МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

Сумська філія

Кафедра соціально-економічних дисциплін

ТЕКСТ ЛЕКЦІЇ

навчальної дисципліни «Інформаційні технології»
обов'язкових компонент
освітньої програми першого (бакалаврського) рівня вищої освіти

262 Правоохоронна діяльність (поліцейські)

за темою – «Безпека роботи з інформацією»

Суми 2022

ЗАТВЕРДЖЕНО
Науково-методичною радою
Харківського національного
університету внутрішніх справ
Протокол від 19.05.2022 № 5

СХВАЛЕНО
Вченою радою Сумської філії
Харківського національного
університету внутрішніх справ
Протокол від 11.05.2022 № 5

ПОГОДЖЕНО
Секцією Науково-методичної ради
ХНУВС з технічних дисциплін
Протокол від 19.05.2022 № 5

Розглянуто на засіданні кафедри соціально-економічних дисциплін Протокол від 10.05.2022 № 16

Розробники:
Доцент кафедри соціально-економічних дисциплін Сумської філії ХНУВС, к.е.н., доцент Виганяйло Світлана Миколаївна

Рецензенти:
1. Доцент кафедри протидії кіберзлочинності, факультету № 4 (кіберполіції) Харківського національного університету внутрішніх справ, к.п.н., доцент Тетяна Петрівна Колісник
2. Доцент кафедри кібернетики та інформатики СНАУ, к.е.н., доцент Олександр Борисович В'юненко

План лекції

1. Вступ. Основні поняття та класифікація комп'ютерних мереж. Принципи функціонування і ресурси мережі Інтернет
2. Пошук інформації в Інтернеті. Метапошукові сервери глобальної мережі Інтернет
3. Пошук людей в глобальної мережі за допомогою он-лайн сервісів
4. Довідково-інформаційні бази даних вільного доступу. Інформаційні обліки МВС
5. Політика інформаційної безпеки при роботі з інформацією
6. Правила ведення радіоефіру під час патрулювання
7. Відеофіксація з допомогою персонального відеореєстратора під час патрулювання. Робота патруля з базами даних
8. Висновки

Рекомендована література

Нормативні документи

1. Про Національну поліцію: Закон України від 02.07.2015 № 580-VIII // Відомості Верховної Ради України. – 2015. – № 40-41. – ст. 379 https://zakon.rada.gov.ua/laws/show/580-19
2. Закон України “Про захист персональних даних” від 01.06.2010 за 2297-VI. https://zakon.rada.gov.ua/laws/show/2297-17
3. Про захист інформації в інформаційно-телекомунікаційних системах. Закон України URL https://zakon2.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80
4. Про затвердження Положення про інформаційно-телекомунікаційну систему “Інформаційний портал Національної поліції України”: Наказ МВС України від 03.08.2017 № 676 URL https://zakon.rada.gov.ua/laws/show/z1059-17
5. Про затвердження Положення про єдину інформаційну систему Міністерства внутрішніх справ та переліку її пріоритетних інформаційних ресурсів: Постанова КМУ від 14 листопада 2018 р. № 1024 URL

https://zakon.rada.gov.ua/laws/show/1024-2018-%D0%BF

Основна

1. Виганяйло С. М. Інформаційне забезпечення професійної діяльності: навч. посіб. Харків: ХНУВС, 2021. 110 с.
2. Клімушин П. С. Інформаційні системи та технології в економіці : навчальний посібник / П. С. Клімушин, О. В. Орлов, А. О. Серенок; Нац. акад. держ. управління при Президентові України, Харк. регіон. ін-т держ. управління. - Харків : Вид-во ХарРІ НАДУ "Магістр", 2011. - 448 **с**http://dspace.univd.edu.ua/xmlui/handle/123456789/4730
3. Сезонова І. К. Інформатика для правоохоронців: навч. посіб. / І. К. Сезонова; МВС України, Харк. нац. ун-т внутр. справ. - Харків, 2015. – 182 с. http://dspace.univd.edu.ua/xmlui/handle/123456789/1311

Допоміжна

1. Вишня В. Б. Основи інформаційної безпеки: навч. посіб. / В.Б. Вишня, О.С. Гавриш, Е.В. Рижков. Дніпро: ДДУВС, 2020. 128 с. http://er.dduvs.in.ua/handle/123456789/4206
2. Заплотинський Б.А. Інформаційні технології в юридичній діяльності. Посібник. Київський інститут інтелектуальної власності та права НУ “Одеська

юридична академія", кафедра інформаційно-аналітичної та інноваційної діяльності, 2018.–108с.

3. Застосування інформаційних технологій у діяльності правоохоронних органів : зб. матеріалів кругл. столу (м. Харків, 9 груд. 2020 р.) / МВС України, Харків. нац. ун-т внутр. справ. – Харків : ХНУВС, 2020. – 132 с. http://dspace.univd.edu.ua/xmlui/handle/123456789/9984 http://dspace.onua.edu.ua/bitstream/handle/11300/11095/%D0%86%D0%A2%20%D0%B2%20%D0%AE%D0%94%20%D0%BF%D0%BE%D1%81%D1%96%D0%B1%D0%BD%D0%B8%D0%BA.pdf?sequence=1&isAllowed=y
4. Інформаційне забезпечення юридичної діяльності : підручник / В.Б. Вишня, Л.В. Рибальченко, О.О. Косиченко та ін.; за заг. ред. В.Б. Вишні; МВС України, Дніпропетр. держ. ун-т внутр. справ.- Дніпро : ДДУВС, 2019.- 227 с. http://er.dduvs.in.ua/handle/123456789/3718
5. Інформаційне забезпечення діяльності Національної поліції України: зб. законодавчих та нормативних документів / уклад.:В.Б. Вишня та ін. Дніпро: ДДУВС, 2016. 476 с. http://er.dduvs.in.ua/handle/123456789/2043
6. Кормич Б.А., Федотов О.П., Аверочкіна Т.В. Правове регулювання інформаційної діяльності: навчально-методичний. Одеська юридична академія. 2018. 150 с. https://pidruchniki.com/15931106/politologiya/pravove_regulyuvannya_informatsiynoyi_sferi_ukrayini
7. Краснобрижий І.В. Інформаційне забезпечення професійної діяльності : навч. посіб. Уклад: І.В. Краснобрижий, С.О. Прокопов, Е.В. Рижков. Дніпро : ДДУВС, 2018. 220 с. http://er.dduvs.in.ua/handle/123456789/2046
8. Методичні рекомендації щодо використання комп'ютерної програми «Навчальний ЄРДР» (для ролі «курсант») / [Розроб. Коршенко В. А., Демидов З. Г., Колмик О. О., Абламський С. Є.]; МВС України, Харків. нац. ун-т внутр. справ, Наук.-досл. лаб. з проблем розвитку інформац. технологій, Каф. крим. процесу та організації досуд. слідства ф-ту № 1. - Харків: ХНУВС, 2019. - 30 с. http://dspace.univd.edu.ua/xmlui/handle/123456789/6675
9. Мордвинцев М. В. Використання автоматизованих систем відеодокументування переміщень об'єкта для протидії торгівлі людьми / М. В. Мордвинцев, О. В. Хлєстков, С. П. Ницюк // Використання сучасних інформаційних технологій в діяльності Національної поліції України: матеріали Всеукр. наук.-практ. семінару (м. Дніпро, 23 листоп. 2018 р.). – Дніпро: Дніпропетр. держ. ун-т внутріш. справ, 2018. – С. 52-54. http://dspace.univd.edu.ua/xmlui/handle/123456789/3953
10. Наказ МВС "Про затвердження Положення про Інтегровану інформаційно-пошукову систему ОВС України" від 12.10.2009 за № 436. http://tranzit.ltd.ua/nakaz/
11. Наказ МВС "Про затвердження Положення про систему Інтернет у телекомунікаційній мережі Національної поліції України" від 22.02.2017 № 141. http://tranzit.ltd.ua/nakaz/
12. Нелюбов В.О., Куруца О.С. Основи інформатики. Microsoft Word 2016: електронний навчальний посібник. Ужгород: ДВНЗ УжНУ, 2018. 96 с. https://dspace.uzhnu.edu.ua/jspui/handle/lib/18659

13. Про електронні довірчі послуги: Закон України від 5 жовтня 2017 р. № 2155-VIII. URL: http://zakon2.rada.gov.ua/laws/show/2155-19/page
14. Проведення оперативно-тактичних навчань на основі інформаційного моделювання дій нарядів та інших підрозділів Національної поліції : методичні рекомендації / О.О. Акімова, О.С. Гавриш, О.В. Махницький, С.О. Прокопов, Е.В. Рижков, Ю.І. Тюря. Дніпро: Дніпроп. держ. ун-т. внутр. справ, 2017. 37 с. https://dduvs.in.ua/wp-content/uploads/files/Structure/library/student/eib2.pdf

Інформаційні ресурси в Інтернеті

1. http://www.nau.kiev.ua
2. http://www.liga.kiev.ua
3. http://www.informjustr.kiev.ua
4. http://www.rada.gov.ua
5. https://zakon.rada.gov.ua
6. http://www.president.gov.ua

Текст лекції

1. Вступ. Основні поняття та класифікація комп'ютерних мереж. Принципи функціонування і ресурси мережі Інтернет

Комп'ютерна мережа – сукупність взаємозв'язаних (через канали передавання даних) комп'ютерів, які забезпечують користувачів засобами обміну інформацією колективного використання апаратних, програмних та інформаційних ресурсів мережі.

Абоненти мережі – об'єкти, що генерують або споживають інформацію в мережі. Абонентами можуть бути окремі комп'ютери, комп'ютерні комплекси, термінали тощо. Будь який абонент підключається до станції.

Сервер – підключений до мережі комп’ютер, що надає її користувачеві певні послуги.

Робоча станція – апаратура (ПК), яка виконує функції, пов'язані з наданням користувачеві доступу до мережі з метою передавання і приймання інформації.

Сукупність абонента та станції утворює абонентську систему(станції) .

Для взаємодії абонентів потрібне фізичне передавальне середовище, тобто лінії зв'язку або простір. На основі фізичного передавального середовища будується комунікаційна мережа, що забезпечує передавання інформації між абонентськими системами.

За територіальним розподілом комп'ютерні мережі поділяють на:

– глобальні мережі WAN), які об'єднують користувачів по всьому світу;

– регіональні мережі (MAN), які об'єднують користувачів міст, областей, невеликих країн;

– локальні мережі (LAN), що об'єднують абонентів однієї установи, підприємства тощо.

За способом взаємодії комп'ютерів локальні мережі бувають двох видів: одноранговi і клієнт-сервер.

В одноранговій мережі всі комп'ютери рівноправні і користувачі, зазвичай, мають доступ до відкритих даних на кожному комп'ютері.

Якщо є комп'ютер, з яким взаємодіють усі інші комп'ютери, то його називають серверним, а інші комп'ютери – клієнтами, а зєднання – мережею типу клієнт-сервер. Комп'ютер-клієнт називають також робочою станцією.

За способом з'єднання комп'ютерів локальні мережі поділяють на три головні види (топології мереж): *зірка, кільце, шина*.

У топології зірка всі абоненти об’єднані з деяким центральним комп'ютером. Приклад – банківська мережа.

У кільці абоненти об'єднані між собою, а не з центральним комп'ютером. Приклад – підприємства і навчальні заклади.

У топології шина (магістраль) усі абоненти приєднані до одного економного каналу який називають шиною. Приклад – Ethernet (сукупність технологій побудови локальної мережі).

Технічні пристрої, які сполучають комп'ютер із каналами зв'язку називають *адаптерами*.

Мережні адаптери (мережні карти) – забезпечують передавання даних. Кожному із них присвоюють унікальну мережну адресу, яку називають MAC-адресою.

Для об’єднання декількох різнорідних мереж, тобто мереж з різними протоколами обміну і керування, методами кодування і швидкостями передавання призначені мости, маршрутизатори і шлюзи.

Мости – це програмно-апаратні засоби, що в разі потреби виконують функції комутування та найпростіше опрацювання пакетів.

Шлюзи – це засоби, що з’єднують цілком різні мережі. Комп’ютер-шлюз забезпечує приєднання локальної мережі до інтернету.

Маршрутизатор (роутер) для кожного пакета вибирає ортимальний маршрут. Якщо їх є декілька, то забезпечує обхід перевантажених чи пошкоджених ділянок.

Дані в мережі передаються пакетами.

Пакет – це порція даних, яку пересилає комп’ютер. Він має таку структуру: адреса отримувача, адреса передавача, номер і обсяг пакета, поле даних, висновок.

Протокол – це сукупність правил і процедур, які регламентують порядок налагодження зв’язку і пересилання пакетів даних у мережі.

За призначенням протоколи поділяються на такі основні групи:

- прикладні (HTTP, SMTP, FTP та інші);
- транспортні (TCP) та інші;
- мережні (IP, Ipv6 та аінші).

Для функціонування однорангових мереж потрібна одна з операційних систем (Linux, Windows NT Workstation, Windows XP чи Vista).

Для функціонування клієнт-серверної мережі потрібна мережна операційна система типу Linux, MS Windows NT.

Інтернет – це глобальна комп’ютерна мережа, яка складається з набору пов'язаних мереж, що взаємодіють як одне ціле і обслуговує десятки міліонів абонентів у понад 150 країнах світу забезпечуючи поширення інформаційних потоків по всій земній кулі.

Мережі, які є складовими Інтернету, поширюються на великі відстані та можуть перекривати одна одну, тому будь-яка пара вузлів пов'язана між собою не одним, а багатьма каналами зв'язку, завдяки чому Інтернет забезпечує стійкий зв'язок навіть в

умовах військових дій. При руйнуванні частини мережі пакети інформації можуть обходити ушкоджені ділянки. Комп'ютери, які працюють у мережі Інтернет, називаються *вузлами* (іноді і хостами, хоча це не одне й ге саме). Інтернет взагалі можна уявити як множину вузлів, кожен з яких може зв'язатися з будь-яким іншим. Вузлами є потужні комп'ютери (мейнфрейми), менш потужні міні-комп'ютери та персональні комп'ютери. Серед них є такі, що надають послуги іншим комп'ютерам – *сервери*.

Сервери – це потужні та надійні комп'ютери, або програми, які цілодобово працюють, постійно підключені до Інтернету, та надають клієнтам певні мережні послуги.

Сервери здатні зберігати та надсилати інформацію за запитами інших комп'ютерів, водночас відповідаючи на десятки або сотні запитів. Сервери захищені від збоїв електромережі та, як правило, керовані операційною системою Unix.

Комп'ютери, які складають і надсилають запити до серверів, називаються *клієнтами*. Вони постійно не під'єднанні до Інтернету, а підключаються до мережі у разі необхідності. Отже, статус серверів і клієнтів в Інтернеті аналогічний їхньому статусу в локальній мережі *клієнт-сервер*.

Термінологія "клієнт-сервер" застосовується і для програмного забезпечення, яке підтримує роботу в Інтернеті. Існує ПЗ для клієнтів, яке взаємодіє з ними та створює запит, і серверне ПЗ, яке відповідає на ці запити. Наприклад, клієнтами є поштова програма, програма браузера для перегляду Web- сторінок тощо.

Для приєднання комп'ютера до глобальної мережі використовують пристрій який називається *модем*.

Модеми можуть бути таких типів:

- вбудовані чи зовнішні звичайні факс-модеми для традиційного дозвону;
- ADSL-модем для швидкісного зв'язку;
- спеціальні USB-модеми чи мережні карти для бездротового зв'язку (Wi-Fi);
- модеми, вбудовані в мобільні телефони і смартфони.

Протокол TCP/IP. Незалежно від того, що комп'ютери в Інтернеті відрізняються своїми платформами, операційними системами, вони прекрасно "спілкуються" один з одним. Це можливо завдяки тому, що вони послуговуються однаковими правилами передавання даних – протоколом TCP/IP. Він прийнятий усіма учасниками Інтернету і підтримується більшістю виробників мережного обладнання.

TCP/IP – основний транспортний протокол передавання даних в Інтернеті, що складається з двох протоколів, які регулюють взаємодію між комп'ютерами в мережі. Абревіатура TCP/IP складається з двох частин : TCP (Transmition Control Protocol – протокол керування передаванням) і IP (Internet Protocol – протокол Internet).

Перша складова протоколу (TCP) забезпечує надійний зв'язок між комп'ютерами і керує передаванням даних. Протокол TCP поділяє інформацію на порції – пакети, кожному з яких надає номер для правильного відновлення інформації під час одержання. Далі інша складова (протокол IP) додає до кожного пакета службову інформацію з адресами відправників і одержувачів, забезпечуючи доставку всіх пакетів одержувачеві. Окремі пакети можуть подорожувати різними шляхами Інтернету та дістатися до одержувача у будь-якому порядку. По надходженні всіх пакетів протокол TCP розміщує їх один за одним і забезпечує складання

повідомлення. Якщо деякі пакети загубилися – протокол TCP вирішує і цю проблему. Маршрути руху пакетів мережею розраховує спеціальна програма – маршрутизатор.

Протокол IP передбачає, що в кожного користувача має бути своя унікальна IP адреса.

Найважливішою властивістю протоколу TCP/IP є його здатність забезпечити взаємодію комп'ютерів за допомогою необмеженої кількості мереж. Зім не важливо, скільки мереж подолає інформація на шляху від віддаленого серверу до клієнта.

Протокол TCP/IP застосовується не лише в Інтернеті, а й, наприклад, для зв'язку локальних мереж на одному великому підприємстві, в якого можуть бути відсутні зв'язки із зовнішніми мережами. TCP/IP іноді застосовується для зв'язку двох віддалених один від одного комп'ютерів.

Провайдери. Ланками зв'язку між клієнтами та Інтернетом є організації або приватні особи, так звані ISP (Internet Service Provider – постачальник послуг Інтернету), або, простіше, провайдери. Сервер провайдера має кілька модемних входів, до яких можуть приєднуватися користувачі для доступу до Інтернету.

Провайдер – це комерційна організація, яка забезпечує зв’язок локального комп’ютера з інтернетом.

Провайдер, як правило, забезпечує користувачам такі послуги Інтернету:

- доступ до інформаційних ресурсів Інтернету;
- надання адреси електронної пошти;
- виділення необхідного простору на своєму вузлі для Web-сторінок абонента.

Можливі також додаткові послуги, наприклад, реєстрація індивідуального домену користувача, надання лінії зв'язку тощо. Нині завдяки постійному розвитку Інтернету користувач може обрати провайдера з потрібним спектром послуг.

Пересічний користувач звичайно з'єднується з провайдером по телефону. Комп'ютер користувача через модем підключається до телефонної лінії, тому при укладенні договору з провайдером або купівлі Інтернет-картки вам мають повідомити номер телефону провайдера, за яким дзвонитиме ваш модем.

Провайдер також повідомить ім'я поштового серверу для обробки електронної пошти. Багато провайдерів надають безкоштовні гостьові підключення для одержання інформації про свої послуги і поповнення суми на рахунку користувача. Для цього провайдер повідомляє URL свого сервера, ім'я (login) і пароль (password) для гостьового підключення. Фактично цих даних достатньо для того, щоб після оплати послуг провайдера і створення з'єднання ви могли почати повноцінну роботу в Інтернеті.

Мільйони користувачів Інтернету приваблює його ресурси, які стають доступними за допомогою провайдера:

1. Гіпертекстова система WWW (World Wide Web) – глобальна система поширення інформації, в якій для пошуку та перегляду файлів застосовуються гіпертекстові зв'язки.
2. Електронна пошта – засіб обміну повідомленнями, який нагадує роботу звичайної пошти, але значно переважає її за швидкістю доставки повідомлень.
3. Віддалений доступ до мережі – забезпечує доступ до вашого комп'ютера з будь-якого, підключеного до Інтернету. Ви можете переглянути вашу електронну пошту, виконати пошук у БД свого комп'ютера тощо.

4. Тематичні конференції Usenet – це електронні дошки, куди учасники конференції можуть передавати повідомлення й отримувати відповіді на них.

5. Розмова в мережі або IRC (Internet Relay Chat) – спілкування співбесідників шляхом уведення тексту з клавіатури.

6. Голосове спілкування і відео конференції – надає можливість двом і більше абонентам чути і бачити один одного. Для проведення голосових та відео-конференцій абоненти повинні мати певне обладнання (мікрофон, динаміки, відеокамеру) і програмне забезпечення.

7. FTP (File Transfer Protocol – протокол передавання файлів) – передавання програм і файлів даних між комп'ютерами глобальної мережі.

*Режими інформаційного обміну***.** В Інтернеті можливі два режими інформаційного обміну – on-line і off-line. Перший термін перекладається як «на лінії», другий – «поза лінією». Йдеться не просто про існування лінії (підключення до телефонної лінії або до ЛОМ, яка має вихід до Інтернету), а про наявність з'єднання через існуючу лінію зв'язку.

On-line (на комп'ютерному жаргоні – «онлайновий» режим) – постійний зв'язок користувача з сервером провайдера. Під час відкриття Web-сторінок, відправлення повідомлень електронної пошти, «перекачування» файлів-архівів користувач лишається підключеним до мережі. Він може отримувати інформацію з мережі і негайно реагувати на неї, тому on-line - це режим реального часу.

Off-line – це режим «відкладеного» зв'язку. Користувач передає порцію інформації або отримує її протягом коротких сеансів зв'язку, а в інший час комп'ютер відключений від Інтернету. Зрозуміло, що це економічніший режим, ніж on-line. У режимі off-line, наприклад, обробляються повідомлення електронної пошти та групи новин.

IP-адреси. Усі комп'ютери, підключені до Інтернету, знаходять один одного в автоматичному режимі. Люди взагалі не беруть участі у пересиланні повідомлень завдяки тому, що кожний комп'ютер (хост або вузол) має свою адресу, яка називається IP-адресою.

IP-адреса – запис, який точно визначає місцезнаходження комп'ютера в Інтернеті і є записом чотирьох чисел у діапазоні від 0 до 255, відділених крапками, наприклад, 220.15.68.33.

Запис IP-адреси складається ніби з двох частин: перша означає адресу підмережі Інтернету, до якої підключено вузол, а друга - адресу локального вузла всередині підмерсжі.

IP-адреси серверів мають бути зареєстровані спеціальною службою імен. Реєстрація – це просто занесення IP-адреси і доменного імені до каталогу. Індивідуальна IP-адреса надається також комп'ютеру клієнта під час його підключення до провайдера Інтернету. Але у цьому разі IP-адреса надається тимчасово, на період з'єднання, тому що адрес у провайдерів, як правило, менше, ніж клієнтів. Надання адреси клієнту відбувається автоматично і клієнт може не знати своєї IP-адрес|и.

Доменні імена DNS. IP-адреси зручні для ідентифікації комп'ютерів в Інтернеті, але неприйнятні для роботи користувачів (не наочні, погано запам'ятовуються, велика ймовірність помилки при введенні). Тому замість числових IP-адрес застосовується літерна система доменних імен DNS (Domain Name Server – доменне ім'я серверу).

Згідно з цією системою ім'я кожного Web-серверу є послідовністю слів, розділених крапками, яка легко запам'ятовується користувачами.

Доменне ім'я однозначно визначає сервер в Інтернеті й складається за ієрархічним принципом.

– На найвищому рівні (домен верхнього рівня) звичайно розташовується назва країни, наприклад, uk (Велика Британія), ru (Росія) або ua (Україна). Але частіше замість назви країни ставиться скорочення, відповідне типу організації, якій належить домен: com (комерційний домен), gov (урядовий), mil (військовий), edu (освітній), net (мережевий), org (інших організацій).

– Ліворуч від домену верхнього рівня через крапку дописується позначення міста або організації. Однак цієї частини імені може не бути.

– Ліворуч від позначення міста (організації) – позначення серверу, яке займає відповідно крайню ліву позицію у доменному імені.

У результаті доменне ім'я серверу (простіше, домен) може мати такий вигляд:

autoland.com.ua – комерційний сервер, присвячений автомобілям, країна ua (Україна);

kyivstar.net – сервер оператора мобільного зв'язку, домен верхнього рівня net.

Відповідність між IP – адресами і доменними іменами встановлюється за допомогою баз даних, розміщених на спеціальних DNS-серверах. Сервери DNS виконують пякденну роботу, необхідну для функціонування системи доменних імен.

Принцип роботи Інтернету. Ви вивчили основні поняття для роботи в Інтернеті. Це – сервери і клієнти, інформаційні ресурси Інтернету, транспортний протокол TCP/IP, IP-адреси, DNS. З іншими важливими поняттями ви ознайомитесь у наступних параграфах. Однак, трохи забігаючи наперед, опишемо роботу Інтернету за допомогою простого прикладу.

Скажімо, ви бажаєте вивести на екран комп'ютера певну Web-сторінку. Для цього вам потрібно запустити програму-клієнт (браузер) і підключитися до Інтернету. У вікні браузера слід набрати URL потрібної сторінки або клацнути по посиланню на Web- сторінку (якщо така є).

Після цього запит з вашого комп'ютера піде на сервер доменних імен (DNS-сервер). Поки він обробляє запит, комп'ютер клієнта зупиняється і чекає відповідні. Сервер намагається знайти IP-адресу, яка відповідає імені, вказаному у запиті, у своїх файлах або у файлах інших DNS-серверів. Якщо ім'я не знайдене, сервер відповідає, що таке доменне ім'я не існує. Якщо ж IP-адресу знайдено, відбувається з'єднання з віддаленим сервером, і вказана вами Web-сторінка передається з нього на ваш комп'ютер. Процес завантаження Web-сторінки ви бачитимете у себе на екрані у вікні браузера.

Обмін даними між вашим комп'ютером і сервером відбуватиметься згідно з протоколом TCP/IP, тобто дані на ваш комп'ютер надходитимуть порціями. Вони послідовно збиратимуться в єдине повідомлення, доки ви не побачите на екрані повну картинку Web-сторінки.

2. Пошук інформації в Інтернеті. Метапошукові сервери глобальної мережі Інтернет

Інформаційно-пошукова веб-система – це сайт, який дає змогу відшукати потрібний ресурс за темами (категоріями), або ключовими словами.

Простий пошук - це пошук за одним або кількома ключовими словами. Причому більш релевантним, безумовно, буде пошук за кількома словами, пов'язаними з необхідною темою. Наприклад, за запитом «екстремізм» буде видано величезне число різноманітних посилань.

Додавання одного або двох ключових слів (наприклад, «екстремізм в ісламі») значно звузить область пошуку. При формуванні запиту кількість слів у групі не обмежується. При простому пошуку можливе використання засобів контекстного пошуку. Якщо ключові слова взяти в лапки, то пошукова система знайде документи, у яких дана фраза присутня дослівно. Так можна знайти цитату з художнього твору, наукової праці тощо.

Розширений пошук – для спрощення завдання формування складних запитів використовують спеціальні форми, за допомогою яких виконується розширений пошук. Для більш швидкого й успішного пошуку в пошукових системах разом із ключовими словами використовуються різні логічні оператори. Завдяки цьому можна сконструювати запит так, що будуть знайдені не тільки сайти на тему, яка вас цікавить, а й конкретні сторінки й навіть окремі документи. Правила складання складних запитів в одній пошуковій системі можуть відрізнятися від таких в іншій, але в кожному разі будуть використовуватися такі основні логічні оператори й синтаксичні вирази.

Відповідно до цих можливостей системи поділяються на каталоги і покажчики.

Каталоги дають доступ до систематизованих за темами найважливіших ресурсів інтернету.

Покажчики (індекси) автоматично (без участі людей) класифікують посилання на веб-ресурси методом аналізування змісту сайтів. Відшукання ресурсу відбувається за ключовими словами.

Інформаційно-пошукова система – це додаток БД, який обирає інформацію на основі переданих йому ключових слів та висловів.

Основною функцією пошукових систем є надання динамічно оновлюваної інформації про Web-вузли та їхній вміст. Якщо користувач надсилає запит до пошукової системи, вона виконує пошук не у всій WWW, а у наявних БД за допомогою засобів швидкого пошуку.

У сучасних пошукових системах є такі основні види пошуку:

- за повною назвою об’єкта чи деякою повною фразою;
- за допомогою Web-каталогів (за темою);
- за ключовими словами.

Ключові слова. До текстового поля пошукової системи, розташованого у верхній частині сторінки, потрібно ввести ключові слова, які мають максимально відображати сутність вашого запитання. Не можна задавати будь-яке одне загальне ключове слово, наприклад, музыка або история, краще обмежити зону пошуку додатковими ключовими словами. Для цього можна задавати цілі вислови, наприклад, легенды Крыма або художники эпохи Возрождения. Мистецтво користування пошуковими машинами полягає насамперед в умінні звузити зону пошуку.

WEB-каталоги. Пошук можна здійснювати не за ключовими словами, а за Web-каталогом, який є у більшості сучасних' пошукових систем. Веб-каталог - це вузол, на

якому розміщено посилання на ВЕБ-сторінки,< класифіковані за певною ієрархічною системою. Вона нагадує системний каталог у звичайній бібліотеці.

Файлові ресурси Інтернету (FTP-вузли). Задовго до появи WWW уже існувала така форма обміну інформацією через Інтернет, як підключення до FTP-вузлів.

Вузол FTP (FTP-сервер) – це комп'ютер в Інтернеті, який містить каталоги з файлами (програмами, текстами, графікою тощо) і забезпечує доступ користувачам до цих каталогів за протоколом FTP.

На відміну від протоколу HTTP, який призначений для передавання HTML-файлів, FTP застосовується для обміну довільними файлами, часто великого розміру. Звичайно FTP-сервери належать великим організаціям та відомствам. Обсяг інформації, яка надається FTP-вузлами, дуже великий, тому їх ще називають FTP-архівами.

Кожен звичайний (назвемо його «традиційним») пошуковик має тільки свій власний, обмежений своїми ресурсами перелік (індекс) документів, які доступні для пошуку. Жодна з подібних систем не може охопити всіх ресурсів, які існують в мережі Інтернет. Тому може виникнути ситуація, коли користувача не задовольняють результати пошукової видачі. В цьому випадку користувач переходить на інший пошуковик і намагається знайти там, що йому потрібно. Але цей вид пошуку займає досить багато часу, і потребує від користувача постійної уваги в процесі проведення пошуку. Для вирішення цієї проблеми були створені так звані метапошукові системи.

Метапошукова система (інша назва: метапошукова машина, мета пошуковий сервер, метакраулер або мультипотокова система, машина) - це пошуковий інструмент, який посилає Ваш запит одночасно на декілька пошукових систем і каталогів. Частина запитів надсилається в так звану невидиму (приховану) павутину, що не проіндексована традиційними пошуковими системами. Зібравши результати, метапошукова система видаляє дублюючі посилання і, відповідно до свого алгоритму об'єднує та ранжує результати в загальному списку. На відміну від класичних пошукових машин не має власної бази даних і власного пошукового індексу.

Найбільш популярні метапошукові системи:

– DuckDuckGo (https://duckduckgo.com/) – це досить відома метапошукова система з відкритим вихідним кодом. Сервери знаходяться в США. Крім власного робота, пошуковик використовує результати інших джерел: Yahoo! Search BOSS, Google, «Вікіпедія», Wolfram | Alpha.

– Metabot (http://www.metabot.ru) – присутня можливість пошуку по російським і світовим ресурсам, а також по MP3, відео файлів і серверів новин. Видається інформація про стратегію пошуку, синтаксисі пошукової машини і опитуваних систем.

– Debriefing (http://www.dogpile.com) Потужна метапошукова система Dogpile використовує для метапошуку не тільки пошукові системи, але і FTP-сервери, а також новинні сайти, котирування фондових бірж і навіть "жовті сторінки" Інтернету.

– Ixquick (https://www.ixquick.com) – система метапошуку Ixquick працює з десятьма зовнішніми базами. Це пошуковики Bing, Yahoo! Ask, All the Web, Cuil, Entire Web, Gigablast, каталоги Qkport і Open Directory, а також Wikipedia. У списку баз відсутня Google, однак охоплення альтернативних систем варто визнати досить широким. Підтримується пошук на вісімнадцяти мовах, в тому числі російською.

– Metabear (http://www.metabear.com) – надає релевантні результати як з міжнародних, так і з російських сайтів.

– Search 66 [http://search66.com] – ця австралійська метапошукова система включає пошук по 10 пошуковим серверам. Групує разом сторінки від одного і того ж домена.

Також особливої уваги потребують так звані пошукові утиліти (пошукові додатки робочого столу). Це завантажуванні інструменти метапошуку, які шукають в численних пошукових системах. Результати упорядковуються і ранжуються за релевантністю з видаленням повторів. Це не безкоштовні системи, але у більшості з них є безкоштовна пробна версія. Ціна – кілька десятків доларів. Найбільш яскраві представники цих програмних комплексів виглядають наступним чином:

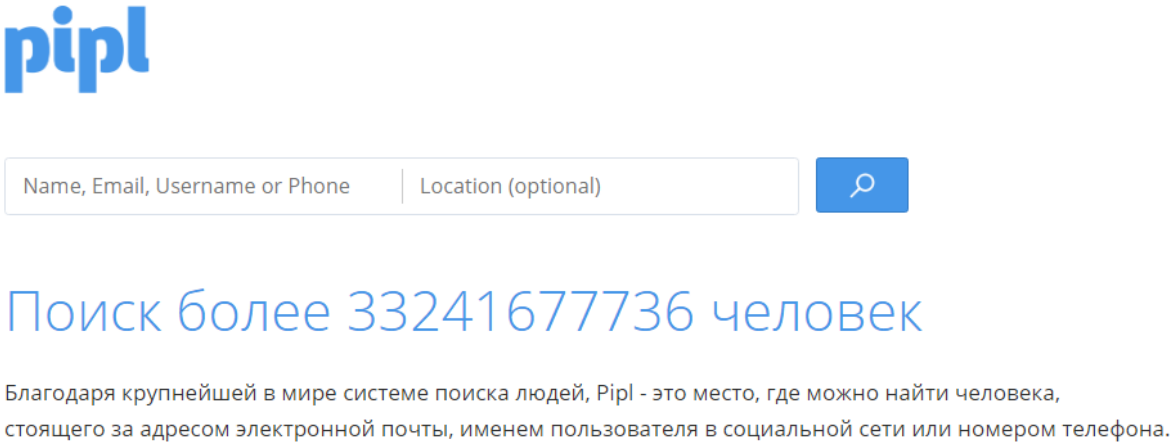
– SiteSputnik;
– PDS Поисковик;
– Info Pilot

SiteSputnik – програмний комплекс, що дозволяє вести пошук і обробку результатів в видимих і невидимих частинах Інтернету, використовуючи всі необхідні користувачу пошуковики. Основне призначення: організація та автоматизація професійного пошуку і збору інформації з відкритих джерел Інтернету, моніторинг появи нових посилань на задану тему. Неофіційне найменування «програма для допиту Інтернету».

3. Пошук людей в глобальної мережі за допомогою он-лайн сервісів

Більшість особистих профілів, державних архівів і документів, пов'язаних з людьми, зберігаються в базах даних, а не на статичних веб-сторінках, тому основна інформація про людей просто «невидима» для регулярних пошукових систем. Нижче приведено список найбільш ефективних он-лайн сервісів для пошуку людей (інформації про них) в мережі Інтернет:

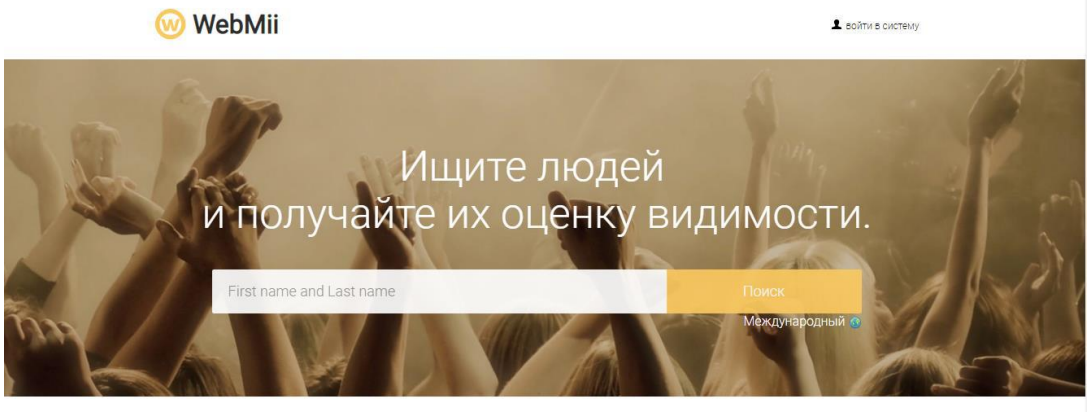
Pipl (https://pipl.com): пошук людей в «невидимому» Інтернеті: пошук по імені, прізвищу, місті, штаті і країні.



Існує щось особливе в цьому пошуковому движку, хоча це лише інструмент для пошуку людей, який знаходить інформацію в тій частині Інтернету, яка, як правило, не індексується іншими великими пошуковими системами.

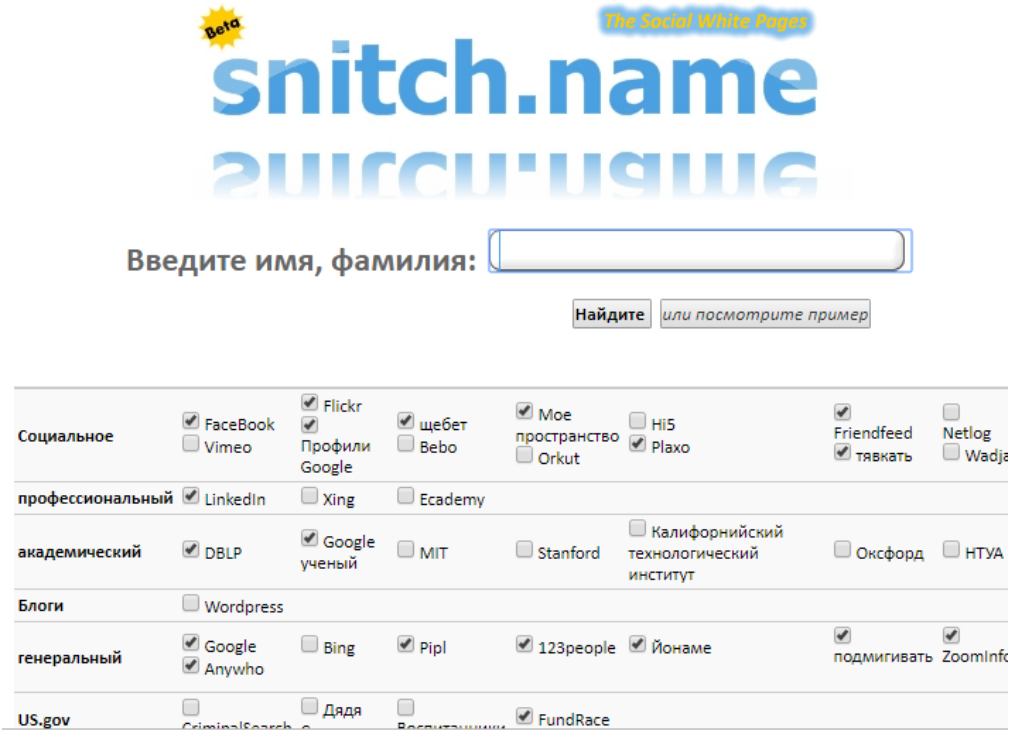
Запит в пошуковику Pipl допоможе знайти «невидимі» веб-сторінки, які не можна знайти на регулярних пошукових системах. На відміну від типових пошуковиків, Pipl призначений для отримання інформації з Deep Web. Його роботи вміють взаємодіяти з базами даних для пошуку і вилучення фактів, контактних даних та іншої відповідної інформації з особистих профілів, каталогів, наукових публікацій, протоколів судових засідань та інших численних джерел «глибинної» мережі.

Webmii (http://webmii.com): сайт відображає інформацію про людину, отриману з різних соціальних мереж, сайтів і онлайн-документів. Кожна людина також має свій власний PeopleRank (ранг популярності) який є оцінкою його видимості в Інтернеті.

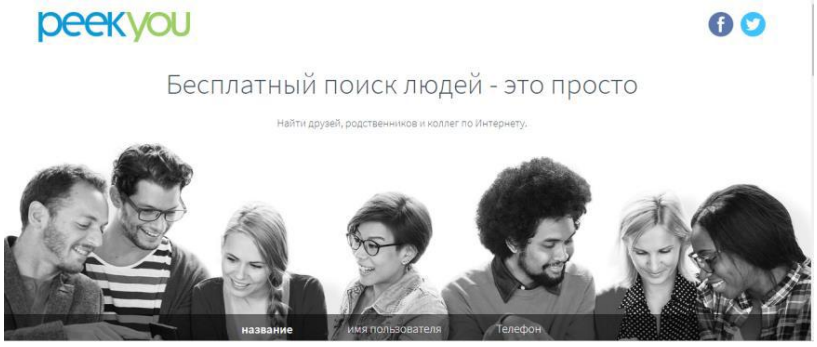


WebMii дозволяє шукати людину з використанням імені, за ключовим словом, або використовуючи розширений пошук. Якщо ім'я, яке потрібно знайти, поширене серед багатьох людей, то Ви можете натиснути на теги для подальшого звуження результатів. WebMii використовує такі різні сайти, як Facebook, Friendster, Google, Twitter і Yahoo для збору інформації. Крім того, сайт містить посилання на Xing і Friendfeed.

Snitch.Name (http://snitch.name) : пошук людей в соціальних мережах. Це сервіс, який дозволяє шукати людину на сайтах соціальних мереж за його ім'ям і прізвищем та видавати результат пошуку в одному інтерфейсі. Замість того, щоб Ви йшли і окремо шукали когось на Facebook, Twitter, Flickr або MySpace – сервіс надає Вам результати пошуку з цих сайтів в окремих блоках на одній сторінці.



Сайт дозволяє знаходити людей на таких популярних соціальних мережах, як Facebook, MySpace, Flickr, LinkedIn, Hi5, Twitter Google, WordPress.org блогах і відеосайтах, подібних Vimeo.



PeekYou (http://www.peekyou.com) : сервіс індексації публічного інтернету про людей і для людей. Пошуковий сервіс, орієнтований на індексацію загальнодоступного Інтернету про людей. Основною метою сервісу є індекс людей з їх публічних веб-адрес.

4. Довідково-інформаційні бази даних вільного доступу. Інформаційні обліки МВС

Державний реєстр, Єдиний державний реєстр – автоматизована система обліку інформації про осіб, майно, документи, яка створюється та ведеться державою з метою реалізації своїх функцій. Державний реєстр ведеться уповноваженим органом держави з метою накопичення, обробки інформації та надання певним відомостям офіційного визнання. Єдині та Державні реєстри інформаційної мережі Міністерства юстиції України створені та функціонують відповідно до законодавства України, що складають закони України, акти Кабінету Міністрів, відомчі нормативно-правові акти, а також інші документи правового характеру. Адміністратором Єдиних та Державних реєстрів інформаційної мережі Мін'юсту є Державне підприємство «Інформаційний центр» Міністерства юстиції України. Уся інформація про правові підстави функціонування Єдиних та Державних реєстрів, умови надання доступу та

користування інформацією з баз даних реєстрів інформаційної мережі Міністерства юстиції є відкритою та розміщена на web-сайтах Міністерства юстиції (www.minjust.gov.ua) та ДП «Інформаційний центр» (www.informjust.ua).

Список найбільш популярних Державних реєстрів та баз даних, які використовуються співробітниками Національної поліції в рамках виконання своїх повноважень:

– Розшук МВС: Зниклі громадяни. Мобільні телефони. Транспортні засоби у розшуку. Зброя у розшуку. Культурні цінності. Непізнанні трупи. Особи, які переховуються від органів влади. Особи, що не можуть надати про себе відомостей внаслідок хвороби або неповнолітнього віку http://mvs.gov.ua/mvs/control/uk/investigation

– Єдиний державний реєстр юридичних осіб та фізичних осіб- підприємців https://usr.minjust.gov.ua/ua/freesearch

– Єдиний ліцензійний реєстр http://irc.gov.ua/ua/Poshuk-v-YeLR.html

– Реєстр наукових організацій http://rni.mon.gov.ua/public/index.php

– Дізнайся більше про свого бізнес-партнера http://sfs.gov.ua/businesspartner

– Електронні декларації чиновників та депутатів https://declarations.com.ua/

– Єдиний державний реєстр судових рішень http://www.reyestr.court.gov.ua/

– Вся Україна – жителі http://www.nomer.org/allukraina

– Телефонний довідник України http://spravochnik109.link/ukraina

– Єдиний реєстр підприємств, щодо яких порушено провадження у справі про банкрутство

https://kap.minjust.gov.ua/services?product_id=3&is_registry=1&keywords&usertype=all

– База даних «Законодавство України» http://zakon4.rada.gov.ua/laws

– Поштові індекси та відділення поштового зв’язку.

http://services.ukrposhta.com/postindex_new

– Пошук поштового відправлення

http://services.ukrposhta.ua/bardcodesingle

– Анульовані свідоцтва. Свідоцтво про встановлення батьківства. Свідоцтво про зміну імені. Свідоцтво про народження. Свідоцтво про шлюб. Свідоцтво про смерть. Свідоцтво про розірвання шлюбу. Свідоцтва про усиновлення http://drsu.gov.ua/show/1034

– Перевірка документа про освіту https://osvita.net/ua/checkdoc

– Реєстр наукових організацій http://store.uintei.kiev.ua/reestr_new.html

– Перелік осіб, пов`язаних із здійсненням терористичної діяльності або стосовно яких застосовано міжнародні санкції

http://www.sdfm.gov.ua/articles.php?cat_id=126&lang=uk та пошук в офіційному списку терористів Держфінмоніторингу http://www.expert-fm.com/blacklist/search

– Телефонний довідник України http://spravochnik109.link/ukraina

– Державний реєстр лікарських засобів. Державний реєстр медичної техніки і виробів медичного призначення. Державний реєстр дезінфекційних засобів. Державний формуляр лікарських засобів. Реєстр оптово-відпускних цін на вироби медичного призначення

http://www.moz.gov.ua/ua/portal/register_medicaltechnics

– Єдиний Реєстр медичних працівників та штампів http://umcbdr.com.ua/reyestri

– Перелік лікарських засобів, заборонених до рекламування, які відпускаються без рецепта http://zakon2.rada.gov.ua/laws/show/z1948-12/paran13

– Зареєстровані ветеринарні препарати
http://www.vet.gov.ua/taxonomy/term/32

– Державний реєстр телерадіоорганізацій
http://www.nrada.gov.ua/ua/13720.html

– Електронний реєстр суб'єктів, які надають послуги, пов'язані з ЕП http://czo.gov.ua/ca-registry

– Реєстр дозволів на міжнародні перевезення
http://www.mtu.gov.ua/uk/1234365r6i8ghjn.html

– База даних підприємств харчової промисловості http://www.ukroliya.kiev.ua/industry

– Єдиний реєстр адвокатів http://www.unba.org.ua/erau

– Реєстр адвокатських об'єднань Києва http://kmkdka.com/reestr-advokatskih-obiednan-kieva

– Перевірка коду IMEI мобільних телефонів http://www.ucrf.gov.ua/baza-imei/perevirka-kodu-imei

– Єдина база даних електронних адрес, номерів факсів (телефаксів) суб'єктів владних повноважень http://email.court.gov.ua/search

– Державний реєстр потенційно шкідливих об'єктів http://sfd.archives.gov.ua/RUS/page4.html

– Єдина база тварин з чіпом http://www.tracer.com.ua/

– Державний реєстр небезпечних факторів Держсанепідемслужби http://uhrc.gov.ua/registr

– Державний реєстр лікарських засобів http://www.drlz.kiev.ua/

– Державний реєстр дитячих закладів оздоровлення та відпочинку http://drdz.mlsp.gov.ua/msm

– Національна комісія регулювання енергетики та комунальних послуг НКРЕКП. Реєстри. Ліцензійні реєстри. Реєстри суб'єктів природних монополій. Реєстр об'єктів електроенергетики (альтернативні джерела енергії) http://www.nerc.gov.ua/?id=11957

– База даних експортерів
http://ukrexport.gov.ua/rus/ukr_export_exporters/…

– База даних інфраструктури експорта
http://ukrexport.gov.ua/rus/baza_ukr_infrastructure/…

– Реєстр виданих ліцензій Держархбудінспекцією. Реєстр дозвільних документів на виконання будівельних робіт. http://www.dabi.gov.ua/index.p…/reestr-dozvilnikh-dokumentiv

– Перелік експертних організацій, які відповідають Критеріям, встановленим наказом Мінрегіону від 23.05.2011 №53, та можуть здійснювати експертизу проектів будівництва
http://www.minregion.gov.ua/…/content…/3099/Perelik_26_1.pdf

– Інформація про власників істотної участі у банках http://bank.gov.ua/control/uk/publish/article…

– Єдиний реєстр бюро кредитних історій. Державний реєстр страхових та перестрахових брокерів та інші http://nfp.gov.ua/content/inshi-reestri-ta-pereliki.html

– Державний реєстр фінансових установ http://kis.nfp.gov.ua/

– Єдиний реєстр нотаріусів http://ern.minjust.gov.ua/pages/default.aspx

– Система електронних торгів арештованим майном http://torgi.minjust.gov.ua/

– Державний реєстр речових прав на нерухоме майно. Електронний суд. Єдиний реєстр підприємств, щодо яких порушено провадження у справі про банкрутство. Система електронної звітності арбітражних керуючих. https://kap.minjust.gov.ua/

– Реєстр адміністративних послуг http://poslugy.gov.ua/AdminService/List

– Перелік організацій-виконавців, які заявили право на податкові пільги http://www.me.gov.ua/Documents/List…

– Електронна система розкриття інформації учасників фондового ринку ЕСКРІН http://smida.gov.ua/db

– Українська міжбанківська валютна біржа . Фондовий, товарний ринок, електронні аукціони з продажу нафтопродуктів http://www.uice.com.ua/

– Фондовий ринок. Реєстри учасників фондового ринку. Рейтингові агентства. Оперативні дані щодо стану фондового ринку. Реєстр аудиторських фірм НКЦПФР http://www.nssmc.gov.ua/fund

– Діяльність НКЦПФР. Реєстрація емісій цінних паперів. Розпорядження стосовно випусків ЦП. Реєстр рішень НКЦПФР щодо реклами цінних паперів та фондового ринку http://www.nssmc.gov.ua/activities

– Судна, сертифіковані Регістром судноплавства http://shipregister.ua/ism.html

– Перевірка оригінальності ідентифікаційного номеру малого судна в Регістрі судноплавства http://shipregister.ua/cin/cin3.html

– Перевірка дійсності документа Регістра судноплавства. Реєстрова книга суден. Пошук суден http://shipregister.ua/ships/index.html

– Список посвідчень громадських інспекторів з охорони навколишнього природного середовища, які є недійсними http://www.menr.gov.ua/control/control1

– Реєстр екологічних аудиторів http://www.menr.gov.ua/…/268-reiestr-ekolohichnykh-audytoriv

– Перелік об'єктів, які є найбільшими забруднювачами довкілля http://www.menr.gov.ua/control/control4

– Державний реєстр пестицидів і агрохімікатів, дозволених до використання http://www.menr.gov.ua/control/control5

– Публічна кадастрова карта http://www.map.land.gov.ua/kadastrova-karta

– Пошук аукціона Держземагентства http://torgy.land.gov.ua/auction

– Реєстр організаторів державної експертизи у сфері технічного захисту інформації http://dstszi.kmu.gov.ua/dstszi/control/uk/publish/article…

– Перелік сертифікованих засобів криптографічного захисту інформації http://dstszi.kmu.gov.ua/dstszi/control/uk/publish/article…

– Перелік засобів технічного захисту інформації, дозволених для забезпечення технічного захисту державних інформаційних ресурсів та інформації http://dstszi.kmu.gov.ua/dstszi/control/uk/publish/article…

– Перелік суб'єктів господарювання, які мають ліцензії на провадження господарської діяльності з надання послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису), торгівлі криптосистемами і засобами криптографічного захисту інформації http://dstszi.kmu.gov.ua/dstszi/control/uk/publish/article…

– Перелік суб'єктів господарювання, які мають ліцензії на провадження господарської діяльності з надання послуг в галузі технічного захисту інформації http://dstszi.kmu.gov.ua/dstszi/control/uk/publish/article…

– Електронна митниця http://sfs.gov.ua/…/mitne…/subektam-zed/elektronna-mitnitsya

– Довідники Державної фіскальної служби. Довідники пільг. Для банківських установ: Довідник SPR_REG.DBF та опис його структури. Довідник кодів товарів згідно з Українською класифікацією товарів зовнішньоекономічної діяльності. Типи об'єктів оподаткування http://sfs.gov.ua/dovidniki--reestri--perelik/dovidniki-

– Реєстр підприємств, яким надано дозвіл на відкриття та експлуатацію митного складу http://sfs.gov.ua/dovidniki--reestri-- perelik/reestri/94929.html

– Єдиний реєстр суб'єктів господарювання, які можуть здійснювати реалізацію безхазяйного майна та майна, що переходить у власність держави, у 2016 році http://sfs.gov.ua/dovidniki--reestri-- perelik/reestri/235648.html

– Єдиний державний реєстр обладнання для промислового виробництва сигарет та цигарок http://sfs.gov.ua/dovidniki--reestri-- perelik/reestri/191577.html

– Реєстр суб'єктів господарювання, які здійснюють оптову торгівлю спиртом коньячним і плодовим на підставі ліцензії на виробництво коньяку та алкогольних напоїв за коньячною технологією http://sfs.gov.ua/dovidniki--reestri--perelik/reestri/152383.html

– Єдиний державний реєстр виробників спирту етилового, коньячного і плодового, спирту етилового ректифікованого виноградного, спирту етилового ректифікованого плодового, спирту-сирцю виноградного, спирту-сирцю плодового, алкогольних напоїв та тютюнових виробів http://sfs.gov.ua/dovidniki--reestri--perelik/reestri/151988.html

– Реєстр підприємств, яким надано дозвіл на провадження митної брокерської діяльності http://sfs.gov.ua/dovidniki--reestri-- perelik/reestri/94921.html

– Реєстр підприємств, яким надано дозвіл на відкриття та експлуатацію складу тимчасового зберігання http://sfs.gov.ua/dovidniki-- reestri--perelik/reestri/94919.html

– Державний реєстр реєстраторів розрахункових операцій http://sfs.gov.ua/dovidniki--reestri--perelik/reestri/94957.html

– Реєстр великих платників податків на 2016 рік http://sfs.gov.ua/dovidniki--reestri--perelik/reestri/214495.html

– Реєстри виданих, призупинених та анульованих ліцензій на право роздрібної торгівлі алкогольними напоями та тютюновими виробами http://sfs.gov.ua/dovidniki--reestri--perelik/reestri/167294.html

5. Політика інформаційної безпеки при роботі з інформацією

Сама по собі політика інформаційної безпеки (ПІБ) є достатньо абстрактним поняттям. Має бути деякий додаток до ПІБ, тобто необхідні систематизація і правила, що дозволяють зробити технології ПІБ застосовними до реального середовища, де і мусить бути забезпечена безпека інформаційного простору. Розробка ПІБ – процес дуже важливий і суто практичного характеру, що безпосередньо застосовує знання і методи абсолютно всіх розділів інформаційної безпеки в конкретній ситуації.

Розробка ПІБ – це питання не тривіальне. Від ретельності її опрацювання залежатиме дієвість решти всіх рівнів забезпечення ПІБ – процедурного і програмно-технічного. Складність розробки ПІБ визначається проблематичністю використання чужого досвіду, оскільки ПІБ ґрунтується на виробничих ресурсах і функціональних залежностях усередині об’єкта.

Необхідність розробки ПІБ пояснюється необхідністю формування основ планування і управління ПІБ. Мета розробки ПІБ – мінімізація ризиків діяльності шляхом захисту інтересів об’єктів в інформаційній сфері, планування і підтримка безперервності функціонування, зниження витрат і підвищення ефективності інвестицій в захист інформації.

ПІБ містить вимоги до персоналу та технічних служб. Основні напрями розробки ПІБ:

- визначення, які данні і наскільки серйозно необхідно захищати;
- визначення, хто і який збиток може завдати об’єкту в інформаційному аспекті;
- оцінки ризиків і визначення схеми зменшення їх до прийнятної величини.

ПІБ повинна стати результатом спільної діяльності технічних фахівців на об’єкті захисту, здатних реалізувати її початкові технічні аспекти, і керівників, зацікавлених в коректній побудові політики з фінансової, законодавчої та технічної сторони, а також персоналу, що зараз та в майбутньому буде стикатися з нормами ПІБ об’єкта та їх дотримуватися.

ПІБ потенційно впливає на роботу всіх користувачів комп’ютерів на об’єкті, причому в декількох аспектах. Якщо ж такий документ (ПІБ об’єкта) передбачається розробляти і втілювати в життя не власними силами, а за допомогою фахівців ззовні, то потрібно, щоб були враховані наступні п’ять критеріїв оцінки політики :

- чи узгоджується ПІБ з існуючим законодавством і обов’язками відносно третіх сторін?
- чи не обмежуються без потреби інтереси працівників, роботодавців чи третіх сторін?
- чи реалістична політика й чи ймовірне її втілення в життя?
- чи зачіпає політика всі види передачі і збереження інформації, які використовуються в об’єкті?
- чи оголошена політика заздалегідь і чи одержала вона схвалення всіх зацікавлених сторін?

Один із головних спонукальних мотивів розробки ПІБ об’єкта полягає в одержанні впевненості, що діяльність з захисту інформації побудована економічно і технічно виправданим способом. Дане положення здається очевидним, але, взагалі, можливі ситуації, коли зусилля прикладаються не там, де потрібно.

Наприклад, основною задачею систем захисту інформації припускають захист від зовнішнього зловмисника, а напади в більшості випадків створюються внутрішніми порушеннями.

Політика звичайно складається з двох частин: загальних принципів і конкретних правил роботи. Загальні принципи визначають підхід до безпеки в Internet, правила регламентують – що дозволено і що заборонено (правила можуть доповнюватися конкретними процедурами і посібниками).

Звичайна політика безпеки регламентує використання основних сервісів мережі і доводить до відома користувачів мережі їхні права доступу, що і є процедурою автентифікації користувачів.

До ПІБ об’єкта, як до регламентуючого документу, варто відноситися серйозно, бо всі інші стратегії захисту будуються на припущенні, що правила політики безпеки неухильно дотримуються.

Інформаційну систему об’єкта захисту можна вважати захищеною, якщо всі операції виконуються згідно зі строго визначеними правилами (рис. 1), що забезпечують безпосередній захист об’єктів, ресурсів і операцій.

Рис. 1. Основні правила забезпечення політики безпеки в інформаційній системі

Основу для формування вимог до захисту складає список загроз. Коли такі вимоги відомі, можуть бути визначені відповідні правила забезпечення захисту, що визначають необхідні функції і засоби захисту. Чим суворіші вимоги до захисту і більше відповідних правил, тим ефективніші її механізми і тим більше захищеною виявляється інформаційна система.

Таким чином, визначаємо, що захист інформації на інформаційному об’єкті – комп’ютерній мережі, буде ефективним, коли проектування та реалізація системи захисту інформаційного об’єкта відбувається згідно з наступними етапами:

1) аналіз ризиків;

2) реалізація політики безпеки;

3) підтримка політики безпеки.

Процес аналізу інформаційних ризиків містить в собі визначення того, що варто захищати, від чого захищати і як це робити. Необхідно розглянути всі можливі ризики і ранжувати їх залежно від потенційного розміру збитку. Цей процес складається з безлічі економічних рішень. Давно визначено, що витрати на захист не повинні перевищувати вартості інформації, що захищається (об’єкта інформації).

Процес аналізу ризиків розділимо на два етапи: ідентифікація активів та ідентифікація загроз.

Розглянемо докладніше ці етапи.

1. Ідентифікація активів. Це один з етапів аналізу ризиків. Він складається з ідентифікації всіх об'єктів, що потребують захисту. Необхідно прийняти до уваги все, що може постраждати від порушення режиму безпеки. Тому необхідно спочатку класифікувати активи:

– апаратура: процесори, модулі, клавіатури, термінали, робочі станції, персональні комп'ютери, принтери, дисководи, мережі зв'язку, термінальні сервери, маршрутизатори;

– програмне забезпечення, вихідні тексти, об'єктні модулі, утиліти, діагностичні та комунікаційні програми, операційні системи;

– дані (інформація) безпосередньо доступні, архівовані, оброблювані, збережені у вигляді резервної копії, реєстраційні журнали, бази даних, що передаються комунікаційними мережами;

– люди: користувачі, обслуговуючий персонал;

– документація: програмна, апаратурна, системна, з адміністративних процедур;

– випадкові матеріали: папір, форми, фарбуючи стрічки, магнітні носії.

2. Ідентифікація загроз. Після того, як були виявлені активи, що потребують захисту, необхідно ідентифікувати загрози цим активам і розміри можливого збитку та втрат. Це допоможе зрозуміти, яких загроз ватро побоюватися більше всього.

Типова загроза для більшості об'єктів інформаційного захисту – несанкціонований доступ до інформації на об'єкті, що захищається – може приймати різні форми. Ступінь важливості проблеми несанкціонованого доступу для різних об'єктів різна.

Несанкціоноване (нелегальне) ознайомлення з інформацією – друга поширена загроза. Дуже важливо правильно визначити ступінь конфіденційності інформації, що зберігається в інформаційних системах об'єкта.

Відмовлення в обслуговуванні порушують цілісність системи, виникають з різних причин, і виявляються по-різному. Мережа може прийти в непрацездатний стан від підробленого пакета, від перевантаження чи через відмовлення компонента. Вірус здатний сповільнити чи паралізувати роботу інформаційної системи.

При розробці ПІБ необхідно дати відповіді на декілька питань:

– хто має право використовувати ресурси?

– як правильно використовувати ресурси?

– хто наділений правом давати привілеї і дозволяти використання?

– хто може мати адміністративні привілеї?

– які права й обов'язки користувачів?

– які права й обов'язки системних адміністраторів стосовно звичайних користувачів?

– як працювати з конфіденційною інформацією?

Власне, організаційна ПІБ описує порядок надання і використання прав доступу користувачів, а також вимоги звітності користувачів за свої дії в питаннях безпеки.

Для інформаційних мереж можна виділити наступні ймовірні загрози, які необхідно враховувати при визначенні ПІБ: випадкові та навмисно створювані загрози.

Розглянемо послідовно ці загрози.

До випадкових загроз можна віднести:

– помилки обслуговуючого персоналу та користувачів;
– втрата чи руйнування інформації, обумовлена неправильним збереженням архівних даних на магнітних носіях;
– випадкове знищення чи зміна даних;
– збої устаткування електроживлення;
– збої кабельної системи;
– перебої в електроживленні;
– збої апаратури запису та вилучення інформації;
– збої системи архівування даних;
– збої роботи серверів, робочих станцій, мережевих карт і т. п.;
– руйнування файлових структур через некоректну роботу чи програми апаратних засобів;
– зміна даних при помилках у програмному забезпеченні;
– зараження системи вірусами;
– несанкціонований доступ;
– випадкове ознайомлення з конфіденційною інформацією сторонніх осіб.

До випадкових (ненавмисних) загроз мають відношення також випадки руйнації, втрати або зміни даних, конфіденційної інформації або ресурсів під час природних катаклізмів, які не підвладні людині (пожари, землетруси, повені, магнітні бурі, падіння метеоритів та радіоактивні випромінювання).

До навмисно створених загроз слід відносити такі:

– ознайомлення працівників з інформацією, до якої вони не повинні мати доступу;
– несанкціонований доступ сторонніх осіб, що не належать до числа працівників, до конфіденційної інформації і мережевих ресурсів;
– розкриття і модифікація інформації і програм;
– копіювання інформації і програм;
– розкриття чи модифікація або підміна трафіку передачі інформації мережею;
– розробка і поширення комп’ютерних вірусів;
– введення в програмне забезпечення логічних бомб;
– крадіжка магнітних та паперових носіїв, що містять конфіденційну інформацію;
– крадіжка розрахункових документів;
– крадіжка устаткування та апаратури;
– руйнування архівної інформації або навмисне її знищення;
– фальсифікація повідомлень, переданих каналами зв’язку;
– відмовлення від авторства повідомлення, переданого каналами зв’язку;
– відмовлення від факту одержання інформації;
– нав’язування раніше переданого повідомлення;

– перехоплення й ознайомлення з інформацією, передана по каналами зв’язку і т. п.

Головною метою діяльності в області інформаційної безпеки є забезпечення властивостей кожного активу:

– доступності (можливість користування деякими ресурсами інформаційної системи й інформацією в довільний момент);

– конфіденційності (недоступність інформації чи сервісів для користувачів, яким апріорно не надана можливість використання зазначених сервісів або інформації);

– цілісності (незалежність властивостей інформації і ресурсів у будь-який момент часу від моменту їх появи чи введення в систему);

– вірогідності (збереження інформацією своїх семантичних властивостей у будь-який момент часу від моменту введення в систему).

При аналізі загроз варто брати до уваги їхній вплив на активи згідно з чотирма названими напрямками.

Реалізація ПІБ об’єкта починається з проведення розрахунку фінансових втрат і вибору відповідних засобів для виконання цих задач. При цьому необхідно врахувати такі фактори як безконфліктність роботи обраних засобів, репутація постачальників засобів захисту, можливість одержання повної інформації про механізми захисту і надані гарантії. Також варто враховувати основні положення з безпеки інформації:

– економічна ефективність – вартість засобів захисту має бути меншою, ніж розміри можливого збитку;

– кожен користувач повинний мати мінімальний набір привілеїв, необхідний при роботі;

– простота системи захисту об’єкта – захист буде тим ефективніший, чим легше користувачу з ним працювати;

– відключення захисту при нормальному функціонуванні – захист не повинен відключатися, за винятком особливих випадків, коли співробітник із спеціальними повноваженнями може мати можливість відключити систему захисту;

– відкритість проектування і функціонування механізму захисту (для можливості адекватного реагування обслуговуючого персоналу на виникнення збоїв у системі);

– незалежність системи захисту від суб’єктів захисту – розроблювачами не повинні бути ті, кого вона буде контролювати;

– загальний контроль без будь-яких виключень з безлічі контрольованих суб’єктів;

– звітність і підконтрольність системи захисту;

– відповідальність осіб, що займаються інформаційною безпекою;

– об’єкти захисту доцільно розділити на групи так, щоб порушення захисту в одній групі не впливало на безпеку інших груп;

– відмова від замовчування – при збої засобів захисту доступ до обчислювальних ресурсів повинен бути заборонений;

– система захисту об’єкту має бути цілком специфікована, протестована та погоджена;

– система повинна допускати зміну своїх параметрів адміністратором;

– важливі критичні рішення повинні прийматися людиною, а не комп'ютером;

– система захисту об'єкта повинна проектуватися в розрахунку на вороже оточення і припускати, що користувачі мають найгірші наміри, будуть робити помилки і шукати шляхи обходу механізмів захисту;

– інформація про існування механізмів захисту повинна бути, по можливості, схована від користувачів, робота яких контролюється.

При підтримці ПІБ потрібно постійне спостереження за вторгненнями зловмисників у мережу, виявлення вад і "дір" у системі захисту об'єкта інформації, обліку випадків несанкціонованого доступу до конфіденційних даних.

При цьому основна відповідальність за підтримку ПІБ мережі (об'єкта інформації) лежить на системному адміністраторі, що повинен оперативно реагувати на всі випадки зламу конкретної системи захисту, аналізувати їх і використовувати необхідні апаратні та програмні засоби захисту з урахуванням максимальної економії фінансових засобів.

Очевидно, що будь-яка офіційна політика поза залежністю від її відношення до інформаційної безпеки, час від часу порушується. Порушення може бути наслідком недбалості користувачів, випадкової помилки, відсутності надійної та належної інформації про поточну політику чи її нерозуміння. Можливо, також, що деяка особа – група осіб свідомо роблять дії, що прямо суперечать затвердженій політиці безпеки.

Необхідно заздалегідь визначити характер дій, що починаються у випадку виявлення порушень ПІБ, щоб ці дії були швидкими й правильними. Варто організувати розслідування, щоб зрозуміти, як і чому порушення стало можливим. Після цього потрібно внести корективи в систему захисту. Тип і серйозність коректив залежить від типу порушення, яке сталося.

Політику безпеки можуть порушувати різні особи. Деякі з них є своїми, місцевими користувачами, інші – здійснюють напади ззовні. Корисно визначити самі поняття «свої» і «чужі», виходячи з адміністративних, правових чи політичних положень. Ці положення окреслюють характер санкцій, які можна застосувати до порушника – від письмової догани до притягнення до суду. Таким чином, послідовність відповідних дій залежить не тільки від типу порушення, але й від виду порушника; вона повинна бути продумана задовго до першого інциденту, хоча це і непросто.

Варто пам'ятати, що правильно організоване навчання – кращий захист. Керівництво об'єкта, що захищає свою конфіденційну інформацію, зобов'язано поставити справу так, щоб не тільки внутрішні, але і зовнішні легальні користувачі знали положення ПІБ об'єкта.

Проблеми з нелегальними користувачами, загалом, ті ж самі. Потрібно одержати відповіді на питання про те, як типи користувачів порушують політику, як і навіщо вони це роблять. Залежно від результатів розслідування можна просто закрити «діру» в системі захисту та задовольнитися отриманим уроком чи застосувати жорсткіші міри.

Кожний об'єкт повинен заздалегідь визначити набір адміністративних санкцій, застосованих до місцевих користувачів, які порушують ПІБ сторонньої організації чи об'єкта. Крім того, необхідно подбати про захист від відповідних дій сторонньої

організації. При розробці ПІБ варто враховувати всі юридичні положення, які застосовуються до подібних ситуацій.

Політика безпеки об’єкта повинна мати процедури для взаємодії з зовнішніми організаціями, в число яких входять правоохоронні органи, інші організації, команди «швидкого реагування», засоби масової інформації. У процедурах повинно бути визначено, хто має право на такі контакти, і як саме вони відбуваються.

Крім політичних положень, необхідно продумати й описати процедури, що виконуються у випадку виявлення порушень режиму безпеки. Для всіх видів порушень мають бути заготовлені відповідні процедури.

6. Правила ведення радіоефіру під час патрулювання

Особливості використання радіозв’язку. Під радіозв’язком розуміємо обмін інформацією на відстані за допомогою радіохвиль.

У порівнянні із провідниковим зв’язком радіозв’язок має суттєві переваги:

- висока мобільність;
- більша швидкість установлення зв’язку;
- можливість підтримання зв’язку з кореспондентами, місце розташування яких невідоме;
- висока швидкість передавання інформації;
- велика відстань передачі сигналів;
- широкий спектр смуги пропускання сигналів;
- можливість одночасного передавання інформації великій кількості кореспондентів;
- велика пропускна здатність каналу зв’язку.

При використанні радіозв’язку кожному екіпажу (патрульному) присвоюється індивідуальний позивний. Виходити в ефір без передачі позивного *заборонено*.

Для передачі інформації необхідно:

1. Переконатися в тому, що канал вільний (радіообмін не ведеться) В разі, якщо канал зайнятий іншими кореспондентами, необхідно дочекатися завершення їх роботи. Втручатися в радіообмін між двома радіостанціями можна тільки при надзвичайних обставинах. Якщо спробувати вклинитися в розмову, не дочекавшись закінчення чужої передачі, буде тільки створено перешкоду. Запам'ятайте: коли хтось щось передає - чути тільки його;
2. Натиснути кнопку передачі та після секундної паузи викликати абонента, назвавши спочатку *його*, а потім *свій* позивний;
3. Через секунду (*не до!)* після завершення виклику відпустити кнопку (*не починати передачу інформації*);
4. Получити підтвердження від абонента і тільки потім передати інформацію. Передача інформації не повинна вестись більш 20-ти секунд. Після цього треба зробити перерву: поки ведеться передача ніхто інший не може скористатися зв'язком;
5. Якщо після отримання інформації необхідно передати свою інформацію, зроби невеличку паузу (1-2 секунди). В цій паузі може надійти інший виклик, можливо з терміновим повідомленням.
6. В кінці сеансу зв'язку кожному учаснику *обов'язково* потрібно повідомити про повне прийняття інформації, передавши одне з наступних слів: «кінець зв'язку», «плюс», «зрозумів.

Приклади радіообміну:

1. Радіообмін між двома абонентами

Радіостанція 1 (позивний Цунамі 7): Цунамі 12, Цунамі 12, я Цунамі 7, де ви знаходитесь, прийом.

Радіостанція 2 (позивний Цунамі 12): Цунамі 7, я Цунамі 12, знаходжусь на об’єкті, прийом.

Радіостанція 1 (позивний Цунамі 7): Залишайтесь на місці, зв’язок закінчено.

Радіостанція 2 (позивний Цунамі 12): Зрозумів, зв’язок закінчено.

2. Передача інформації декільком абонентам:

Радіостанція 1 (позивний Цунамі 7): Цунамі 10, 11, 12, я Цунамі 7, приготуватись до прийому. Цунамі 10, 11, 12, я Цунамі 7, приготуватись до прийому.

ПАУЗА

Радіостанція 1 (позивний Цунамі 7): Цунамі 10, 11, 12, я Цунамі 7, повернутися на базу.

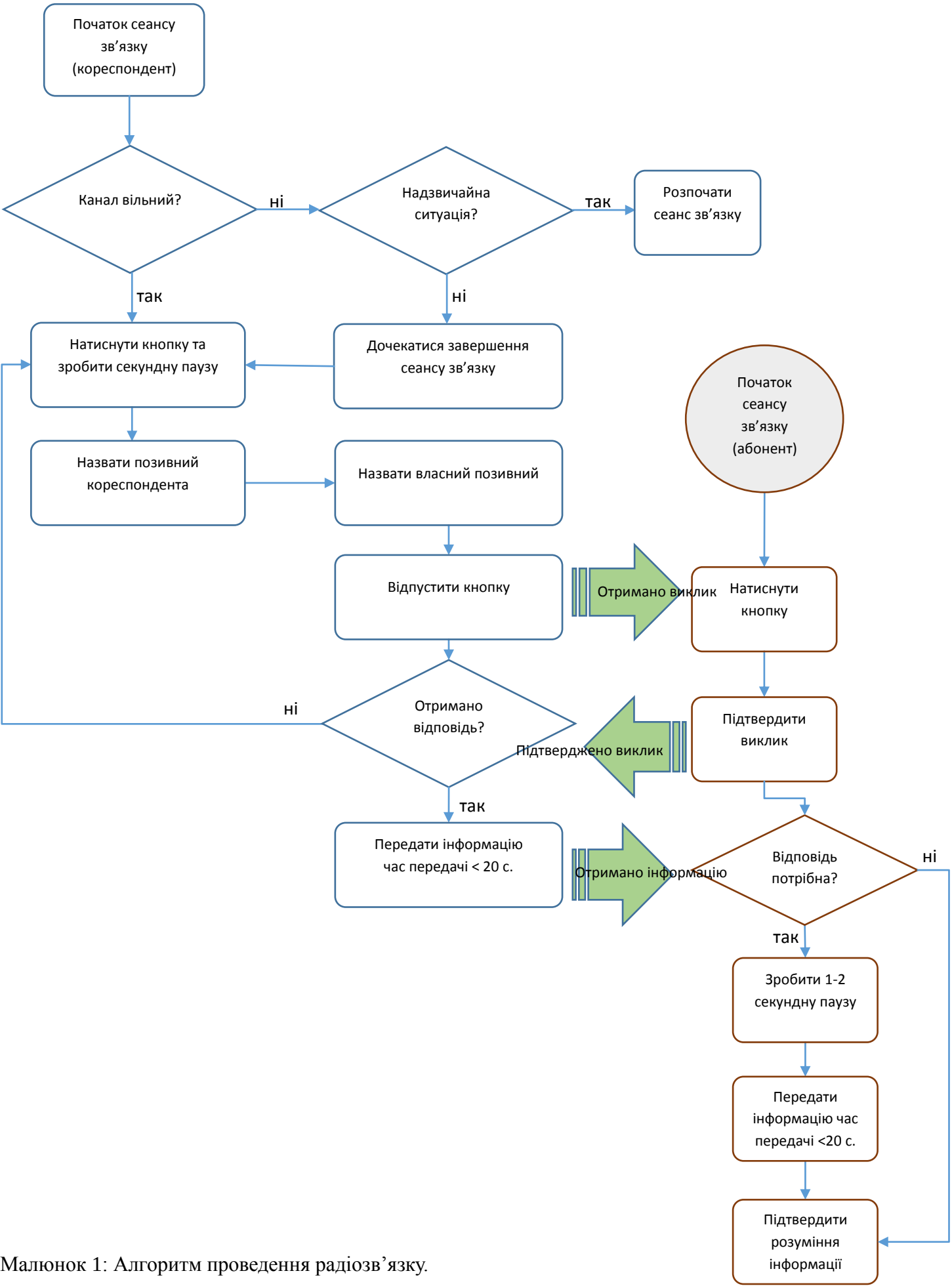
Радіостанція 2 (позивний Цунамі 10): Цунамі 7, я Цунамі 10, Вас зрозумів.

Радіостанція 3 (позивний Цунамі 11): Цунамі 7, я Цунамі 11, Вас зрозумів.

Радіостанція 4 (позивний Цунамі 12): Цунамі 7, я Цунамі 12, Вас зрозумів.

Правила проведення сеансів радіозв’язку. Під час проведення сеансу необхідно дотримуватися наступних правил:

– Говори коротко, стисло і з максимальним змістом. Не «думай» в ефір. Перш ніж почати передачу, подумай і сформулюй що саме ти хочеш сказати, потім скороти це в кілька разів і тільки потім говори коротко, чітко і по суті.



Малюнок 1: Алгоритм проведення радіозв'язку.

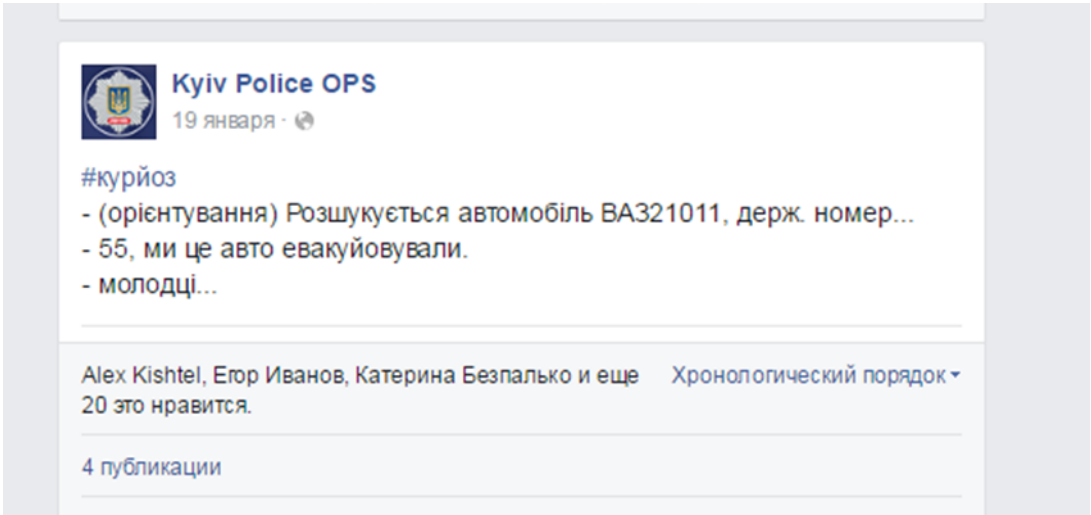
– Пам'ятай, що тебе чує не тільки той, до кого ти звертаєшся, а ще багато людей. І зловмисники в тому числі. Думай якою інформацією ти можеш нашкодити собі, колегам, потерпілим і як її передати, щоб зрозумів тільки адресат.

– Під час передачі слова треба вимовляти чітко, не поспішаючи. При низькій якості зв'язку не можна кричати в мікрофон, це лише погіршує якість зв'язку. Інформацію в такому випадку необхідно доводити з повтором фраз, або по літерах, а числа – по цифрах.

– При вході в «радіопаузу» (тобто при виключенні рації або неможливості її слухати) необхідно повідомити про це на базову станцію сказавши, які позивні і приблизно на який час вийшли з ефіру. Про закінчення радіопаузи обов'язково повідомляти, командиру або в ефір.

Слід пам'ятати, що канали передачі даних не є шифрованими і інформація може бути перехвачено іншими особами. Сьогодні в мережі Інтернет існує достатня кількість сайтів на сторінках яких можна знайти у текстовому вигляді «стенограми» розмов патрульної поліції у сеансах радіозв'язку.

Малюнок 2: Приклад сайту з текстовими «стенограмами» розмов патрульної поліції.



Малюнок 3: Приклад розмішеної «стенограми» сеансу зв'язку.

Періодично з'являються також сторінки у мережі Інтернет які дозволяють у режимі онлайн прослуховувати радіозв'язок патрульної поліції різних міст України.

При проведенні сеансу радіозв'язку КАТЕГОРИЧНО ЗАБОРОНЯЄТЬСЯ:

– Називати посади, прізвища, імена та звання посадових осіб.

– Вести особисті розмови.

– Передавати повідомлення, які розголошують державну або службову таємницю.

– Передавати повідомлення, які можуть розкрити сутність оперативних заходів.

– Використовувати при передачі довільні радіопозивні.

– Самовільно без дозволу керівництва вимикати радіостанцію.

– Перевіряти канал зв’язку шляхом проведення переговорів.

– Не виходити на зв’язок, ігноруючи виклик.

Перелік повідомлень, дозволених для відкритої передачі. При організації радіозв’язку до відкритої (некодованої) передачі дозволені наступні повідомлення:

– Про розбійний напад, крадіжки, пограбування та інші правопорушення (вид, місце, час).

– Про виявлення трупа чи людини, яка знаходиться в безпорадному стані.

– Про стихійні лиха, нещасні випадки (крім особливо важливих об’єктів і кількості жертв).

– Про окремі пожежі, не розкриваючи найменування і дислокацію особливо важливих об’єктів, відомості, які заборонені для опублікування в пресі.

– Про стан справ на пожежах і відомості про стан їх гасіння (крім інформації про смерть людей).

– Про викрадення автомототранспорту.

– Про належність автомототранспорту і місце його стоянки.

– ДТП (крім тих, у яких загинуло 5 і більше людей, травмовано 10 і більше людей).

– Виклик працівників швидкої допомоги до місця пригоди.

– Про технічний стан наявних засобів зв’язку і службового транспорту.

– Про стан системи ОПС, електроживлення і телефонного зв’язку на об’єкті, що охороняється, здачі об’єкту під охорону або зняття з-під охорони, отримання сигналу «ТРИВОГА» з об’єкту, що охороняється.

– Про перебіг спортивно-масових та інших подібних заходів та про стан громадського порядку під час їх проведення.

– Про метеорологічні та дорожні умови.

Можливі проблеми та їх усунення під час роботи з радіостанцією.

– Відбувається «спонтанний» вихід в ефір. Необхідно перевірити розташування рації на спорядженні. Обов'язково розташуйте станцію на спорядженні так, щоб ніщо випадково не могло зачепити кнопку передачі.

– Рацію включено, але не можливо провести сеанс зв’язку. Необхідно перевірити антену. Радіостанція з пошкодженою антеною працювати не буде. Для уникнення пошкодження антени не беріть портативну радіостанцію за антену – (антенна) від цього виходить з ладу

– Є проблеми з отриманням викликів під час руху. Треба перевірити розміщення рації. При перенесенні антена рації не повинна впритул прилягати до тіла, і бути по можливості вертикально спрямованою.

– Під час патрулювання в зимовий час рація швидко розряджається. В умовах низьких температур бажано тримати портативну радіостанцію в кишені або під одягом. Охолоджений до мінусових температур акумулятор розряджається значно швидше.

– Зв’язок під час сеансу поганий, абонент не чує інформацію. Необхідно перевірити правильність тримання рації. При передачі антена рації має бути спрямована вертикально. Мікрофон радіостанції, або саму станцію з вбудованим мікрофоном слід тримати на відстані близько 5 см від рота, говорити голосно і виразно, але не кричати, розбірливість це не підвищить, а знизить

– При знаходженні на далеких відстанях пропускаються виклики. Необхідно, якщо станція обладнана шумоподавлювачем який відключається, відключіть його, на граничних відстанях зв'язку це допоможе не пропустити виклик.

– Прийом кореспондента супроводжується шумами і спотвореннями. Після перевірки правильності тримання рації, проблема не зникає. Це означає, що ви перебуваєте або на максимальній відстані або потрапили в «погане місце» для зв'язку. У цьому випадку абонент/кореспондент теж чує погано. Необхідно під час передачі абонента/кореспондента знайти «гарне місце», пересунутися в сторону на невелику відстань, повернутися навколо своєї осі, орієнтуючись за рівнем шуму в прийнятому сигналі. Як тільки шум зменшиться, розбірливість сигналу зросте.

– Якщо є можливість, вибирайте для зв'язку піднесені місця, в лісі або серед висотних домів виходьте на вільні місця, але не їх середину, а на край максимально віддалений від кореспондента. При зв'язку з автомобіля, виставте антену назовні або, принаймні, притисніть її до скла. Використання зовнішньої антени дозволяє, до речі, значно збільшити дальність зв'язку.

Будь-яка радіостанція під час передачі виділяє в атмосферу енергію, що за відповідних обставин може обумовити появу іскри. Це одна з причин того, що під час роботи з радіостанцією необхідно дотримуватися певних заходів безпеки:

– Радіостанції можна встановлювати в автомобілях із заземленою мінусовою клемою акумулятора.

– Забороняється включати радіостанцію в безпосередній близькості від займистих рідин чи вибухонебезпечних приладів!

– Під час установки чи зняття з транспортного засобу мобільна радіостанція повинна бути вимкнена.

– Не можна використовувати передавач поблизу незахищених електродетонаторів чи у вибухонебезпечній атмосфері.

– Не можна дозволяти дітям гратися радіостанцією.

– Не рекомендовано використовувати радіостанцію з головним телефоном чи звуковим приладдям з високим рівнем гучності

– Не можна робити підзарядку акумулятора при температурі нижче 10°C чи вище 40°C, адже це може зменшити термін служби акумулятора.

– Заборонено використовувати зарядний пристрій, якщо він вологий чи ушкоджений.

– Заборонено розбирати акумулятор.

– Заборонено кидати акумулятори у вогонь – вони можуть вибухнути.

7. Відеофіксація з допомогою персонального відеореєстратора під час патрулювання. Робота патруля з базами даних

Інструкція щодо порядку зберігання, видачі, приймання, використання нагрудних відеокамер (відеореєстраторів) працівниками патрульної поліції та порядок доступу до відео з них регламентувався Наказом Департаменту патрульної поліції національної поліції України № 1026 від 18.12.2018 року.

Персональний відеореєстратор є важливим елементом у роботі патрульного поліцейського. Використання нагрудних відеокамер (персональних відеореєстраторів) є превентивним поліцейським заходом, є одним з елементів, що дозволяє наглядно продемонструвати чесність, відкритість та антикорупційну спрямованість діяльності патрульної поліції.

Крім того відеореєстратор виконує профілактичну роль. Наявність відеореєстратора стримує громадян від вчинення певних дій. Ведення відеозапису працює як психологічний стримуючий фактор відносно більшості правопорушників (за винятком особливо зухвалих та цілком неадекватних осіб).

Використання відеореєстратора є засобом об‘єктивного контролю місця подій. Відеозапис з місця події – це в рівній мірі як контроль дій патрульного, так і документальне підтвердження правомірності його вимог і вжитих заходів.

Метою використання персональних відеореєстраторів працівниками патрульної поліції є:

– підвищення відповідальності працівників патрульної поліції під час виконання службових обов’язків;

– підвищення рівня довіри суспільства до працівників патрульної поліції;

– підвищення рівня захисту прав та свобод людини і громадянина;

– попередження випадків невиправданого застосування фізичної сили, спеціальних засобів та вогнепальної зброї працівниками патрульної поліції та/або щодо працівників патрульної поліції;

– забезпечення об’єктивного розгляду справ уповноваженими органами шляхом створення додаткових належних доказів;

– підвищення відкритості патрульної поліції;

– забезпечення об’єктивного розгляду скарг на рішення, дії чи бездіяльність працівників патрульної поліції, зменшення кількості безпідставних скарг;

– запобігання конфліктним ситуаціям.

Отримання та використання реєстратора під час патрулювання.

Починати патрулювання працівник патрульної поліції повинен при наявності відеореєстратора. Нагрудною відеокамерою (відеореєстратором) забезпечується кожен працівник патрульної поліції, який заступає на зміну, в будь-якому випадку хоча б однією нагрудною відеокамерою (відеореєстратором) забезпечується екіпаж.

Перед початком зміни працівник патрульної поліції зобов’язаний самостійно отримати нагрудну відеокамеру (відеореєстратор) у структурному підрозділі інформаційних технологій та зв’язку управління патрульної поліції. Нагрудні відеокамери (відеоресстратори) зберігаються у спеціально відведених приміщеннях управлінь патрульної поліції. Відповідальність за зберігання нагрудних відеокамер (відеореєстраторів), їх видачу працівникам патрульної поліції та приймання від

працівників патрульної поліції несуть уповноважені працівники структурних підрозділів інформаційних технологій та зв’язку управлінь патрульної поліції.

Після отримання відеореєстратора, з метою забезпечення належного функціонування нагрудної відеокамери (відеореєстратора) протягом зміни, працівник патрульної поліції після отримання нагрудної відеокамери (відеореєстратора) зобов’язаний самостійно оглянути та перевірити її.

Переконавшись у справності нагрудної відеокамери (відеореєстратора) та відсутності зовнішніх пошкоджень, працівник патрульної поліції здійснює запис у спеціальному журналі, зазначаючи своє прізвище, ім’я, по батькові, роту, номер отриманої нагрудної відеокамери (відеореєстратора) та особистий підпис.

Під час отримання відеореєстратора необхідно звернути увагу на наявність ідентифікаційного номера. Кожній нагрудній відеокамері (відеореєстратору) присвоюється такий ідентифікаційний номер.

Використання нагрудних відеокамер (відеореєстраторів) працівниками патрульної поліції під час виконання своїх службових обов’язків здійснюється на підставі статті 40 Закону України «Про Національну поліцію».

Після отримання, перевірки та реєстрації у журналі видачі, перед початком патрулювання необхідно правильно закріпити відеореєстратор. Нагрудна відеокамера (відеореєстратор) закріплюється з правого боку на форменому одязі працівника патрульної поліції у позиції, яка забезпечує ефективну та якісну відеозйомку.

Відеореєстратор необхідно розташувати на одязі таким чином, щоб в поле зору камери потрапляло лице співрозмовника, щоб камера не заважала рухам і була надійно закріплена.

Патрульний ЗОБОВ’ЯЗАНИЙ включити відеозапис під час будь-якого спілкування з громадянами або одразу після прибуття на місце виклику.

Нагрудна відеокамера (відеореєстратор) повинна бути включена працівником патрульної поліції та знаходитись в режимі відеозйомки:

- при оформленні дорожньо-транспортної пригоди;
- при перевірці документів;
- при арешті або затриманні особи;
- при поверхневому огляді;
- при загрозі використання фізичної сили, спеціальних засобів або вогнепальної зброї;
- при наданні допомоги особам;
- у випадках, коли усвідомлення особою факту відеофіксації її поведінки може сприяти вирішенню конфліктної ситуації.
- У будь-якому іншому випадку контакту з громадянами відеореєстратор повинен бути включений та знаходитись в режимі відеозйомки.
- У разі активації відеозйомки вона повинна вестися безперервно під час спілкування. Забороняється ставити запис на паузу, або виключати до закінчення спілкування з громадянами.

Необхідно контролювати своєчасність включення режиму нічної зйомки у разі необхідності.

Нагрудні відеокамери (відеореєстратори) не повинні використовуватись під час:

– розмови з іншими поліцейськими;

– зустрічі з таємними агентами та/або таємними інформаторами з метою забезпечення конфіденційності інформації при виконанні службових обов'язків;

– обідньої перерви;

– перебування у приміщеннях, де працівник патрульної поліції може розраховувати на приватність (вбиральня, кімната відпочинку тощо);

– в інший час, коли немає контакту з особами.

Працівникам патрульної поліції ЗАБОРОНЕНО:

– використовувати нагрудні відеокамери (відеореєстратори) в особистих цілях;

– використовувати нагрудні відеокамери (відеореєстратори) не під час несення служби;

– демонструвати відеозапис з нагрудних відеокамер (відеореєстраторів) третім особам без погодження начальника Департаменту патрульної поліції або начальника управління патрульної поліції у місті;

– змінювати, редагувати, видаляти, копіювати, передавати третім особам

– або іншим чином поширювати відеозаписи, зроблені на нагрудну відеокамеру (відеореєстратор) без дозволу начальника Департаменту патрульної поліції або начальника управління патрульної поліції у місті.

Дії з реєстратором після закінчення патрулювання.

Процедуру копіювання інформації з камери здійснює уповноважена особа. Самостійно патрульні поліцейські не мають права здійснювати копіювання інформації.

Відеореєстратор дозволяє зняти з нього інформацію тільки за допомогою спеціального програмного забезпечення. Це автоматично захищає патрульного від підозр щодо знищення або зміни відеозапису. Не варто намагатися самостійно підключити реєстратор до комп'ютера та скопіювати записи – не вийде.

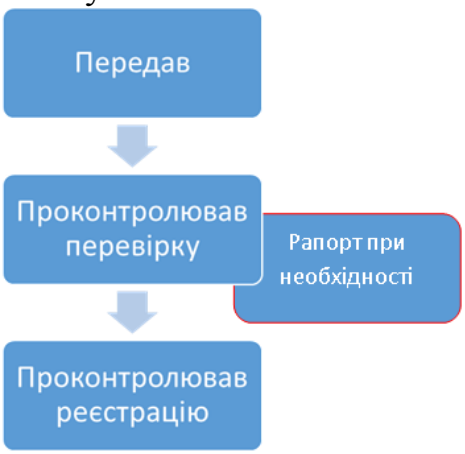
Інформація зберігається протягом 30 діб на сервері, цей термін може бути подовжено у випадку отримання скарги від особи на рішення, дії чи бездіяльність працівників патрульної поліції та в інших виключних випадках. Термін зберігання відеозаписів на сервері може бути продовжено за розпорядженням начальника Департаменту патрульної поліції або начальників управлінь патрульної поліції у містах.

Після закінчення зміни та по прибуттю на місце дислокації працівник патрульної поліції у найкоротший строк передає нагрудну відеокамеру (відеореєстратор) до структурного підрозділу інформаційних технологій та зв'язку управління патрульної поліції.

Уповноважений працівник структурного підрозділу інформаційних технологій та зв'язку управління патрульної поліції у присутності працівника патрульної поліції, який передає камеру, здійснює зовнішній огляд переданої нагрудної відеокамери (відеореєстратора) та перевіряє її справність.

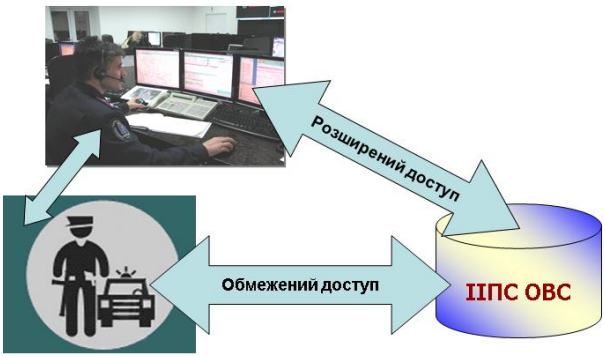
У разі відсутності зауважень до технічного стану переданої нагрудної відеокамери (відеореєстратора), уповноважений працівник структурного підрозділу

інформаційних технологій та зв’язку управління патрульної поліції робить помітку у відповідному журналі та кладе нагрудну відеокамеру (відеореєстратор) у відповідне місце зберігання для подальшого проведення процедури довготривалого збереження відеозаписів на сервері та підготовки нагрудної відеокамери (відеореєстратора) для видачі наступній зміні.



У разі виявлення пошкоджень нагрудної відеокамери (відеореєстратора) або її несправності, працівник патрульної поліції, який використовував нагрудну відеокамеру (відеореєстратор), зобов’язаний скласти рапорт, де повідомити, з яких причин та за яких умов відбулося пошкодження нагрудної відеокамери (відеореєстратора).

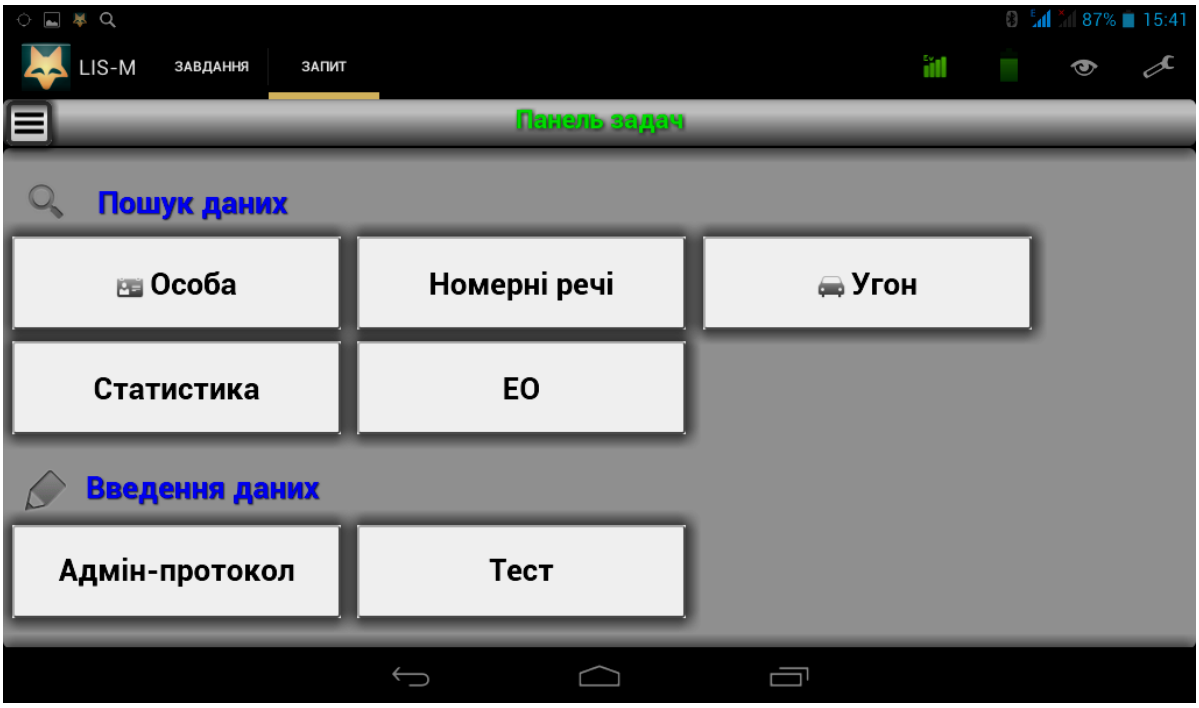
Спрощена схема роботи патруля з базами даних



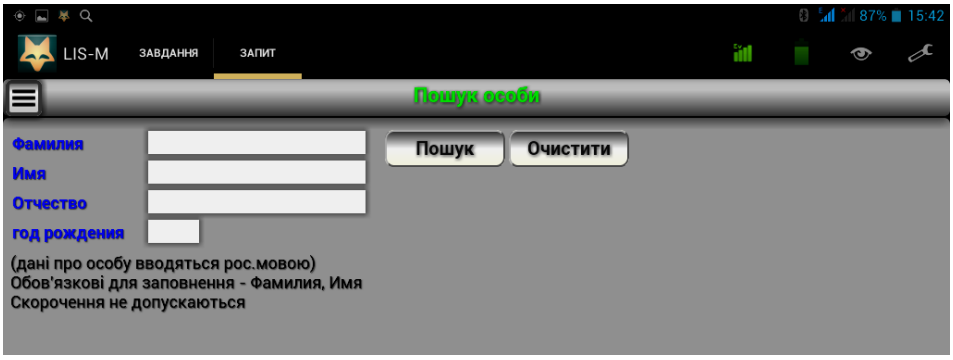
ІІПС ОНП (також ІІПС «АРМОР») – це сукупність організаційно-розпорядчих заходів, програмно-технічних та інформаційно-телекомунікаційних засобів, що забезпечують формування та ведення довідково-інформаційних, оперативно-розшукових обліків, авторизований доступ до інформаційних ресурсів ІІПС.

Інтеграція відомостей здійснюється за установчими даними на особу (ПІБ, дата народження, місце народження)

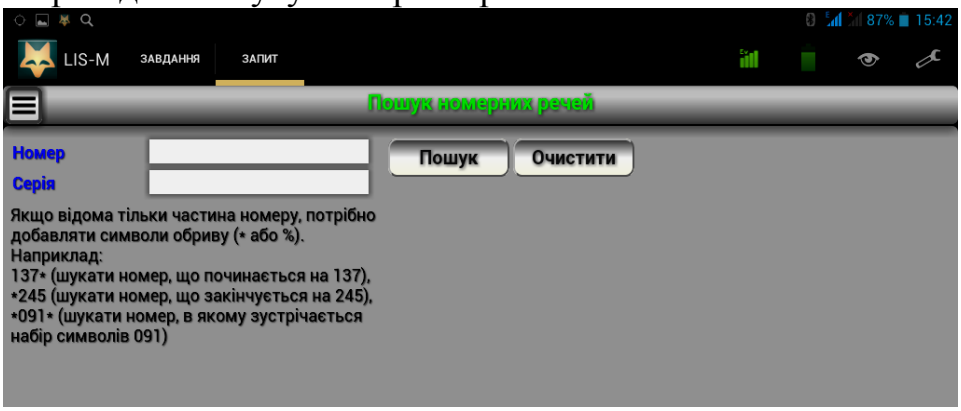
Панель задач після реєстрації (горизонтальна орієнтація)



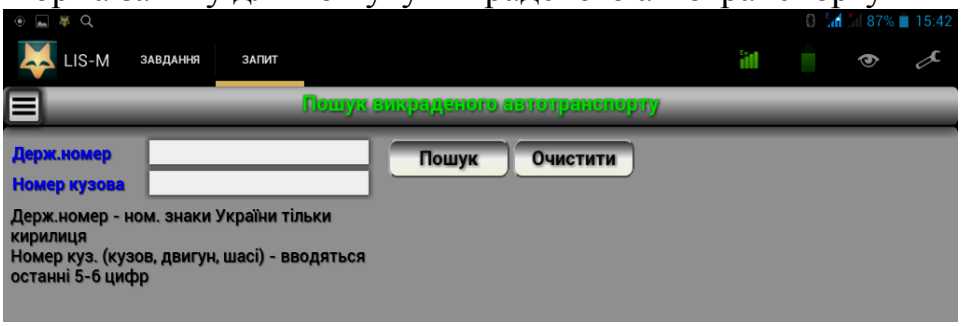
Форма для пошуку особи



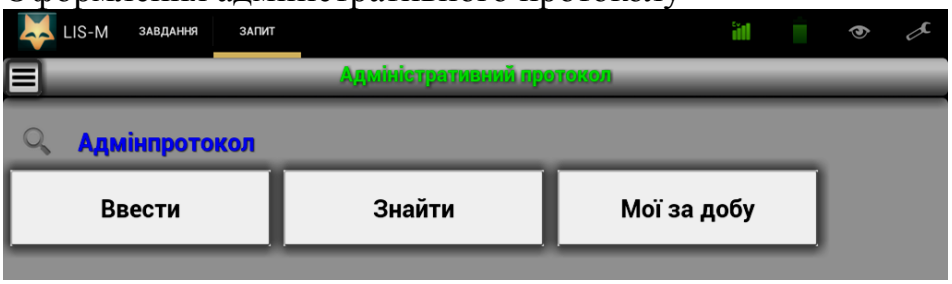
Форма для пошуку номерних речей



Форма запиту для пошуку викраденого автотранспорту



Оформлення адміністративного протоколу



8. Висновки

Коли на об’єкт відбувається напад, що загрожує порушенням інформаційної безпеки, стратегія відповідних дій може будуватися під впливом двох протилежних підходів.

1. Якщо керівництво побоюється вразливості об’єкта, воно може віддати перевагу стратегії «захиститися і продовжити». Головною метою подібного підходу є захист інформаційних ресурсів і максимально швидке відновлення нормальної роботи користувачів. Діям порушника виявляється максимальна протидія, подальший доступ забороняється, після чого негайно починається процес оцінки нанесених ушкоджень і

відновлення інформації. Можливо, доведеться виключити комп'ютерну систему, закрити доступ до мережі чи почати інші жорсткі міри. Зворотній бік даної моделі полягає в тому, що поки зловмисник невиявлений, він може знову напасти на ту ж саму чи іншу організацію колишнім чи новим способом.

2. Інший підхід, «вистежити і засудити», спирається на інші філософію та систему цілей. Основна мета полягає в тому, щоб дозволити зловмиснику продовжувати свої дії, доки об'єкт не зможе встановити його особистість. Такий підхід подобається правоохоронним органам. Нажаль, ці органи не зможуть звільнити об'єкт від відповідальності, якщо користувачі звернуться до суду з позивом із приводу збитку, нанесеного їхнім програмам та інформації.

Політика інформаційної безпеки об'єкта не може бути ідеальною і довговічною, бо з часом усе змінюється: устрій життя та канони в нормативній базі, модернізується устаткування і змінюється обслуговуючий персонал. Отже, політика інформаційної безпеки об'єкта має доповнюватися і змінюватися згідно з усіма перерахованими критеріями змін і цінності інформації, що підлягає захисту.

У порівнянні із провідниковим зв'язком радіозв'язок має суттєві переваги:

- висока мобільність;
- більша швидкість установлення зв'язку;
- можливість підтримання зв'язку з кореспондентами, місце розташування яких невідоме;
- висока швидкість передавання інформації;
- велика відстань передачі сигналів;
- широкий спектр смуги пропускання сигналів;
- можливість одночасного передавання інформації великій кількості кореспондентів;
- велика пропускна здатність каналу зв'язку.

Метою використання персональних відеореєстраторів працівниками патрульної поліції є:

- підвищення відповідальності працівників патрульної поліції під час виконання службових обов'язків;
- підвищення рівня довіри суспільства до працівників патрульної поліції;
- підвищення рівня захисту прав та свобод людини і громадянина;
- попередження випадків невиправданого застосування фізичної сили, спеціальних засобів та вогнепальної зброї працівниками патрульної поліції та/або щодо працівників патрульної поліції;
- забезпечення об'єктивного розгляду справ уповноваженими органами шляхом створення додаткових належних доказів;
- підвищення відкритості патрульної поліції;
- забезпечення об'єктивного розгляду скарг на рішення, дії чи бездіяльність працівників патрульної поліції, зменшення кількості безпідставних скарг;
- запобігання конфліктним ситуаціям.