УДК 351.746.1:614

Волянський Петро Борисович
здобувач Інституту державного управління
у сфері цивільного захисту, заслужений лікар України,
к.мед.н. доцент.

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ МЕДИЧНИХ УСТАНОВ У МЕЖАХ МЕДИЧНОГО ЗАХИСТУ ЗА УМОВ НАДЗВИЧАЙНИХ СИТУАЦІЙ МИРНОГО ХАРАКТЕРУ

У статті досліджені проблеми забезпечення інформаційної безпеки лікувальних закладів, що включені до переліку установ і закладів системи охорони здоров'я у складі сил і засобів державної служби медицини катастроф України для ліквідації медико-санітарних наслідків надзвичайних ситуацій природного і техногенного характеру.

Ключові слова: медичний захист, надзвичайна ситуація, інформація, безпека.

Volyanskiy Petr

A MANAGEMENT OF MEDICAL ESTABLISHMENTS OF INFORMATIVE SAFETY IS CONSEQUENCIES OF MEDICAL DEFENCE AT TERMS OF EMERGENCIES OF PEACEFUL CHARACTER

In the article the considered questions of providing of informative safety of medical establishments are in the conditions of overcoming of medical consequences of emergencies of peace-time.

Key words: medical defence, emergencies, information, safety.

Волянский Петр Борисович

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ МЕДИЦИНСКИХ УЧРЕЖДЕНИЙ В ПРЕДЕЛАХ МЕДИЦИНСКОЙ ЗАЩИТЫ ПРИ УСЛОВИЯХ ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЙ МИРНОГО ХАРАКТЕРА

В статье исследованы проблемы обеспечения информационной безопасности лечебных заведений, которые включены к перечню учреждений и заведений системы здравоохранения в составе сил и средств государственной службы медицины катастроф Украины для ликвидации медико-санитарных последствий чрезвычайных ситуаций естественного и техногенного характера.
Ключевые слова: медицинская защита, чрезвычайная ситуация, информация, безопасность.

Постановка проблеми. Доведено, що для вирішення проблеми забезпечення інформаційної безпеки необхідно застосування законодавчих, організаційних та програмно-технічних заходів. Нехтування хоч би одним з аспектів цієї проблеми може призвести до втрати або витоку інформації, вартість і роль якої в житті сучасного суспільства набуває все більш важливе значення.

Аналіз останніх досліджень і публікацій. Для ефективного функціонування системи запобігання та реагування на НС природного та техногенного характеру потрібна своєчасна, безперервна, повна та достовірна інформація, без якої важко оцінити обстановку, можливості сил та засобів служб, призначених для запобігання та ліквідації НС, координувати їх зусилля. Говорячи про роль інформації, ст. 8 Закону України «Про захист населення і територій від надзвичайних ситуацій техногенного та природного характеру» твердить: «Інформування та оповіщення у сфері захисту населення й територій від НС техногенного та природного характеру є основним принципом та головним невід'ємним елементом усієї системи заходів такого захисту».

Виклад основного матеріалу. Інформацію у сфері захисту населення і територій від НС техногенного та природного характеру становлять відомості про НС будь-якого характеру, що прогнозуються або виникли, з визначенням їх класифікації, меж поширення й наслідків, а також способи й методи реагування на них.

Інформація у сфері захисту населення й територій від НС техногенного та природного характеру, діяльність центральних та місцевих органів виконавчої влади, виконавчих органів рад у цій сфері є гласними і відкритими, якщо інше не передбачено законом».

При управлінні за умов надзвичайної ситуації (НС) не існує витрат праці й коштів, що не пов’язані з використанням інформації. Інформація, інформаційний фонд за умов НС стає основним ресурсом ефективного прийняття рішень, спрямованих на ліквідацію НС. Як правило, за умов НС основною проблемою в прийнятті рішень і реалізації ефективних управлінських рішень є нестача не ресурсів і коштів, а саме – інформації, яка необхідна для використання цих ресурсів і коштів з найбільшим успіхом.

Інформація про можливість виникнення НС і тенденції її розвитку надходить до системи управління у ході вивчення оточуючого середовища, прогнозування та аналізу стану.

Населення в зоні НС та поза неї отримує уявлення про ситуацію із засобів масової інформації: газет, журналів, радіо і телебачення. Влада завжди визнавала, що для контролю над суспільством вона повинна взяти в свої руки засоби масової інформації, та особливо важливо це за умов НС. Всі засоби масової інформації на адміністративній території повинні бути підпорядковані керівництву з ліквідації НС, а вся інформація повинна контролюватися. Це допоможе уникнути самих неприємних і небажаних наслідків у цей складний період часу.

Окрім широкого застосування базових засобів підтримки управлінської діяльності, необхідна також розробка систем для вирішення значної кількості функціональних задач.

Для ефективного функціонування системи запобігання та реагування на НС природного та техногенного характеру потрібна своєчасна, безперервна, повна та достовірна інформація, без якої важко оцінити обстановку, можливості сил та засобів служб, призначених для запобігання та ліквідації НС, координувати їх зусилля. Говорячи про роль інформації, ст. 8 Закону України «Про захист населення і територій від надзвичайних ситуацій техногенного та природного характеру» твердить: «Інформування та оповіщення у сфері захисту населення й територій від НС техногенного та природного характеру є основним принципом та головним невід'ємним елементом усієї системи заходів такого захисту».

Інформацію у сфері захисту населення і територій від НС техногенного та природного характеру становлять відомості про НС будь-якого характеру, що прогнозуються або виникли, з визначенням їх класифікації, меж поширення й наслідків, а також способи й методи реагування на них.

Інформація у сфері захисту населення й територій від НС техногенного та природного характеру, діяльність центральних та місцевих органів виконавчої влади, виконавчих органів рад у цій сфері є гласними і відкритими, якщо інше не передбачено законом».

З метою інформаційно-аналітичного забезпечення процесів підготовки, прийняття та контролю виконання рішень з питань НС створена в масштабах держави Урядова інформаційно-аналітична система з питань НС (УІАС НС). Основним призначенням УІАС НС є забезпечення Кабінету Міністрів України та інших органів виконавчої влади достовірною інформацією щодо екологічної безпеки, факторів ризику виникнення НС, а при виникненні НС – про її наслідки, хід робіт з ліквідації наслідків НС [1].

Питання інформаційного забезпечення ліквідації наслідків НС природного і техногенного характеру можна розділити на два напрями: перший – інформаційне забезпечення органів місцевої влади постраждалої території під час проведення аварійно-рятувальних і гуманітарних операцій; другий –

інформаційне забезпечення мобільних рятувальних і медичних формувань, які працюють в локальних районах постраждалої території [2].

У даний час благополуччя і навіть життя багатьох людей залежать від забезпечення інформаційної безпеки безлічі комп'ютерних систем обробки інформації, контролю і управління різними об'єктами. До таких систем медичні інформаційні системи. Їх особливістю є, насамперед, те, що в них зберігається та обробляється інформація, всебічно визначальна соціальний статус людини, а це зумовлює особливу форму відносин між тими, хто її формує, і тими, хто використовує. Значить, поряд з підвищеними вимогами до достовірності інформації повинні накладатися моральні обмеження на доступ до неї, а також юридична відповідальність надають її осіб.

Будь-який медичний працівник несе повну відповідальність (моральну, адміністративну і кримінальну) за конфіденційність інформації, до якої він отримує доступ в ході своєї професійної діяльності [3].

Актуальність теми забезпечення інформаційної безпеки в медицині підтверджується тим, що у більшості медичних установ питання інформаційної безпеки не розглядаються в принципі, а також відсутністю будь-яких заходов, спрямованих на забезпечення інформаційної безпеки та збереження лікарської таємниці. Проблема безпеки інформаційних технологій виникла на перетині двох активно розвиваються і, напевно, найбільш передових у плані використання технічних досягнень напрямів – безпеки технологій та інформатизації. Сама проблема безпеки, звичайно, не є новою, адже забезпечення власної безпеки – задача першорядної важливості для будь-якої системи незалежно від її складності і призначення будь-то соціальне утворення, біологічний організм або система обробки інформації. Однак в умовах, коли об'єкт, що захищається являє собою інформаційну систему, або коли кошти нападу мають форму інформаційних впливів, необхідно розробляти і застосовувати зовсім нові технології та методи.

Системний підхід до аналізу та управління безпекою безпосередньо пов'язаний з визначенням факторів безпосереднього ризику.

Для визначення реального (можливого) ризику цих небезпечних чинників, треба спочатку їх ідентифікувати. З метою ідентифікації можна використовувати результати атестації робочих місць за умовами праці та травмоопасності. Це дозволить різко скоротити кількість небезпечних факторів за рахунок тих, які за результатами атестації не представляють реальну небезпеку.

Потім, використовуючи якісний і кількісний метод оцінки ризиків (на базі минулого досвіду і шляхом аналізу статистичних даних за останні 10–15 років, виділяємо найбільш високі (неприйнятні) ризики, і проводимо їх детальний аналіз з допомогою відповідних методів: · Аналіз небезпеки та зв'язок з втратою працездатності; · Аналіз «дерева відмов»; · Аналіз «дерева подій».

До основних заходів щодо забезпечення безпеки населення в надзвичайних ситуаціях належать такі: прогнозування і оцінка можливості наслідків надзвичайних ситуацій; розробка заходів, спрямованих на запобігання або зниження ймовірності виникнення таких ситуацій, а також на зменшення їх наслідків. Крім того, дуже важливим є навчання населення діям у надзвичайних ситуаціях і розробка ефективних способів його захисту.

Прогнозування надзвичайних ситуацій – це метод орієнтовного виявлення та оцінки обстановки, що складається в результаті стихійних лих, аварій і катастроф. Розрізняють довгострокові й короткострокові прогнози. Довгострокові прогнози спрямовані на вивчення і визначення сейсмічних районів, територій, де можливі селеві потоки чи зсуви, меж зон ймовірного затоплення при аваріях гребель або природних повенях, а також кордонів вогнищ ураження при техногенних аваріях. Короткострокові прогнози використовуються для орієнтовного визначення часу виникнення надзвичайної ситуації.

Для складання прогнозів використовуються різні статистичні дані, а також відомості про деякі фізичні і хімічні характеристики навколишніх природних середовищ. Так, для прогнозування землетрусів у сейсмонебезпечних районах вивчають зміну хімічного складу природних вод,

проводять спостереження за зміною рівня води в колодязях, визначають механічні та фізичні (електричні та магнітні) властивості грунту. Значну інформацію для прогнозу землетрусів може дати спостереження за поведінкою деяких тварин.

Розроблено методи прогнозування пожеж – лісових, торф'яних і ін. Для прогнозування впливу прихованих вогнищ пожежі (підземних або торф'яних) на можливість виникнення лісових пожеж використовується фотозйомка в інфрачервоній частині спектру, здійснювана з літаків чи космічних апаратів.

Для прогнозування обстановки, що виникає при розвитку різних надзвичайних ситуацій, застосовують математичні методи (математичне моделювання).

При прогнозуванні надзвичайної ситуації планують постійно проводяться фонові і захисні заходи.

До постійно проводимих заходів належать постійний контроль за якістю будівельно-монтажних робіт при зведенні будинків і споруд, створення надійної системи оповіщення про виникнення надзвичайної ситуації, будівництво захисних укриттів і притулків, постачання населення засобами індивідуального захисту (наприклад, протигазами), обов'язкове навчання населення правилам поведінки у надзвичайних ситуаціях, розробка планів ліквідації наслідків надзвичайних ситуацій та їх фінансове і матеріальне забезпечення та ін.

При прогнозі моменту надзвичайної ситуації перевіряються і приводяться в готовність система оповіщення населення, а також аварійно-рятувальні служби, розгортається система спостереження і розвідки, нейтралізуються особо небезпечним виробництва та об'єкти (хімічні підприємства, атомні електростанції та ін), проводиться часткова евакуація населення.

Серед заходів для підвищення надійність систем безпеки медичних інформаційних систем доцільно використовувати такі основні методи і способи захисту: кардинальне поліпшення системи реєстрації первинних медичних даних на основі застосування індивідуальних носіїв інформації (ІНІ);

обов’язкове дублювання інформації, що зберігається в ІНІ, в базах даних різних рівнів; періодична (краще щоденна) актуалізація всіх баз даних в інформаційній системі (ця міра виключає можливість фальсифікації медичних відомостей «заднім числом»); забезпечення доступу до інформації різними шляхами: відкрити частину інформації для всіх, відкрити частину інформації для співу і записи медичним фахівцям за умови їх ідентифікації, і, нарешті, частину інформації відкрити для читання з дозволу пацієнта; для досягнення необхідного рівня захисту інформації з боку програмних засобів використовувати кошти мережевих операційних систем. Захист інформації від несанкціонованого доступу повинна забезпечуватися блокуванням доступу до інформації:

- для СУБД – з боку як персоналу, так і тих завдань системи, яким дана інформація не вимагається в силу функціонального призначення;
- на робочому місці – з боку користувачів, що не володіють відповідними повноваженнями на доступ до різних інформаційних ресурсів;
- по каналах зв’язку – з боку мережевих користувачів і тих завдань системи, яким дана інформація не потрібно знову-таки в силу функціонального призначення. Сучасний досвід вирішення проблем інформаційної безпеки показує, що для досягнення найбільшого ефекту при організації захисту інформації необхідно керуватися рядом принципів. Першим і найбільш важливим є принцип безперервності вдосконалення та розвитку системи інформаційної безпеки: постійний контроль функціонування системи, виявленні її слабких місць, можливих каналів витоку інформації і НСД, оновлення і доповнення механізмів захисту в залежності від зміни характеру внутрішніх та зовнішніх загроз, обгрунтування та реалізація на цій основі найбільш раціональних методів, способів та шляхів захисту інформації. Таким чином, забезпечення інформаційної безпеки не може бути разовим заходом. Другим є принцип комплексного використання всього арсеналу наявних засобів захисту у всіх структурних елементах

виробництва і на всіх етапах технологічного циклу обробки інформації. Комплексний характер захисту інформації зумовлений діями зловмисників. Тут правомірне твердження, що зброя захисту має бути адекватно зброї нападу. Крім того, найбільший ефект досягається в тому випадку, коли всі використовувані засоби, методи та заходи об'єднуються в єдиний, цілісний механізм – систему інформаційної безпеки. Тільки в цьому випадку з'являються системні властивості, не притаманні жодному з окремих елементів системи захисту, а також можливість керувати системою, перерозподіляти її ресурси і застосовувати сучасні методи підвищення ефективності її функціонування. Найважливішими умовами забезпечення безпеки є законність, достатність, дотримання балансу інтересів особи і підприємства, високий професіоналізм представників служби інформаційної безпеки, підготовка користувачів та дотримання ними всіх встановлених правил збереження конфіденційності, взаємна відповідальність персоналу та керівництва, взаємодія з державними правоохоронними органами. Без дотримання цих умов ніяка система інформаційної безпеки не може забезпечити необхідного рівня захисту.

Поряд з основними вимогами існує ряд усталених рекомендацій, які будуть корисні, творцям систем інформаційної безпеки:

- засоби захисту повинні бути прості для технічного обслуговування і «прозорі» для користувачів;
- кожен користувач повинен мати мінімальний набір привілеїв, необхідних для роботи;
- можливість відключення захисту в особливих випадках, наприклад, коли механізми захисту реально заважають виконанню робіт;
- незалежність системи захисту від суб'єктів захисту;
- розробники повинні припускати, що користувачі мають найгірші наміри (ворожість оточення), що вони будуть робити серйозні помилки і шукати до шляхи обходу механізмів захисту;

- відсутність на підприємстві зайвої інформації про існування механізмів захисту [4, с. 83].

Заходи, що вживаються захисту, повинні бути адекватні імовірності здійснення даного типу загрози і потенційному збитку, який може бути нанесений в тому випадку, якщо загроза здійсниться (включаючи витрати на захист від неї).

Вибираючи захисні заходи, доводитися враховувати не тільки прямі витрати на закупівлю обладнання та програм, а й витрати на їх впровадження, зокрема – на навчання та перепідготовку персоналу. Важливою обставиною є сумісність нового засобу з ситуацією, апаратно-програмної структурою об'єкта. На думку фахівців, організаційні заходи відіграють велику роль у створенні надійного механізму захисту інформації, так як можливості несанкціонованого використання конфіденційних відомостей в значній мірі обумовлені не технічними аспектами, а зловмисними діями, недбальством, недбалістю і халатністю користувачів або персоналу захисту.

Сформована сукупність правових, організаційних та инженерно-технічних заходів виливається у відповідну політику безпеки, відображену в концепції інформаційної безпеки закладу охорони здоров'я. Концепція розробляється на основі аналізу сучасного стану інформаційної безпеки, джерел, видів загроз і динаміки їх розвитку. Концепція системи захисту представляє собою систематизоване викладення цілей, завдань, принципів і способів досягнення інформаційної безпеки.

Концепція інформаційної безпеки повинна містити:

- загальну характеристику об'єкта захисту (опис складу, функцій і існуючої технології обробки інформації);
- Формулювання цілей створення системи захисту, основних завдань забезпечення інформаційної безпеки і шляхів досягнення цілей;
- основні класи загроз інформаційної безпеки, які беруться до уваги при розробці підсистеми захисту;

- основні принципи і підходи до побудови системи забезпечення інформаційної безпеки, заходи, методи і засоби досягнення цілей захисту.

Концепція являє собою офіційну прийняту систему поглядів на проблему інформаційної безпеки та шляхи її вирішення з урахуванням сучасних тенденцій розвитку інформатизації медичної установи. Вона є методологічною основою політики в розробці практичних заходів щодо її реалізації.

Висновки. В даний час благополуччя і навіть життя багатьох людей залежать від забезпечення інформаційної безпеки безлічі комп'ютерних систем обробки інформації, контролю і управління різними об'єктами. До таких систем відносяться і медичні інформаційні системи.

Їх особливістю є, насамперед, те, що в них зберігається та обробляється інформація, всебічно визначальна соціальний статус людини, а це зумовлює особливу форму відносин між тими, хто її формує, і тими, хто використовує. А саме – поряд з підвищеними вимогами до достовірності інформації повинні накладатися моральні обмеження на доступ до неї, а також юридична відповідальність надають її осіб. Будь-який медичний працівник несе повну відповідальність (моральну, адміністративну і кримінальну) за конфіденційність інформації, до якої він отримує доступ в ході своєї професійної діяльності. З розглянутого стає очевидно, що забезпечення інформаційної безпеки є комплексним завданням.

Це обумовлено тим, що інформаційне середовище є складним багатоплановим механізмом, в якому діють такі компоненти, як електронне обладнання, програмне забезпечення, персонал. Для вирішення проблеми забезпечення інформаційної безпеки необхідно застосування законодавчих, організаційних та програмно-технічних заходів. Нехтування хоч би одним з аспектів цієї проблеми може призвести до втрати або витоку інформації, вартість і роль якої в житті сучасного суспільства набуває все більш важливе значення.

Література.

1. Організація роботи інформаційно-аналітичної системи МОЗ України з питань надзвичайних ситуацій. Практ. пос. / під заг. ред. В.О. Волошина // МОЗ України, УНПЦ ЕМД та МК, КМАПО ім. П.Л. Шупика. – К., 2002. – 102 с.

2. Кризовий менеджмент та принципи управління ризиками в процесі ліквідації надзвичайних ситуацій / С.О. Гур'єв, А.В. Терент'єва, П.Б. Волянський / А.В. Терент'єва. – К., 2008. – 148с.

3. Безопасность життєдіяльності. Безпека технологічних процесів і виробництв: Охорона праці: Учеб. посібник / Кукін П.П., Лапін В.Л., Пономарьов Н.Л. Сердюк Н.І-2-е вид. Испр, і доп .. -М.: Вища школа, 2001. – 318 с.

4. Інформаціонно-аналітичні системи та технології в охороні здоров'я та ОМС. «Збірник праць Всеросійської конференції». Красноярськ, 15–17 вересня 2004 р. – С. 402–411.