запис/зберігання інформації, як правило, з оригінального джерела, з використанням як людських, так і технічних засобів для введення в розвідувальний цикл з метою досягнення визначеної тактичної або стратегічної мети розвідки.

План збору

Попередній крок до завершення оцінки потреб у розвідданих для визначення типу інформації, яку необхідно зібрати, альтернативних способів збору інформації та графіку збору інформації.

Координація

Процес взаємозв'язку робочих функцій, відповідальності, обов'язків, ресурсів та ініціатив, спрямованих на досягнення мети.

Критична інфраструктура та ключові ресурси (CIKR)

Системи, активи та мережі, як фізичні, так і віртуальні, настільки життєво важливі для Сполучених Штатів, що виведення з ладу або знищення таких систем та активів матиме виснажливий вплив на безпеку, національну економічну безпеку, національне здоров'я та безпеку населення або будь-яку комбінацію цих питань. Ключові ресурси - це будь-які ресурси, що перебувають під державним або приватним контролем, необхідні для мінімального функціонування економіки та уряду.

Поширення (розвідданих)

Процес ефективного розповсюдження проаналізованих розвідувальних даних з використанням певних протоколів у найбільш прийнятному форматі серед тих, хто потребує інформації, щоб сприяти досягненню цілей організації.

Центр управління в надзвичайних ситуаціях (EOC)

Фізичне місце, де зазвичай відбувається координація інформації та ресурсів для підтримки заходів з управління інцидентом (операцій на місці події). Координаційний центр може бути тимчасовим об'єктом або розташовуватися в більш центральному чи постійно діючому об'єкті, можливо, на вищому рівні організації в межах юрисдикції. EOC можуть бути організовані за основними функціональними дисциплінами (наприклад, пожежні, правоохоронні та медичні служби), за юрисдикцією (наприклад, федеральна, штатна, регіональна, племінна, міська, окружна) або за певною комбінацією цих дисциплін.

Функції підтримки в надзвичайних ситуаціях (ESF)

Використовується федеральним урядом та урядами багатьох штатів як основний механізм на оперативному рівні для організації та надання допомоги. ESFs узгоджують категорії ресурсів і визначають стратегічні цілі їх використання. ESF використовують стандартизовані концепції управління ресурсами, такі як типізація, інвентаризація та відстеження, щоб полегшити відправлення, розгортання і відновлення ресурсів до, під час і після інциденту.

Для службового користування (FOUO)

Позначення, яке раніше використовувалося для маркування несекретної конфіденційної інформації. Це позначення було замінено на Рамкову систему контрольованої несекретної інформації (CUI).

Об’єднаний центр (або центр злиття, або ф’южн центр)

Спільні зусилля двох або більше відомств, які надають ресурси, експертизу та інформацію центру з метою максимізації здатності виявляти, запобігати, розслідувати та реагувати на злочинну та терористичну діяльність (Fusion Center Guidelines, серпень 2006 р.). Визнані цінним ресурсом для обміну інформацією, штатні та великі міські об'єднані центри є основними, але не єдиними пунктами в штатному та місцевому середовищі для отримання та обміну інформацією про тероризм, національну безпеку та інформацією правоохоронних органів, пов'язаною з тероризмом.

Керівництво Центру злиття, серпень 2006 року

Визнаний на національному рівні документ, розроблений для забезпечення послідовного створення та функціонування центрів злиття, що сприятиме посиленню координації зусиль, зміцненню партнерських відносин та покращенню можливостей боротьби зі злочинністю та тероризмом.

Процес злиття

Всеохоплюючий процес управління потоками інформації та розвідувальних даних між рівнями і секторами уряду та приватного сектору. Він виходить за рамки створення інформаційно-розвідувального центру або комп'ютерної мережі. Процес злиття підтримує реалізацію програм запобігання, реагування і подолання наслідків, що ґрунтуються на оцінці ризиків та керуються інформацією. Процес злиття перетворює інформацію і розвіддані на практичні знання (Керівництво для центрів злиття, серпень 2006 р.).

Інцидент

Подія природного чи антропогенного характеру, яка вимагає реагування для захисту життя або майна. Інциденти можуть, наприклад, включати великі катастрофи, надзвичайні ситуації, терористичні атаки, терористичні загрози, громадянські заворушення, лісові та міські пожежі, повені, розливи небезпечних матеріалів, ядерні аварії, авіакатастрофи, землетруси, урагани, торнадо, тропічні шторми, цунамі, катастрофи, пов'язані з війною, надзвичайні ситуації в галузі охорони здоров'я та медицини, а також інші події, що потребують екстреного реагування.

Командування інцидентом

Організаційний елемент ICS, що відповідає за загальне управління інцидентом і складається з Командувача інцидентом (єдиної або об'єднаної командної структури) та будь-якого призначеного допоміжного персоналу.

Інформація

Фрагменти необроблених, неаналізованих даних, які ідентифікують осіб, докази чи події або ілюструють процеси, що вказують на злочинну подію, свідків чи докази злочинної події.

Середовище обміну інформацією (ISE)

Довірче партнерство між усіма рівнями влади, приватним сектором та іноземними партнерами з метою виявлення, запобігання, упередження та пом'якшення наслідків тероризму проти території, людей та інтересів Сполучених Штатів. Це партнерство уможливлює довірливий, безпечний і належний обмін інформацією про тероризм, насамперед, між п'ятьма федеральними громадами; до і від урядів штатів, місцевих, племінних і територіальних урядів, іноземних союзників і приватного сектору, а також на всіх рівнях класифікації безпеки.

Система обміну інформацією

Інтегрована та безпечна методологія, комп'ютеризована або ручна, призначена для ефективного та результативного розповсюдження важливої інформації про правопорушників, злочини та/або події з метою покращення діяльності правоохоронних органів щодо запобігання та затримання правопорушень.

Інформаційна система

Організований засіб, ручний або електронний, для збору, обробки, зберігання та пошуку інформації про окремих суб'єктів з метою обліку та довідок.

Розвіддані (кримінальна)

Результат аналізу необробленої інформації, пов'язаної зі злочинами або схемами злочинів, стосовно особи або групи осіб, яку можна ідентифікувати, з метою передбачення, запобігання або моніторингу можливої злочинної діяльності (або розслідування чи судового переслідування).

Аналітик з питань розвідки

Професійна посада, на якій працівник відповідає за збір різноманітних фактів, документування обставин, доказів, інтерв'ю та будь-якого іншого матеріалу, пов'язаного зі злочином, та організацію їх у логічну та взаємопов'язану структуру з метою розробки кримінальної справи, пояснення злочинного явища, опису злочинів та тенденцій злочинності та/або підготовки матеріалів для суду та обвинувачення, або для оцінки проблеми злочинності чи злочинної групи.

Розвідувальне співтовариство

Розвідувальне співтовариство - це федерація агентств і організацій виконавчої влади, які працюють окремо і разом для здійснення розвідувальної діяльності, необхідної для ведення зовнішніх зносин і захисту національної безпеки Сполучених Штатів.

Цикл розвідки

Також відомий як процес злиття. Дивіться Процес злиття.

Інтелектуальна функція

Діяльність у межах правоохоронного органу, що відповідає за певний аспект правоохоронної розвідки, чи то збір, аналіз та/або розповсюдження інформації.

Процес розвідки

Організований процес, за допомогою якого інформація збирається, оцінюється і розподіляється з метою досягнення цілей розвідувальної функції - це метод виконання аналітичної діяльності та надання аналізу у формі, придатній для використання.

Продукти розвідки

Звіти або документи, що містять оцінки, прогнози, асоціації, зв'язки та інші результати аналітичного процесу, які можуть бути поширені для використання правоохоронними органами з метою запобігання злочинам, посилення цільової спрямованості, затримання правопорушників та притягнення їх до відповідальності.

Посібник з ведення розвідувальної документації

Засновані на федеральному положенні 28 CFR, частина 23, це керівні принципи/стандарти для розробки політик і процедур управління документацією, що використовуються правоохоронними органами.

Об'єднана антитерористична група (JTTF)

Спільна оперативна група на чолі з FBI, яка використовує колективні ресурси агентств-членів для запобігання, розслідування, підриву і стримування терористичних загроз, що зачіпають інтереси США, а також для сприяння обміну інформацією між агентствами-партнерами.

Правоохоронна розвідка

Кінцевий продукт (результат) аналітичного процесу, який збирає та оцінює інформацію про злочини та/або злочинні підприємства з метою формування суджень та висновків про стан суспільства, потенційні проблеми та злочинну діяльність з метою здійснення кримінального переслідування, прогнозування тенденцій розвитку злочинності або підтримки прийняття обґрунтованих рішень керівництвом.

Правоохоронні органи Конфіденційна інформація (LES)

Делікатна, але несекретна інформація, спеціально зібрана для правоохоронних цілей, яка, якщо не буде захищена від несанкціонованого доступу, може (1) перешкоджати правоохоронній діяльності, (2) позбавити особу права на справедливий судовий розгляд або неупереджене судове рішення, (3) становити необґрунтоване втручання в особисте життя інших осіб, (4) розкрити особу конфіденційного джерела, (5) розкрити методи та процедури розслідування та/або (6) поставити під загрозу життя або фізичну безпеку людини.

Міжвідомча координаційна система (MACS)

Система, яка забезпечує архітектуру для підтримки координації для визначення пріоритетів інцидентів, розподілу критично важливих ресурсів, інтеграції систем зв'язку та інформаційної координації. MACS допомагає установам і організаціям, які реагують на інцидент. Елементами MACS є приміщення, обладнання, персонал, процедури і комунікації. Двома найбільш часто використовуваними елементами є EOC і міжвідомчі координаційні групи .

Національна система управління інцидентами (NIMS)

Набір принципів, який забезпечує систематичний, проактивний підхід, що спрямовує державні установи на всіх рівнях, неурядові організації та приватний сектор на безперебійну роботу із запобігання, захисту, реагування, відновлення та пом'якшення наслідків інцидентів, незалежно від причини, розміру, місцезнаходження або складності, з метою зменшення людських і матеріальних втрат та шкоди навколишньому середовищу.

Національна модель обміну інформацією (NIEM)

Спільна програма технічних і функціональних стандартів, ініційована DHS та DOJ, яка підтримує інтероперабельний обмін інформацією на національному рівні.

Національні розвіддані або розвіддані, пов'язані з національною безпекою

Визначається розділом 3 Закону про національну безпеку від 1947 року, зі змінами та доповненнями, як "A) інформація, що стосується можливостей, намірів або діяльності іноземних урядів або їхніх елементів, іноземних організацій або іноземних осіб, або міжнародної терористичної діяльності" (відома як іноземна розвідка); та Б) "інформація, зібрана та діяльність, що здійснюється для захисту від шпигунства, іншої розвідувальної діяльності, саботажу або вбивств, що здійснюються іноземними урядами або їх елементами, іноземними організаціями або іноземними особами, або від їх імені, або від міжнародної терористичної діяльності (відома як "контррозвідка"), незалежно від джерела її отримання, включаючи інформацію, зібрану на території Сполучених Штатів або за її межами, яка (A) стосується більш ніж одного урядового агентства Сполучених Штатів; і (B) стосується (i) загроз Сполученим Штатам, їхньому народу, власності або інтересам; (ii) розробки, розповсюдження або використання зброї масового знищення; або (iii) будь-якого іншого питання, що має відношення до національної або внутрішньої безпеки Сполучених Штатів". " (50 U.S.C. § 401a) Метою діяльності Національної розвідки є надання Президенту і Раді національної безпеки необхідної інформації, на основі якої приймаються рішення щодо проведення і розвитку зовнішньої, оборонної та економічної політики, а також захисту національних інтересів Сполучених Штатів від зовнішніх загроз безпеці. (Виконавчий наказ 12333)

Національний оперативний центр (NOC)

Слугує основним національним центром ситуаційної обізнаності та координації операцій федерального уряду з управління інцидентами. NOC надає міністру внутрішньої безпеки та іншим керівникам інформацію, необхідну для прийняття критично важливих рішень щодо управління інцидентами на національному рівні.

Мережа

Структура взаємопов'язаних компонентів, призначених для взаємодії один з одним і виконання функції або функцій як єдине ціле у визначений спосіб.

Офіс розвідки та аналізу (I&A)

Розвідувально-аналітичний відділ є складовою DHS та національного розвідувального співтовариства (РС). Вона забезпечує збір, аналіз і поширення інформації, пов'язаної із загрозами національній безпеці, серед усього спектру споживачів послуг у сфері національної безпеки в DHS, на штатному, місцевому, племінному і територіальному рівнях, у приватному секторі та в розвідувальному співтоваристві.

Планування

Підготовка до майбутніх ситуацій, оцінка потреб організації та ресурсів, необхідних для реагування на ці ситуації, а також розробка стратегій реагування на них.

Політика

Принципи та цінності, якими керуються при виконанні обов'язків. Політика - це не заява про те, що потрібно робити в конкретній ситуації. Це радше виклад керівних принципів, яких слід дотримуватися в діяльності, спрямованій на досягнення цілей.

Конфіденційність (Інформація)

Запевнення, що органи кримінального правосуддя дотримуватимуться правових та конституційних обмежень щодо збору, зберігання, використання та розкриття інформації, що ідентифікує особу, а використання такої інформації буде суворо обмежено обставинами, за яких судовий процес дозволяє використання інформації, що ідентифікує особу.

Конфіденційність (Персональні дані)

Запевнення, що органи кримінального правосуддя дотримуватимуться правових та конституційних обмежень щодо збору, зберігання, використання та розкриття інформації про поведінку особи, включаючи її комунікації, зв'язки та транзакції, а використання такої інформації суворо обмежуватиметься обставинами, за яких правова процедура санкціонує спостереження та розслідування.

Закон про конфіденційність

Законодавство, яке дозволяє особі переглядати майже всі федеральні файли, що стосуються її/його, накладає обмеження на розкриття інформації, що ідентифікує особу, визначає відсутність таємних систем обліку фізичних осіб і зобов'язує уряд розкривати свої джерела інформації.

Процедура

Метод виконання операції або спосіб продовження курсу дій. Процедура відрізняється від політики тим, що спрямовує дії в конкретній ситуації на виконання конкретного завдання в рамках політики. І політика, і процедура орієнтовані на досягнення певної мети. Однак політика встановлює межі для дій, тоді як процедури спрямовують відповіді в межах цих меж.

Рекомендації

Пропозиції щодо дій, які необхідно вжити за результатами аналізу.

Відповідальність

Відповідальність відображає, як використовуються повноваження підрозділу або окремої особи, і визначає, чи були досягнуті цілі та виконана місія у спосіб, що відповідає визначеним межам повноважень.

Оцінка ризиків

Ризик визначається як добуток трьох основних змінних: 1) загроза (ймовірність виникнення атаки), 2) вразливість і 3) наслідки (відносна вразливість і очікуваний вплив атаки). Оцінка ризику - це процес якісного або кількісного визначення ймовірності настання несприятливої події та серйозності її впливу на актив. Це функція загрози, вразливості та наслідків. Оцінка ризику може включати сценарії, в яких два або більше ризиків взаємодіють, створюючи більший або менший вплив. Оцінка ризиків є основою для ранжування ризиків і визначення пріоритетів для контрзаходів.

Ризик класично представляється як добуток ймовірності певного результату і наслідків цього результату. Оцінка загроз, вразливостей і наслідків, з якими стикається географічна зона відповідальності об'єднаного центру, на рівні штату або регіону. Оцінка ризиків використовується для визначення пріоритетних інформаційних потреб об'єднаного центру, а також для підтримки зусиль з планування готовності до внутрішньої безпеки на рівні штатів і міст з метою розподілу фінансування, сил і засобів та інших ресурсів.
У традиційній кримінальній розвідці оцінка ризиків означає аналіз цілі, нелегального товару або жертви для визначення ймовірності нападу або злочинної компрометації, а також для аналізу вразливих місць.

Безпека

Ряд процедур і заходів, які в поєднанні забезпечують захист людей від шкоди, інформації від неналежного розголошення або зміни та активів від крадіжки або пошкодження (Комісія з питань кримінального правосуддя, 1995 р).

Ситуаційний звіт (SitRep)

Документ, який містить підтверджену або перевірену інформацію та чіткі деталі (хто, що, де і як), що стосуються інциденту.

Оцінка загроз

Оцінка присутності злочинця або терориста в межах юрисдикції, інтегрована з оцінкою потенційних цілей цієї присутності та заявою про ймовірність того, що злочинець або терорист вчинить протиправний акт. Оцінка фокусується на можливості, здатності та готовності злочинця або терориста реалізувати загрозу.

Об'єднане командування (UC)

Застосування ICS, що використовується, коли більше ніж одне відомство має юрисдикцію щодо інциденту або коли інциденти перетинають політичні юрисдикції. Відомства працюють разом через призначених членів UC, часто старших осіб відомств та/або дисциплін, які беруть участь в UC, для встановлення спільного набору цілей і стратегій та єдиного плану дій щодо інциденту.

Ініціатива з безпеки міських територій (UASI)

UASI задовольняє унікальні міждисциплінарні потреби у плануванні, операціях, обладнанні, навчанні та тренуваннях для міських районів з високою щільністю населення, що характеризуються підвищеною небезпекою.

Попередження

Заздалегідь повідомляти про можливу шкоду або віктимізацію в результаті отриманої інформації та розвідувальних даних про ймовірність злочину або терористичного акту.

Абревіатури

ACAMS	Автоматизована система управління критичними активами
AIATP	Навчальна програма з підвищення обізнаності у сфері антитерористичної розвідки
BJA	Бюро сприяння правосуддю
CFR	Кодекс федеральних правил
CIAC	Колорадський центр розвідувального аналізу
CICC	Координаційна рада з питань кримінальної розвідки
CIKR	Критична інфраструктура та ключові ресурси
CONOPS	Концепція операцій
COOP	План безперервності операцій
CPG	Посібник з комплексної готовності
CVI	Інформація про вразливість до хімічного тероризму
DHS	Міністерство національної безпеки
DNC	Національний з'їзд Демократичної партії
DOC	Оперативні центри департаментів
DOJ	Міністерство юстиції
EEI	Основні елементи інформації
EOC	Центр управління в надзвичайних ситуаціях
EOP	План дій у надзвичайних ситуаціях
Epi-X	Обмін епідемічною інформацією
ESF	Функції підтримки в надзвичайних ситуаціях
ФБР	Федеральне бюро розслідувань
FEMA	Федеральне агентство з надзвичайних ситуацій
FLETC	Федеральний центр підготовки правоохоронних органів
FLO	Офіцер зв'язку з питань процесу злиття
FOUO	Для службового користування
FPC	Федеральний координатор з питань готовності
ГІС	Географічна інформаційна система
GIWG	Глобальна робоча група з питань розвідки
Global	Глобальна ініціатива з обміну інформацією у сфері правосуддя
HAN	Мережа оповіщення про стан здоров'я
HSDN	Мережа даних внутрішньої безпеки
HSEEP	Програма навчань та оцінювання у сфері внутрішньої безпеки
HSGP	Програма грантів у сфері внутрішньої безпеки
HSIN	Інформаційна мережа внутрішньої безпеки
I&A	Управління розвідки та аналізу
IAP	План дій на випадок інциденту
IC	Командування інцидентом
ICP	План збору інформації
ICS	Система управління інцидентами
IEMC	Інтегрований курс з управління надзвичайними ситуаціями
IIATP	Вступна програма підготовки розвідувальних аналітиків
IOC	Центр розвідувальних операцій
IP	Управління захисту інфраструктури
ISE	Середовище обміну інформацією
IT	Інформаційні технології
JTTF	Об'єднана антитерористична група
LEO	Правоохоронні органи онлайн

LLIS	Обмін інформацією про вивчені уроки
LOA	Лист-угода
MACS	Міжвідомча координаційна система
MNJAC	Міннесотський об'єднаний аналітичний центр
MOU	Меморандум про взаєморозуміння
NCIRC	Національний ресурсний центр кримінальної розвідки
NEDSS	Національна електронна система епіднагляду за захворюваннями
NDA	Угода про нерозголошення
НІЦ	Національний інтеграційний центр
NIEM	Національна модель обміну інформацією
NIMS	Національна система управління інцидентами
NIPP	Національний план захисту інфраструктури
NOC	Національний оперативний центр
NPD	Національний директорат з питань готовності
NRCC	Національний координаційний центр реагування
NRF	Національна рамка реагування
NSSE	Національна спеціальна подія у сфері безпеки
ODNI	Офіс директора національної розвідки
OHA	Управління з питань охорони здоров'я
PCII	Інформація про захищену критичну інфраструктуру
PM-ISE	Програмний менеджер середовища обміну інформацією
RFI	Запит на інформацію
RISS	Регіональні системи обміну інформацією
RNC	Республіканський національний з'їзд
RRCC	Регіональний центр координації реагування
SGI	Інформація про гарантії
SINs	Постійні інформаційні потреби
SME	Експерт з предметної області
SOP	Стандартні операційні процедури
SSI	Конфіденційна інформація про безпеку
TCL	Перелік цільових можливостей
TPEP	Програма навчань із запобігання тероризму
UASI	Ініціатива з безпеки міських територій
UC	Об'єднане командування
USSS	Секретна служба США
WMD	Зброя масового знищення

Додаток Б: Проект Меморандуму про взаєморозуміння

Цей проект Меморандуму про взаєморозуміння надається лише в якості керівництва для опису того, як можуть взаємодіяти між собою об’єднаний центр та ЕОС. Він не є Меморандумом про взаєморозуміння для створення об’єднаного центру або ЕОС. Посібник з написання меморандуму про взаєморозуміння для роботи об’єднаного центру доступний за посиланням www.iir.com/global/resourcesGuidelines.htm.

Спільне розташування або спільна діяльність об'єднаного центру і ЕОС здійснюється не в кожному штаті, тому в цьому проекті будуть розглянуті відмінності між спільною діяльністю і окремими операціями. У деяких випадках центри можуть функціонувати як об'єднані центри зі спільним персоналом або як окремі об'єкти, що охороняються, з функціями об'єднаного центру і ЕОС.

Деякі частини цього проєкту можуть не стосуватися вашої юрисдикції. Можливо, у вашій юрисдикції буде потрібно додати додаткові формулювання для роз'яснення питань, взаємовідносин або для отримання підписів. Він не претендує на всеохоплюючий характер, а радше є прикладом для центрів злиття і ЕОС для початку процесу розробки Меморандуму про взаєморозуміння, що відповідає їхній ситуації і юрисдикції.

Проект Меморандуму про взаєморозуміння

Між_____Штатним об'єднаним центром та _Штатною службою з надзвичайних ситуацій

I. Мета

(У цьому розділі чітко сформулюйте мету цього Меморандуму про взаєморозуміння. Зазначте, що вона полягає лише у визначенні того, як два вже створені центри будуть взаємодіяти для обміну інформацією на благо держави та нації.)

Метою цього Меморандуму про взаєморозуміння є встановлення політики, що регулює діяльність відомств, які беруть участь у взаємодії між Об'єднаним центром та Центром з надзвичайних ситуацій ("EOC"). Керівні принципи, викладені в цьому документі, слугуватимуть максимізації співпраці та створенню офіційної, ефективної робочої групи, здатної вирішувати питання ефективного та результативного управління, класифікації та розповсюдження інформації про кримінальні злочини, загрози та/або небезпеки, пов'язані з національною безпекою та/або тероризмом, у штаті та Сполучених Штатах Америки.

II. Місія

(Цей розділ повинен містити заяву про місію термоядерного центру та EOC з коротким, стислим і чітким викладом цілей і ролей центрів.)

Ця угода відображає спільні зусилля між Fusion Center та Агентством з управління надзвичайними ситуаціями щодо обміну стратегічною, оперативною та/або тактичною інформацією та розвідданими з питань національної безпеки, тероризму та/або злочинності на підтримку операцій з управління надзвичайними ситуаціями, реагування та/або відновлення, зокрема інформацією, яка була визнана важливою для підтримки діяльності EOC до, під час та після активації EOC під час інциденту, відповідно до основних інформаційних потреб, викладених нижче. *(Якщо були визначені конкретні типи інформації, які будуть обмінюватися, їх можна описати нижче або в додатку)*.

III. Управління

(Вставити склад Консультативної ради. Розглянути питання про те, щоб до складу ради входили керівник державного правоохоронного органу або агентства внутрішньої безпеки в якості голови, державний координатор з управління надзвичайними ситуаціями (співголова), представники адміністрації губернатора або агентства/відомства внутрішньої безпеки або готовності, представник(и) від законодавчої гілки влади, представник Федерального бюро розслідувань, представник Національної гвардії штату, представник асоціацій начальників, що представляють поліцію, пожежників, шерифів, представник державних протипожежних програм і будь-яких інших організацій, які вважатимуться зацікавленими в процесі взаємодії між Об'єднаним центром і EOC. Також розгляньте, як ці члени будуть відбиратися, призначатися та замінюватися.)

Відповідальність за діяльність Центру злиття несе (керівник правоохоронного органу або органу внутрішньої безпеки). Однак, багатопрофільна Керівна/Консультативна рада під головуванням (керівника правоохоронного органу або органу внутрішньої безпеки держави) або його/її уповноваженої особи матиме завдання переглядати операційні процеси та ефективні і дієві системи управління інформацією та обміну інформацією на штатному рівні, включаючи обмін інформацією між об'єднаним центром та EOC.

Консультативна рада надаватиме рекомендації Голові щодо розробки політики, вирішення конфліктів та забезпечення дотримання Меморандуму про взаєморозуміння. Консультативна рада також розглядатиме звіти, подані будь-якими робочими групами Центру, та готуватиме щорічні звіти для Губернатора.

Для надання рекомендацій Консультативній раді буде створена міждисциплінарна Робоча група Центру з питань ф'южн-інжинірингу. Співголовами Робочої групи будуть керівники Центру злиття та ЕОС на місцях, які щомісяця звітуватимуть Консультативній раді про операційні проблеми, вдосконалення та потреби разом із щомісячним звітом про діяльність Центру.

IV. Організаційна структура

(У цьому розділі ми почнемо визначати глобальні організаційні та управлінські структури. Пам'ятайте, що мета Меморандуму про взаєморозуміння полягає в тому, щоб особи, які приймають рішення, погодилися і взяли на себе зобов'язання щодо глобальних робочих відносин. Деякі деталі, що стосуються конкретних операцій, можуть бути більш придатними для Посібника з експлуатації або стандартної операційної процедури ("SOP"),

A. Об'єднаний центр складається з керівників та аналітиків від кожного відомства-учасника. В Об'єднаному центрі працюють представники (штатного) ЕОС та інших партнерів на умовах повної або часткової зайнятості, залежно від рівня загрози та ситуацій кризового менеджменту.

Об'єднаний центр складається з двох окремих підрозділів: 1) Відділ спостереження і 2) Аналітичний відділ, до складу якого входять Антитерористичний підрозділ та Відділ інформації та розвідки національної безпеки. Група спостереження буде укомплектована співробітниками, які пройшли спеціальну підготовку і відповідають за отримання, обробку та поширення інформації, а також за запити на інформацію (RFI). Аналітичний відділ зосередиться на інтеграції та аналізі розвідувальної інформації і готуватиме звіти, продукти та брифінги. Управління інформаційними системами та обладнанням для Державного комітету з питань розвідки та Об'єднаного центру, відповідно, здійснюватимуть (відомства/організації).

Звіти, продукти та інформація, які відповідають або задовольняють заздалегідь визначені інформаційні потреби ЕОС, надаватимуться до центру спостереження ЕОС як звичайний хід діяльності об'єднаного центру під час стабільного стану роботи ЕОС.

За запитом на підтримку активації ЕОС або інциденту (активний стан), окремі функції об'єднаного центру повинні надавати додаткову підтримку:

1. Відділ спостереження отримуватиме звіти про ситуацію від ЕОС та надаватиме інформацію для брифінгів, звітів та презентацій у разі потреби. Надана інформація допоможе забезпечити ЕОС та (штатні органи, що приймають рішення) більш повною ситуаційною обізнаністю.

2. Аналітичний відділ додає звіти про ситуацію з ЕОС до загального ситуаційного аналізу. Аналітики доповнюють персонал ЕОС в рамках Функції підтримки в надзвичайних ситуаціях (ESF) 13 (Правоохоронні органи) і можуть доповнювати інші ESF або операції ЕОС за запитом (наприклад, транспорт, енергетика, охорона здоров'я). Залежно від обставин, таке посилення може полягати в нарощуванні додаткової аналітичної підтримки в рамках об'єднаного центру, або ж може вимагати передислокації аналітиків до ЕОС з відповідною можливістю зворотного зв'язку з об'єднаним центром. Остаточне рішення щодо обсягу ресурсів, необхідних для посилення ЕОС під час активної фази, прийматиметься об'єднаним центром. При цьому буде врахована вся діяльність об'єднаного центру на момент і під час активації ЕОС.

B. EOC складається зі спеціального персоналу, який працює, підтримує загальну обізнаність про ситуацію в штаті та готовий активувати додаткові ресурси штату для задоволення будь-яких потреб у запобіганні, реагуванні, відновленні або пом'якшенні наслідків будь-якої надзвичайної ситуації. Оперативний штаб знаходиться у віданні ( ) Державного агентства з надзвичайних ситуацій. Для забезпечення постійної оперативної картини по всій території штату до штату можуть залучатися співробітники інших відомств. Для отримання та розповсюдження інформації про надзвичайні ситуації серед осіб, які приймають рішення, персоналу та допоміжних установ буде функціонувати центр спостереження.

1. Центр спостереження надаватиме інформацію центру злиття, щоб обидва центри мали повну оперативну картину в будь-який час, і консультуватиме центр злиття щодо будь-яких додаткових інформаційних потреб, які виникають в результаті переходу від стаціонарного стану до активного стану. Центр спостереження також інформуватиме об'єднаний центр, коли активується EOC, і даватиме рекомендації щодо того, наскільки об'єднаному центру необхідно посилити EOC.

2. Секції EOC, коли вони активовані, повідомляють про свої інформаційні потреби об'єднаному центру через диспетчерський центр EOC. Якщо запитується і отримується посилення об'єднаного центру, заохочується прямий зв'язок між командуванням або секціями EOC і аналітичним відділом об'єднаного центру. Всі звіти про ситуацію, розроблені в EOC, будуть надаватися як до чергового підрозділу об'єднаного центру, так і до підрозділу аналізу. Аналіз об'єднаного центру може бути доданий до звітів про ситуацію, брифінгів і презентацій, що проводяться в EOC або для нього, відповідно до класифікації документів. EOC буде дотримуватися всіх грифів секретності та протоколів безпеки об'єднаних центрів. *(Якщо конкретні протоколи безпеки були узгоджені, вони можуть бути описані нижче або у додатку)*

EOC повинен бути готовий забезпечити відповідну робочу зону для роботи персоналу об'єднаного центру, якщо розширення вимагає переміщення ресурсів об'єднаного центру до EOC.

Це може включати доступ до захищених приміщень, доступ до захищених засобів зв'язку, включаючи телефон та/або електронну пошту, а також доступ до захищених контейнерів для зберігання захищених документів.

C. Нагляд

(У цьому розділі має бути визначена субординація між керівниками та персоналом.)

Майте на увазі, що після активації EOC може використовувати персонал штатних установ з багатьох дисциплін, зовнішні ресурси та приватний сектор. Меморандум про взаєморозуміння між об'єднаним центром і EOC повинен бути складений таким чином, щоб окреслити загальну взаємодію між двома центрами, не створюючи прецеденту, що кожне відомство вимагатиме окремих угод для укомплектування штату EOC.

Меморандум про взаєморозуміння має зосередитися на тому, як обидва центри обмінюються інформацією в стаціонарному та активному стані, щоб задовольнити операційні вимоги обох центрів та очікування осіб, які приймають рішення.

Керівник об'єднаного центру підпорядковується (наприклад, командиру підрозділу державної поліції), який через канали підпорядковується (голові державного правоохоронного органу або агентства внутрішньої безпеки), посадовій особі на рівні Кабінету міністрів, відповідальній за громадську безпеку та/або правоохоронну діяльність, а також губернатору області. Призначена посадова особа з управління в надзвичайних ситуаціях, призначена на об'єднаний центр, підпорядковується Директору Оперативного відділу Державного управління з надзвичайних ситуацій,

який через канали підпорядковується Державному координатору з управління в надзвичайних ситуаціях, посадовій особі Кабінету Міністрів, яка здійснює нагляд за громадською безпекою та/або управлінням в надзвичайних ситуаціях, а також Губернатору області.

Під час активації ЕОС ресурси об'єднаного центру, що використовуються для посилення ЕОС, продовжуватимуть діяти в межах свого підпорядкування, перебуваючи в межах об'єднаного центру. Якщо посилення ЕОС вимагає переміщення персоналу об'єднаного центру до ЕОС, вони підпорядковуються і діють відповідно до встановленої структури ЕОС. Це не повинно відрізнятися від будь-якого іншого ресурсу ЕОС, що працює в ЕОС під час активації.

Проблеми та труднощі, які можуть виникнути під час будь-якої операції, будуть взаємно вирішуватися керівниками відповідних відомств і вирішуватимуться якомога швидше. Домовлено, що вирішення будь-яких проблем на найнижчому можливому адміністративному рівні відповідає інтересам усіх сторін.

Організаційна схема, яка визначає, куди буде призначений персонал об'єднаного центру під час активації ЕОС, може допомогти прояснити розподіл повноважень.

Залежно від потреб інциденту, функція інформації та розвідки може бути активована як п'ята секція, як елемент у складі оперативної секції або секції планування, або як частина командного штабу.

D. Персонал

(Цей розділ описує зобов'язання щодо кадрових ресурсів, необхідних для підтримки ЕОС в стаціонарному та активному станах. Включення мінімальної і, якщо можливо, максимальної кількості персоналу, який буде відряджений з об'єднаного центру (і де він буде підпорядковуватися), допоможе задовольнити потреби ЕОС.)

Центр злиття погоджується призначити принаймні одного керівника і одного аналітика для активації ЕОС. Початкове посилення буде здійснюватися в центрі злиття. Керівник обговорює рекомендації ЕОС з черговим персоналом об'єднаного центру, беручи до уваги інші оперативні вимоги та наявні ресурси. Якщо ЕОС рекомендує посилення на місці, керівник об'єднаного центру визначає рівень необхідної підтримки і перевіряє, який організаційний елемент ЕОС буде підтримуватися ресурсами об'єднаного центру

(Нижче наведено приклад штатного розкладу, який може бути скоригований за необхідності, виходячи зі стану ЕОК та діяльності центрів злиття.)

Зона ЕОС	В об'єднаному центрі	В ЕОС
Офіцер розвідки	1 Аналітик	1 Офіцер розвідки керівного рівня
Секція розвідки/інформації	1 Керівник 1 Аналітик	1 Начальник відділу 1 Керівник 3 Аналітики 1 Адміністратор
Оперативний відділ: Відділ розвідки/інформації	1 Керівник 1 Аналітик	1 Директор філії 3 Аналітик
Секція планування: Розвідка/інформація	1 Керівник 1 Аналітик	1 Керівник групи 3 Аналітика
Підтримка ESF-13	1 Керівник	1 Аналітик

E. Допуски до державної таємниці та класифікація документів

(Цей розділ визначає, кому надається/може бути наданий допуск до державної таємниці на основі вимог федерального агентства-спонсора та згоди дотримуватися класифікації документів, встановленої центром злиття або оригінатором.)

(Ідентифіковані (всі) члени Ф'южн Центру, незалежно від відомства-спонсора, повинні мати допуск до секретної інформації (або вищий), виданий федеральним відомством-спонсором для доступу до інформації, що становить загрозу національній безпеці. Крім того, всі члени Центру зобов'язані пройти перевірку на благонадійність (Державна поліція охорони правопорядку). Персонал, який не має відповідних допусків, повинен буде пройти перевірку, що проводиться Федеральним бюро розслідувань ("FBI") та/або відомством, що бере участь у проекті. Усі підписанти погоджуються дотримуватися правил щодо документів, які контролюються оригінатором, та правил розповсюдження третіми особами

Співробітники ЕОС, включаючи Державного координатора, заступників Державного координатора, керівників оперативних відділів, повинні мати допуск до секретної інформації (або вищий). Начальники відділів планування та керівники центрів спостереження повинні мати допуск "СЕКРЕТНО", виданий відповідним федеральним агентством для доступу до інформації, що становить державну таємницю.

V. Записи та звіти

(Цей розділ забезпечить загальне розуміння записів, зберігання, звітів і продуктів об'єднаного центру. Знову ж таки, важливо пам'ятати, що метою Меморандуму про взаєморозуміння є не документування деталей, а широкі, всеохоплюючі елементи, з якими можуть працювати операційні менеджери.)

З метою досягнення однаковості та узгодженості між установами-учасницями, погоджено, що вхідна інформація, отримана в об'єднаному центрі, буде фіксуватися і документуватися відповідно до існуючих протоколів, що використовуються в даний час або розроблені об'єднаним центром.

У разі розробки оригінальної інформації, яку дозволено поширювати згідно з існуючими протоколами в правоохоронних органах, органах внутрішньої безпеки та розвідки, об'єднаний центр координуватиме таке поширення.

Вся інформація з обмеженим доступом, отримана або створена Об'єднаним центром та/або ЕОС, повинна контролюватися виключно відповідно до чинної політики уряду США щодо засекречення та поводження з інформацією з обмеженим доступом. Робоча група Об'єднаного центру може встановлювати політику та рекомендувати Керівництву та/або Консультативній раді необхідність дублювання звітів за формами відомств-учасників, доступності інформації під час активації ЕОС та захисту документів в ЕОС під час активного стану.

Доступ до цих записів та їх використання здійснюється відповідно до федерального законодавства, законодавства штату та місцевих законів, а також політики та процедур об’єднаного центру та/або ЕОС. Усі записи (правоохоронних органів штату) та їх використання будуть відповідати федеральному законодавству, правилам Міністерства юстиції ("DOJ"), Розділу 28 Кодексу федеральних правил (CFR), частині 23, а також правилам і політиці агентства, включаючи, але не обмежуючись ними (Закони штату про свободу інформації та конфіденційність).

Безпечна кімната, розташована в об’єднаному центрі, є сертифікованим FBI/DHS об'єктом для роботи з інформацією та системами, що становлять загрозу національній безпеці, до рівня (СЕКРЕТНО/НАДЗВИЧАЙНО СЕКРЕТНО) включно для об’єднаного центру. Таким чином, інформація, що отримується, зберігається і управляється в цьому об'єкті, буде оброблятися відповідно до вимог (FBI/DHS). Інформація, пов'язана з ЕОС штату, буде надаватися до ЕОС для відповідної обробки згідно з встановленими протоколами ЕОС. За зареєстрований графік подій (зустрічей, операцій, тестування систем тощо) відповідає адміністративний асистент Ф'южн Центру.

У Штатному ЕОС буде обладнано захищену конференц-залу. Ця кімната буде захищена таким чином, щоб забезпечити роботу, обговорення, брифінги, відео-телеконференції, тимчасове зберігання секретної інформації до рівня "СЕКРЕТНО". До цього приміщення матимуть доступ розширені ресурси об'єднаного центру, що знаходяться на території ЕОС, для роботи з секретною інформацією або її обговорення.
У цьому захищеному конференц-залі буде забезпечено зв'язок з центром злиття, здатний передавати секретну інформацію між центрами.

VI. VI. Фізичне розташування та доступ

(Цей розділ містить інформацію про фізичне місцезнаходження ЕОС або об'єднаного центру. У ньому розглядаються основні питання доступу до інформації, записів або самих центрів. Оскільки обсяг інформації та класифікація документів в об'єднаному центрі, як правило, буде більш суворою, ніж в ЕОС, більша увага може бути приділена доступу до об'єднаного центру. Це повинно допомогти забезпечити співпрацю центру з партнерами, які не є правоохоронними органами, при збереженні належного рівня безпеки для персоналу, приміщень і продуктів.)

Якщо суб'єкти не розташовані спільно, вкажіть окремі місця та засоби зв'язку, що використовуються для передачі інформації під час стаціонарного та активного стану операцій ЕОС, а також під час надзвичайних ситуацій.

Якщо вони спільно використовують захищену кімнату спостереження як засіб координації інформації, вкажіть, де це відбувається.

Центр злиття знаходиться за адресою (вкажіть місцезнаходження та адресу; розгляньте можливість додавання координат широти/довготи). ЕОС знаходиться за адресою (вкажіть місцезнаходження та адресу; розгляньте можливість додавання координат широти/довготи).

Для забезпечення обізнаності про всі операції об'єднаного центру старші посадові особи ЕОС будуть проінформовані за запитом і отримають дозвіл на доступ до відповідної документації об'єднаного центру, з урахуванням будь-яких відповідних правових норм та/або обмежень на доступ до неї. Старші посадові особи ЕОС та їхні представники можуть у будь-який час безпосередньо зв'язатися з об'єднаним центром для отримання оновленої інформації про розслідування/загрози, а також для запиту або надання інформації. Крім того, ЕОС готовий проводити відповідні брифінги та надавати доступ співробітникам об'єднаного центру або іншим посадовим особам за необхідності.

VII. Засоби масової інформації та преса

(У цьому розділі надайте угоду про надання інформації ЗМІ. Під час активації ЕОС Об'єднаний інформаційний центр (JIC), ймовірно, буде керувати розповсюдженням інформації для громадськості. Домовленість тут полягає лише в тому, щоб сформулювати, хто має провідну роль в інших випадках.)

Всі прес-релізи будуть взаємно узгоджуватися і спільно оброблятися відповідно до існуючих інструкцій відомств-учасників. Релізи для ЗМІ повинні мати попереднє схвалення (керівника правоохоронних органів або Агентства внутрішньої безпеки), коли ЕОС перебуває у стаціонарному стані. Під час активної фази ЕОС всі прес-релізи будуть оброблятися Об'єднаним інформаційним центром (JIC). Інформація, отримана з документів або звітів об'єднаного центру, повинна бути узгоджена з об'єднаним центром, представником об'єднаного центру або контактною особою, яка працює в ЕОС, перш ніж вона буде включена в прес-релізи.

VIII. Внесення змін до Угоди

(Цей розділ надає інструмент для внесення змін до Меморандуму про взаєморозуміння після того, як первинна угода буде завершена і підписана. Він також може містити графік перегляду або переробки Меморандуму про взаєморозуміння.)

Зміни до цієї угоди можуть бути внесені лише за взаємною згодою установ-учасниць або шляхом підписання наступного Меморандуму про взаєморозуміння. Приєднання нових агентств-учасників до будь-якого з центрів не вважатиметься формальною зміною Меморандуму про взаєморозуміння і, отже, не вимагатиме схвалення кожного з нинішніх членів; однак нові члени будь-якого з центрів повинні дотримуватися цього Меморандуму про взаєморозуміння як умови участі в об'єднаному центрі або в ЕОС. Після припинення дії меморандуму або виходу з центру все обладнання буде повернуто агентству-постачальнику.

IX. Заробітна плата та компенсації

(У цьому розділі, за необхідності, наводяться формулювання, що дозволяють визначити, яке відомство несе відповідальність за витрати на персонал об'єднаного центру. Тут також роз'яснюються витрати, які будуть включені в будь-які запити на відшкодування за Законом Стаффорда відповідно до оголошеної президентом надзвичайної ситуації. Ці формулювання будуть відрізнятися залежно від того, як фінансується центр.)

Заробітна плата та дозволені понаднормові роботи членів центру злиття або членів КРН оплачуються їхніми відповідними установами. Витрати, пов'язані з активним станом ЕОС, будуть реєструватися і звітуватися відповідно до встановлених ЕОС процедур, щоб максимально задокументувати витрати штату, пов'язані з катастрофою, і допомогти в документуванні прийнятних витрат, що підлягають відшкодуванню, коли буде дозволена федеральна допомога.

X. Дисципліна та безпека

(Цей розділ містить загальні рекомендації щодо діяльності об'єднаного центру. Беручи до уваги мету Меморандуму про взаєморозуміння, цей розділ може бути загальним, з посиланнями на конкретну Концепцію діяльності або Операційний посібник для отримання більш детальної інформації. Цей розділ призначений для того, щоб надати особам, які приймають рішення, схвалення на розробку операційних документів, створених операційними менеджерами. Він не є єдиним документом для керівних принципів роботи центру.)

Персонал обох центрів, незалежно від відомства-спонсора, керуватиметься SOP, в тому числі Політикою безпеки та Розкладом засекречування і розповсюдження інформації. На додаток до будь-яких стандартів політики поведінки, що керують персоналом (Державного управління з надзвичайних ситуацій) або будь-якого іншого агентства, що бере участь у роботі об'єднаного центру, весь персонал центру підлягатиме внутрішньому розслідуванню (Державним правоохоронним органом або Агентством внутрішньої безпеки) за будь-які дії або поведінку, що впливають на безпеку центру або Державного управління з питань надзвичайних ситуацій. Порушення безпеки підлягають внутрішньому розслідуванню (правоохоронними органами штату або Агентством внутрішньої безпеки) або розслідуванням спонсорського федерального агентства. Видалення з центрів та/або припинення доступу відбуватиметься відповідно до SOPs або політики, встановленої Робочою групою Центру злиття.

XI. Управління об'єктами та доступ до них

(Цей розділ передбачає загальну відповідальність за управління об'єктом і безпеку. У ньому може бути визнано, що співробітники відомств, які не належать до державних правоохоронних органів або Агентства національної безпеки, матимуть контрольований, але обмежений доступ до об'єднаного центру. Аналогічно, тут може бути розглянутий доступ до ЕОС, але це не повинно плутати доступ до ЕОС для всіх учасників ЕОС. Майте на увазі, що не всі учасники ЕОС мають доступ до центру, але, як до менш захищеного об'єкту, доступ до ЕОС може бути наданий персоналу об'єднаного центру, особливо, коли вони знаходяться в одному приміщенні.)

Управління об'єктом об'єднаного центру здійснюватиметься (Державною службою охорони правопорядку або Агентством національної безпеки) за домовленістю між ними, включаючи загальну безпеку об'єкту. Об'єктом ЕОС буде керувати Державна служба з надзвичайних ситуацій. Відповідальність за видачу посвідчень/перепусток та контроль доступу покладається на кожен центр. Для забезпечення доступу до обох центрів особам, які за взаємною згодою мають потребу в такому доступі, слід використовувати спільні перепустки/картки доступу.

Достатня кількість персоналу з управління аварійними ситуаціями з допуском федеральної служби безпеки, який пройшов необхідне попереднє розслідування, матиме відповідний доступ до захищеного приміщення і систем, наданий відповідними федеральними агентствами, розташованих в центрі злиття, для проведення операцій і випробувань систем. Будь-які телекомунікаційні канали для підтримки систем управління в надзвичайних ситуаціях (наприклад, інформаційна мережа національної безпеки, захищене відео та підключення до інформаційної мережі попередження про загрозу для критичної інфраструктури), такі як голосовий та факсимільний зв'язок, залишатимуться під відповідальністю (Державного агентства з надзвичайних ситуацій) за технічне обслуговування та покриття витрат. Аналогічно, подібні канали (Державного агентства з питань правопорядку або Агентства внутрішньої безпеки) тощо залишатимуться у віданні (Державного агентства з питань правопорядку або Агентства внутрішньої безпеки), а витрати на їх утримання та експлуатацію - у віданні (Державного агентства з питань правопорядку або Агентства внутрішньої безпеки).

XII. Цивільна відповідальність та відшкодування збитків

(Цей розділ повинен містити юридичні формулювання, визначені сторонами-партнерами Меморандуму як необхідні для покриття цивільної відповідальності та відшкодування збитків за дії та бездіяльність персоналу.)

За жодних обставин установа-учасниця не несе відповідальності за дії персоналу центрів, який не працює в цій установі. Установи-учасниці не вимагатимуть і не матимуть права на відшкодування від інших установ-учасниць за будь-які судові рішення, судові витрати, що виникають у зв'язку з діями персоналу центрів, який працює в цій установі.

Кожна установа-учасниця погоджується захищати, відшкодовувати збитки та убезпечувати всі інші установи-учасниці та їхніх відповідних посадових осіб, агентів та працівників від будь-яких претензій, дій та позовів, а також захищатиме всі інші установи-учасниці та їхніх відповідних посадових осіб, агентів та працівників за власний рахунок і безоплатно для інших установ-учасниць у будь-якому позові, дії або претензії, включаючи позови, пов'язані з тілесними ушкодженнями або смертю будь-якої особи, а також втратою або пошкодженням майна, що виникають у зв'язку з діяльністю або упущеннями, допущеними в ході виконання зазначеними установами-учасницями положень цієї угоди. Ці положення про відшкодування призначені для захисту установ-учасниць та їхніх відповідних посадових осіб, агентів і працівників і не встановлюють жодної відповідальності перед третіми сторонами. Положення цього розділу залишаються чинними після припинення дії цієї Угоди

XIII. Тривалість

(Цей розділ може містити графік, який сторони визначили для перегляду Меморандуму про взаєморозуміння, або коли він буде переглянутий у повному обсязі. Він може бути включений або об'єднаний з розділом про внесення змін до меморандуму, наведеним вище.)

Ця угода набуває чинності з дати, коли останній з представників агентств-учасників, що підписалися нижче, скріпить її своїм підписом. Ця угода залишатиметься чинною до моменту розформування одного з центрів. Під розформуванням не мається на увазі деактивація ЕОС після інциденту. Цей Меморандум про взаєморозуміння є безстроковим. Установи-учасниці можуть припинити свою участь у будь-який час, повідомивши про це за шістдесят днів усі сторони, що підписали цей документ.

Примітка: Питанням комунікації може бути присвячений окремий розділ вище, або вони можуть бути висвітлені в операційних настановах.

Додаток C: Інтерфейс між Центром злиття та EOC: Аналіз найкращих практик координації та інтеграції

DHS/DOJ Fusion Process Technical Assistance Program and Services

United States Department of Justice

FUSION CENTER AND EMERGENCY OPERATIONS CENTER INTERFACE

Аналіз кращих практик координації та інтеграції

Огляд

Спільна Програма технічної підтримки процесу злиття Міністерства національної безпеки (DHS) та Міністерства юстиції (DOJ) підтримує обмін передовим досвідом та отриманими уроками з метою зміцнення національної мережі центрів злиття. На підтримку цієї ініціативи в рамках Програми технічної допомоги у сфері злиття вивчався взаємозв'язок між центрами злиття і центрами управління в надзвичайних ситуаціях ("EOC"), щоб визначити, яким чином ці дві структури взаємно підтримують одна одну.

Цілі цієї роботи полягали в наступному:

1. Визначити можливості та інструменти кожної структури і те, як вони використовуються;
2. Визначити, як ці можливості можна було б краще об'єднати або скоординувати; і
3. визначити, які ресурси, навчання і технічна допомога могли б підтримати зусилля з координації та/або інтеграції між двома організаціями.

Були відвідані наступні об'єкти: Антитерористичний інформаційний центр Арізони (ACTIC), Інформаційно-аналітичний центр Колорадо (CIAC), Об'єднаний центр Флориди (FFC), Центр обміну та аналізу інформації Джорджії (GISAC), Об'єднаний центр розвідки Індіани (IFC), Аналітичний центр штату Луїзіана (LA-SAFE), Об'єднаний центр розвідки штату Луїзіана, Центр обміну інформацією та

обміну штату Луїзіана (LA-SAFE), Центр розвідувальних операцій штату Мічиган (MIOC) і Центр злиття даних штату Вірджинія (VFC).

Кожен візит включав в себе обговорення з персоналом центру злиття і EOC, в тому числі з представниками правоохоронних органів, пожежної служби, служби екстреної медичної допомоги (EMS) і дисциплін з управління в надзвичайних ситуаціях. Під час кожного візиту ставилися наступні питання:

- Чи існує офіційна угода, яка детально описує, як ці дві організації будуть взаємодіяти?
- Які системи або протоколи сприяють комунікації між двома установами?
- Чи проводилося перехресне навчання або вправи для розбудови відносин?
- Якщо обидва органи розташовані разом, чи сприятливо таке розташування для обміну інформацією?
- Якщо вони не розташовані разом, як вони спілкуються та обмінюються інформацією?
- Якими типами інформації обмінюються обидва суб'єкти?
- Як можна покращити відносини між термоядерним центром і EOC?

Інформаційний центр по боротьбі з тероризмом в Арізоні

ACTIC, в якому працює понад 200 осіб, є міжюрисдикційним партнерством, керованим Департаментом громадської безпеки Арізони (DPS) і Федеральним бюро розслідувань (FBI). Центр об'єднує федеральні, штатні та місцеві правоохоронні органи, а також служби швидкого реагування та управління в надзвичайних ситуаціях. Центр спостереження є центральним місцем для інформації, що надходить і виходить з ACTIC, а керівна рада на чолі з DPS Арізони здійснює нагляд за його діяльністю, яка включає в себе потужну програму офіцерів зв'язку з тероризмом (TLO). Програма TLO, створена для вирішення проблем, пов'язаних з усіма видами небезпек, поступово впроваджується в усі заходи із запобігання, захисту, реагування та відновлення в Арізоні.

Координаційні центри з надзвичайних ситуацій по всій Арізоні, як на рівні штату, так і на місцевому чи окружному рівнях, отримують підтримку від програми TLO, коли вони активуються під час інциденту. Вивчення цієї взаємодії було зосереджено на EOC штату Арізона, і були проведені інтерв'ю з персоналом ACTIC, менеджерами з надзвичайних ситуацій, першими особами, які реагують на надзвичайні ситуації, і правоохоронцями з міста Фенікс і округу Марікопа.

EOC штату Арізона знаходиться під наглядом Департаменту з надзвичайних ситуацій штату Арізона і не знаходиться в одному приміщенні з ACTIC. TLO вважали, що їхня участь була цінною під час активації EOC. У таких ситуаціях ACTIC надає всю свою незасекречену інформацію в розпорядження EOC - домовленість, яка дозволяє TLO отримати доступ до різних баз даних об'єднаного центру і аналітичних ресурсів, таких як e-Team і правоохоронна система штату. Ці ресурси також включають перевірку записів у базах даних, геопросторовий аналіз, фотографії Департаменту автотранспорту і тактичні аналітичні продукти.

TLO, які представляють правоохоронні органи, пожежну охорону, швидку медичну допомогу, охорону здоров'я та управління надзвичайними ситуаціями, зобов'язані підписати угоду про нерозголошення інформації, щоб допомогти забезпечити захист прав, свобод і приватного життя громадян. Представники органів управління надзвичайними ситуаціями зазначили, що наявність TLO в їхніх EOC надала їм доступ до відповідних даних, накопичених ACTIC, що зменшило потребу в спільному розташуванні з об'єднаним центром і підвищило їхню здатність реагувати на будь-яку ситуацію. Наразі ACTIC розробляє стандартні операційні процедури ("SOPs"), які визначатимуть, як TLO взаємодіятимуть з EOC Арізони під час інциденту. Ці SOPs будуть підтримуватися ACTIC і поширюватися серед його партнерів.

Інформаційно-просвітницькі та навчальні програми ACTIC, а також потужні аналітичні та слідчі можливості зміцнили відносини між центром злиття та його партнерами з державного та приватного секторів.1 Крім того, ACTIC часто проводить навчання та тренінги з штатними та місцевими EOC, а також брав участь у навчаннях національного рівня (NLE) 2008 року, також відомих як TOPOFF, які надали можливості для навчань та тренувань для всієї спільноти громадської безпеки штату.

Інформаційно-аналітичний центр штату Колорадо

Взаємовідносини між CIAC та EOC штату Колорадо були розглянуті під час Національного з'їзду Демократичної партії (DNC), що відбувся в серпні 2008 року. Хоча CIAC та EOC штату розташовані в одній будівлі, комунікація між ними була епізодичною через еволюцію їхніх відповідних ролей та обов'язків.

[1] 1 Додаткову інформацію про ACTIC та її Програму TLO можна знайти в Системі обміну інформацією про набутий досвід (LLIS) за адресою www.llis.dhs.gov.

У штаті EOC 24/7 працює черговий офіцер, який слугує зв'язком між EOC та CIAC. Черговий офіс EOC отримує продукти CIAC, такі як щоденні/щотижневі звіти та будь-які спеціальні бюлетені, в той час як CIAC періодично отримує звіти та брифінги від чергового офісу EOC.

Готуючись до цієї події, CIAC провів тренінги для більш ніж 200 осіб, включаючи представників правоохоронних органів, пожежної охорони, швидкої медичної допомоги, управління в надзвичайних ситуаціях, охорони здоров'я, сільського господарства, транспорту та військовослужбовців. Деякі з цих працівників були призначені до різних командних центрів, що діяли під час DNC, а персонал з управління надзвичайними ситуаціями продовжує брати участь у програмі з підготовки інструкторів і проходить таку саму підготовку, як і правоохоронці з підготовки інструкторів.

DNC був унікальною і складною подією як для CIAC, так і для EOC. За взаємною домовленістю, основним координатором заходу був EOC Департаменту поліції Денвера. Державний штаб з питань надзвичайних ситуацій відповідав за будь-які надзвичайні потреби за межами міста та округу Денвер. EOC штату надавав підтримку установам, що брали участь в управлінні DNC, які не були укладені контракти з EOC Денвера або керівництвом DNC. У штаті Колорадо паралельно з DNC відбувалося кілька великих заходів (Ярмарок штату Колорадо, "Смак Колорадо" та "Кантрі Джем"). Ці заходи потребують допомоги та моніторингу з боку EOC штату. CIAC надав оцінку загроз для нагляду за цими заходами, а також членам EOC штату в рамках підготовки до можливого запиту на допомогу.

Директор CIAC був призначений до EOC під час DNC і забезпечував керівництво та ситуаційну обізнаність щодо розвідки DNC та Функції підтримки в надзвичайних ситуаціях (ESF) 13 - Координація громадської безпеки та безпеки. Директор також перевіряв інформацію, яку CIAC надавав EOC, щоб гарантувати, що секретна інформація та чутливі розслідування не були скомпрометовані. CIAC проводив брифінги для персоналу EOC щодо розслідувань та потенційних загроз під час змін. Співробітники EOC вважали ці інструктажі цінними і підтримували канали зв'язку відкритими. EOC, як і інші слідчі та аналітичні оперативні центри, використовували WebEOC як один з інструментів зв'язку для надання інформації про FOUO. Загалом, було відзначено, що додаткові тренінги та навчання сприятимуть покращенню каналів комунікації та побудові довірливих відносин.[2]

Флоридський центр злиття

FFC управляється Управлінням розвідки Департаменту правоохоронних органів штату Флорида (FDLE) і є багатопрофільним міждисциплінарним об'єднаним центром по боротьбі з усіма видами злочинів. Згідно із законодавством штату Флорида, його визначено головним об'єднаним центром штату Флорида, що спеціалізується на боротьбі з тероризмом. Частина цього закону кодифікує їхні стосунки з Державним департаментом з питань надзвичайних ситуацій (DEM) і описує ролі та обов'язки кожного з відомств. DEM відповідає за Державний оперативний центр (SOC). У стаціонарному стані чергова служба в SOC забезпечує цілодобовий моніторинг діяльності та подій у штаті і передає будь-яку відповідну інформацію про ситуацію до FFC. FFC також має цілодобовий оперативний компонент, який виконує функції спостереження, попередження та ситуаційної обізнаності для правоохоронних органів та органів громадської безпеки по всьому штату. FFC створила програму офіцерів зв'язку з розвідкою (ILO) з відомствами, які відряджають персонал до FFC. Ці співробітники представляють Міністерства охорони здоров'я, виконання покарань, фінансових послуг, сільського господарства, дорожньо-патрульної служби, охорони навколишнього середовища, освіти, Генеральну прокуратуру, а також Управління з контролю за виробництвом алкоголю, напоїв і тютюну та Національну гвардію штату Флорида, а федеральні компоненти FFC включають Міністерство внутрішніх справ, Генеральну прокуратуру США, Управління транспортної безпеки і Агентство з боротьби з наркотиками (DEA). З ФБР також було створено POC, і два офіцери зв'язку від DEM також призначені до FFC.

[2] 2 Додаткову інформацію про роль ЦПІК у DNC можна знайти на сайті LLIS at www.llis.dhs.gov.

Поліція Флориди виділила спеціальний персонал для укомплектування SOC під час активації. Це дозволяє FFC проводити незалежні розвідувальні операції і надавати підтримку SOC під час інцидентів. Флорида визначила функцію підтримки правоохоронних органів як ESF 16 штату Флорида - "Правоохоронні органи та безпека". Під час активації ESF-16 очолює FDLE, а FFC виконує допоміжну роль. FFC надає інформацію, яка використовується для задоволення потреб у ресурсах, допомоги в плануванні та розгортанні ресурсів, пов'язаних із запобіганням злочинам. Як FFC, так і SOC мають необхідні засоби для отримання та зберігання секретних матеріалів з грифом "Таємно". Крім того, FFC має доступ до національної захищеної мережі передачі даних (Homeland Secure Data Network, HSDN). Для обробки і зберігання цієї інформації були розроблені протоколи безпеки, а офіцер державної безпеки контролює поводження з цими матеріалами і здійснює нагляд за питаннями допуску до них обох організацій.

FFC та SOC мають Меморандум про взаєморозуміння, який описує їхні функції та обов'язки, а також уклали Меморандуми про взаєморозуміння з відповідними установами-учасницями, щоб закріпити їхні робочі відносини. Крім того, FFC розробив політику конфіденційності, яка була доведена до відома і прийнята SOC. FFC та SOC також підтримали перехресне навчання персоналу, забезпечивши, щоб окремі співробітники DEM пройшли базову підготовку ILO від FFC. Цей персонал також бере участь у щомісячних оперативних нарадах.

FFC та SOC відреагували на кілька стихійних лих та техногенних катастроф, а також взяли участь у щорічних командно-штабних навчаннях, що дозволило їм протестувати свої процеси та процедури. Зрештою, ці заходи сприяли вдосконаленню протоколів та особистих стосунків.

Співробітники SOC та FFC відзначили, що семінари для ознайомлення всіх партнерів покращують взаємне розуміння того, яка інформація доступна і як нею можна обмінюватися. Вони також відзначили, що така координація дозволяє уникнути єдиної точки відмови у випадку, якщо інцидент виведе з ладу ту чи іншу систему.

Грузинський центр обміну інформацією та аналізу

У 2007 році губернатор Джорджії об'єднав Агентство з надзвичайних ситуацій Джорджії (GEMA) та Управління внутрішньої безпеки (OHS), створивши GEMA-OHS. Це забезпечило єдині операційні процедури та керівництво з боку керівництва. GISAC управляється Бюро розслідувань Джорджії (GBI), але підпорядковується GEMA-OHS. На рівні кабінету міністрів директор GBI і директор GEMA-OHS підпорядковуються безпосередньо губернатору Грузії.

GISAC укомплектований персоналом з штатних, місцевих і федеральних установ. Наразі до складу GISAC входять співробітники GBI, GEMA-OHS, Патрульної поліції штату Джорджія, Департаменту виконання покарань штату Джорджія, а також представники Асоціації начальників поліції штату Джорджія, Асоціації шерифів штату Джорджія та Асоціації начальників пожежної охорони штату Джорджія. Федеральні партнери, що працюють в GISAC, включають Імміграційну та митну службу США та Міністерство внутрішньої безпеки. GISAC також розміщений в одній будівлі з Атлантським відділенням FBI -JTTF. Щоранку проводяться брифінги між керівниками GISAC та членами FBI JTTF.

SOC підтримує комунікаційні операції (COMMO) в режимі 24/7 під час стабільної роботи. COMMO обробляє всі дзвінки від партнерських агентств у неробочий час, а також спрямовує дзвінки та звіти для агентств по мірі їх надходження. Оператори COMMO мають письмові протоколи, яких дотримуються щодо обробки дзвінків та процедур сповіщення. Це включає в себе повідомлення чергового персоналу GISAC у неробочий час. SOC надсилає ранкову доповідну записку директору GEMA-OHS та іншим старшим посадовим особам, включаючи керівників GISAC.

Зв'язок між GISAC та SOC добре налагоджений і практикується, незважаючи на відсутність формальних SOP для обміну інформацією між цими двома організаціями. Обидві організації визнали, що це є прямим результатом особистих стосунків і комунікації між керівництвом кожного центру.

Хоча було зазначено, що SOP, який би кодифікував таку взаємодію, може бути корисним, відносини між співробітниками об'єднаного центру та EOC виграли від тісної співпраці та комунікації на рівні керівництва.

Хоча спеціальних спільних навчань або тренувань між GISAC і SOC не проводиться, було відзначено, що в них немає необхідності, оскільки ці дві структури координують і співпрацюють на регулярній основі.
Крім того, щоразу, коли проводяться шттані або регіональні навчання, до них залучаються всі відповідні органи. Проте GEMA- OHS і GISAC зазначили, що майбутня розробка спільних навчальних сценаріїв, навчань і SOPs сприятиме подальшому зміцненню існуючих зв'язків.

Луїзіанська штатна аналітична та об'єднана біржа

LA-SAFE був призначений головним штатним центром збору, обробки, аналізу та поширення інформації, пов'язаної з тероризмом, внутрішньою безпекою та правоохоронною діяльністю. Таким чином, він відповідає за моніторинг загроз і надання своїм партнерам і зацікавленим сторонам ситуаційної обізнаності на 24/7 основі. LA- SAFE розташований на території Департаменту громадської безпеки в Батон-Руж.

Державний центр з питань надзвичайних ситуацій управляється Управлінням внутрішньої безпеки та готовності до надзвичайних ситуацій губернатора штату (GOHSEP) і знаходиться на тому ж об'єкті, але не в одному приміщенні з LA-SAFE. Два аналітики GOHSEP призначені до LA-SAFE і служать зв'язковими між двома організаціями. Обидві організації зазвичай використовують WebEOC для розміщення та обміну інформацією, а аналітики GOHSEP також мають можливість отримувати інформацію до рівня LES (Law Enforcement Sensitive), що є конфіденційною для правоохоронних органів. EOC активується під час окремих навчань і великих інцидентів, які вимагають широкої міжвідомчої комунікації. У цей час LA-SAFE регулярно надає підтримку Державному штабу з питань надзвичайних ситуацій, а саме:

- Оновлені оцінки ситуації;
- Ситуаційні звіти (SitReps);
- Аналітична підтримка;
- Надання всіх документів і довідкових матеріалів, включаючи накладення геоінформаційної системи (GIS)3 , графіки, а також можливість проведення відео-телеконференцій; і
- Додаткова підтримка за потреби.

Під час урагану Густав LA-SAFE підтримала GOHSEP, використовуючи GIS для планування маршрутів евакуації, визначення об'єктів, які потребують заходів захисту, і визначення доступності ресурсів. Зовсім недавно вони взяли участь у навчаннях NLE 2009, які були зосереджені на запобіганні і дозволили організаціям ознайомитися з можливостями один одного. Зрештою, відповідні ролі та обов'язки, що визначають взаємодію між LA-SAFE та Державним комітетом з питань надзвичайних ситуацій, визначаються SOP, які наразі переглядаються.

Мічиганський розвідувально-оперативний центр

Поліція штату Мічиган (MSP) підпорядковується MIOC, EOC штату та офісу спостереження MSP, який знаходиться в одному приміщенні з MIOC. MIOC та EOC штату не розташовані разом, і немає офіційної угоди про те, як ці дві структури будуть взаємодіяти.

[3] Див. розділ Штатні та місцеві центри злиття: Розробка процесів збору та використання геопросторової інформації для підтримки планування та реагування на всі види небезпек для отримання додаткової інформації про використання ГІС.

Для управління кожним підрозділом призначається лейтенант MSP. В той час як лейтенанти в центрі злиття і вахтовому пункті підпорядковуються одному капітану, лейтенант в EOC підпорядковується іншому капітану, який відповідає за всі функції з управління в надзвичайних ситуаціях. Всі три лейтенанти тісно співпрацюють між собою і мають багато обов'язків, що перетинаються, а при активації EOC, MIOC фактично підтримує функцію ESF-13.

Крім того, кожен лейтенант отримує і передає інформацію з таких джерел, як Національний оперативний центр ("NOC") DHS, DHS I&A, регіональні відділення FEMA та інші державні установи. Ці три функціональні компоненти використовують декілька інструментів для забезпечення обміну інформацією між собою, в тому числі Інформаційну мережу національної безпеки (HSIN) і WebEOC, на яку також покладаються під час часткової і повної активації. Офіс спостереження забезпечує ситуаційну обізнаність щодо подій по всьому штаті, наприклад, інформацію про перекриття доріг та інциденти, які впливають на MSP, в той час як MIOC готує щоденні брифінги з відкритим вихідним кодом та інші спеціалізовані продукти для EOC та його партнерів. MIOC і EOC також проводять від шести до дев'яти спільних навчань на рік, щоб перевірити і поліпшити свої робочі відносини. Ці навчання доповнюються тренінгами з NIMS, які проводяться для обох організацій.

Ці процеси та навчання також добре перевірені під час реальних подій. Наприклад, коли під час фіналу чотирьох чоловічого баскетбольного турніру NCAA був задіяний EOC, MIOC розробив оцінку загроз до початку заходу і надав аналітичну допомогу під час турніру. Водночас, MIOC та EOC зазначили, що тісний зв'язок між ними може бути посилений завдяки розробці та впровадженню SOPs, а також завдяки участі у навчаннях, що базуються на сценаріях. Ці навчання допоможуть підвищити обізнаність про їхні відповідні інформаційні вимоги, особливо перед початком заходу або під час стабілізації ситуації.

Вірджинський центр злиття

Поліція штату Вірджинія (VSP) та Департамент з питань надзвичайних ситуацій штату Вірджинія (VDEM) мають зразкові відносини. VFC і EOC штату Вірджинія розташовані в одному приміщенні і розробили взаємодоповнюючі політики і процедури.

Законодавчий орган штату Вірджинія визначив VFC як міжвідомчий розвідувальний центр злиття для штату Вірджинія, яким керуватиме VSP у співпраці з VDEM. Меморандум про взаєморозуміння також визначає відносини між департаментом поліції і VDEM. Політика і процедури взаємодії між VFC і VDEM включені в SOP, в яких визначені ролі і обов'язки учасників.4

Перший сержант VSP, спеціальний помічник VDEM з питань безпеки Співдружності і аналітик VSP з питань нагляду розподіляють обов'язки з управління VFC. VDEM забезпечує об'єднаний центр аналітичним персоналом, який працює пліч-о-пліч з аналітиками VSP та інших відомств; весь персонал проходить перехресну підготовку, має однаковий рівень допуску до секретної інформації і однаковий рівень доступу до секретної інформації. Спостережні офіси VFC та EOC регулярно обмінюються інформацією.

Аналіз

Успіх взаємодії між центрами термоядерного синтезу та EOC безпосередньо пов'язаний з кількома факторами. По-перше, це дух співробітництва і взаємодії між установами, який допомагає будувати довірчі відносини, подібні до тих, що склалися у Вірджинії. Спільне розташування і постійні контакти, які воно пропонує, можуть сприяти розвитку цих відносин, але це не завжди можливо з огляду на фінансові та фізичні обмеження.

[4] Меморандум про взаєморозуміння з VFC та інші SOPS знаходяться на LLIS at www.llis.dhs.gov.

Якщо спільне розташування не є можливим, ЕОС і центр злиття повинні організовувати регулярні зустрічі, навчальні заходи, семінари та вправи для налагодження відносин. Набуте в результаті знайомство забезпечить плавний перехід від стаціонарного стану до активації.

Незалежно від того, чи мають ЕОС і об'єднаний центр спільний фізичний простір, їхня взаємодія має бути чітко визначена, взаємно узгоджена і формалізована законодавством та іншими документами. До них відносяться Меморандуми про взаєморозуміння і SOP, які потенційно можуть слугувати додатком до CONOPS центру і/або планів аварійної експлуатації (EOP) ЕОС в стаціонарному стані і під час активації. SOP між цими двома структурами повинні визначати, як буде здійснюватися обмін інформацією, з ким і за яких обставин (наприклад, щоденна взаємодія з диспетчерською службою, рівень взаємодії під час інциденту). Вони також повинні описувати процес обміну та перехресного навчання персоналу відомства як у стаціонарному стані, так і під час активації, а також взаємодію з відповідними ESF під час активації.

Іншими механізмами побудови відносин є програми офіцерів зв'язку (FLO) або TLO, які можуть розширити доступ об'єднаного центру до служб екстреного реагування та управління надзвичайними ситуаціями. Залучення персоналу ЕОС до програми FLO забезпечить міцні зв'язки та знайомство з об'єднаним центром.

На основі аналізу попередньо визначених взаємовідносин між об'єднаними центрами та ЕОС, нижче наведені потенційні рішення, які слід розглянути окремо або в тандемі з іншими для посилення співпраці:

- **Спільне розташування:** Спільне розташування є ідеальним способом побудови міцних відносин між центром злиття та ЕОС завдяки довірі та розумінню, які розвиваються завдяки постійним контактам та взаємодії. У багатьох юрисдикціях це може бути нездійсненним, тому слід розглянути можливість використання віртуальних платформ для спілкування та співпраці.

- **Документація з питань політики та процедур:** Для формалізації узгоджених взаємовідносин і будь-яких пов'язаних з ними ролей та обов'язків слід розробити SOP та MOU. Вони також слугуватимуть основою для навчання персоналу. У цій документації також слід передбачити доступ до секретної та несекретної інформації, поводження з нею та обмін нею, включаючи персонал, який має допуск і доступ до систем, що використовуються для передачі інформації та розвідувальних даних.

- **Тренування:** Будь-які визначені контактні особи/представники повинні пройти широке перехресне навчання з питань роботи об'єднаних центрів та ЕОС, щоб переконатися, що вони добре знайомі з обома організаціями. Співробітники об'єднаних центрів і ЕОС також повинні мати можливість ознайомитися з роботою кожного з них, а також з усіма відповідними системами та інструментами, що використовуються в них. Це допоможе налагодити особисті стосунки між співробітниками обох установ. Крім того, спільне навчання з питань безпеки (поводження, зберігання, 28 CFR, частина 23 і т.д.) і засекречування ([LES, тільки для службового користування [FOUO], захищена інформація критичної інфраструктури [PCII], засекречена інформація і т.д.), а також з питань управління надзвичайними ситуаціями та реагування на інциденти (Національна система управління інцидентами [NIMS], Національна система реагування [NRF], Система управління інцидентами [ICS] і т.д.) значно покращить розуміння того, як правильно взаємодіяти і обмінюватися інформацією.

- **Вправи:** Об'єднані центри та ЕОС повинні регулярно проводити спільні тренування на основі сценаріїв та реальних ситуацій для оцінки своїх комунікаційних можливостей та обміну оперативною інформацією, визначених у їхніх SOP та меморандумах про взаєморозуміння. Ці навчання також повинні слугувати для оцінки та усунення конфліктів між ролями та обов'язками персоналу, відповідального за координацію та/або інтеграцію цих зусиль. SOPs повинні регулярно оновлюватися на основі результатів навчань.

- **Комунікаційні системи:** Об'єднані центри і ЕОС повинні вивчити наявні в них засоби зв'язку і використовувати ті з них, які забезпечують найбільший зв'язок і найкращим чином дозволяють організаціям обмінюватися оперативною інформацією і продуктами, такими як оповіщення і попередження. Обговорення між об'єднаним центром і ЕОС повинні стосуватися рівнів класифікації систем, доступу, навчання і обмежень щодо того, що можна і що не можна обмінюватися. Крім того, слід обговорити можливості відеотелеконференцій (VTC) і захищених VTC (SVTC), а також альтернативні механізми обміну чутливою або засекреченою інформацією (наприклад, HSDN).

Існує також кілька кадрових підходів, які можуть бути використані для побудови та підтримки відносин між ЕОС та центрами злиття, зокрема:

- **Визначення зв'язкових/представників**: Між центром злиття та ЕОС має бути визначений зв'язковий/представник, основним обов'язком якого є забезпечення координації між цими двома організаціями. Це може бути неповний робочий день або додаткова робота. Ролі цієї особи/представника повинні бути чітко задокументовані та визначені.

    - **ESF-13:** Слід розглянути можливість використання персоналу об'єднаного центру для виконання функцій ESF-13 під час активації ЕОС. Це підвищить спроможність об'єднаного центру надавати аналітичну підтримку ЕОС і забезпечить можливість зворотного зв'язку з федеральними, державними і місцевими розвідувальними ресурсами.

- **Призначення штатних аналітиків/персоналу:** Виходячи з наявних ресурсів, ЕОС або відповідальний орган з управління надзвичайними ситуаціями повинен розглянути питання про призначення або деталізацію штатного аналітика в об'єднаному центрі. Цей аналітик повинен мати глибокі знання про операції з управління надзвичайними ситуаціями і виступати в якості експерта з питань управління/реагування на надзвичайні ситуації (SME). До обов'язків аналітика входило б надання підтримки SME в операціях і аналізі об'єднаного центру та забезпечення своєчасного і точного потоку інформації між об'єднаним центром і ЕОС до, під час і після інцидентів.

  Крім того, об'єднаний центр повинен розглянути можливість призначення або включення офіцера розвідки з відповідним допуском до роботи в ЕОС під час активації. Це забезпечить безперервний і життєво важливий потік інформації та розвідувальних даних до ЕОС, а також зворотний зв'язок для отримання підтримки від об'єднаного центру.

- **Об'єднання або віртуальне з'єднання вахтових офісів/відділень:** Вартові або чергові служби як об'єднаного центру, так і ЕОС повинні розглянути можливість фактичного об'єднання, щоб забезпечити максимально своєчасний і точний обмін повідомленнями. Це дозволило б своєчасно обмінюватися інформацією, координувати її та/або усунути конфлікти, а також слугувало б механізмом офіційної інтеграції зусиль об'єднаного центру з попередження з зусиллями ЕОС з реагування на інциденти. Такий механізм також дозволить ефективно використовувати обмежені ресурси/персонал.

- **Розширення програм FLO:** Існуючі програми FLO слід розглядати як механізм покращення комунікації між центром злиття та ЕОС, особливо якщо не було визначено спеціальних аналітиків або зв'язкових, відповідальних за цю взаємодію. Слід розглянути можливість включення до програми персоналу з управління надзвичайними ситуаціями, якщо він ще не бере в ній участі. Якщо програма FLO ще не існує, об'єднаний центр повинен розглянути можливість її впровадження з метою налагодження відносин з ЕОС через мультидисциплінарний та малий і середній персонал (наприклад, пожежники, служби екстреної медичної допомоги, управління в надзвичайних ситуаціях, органи охорони здоров'я та ін).

This page intentionally left blank.

Додаток D: Розробка процесів збору та використання геопросторової інформації для підтримки планування та реагування на всі види небезпек

DHS/DOJ Fusion Process Technical Assistance Program and Services

Fusion Center Spotlight

Державні та місцеві центри злиття: Розробка процесів збору та використання геопросторової інформації для підтримки планування та реагування на всі види небезпек

Передумови

Ряд штатних і місцевих центрів злиття даних (SLFC) знаходяться на різних етапах розробки формалізованих процесів і процедур для запиту, доступу і використання геопросторових даних для підтримки планування і реагування на всі види небезпек. Визнання SLFC необхідності і корисності цієї інформації часто передує масштабній події, як це було у випадку з сезоном ураганів 2005 року і повенями на Середньому Заході влітку 2008 року. Корисні геопросторові дані можуть охоплювати діапазон від аерофотозйомки до/після повені або супутникових знімків до точкових місць водозаборів у заплаві до місць розташування об'єктів критичної інфраструктури та ключових ресурсів ("CIKR") по всій території штату. SLFC повинні займатися ретельним плануванням, щоб бути готовими запитувати, отримувати доступ і ефективно використовувати геопросторові ресурси.

Питання для розгляду

Координація вимог до збору

Координація до початку події між центром злиття, штатним/регіональним центром з надзвичайних ситуацій (EOC), США Міністерством національної безпеки (DHS), Федеральним агентством з надзвичайних ситуацій (FEMA), регіоном, штаб-квартирою FEMA

Штаб-квартира FEMA та Національна гвардія штату є ключовим елементом успіху. В ідеалі, така координація має відбуватися задовго до серйозної техногенної або природної катастрофи, щоб переконатися, що вже існує процес визначення та розподілу потенційних ресурсів для збору. Ключовими місцевими та регіональними учасниками цього постійного партнерства є наступні особи або їхні еквіваленти:

- Директор Центру злиття
- Керівник державної програми з геоінформаційних систем (GIS)
- Начальник відділу планування штату з питань надзвичайних ситуацій
- Представник розвідки Управління розвідки та аналізу ("I&A") МНБ США в Об'єднаному центрі розвідки
- Планувальник GIS Національної гвардії штату та/або представник рівня J2/3
- Регіональний координатор GIS FEMA
- Радники з питань безпеки, регіональні геопросторові аналітики та регіональні брокери з обміну інформацією Управління захисту інфраструктури DHS

Ця формальна або неформальна Рада з питань збору даних має найкращі можливості на штатному/регіональному рівні для визначення того, які геопросторові ресурси збору даних можуть бути використані для вирішення конкретної проблеми; як співпрацювати для визначення пріоритетності зусиль зі збору даних; і як найкраще розподілити обмежені ресурси для збору даних ефективно.

Базові геопросторові дані

Перш ніж подавати запит на нові геопросторові дані, Рада з питань колекціонування повинна мати чітке уявлення про те, які базові дані вже є в наявності. Сюди входять знімки, точкове розташування (наприклад, невеликих об'єктів CIKR), лінійні (наприклад, залізничні колії та лінії електропередач) і полігональні набори даних (наприклад, більші об'єкти CIKR, такі як військові бази). Потенційні джерела даних, які можна перевірити на точність і повноту в рамках цього огляду, включають:

- Державний інформаційно-аналітичний центр GIS
- Засекречені списки рівнів DHS
- Несекретні дані, що містяться в системі Constellation/Automated Critical Asset Management System (C/ACAMS)
- Несекретні дані, що містяться в Програмі інфраструктури національної безпеки, які доступні через DHS Earth та Інтегрований загальний аналітичний переглядач DHS
- FEMA's Hazards U.S. (HAZUS), програмне забезпечення, яке картографує та відображає дані про небезпеку (землетруси, ураганні вітри та повені), а також результати оцінок пошкоджень та економічних втрат для будівель та інфраструктури

Запит нових геопросторових даних

Після того, як Рада збору даних добре зрозуміє, які дані вже доступні, вона зможе краще оцінити, які існують прогалини, які вона, можливо, захоче заповнити заздалегідь, до настання масштабної небезпечної події або в розпалі її розвитку. Тип даних, який, можливо, найчастіше потрібен після того, як сталася природна загроза, - це знімки після події. Ці дані можуть бути використані для кращої оцінки пошкодження територій і рівня збитків, тривалості затоплення, придатності автомобільних і залізничних коридорів тощо. Важливо, щоб Комісія з питань збору даних розуміла різні типи і класифікації наявних продуктів і те, що можна з них отримати, а також те, як запитувати конкретну інформацію, наприклад, через процедуру запиту на штатну і місцеву підтримку (SLSR), яку проводить I&A, або через Національний координаційний центр з реагування (NRCC). Хорошим прикладом є повені в Індіані в червні 2008 року, коли засекречені знімки були єдиним типом інформації, який можна було своєчасно отримати, щоб задовольнити вимоги щодо збору даних. Однак більшість штатних і місцевих органів влади, які потребували цих даних, не мали допуску до них. В результаті Національне агентство геопросторової розвідки (NGA) змогло створити лінійні графічні зображення з грифом "Для службового користування" (U-FOUO), отримані на основі засекречених знімків, щоб задовольнити потреби штатів і місцевих органів влади.

Розповсюдження за принципом "єдиного вікна

Не менш важливою, ніж розуміння повного спектру доступної інформації, є здатність центру злиття та інших штатних і місцевих замовників мати доступ до якомога більшої кількості даних і пов'язаних з ними продуктів в єдиній веб-системі або платформі.

Під час повені на Середньому Заході у 2008 році нещодавно отримані знімки і похідні продукти були доступні в різних системах, в тому числі в Intelink-U Intellipedia, веб-порталі доступу і пошуку NGA, Інформаційній мережі національної безпеки - управління в надзвичайних ситуаціях, системах Національної гвардії, а також в електронній пошті Національної захищеної мережі передачі даних. Це створило проблеми з доступом і доступністю даних, які можна було б суттєво вирішити, розмістивши якомога більше даних і контенту U-FOUO на веб-сайті Intellipedia, який функціонував дуже ефективно і був визнаний найкращою практикою після проведення навчань. Однак, якщо Intelink-U/Intellipedia буде використовуватися на повну потужність під час і після великомасштабної небезпечної події, штатні та місцеві зацікавлені сторони повинні переконатися, що всі, кому потрібен доступ до облікового запису, зробили це в рамках процесу планування і координації перед подією.

Рекомендації

У міру того, як SLFC досягатимуть цілей, викладених у Базових можливостях для центрів злиття штатів і великих міських територій, кожен з них повинен буде вирішувати питання збору, використання і подальшого поширення геопросторової інформації та продуктів серед різних клієнтів. Це передбачає розуміння геопросторових потреб клієнтів SLFC, які дані вже доступні, які існують прогалини, як визначити пріоритети і завдання для збору або створення наборів даних, а потім як обробити і упакувати інформацію у форматі, що відповідає потребам клієнтів, забезпечуючи при цьому цілісність процесу. Коли SLFC починають визначати ці вимоги та окреслювати коло пов'язаних з ними питань, вони повинні переконатися, що всі штатні/регіональні ключові партнери представлені. Наведені вище питання для розгляду дають просту схему для початкових обговорень між зацікавленими сторонами у сфері геопросторових даних.

Ця сторінка навмисно залишена порожньою.

Додаток E: Державно-приватне партнерство: Посібник з Кодексу поведінки партнерства "Сейфгард Айова" для зв'язківців, які працюють у центрах з надзвичайних ситуацій

Lessons Learned Information Sharing
LLIS.gov

Sharing Information
Enhancing Preparedness
Strengthening Homeland Security

PRACTICE NOTE

Державно-приватне партнерство: Посібник з Кодексу поведінки для зв'язкових, які працюють у центрах реагування на надзвичайні ситуації Партнерства Safeguard Iowa

ПРАКТИКА

Партнерство "Сейфгард Айова" (SIP) розробило посібник з кодексу поведінки для своїх координаторів, які працюють у центрах оперативного реагування на надзвичайні ситуації ("EOC"). Посібник з кодексу поведінки допомагає гарантувати, що всі контактні особи SIP розуміють свої ролі та обов'язки під час перебування в EOC.

ОПИС

SIP - це коаліція приватного сектору, метою якої є зміцнення потенціалу штату Айова у сфері запобігання, підготовки, реагування та відновлення після природних і техногенних катастроф шляхом співпраці між державним і приватним секторами. Комісія з надзвичайних ситуацій штату Айова (SEOC) або окружна комісія з надзвичайних ситуацій може звернутися до SIP з проханням відрядити одного або більше представників на свій об'єкт під час інциденту, залежно від масштабу інциденту

Партнери SIP зменшують вплив надзвичайних ситуацій на свої громади, доповнюючи державну систему готовності та реагування власними ресурсами та досвідом. Для отримання додаткової інформації про SIP, будь ласка, зверніться до "Історії успіху" проекту "Обмін інформацією,The Safeguard Iowa Partnership.

Координатори SIP слугують каналом передачі інформації та рекомендацій між EOC та організаціями приватного сектору. Під час операцій з ліквідації наслідків НС SIP-координатори сприяють наданню приватним сектором матеріальних ресурсів, зокрема води, продуктів харчування, льоду та одягу. Вони допомагають координатору з управління пожертвами, але не керують операціями зі збору пожертв. Координатори SIP також надають EOC інформацію щодо питань приватного сектору, таких як графіки роботи, місця розташування об'єктів, потреби у доступі до будівель, транспортні потреби, логістика переїзду, питання безпеки та пріоритети відновлення.

Під час літніх штормів 2008 року координатор SIP в штаті Айова координував роботу волонтерів та пожертвування ресурсів. SIP сприяла державно-приватній координації, що покращило загальні зусилля SEOC з ліквідації наслідків стихійного лиха.

Для отримання додаткової інформації про участь SIP у ліквідації наслідків літнього шторму 2008 року, будь ласка, ознайомтеся зі звітом SIP про результати роботи, *Safeguard Iowa Partnership After-Action Report, September 2008*.

Однак на момент штормів SIP не розробила інструкцій для своїх зв'язкових, які працюють в EOC. Після завершення операцій з ліквідації наслідків урагану SIP вирішила розробити посібник з кодексу поведінки для підтримки та керівництва своїми зв'язківцями, які працюють в EOCs, під час майбутніх активацій.

Посібник з кодексу поведінки SIP розглядає кваліфікацію та обов'язки контактної особи. Перш ніж особа може виконувати функції представника SIP, вона повинна пройти навчання з операцій з ліквідації наслідків аварійних ситуацій та володіти повними знаннями про управління інцидентами. Кожен представник SIP повинен:

- Знати назви та типи різних організацій приватного сектору та їхні функції;
- Мати сильні навички усного та письмового спілкування, а також навички аналізу та оцінки проблем;
- Володіти навичками роботи з текстовими редакторами, електронними таблицями та базами даних;
- Закінчити серію курсів незалежного навчання (IS), що пропонуються Інститутом управління в надзвичайних ситуаціях Федерального агентства з надзвичайних ситуацій:
  - IS 100: Система управління інцидентами,
  - IS 700: Національна система управління інцидентами,
  - IS 701: Міжвідомча система координації, та
  - IS 775: Управління та операції з ліквідації наслідків надзвичайних ситуацій;
- Пройти навчальні тренінги з наступних тем:
  - Реєстр бізнес-ресурсів,
  - Мережа оповіщення про стан здоров'я,
  - Інформаційна мережа національної безпеки
  - WebEOC.

WebEOC - це програмне забезпечення для управління інформацією про кризові ситуації, яке надає дані в режимі реального часу керівникам та працівникам служб реагування на надзвичайні ситуації. Програмне забезпечення дозволяє користувачам обмінюватися даними через дошки оголошень, карти на основі геоінформаційних систем, каталоги ресурсів та інші інструменти.

Для того, щоб служити в EOC, кожен зв'язковий SIP повинен отримати спонсорську підтримку від свого роботодавця. Крім того, як волонтер, кожен зв'язковий повинен нести відповідальність за всі свої витрати на проїзд, проживання та харчування.

Посібник з кодексу поведінки також визначає обов'язки зв'язкових під час перебування в EOC під час активації. Після прибуття до EOC зв'язковий SIP повинен з'явитися безпосередньо до офіцера зв'язку EOC, щоб отримати набір операційних процедур, логістичну інформацію та спорядження. Як правило, в EOC надається комп'ютер, доступ до Інтернету, можливість друку, стаціонарний телефон, факс та канцелярське приладдя. Однак посібник SIP рекомендує, щоб кожен зв'язковий також мав особистий мобільний телефон і зарядний пристрій для резервного зв'язку на випадок, якщо в EOC виникнуть проблеми зі зв'язком. Координатори повинні укомплектувати повну зміну EOC, як це визначено черговим керівником робіт з ліквідації наслідків надзвичайної ситуації. Посібник SIP також вимагає, щоб під час роботи в EOC зв'язківці завжди носили діловий одяг.

ПОСИЛАННЯ

Партнерство Safeguard Iowa
http://www.safeguardiowa.org

ЦИТАТИ

Хаберл, Джамі. Виконавчий директор, Партнерство "Сейфгард Айова". Інтерв'ю з організацією "Обмін інформацією про набутий досвід", 09 липня 2009 року.

Партнерство "Захистимо Айову". Звіт про результати діяльності партнерства "Захистимо Айову", вересень 2008 року. Вересень 2008 р.
https://www.llis.dhs.gov/docdetails/details.do?contentID=32905

ВІДМОВА ВІД ВІДПОВІДАЛЬНОСТІ