ДЕРЖАВНА СЛУЖБА УКРАЇНИ З НАДЗВИЧАЙНИХ СИТУАЦІЙ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ЦИВІЛЬНОГО ЗАХИСТУ УКРАЇНИ

МАТЕРІАЛИ

Круглого столу «Суб'єкти забезпечення цивільного захисту (регіонального та місцевого рівня) в реалізації завдань із запобігання та ліквідації наслідків НС»

26 лютого 2021 року

Харків – 2021

УДК 341

СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ДСНС УКРАЇНИ

Л.В. Борисова, к.ю.н., доцент, Національний університет цивільного захисту України,
В.В.Чумак, д.ю.н., доцент, Харківський національний університет внутрішніх справ

Виконання Стратегії реформування системи Державної служби України з надзвичайних ситуацій визначено Наказом ДСНС України від 02.03.2017 № 132 «Про затвердження Плану заходів щодо реалізації Стратегії реформування системи Державної служби України з надзвичайних ситуацій». Третім етапом впровадження Стратегії (2019-2020 роки) забезпечується функціонування автоматизованої системи управління телекомунікаційними мережами, центру обробки даних, комплексної підсистеми інформаційної підтримки прийняття рішень з питань надзвичайних ситуацій, у тому числі комплексної системи захисту інформації.

Основним завданням є:

поєднання функціональних можливостей інформаційних і телекомунікаційних систем задля побудови єдиної системи управління службами екстреної допомоги населенню незалежно від відомчого підпорядкування;

організація взаємодії та координацію в он-лайн режимі всіх державних, муніципальних (комунальних), обласних служб, діяльність яких пов'язана з реагуванням на надзвичайні (небезпечні) події, виклики громадян, аварії, стихійні лиха, або ліквідацією їх наслідків;

забезпечення інформування (оповіщення) керівного складу та населення, збір, обробку та аналіз всієї інформації, що надходить, в одному місці – єдиній оперативно-черговій службі ОТГ (центральній диспетчерській службі ОТГ).

Відповідно до українського законодавства, кібербезпека – це захищеність життєво важливих інтересів людини й громадянина, суспільства та держави у процесі використання кіберпростору, яка забезпечує сталий розвиток інформаційного суспільства і цифрового комунікативного середовища, своєчасне виявлення, запобігання та нейтралізацію реальних і потенційних загроз національній безпеці України у кіберпросторі (ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII). Забезпечення безпеки критичної інфраструктури – це концепція готовності протистояти серйозним загрозам роботи важливих об'єктів інфраструктури та об'єктів підвищеної загрози в умовах розповсюдження інформаційних технологій.

До об'єктів кібербезпеки та кіберзахисту віднесено:

– комунікаційні системи всіх форм власності, в яких обробляються національні інформаційні ресурси;

– об'єкти критичної інформаційної інфраструктури (перелік затверджується КМ України);

– комунікаційні системи, які використовуються для задоволення суспільних потреб та/або реалізації правовідносин у сферах електронного урядування, електронних державних послуг, електронної комерції, електронного документообігу.

Найбільш уразливими об'єктами забезпечення інформаційної безпеки України в умовах надзвичайних ситуацій є система прийняття рішень з оперативних дій (реакцій), пов'язаних із розвитком таких ситуацій і ходом ліквідації їхніх наслідків, а також система збору й обробки інформації про можливе виникнення надзвичайних ситуацій.

Особливе значення для нормального функціонування зазначених об'єктів має забезпечення безпеки інформаційної інфраструктури країни при аваріях, катастрофах і стихійних лихах. Особливе значення для нормального функціонування зазначених об'єктів має забезпечення безпеки інформаційної інфраструктури при аваріях, катастрофах і стихійних лихах.

Отже, важливо дотримуватися організаційно-технічних принципів, порядку здійснення заходів із технічного захисту інформації, порядку контролю в цій сфері, характеристик загроз для інформації, норм та вимог з технічного захисту інформації, порядку атестації та експертизи комплексних систем захисту інформації та комплексів технічного захисту інформації, що визначаються нормативно-правовими актами, прийнятими в установленому порядку відповідними органами.

Обов'язковою є реєстрація всіх подій, що мають безпосереднє відношення до безпеки, здійснюється в журналі реєстрації, який містить інформацію щодо дати, часу, місця (адреси робочої станції в АС), імені користувача, типу й успішності чи неуспішності кожної зареєстрованої події. Журнал реєстрації повинен містити інформацію достатню для однозначної ідентифікації робочої станції, користувача, процесу і/або об'єкта, що мали відношення до кожної зареєстрованої події.

Повинна бути реалізована можливість виявлення фактів несанкціонованого доступу до об'єктів та (або) процесів, що потенційно можуть призвести до виникнення загроз для інформації, і забезпечена фіксація в журналі системи: імені користувача, об'єкта та (або) процесу, до якого була спроба доступу, місця та часу, коли виникла загроза. Допускається фіксація додаткової інформації, яка дозволяє однозначно ідентифікувати процеси, що створили загрозу. КСЗІ повинна забезпечити блокування роботи робочих станцій, з яких була здійснена загроза інформації.

Виведення інформації у текстовому вигляді повинно здійснюватися на зареєстровані в установленому порядку паперові носії на спеціально виділених для цього пристроях друку. КСЗІ повинна забезпечити контроль за процесом виконання роздруку інформації з фіксацією в системному журналі: імені користувача, об'єкта, робочої станції та часу, коли здійснюється роздрук. У разі необхідності можлива фіксація додаткової інформації, що характеризує процес роздруку і дозволяє його однозначно ідентифікувати.

Використовуючи міжнародний стандарт ISO/IEC 15408 «Загальні критерії оцінки безпеки інформаційних технологій», можна проаналізувати динаміку побудови системи захисту інформації й процеси, що відбуваються при цьому.

контрзаходи – комплекс засобів захисту;загрози події, які потенційно можуть порушити одне із властивостей інформації, що захищають;

порушник – людина, діяльність якого може привести до реалізації загроз, тобто він є джерелом;

уразливості – властивості носіїв інформації, які можуть сприяти реалізації загроз безпеки інформації;

ризик – величина, що характеризує можливість зазнати шкоди через порушення режиму інформаційної безпеки;

керуванням ризиками – процес ідентифікації й зменшення ризиків, які можуть впливати на інформаційну систему.

Усі параметри інформаційної бази взаємозалежні, впливаючи один на одного тою чи іншою мірою. Найбільш уразливим об'єктами забезпечення інформаційної безпеки є системи збору і обробки інформації про можливе виникнення надзвичайних ситуацій і прийняття рішень щодо оперативних дій, пов'язаних із розвитком таких ситуацій і ходом ліквідації їх наслідків. Слід зазначити, що розвиток інформаційно-телекомунікаційних технологій встановлює, що межі модернізації програмно-технічного забезпечення не повинні знаходитись у яких-небудь рамках, вони повинні мати можливість гнучко змінюватися з урахуванням вимог та сучасних умов для безперебійного функціонування зв'язку, телекомунікацій та інформатизації в системі ДСНС.