МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ АЕРОНАВІГАЦІЇ,
ЕЛЕКТРОНІКИ ТА ТЕЛЕКОМУНІКАЦІЙ
КАФЕДРА ТЕЛЕКОМУНІКАЦІЙНИХ ТА РАДІОЕЛЕКТРОННИХ СИСТЕМ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри

_____ Одарченко Р.С.
“_____”_____2021 р.

ДИПЛОМНА РОБОТА

(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ БАКАЛАВР

Тема:«Система оперативно розшукувальних заходів оператора мобільного зв'язку»

Виконавець: _____ Гринчук О. О.
(підпис)

Керівник: _____ Мачалін І. О.
(підпис)

Нормоконтролер: _____ Бахтіяров Д. І.
(підпис)

Київ 2021

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет аеронавігації, електроніки та телекомунікацій
Кафедра телекомунікаційних та радіоелектронних систем
Спеціальність 172 «Телекомунікації та радіотехніка»
Освітньо-професійна програма «Телекомунікаційні системи та мережі»

ЗАТВЕРДЖУЮ
Завідувач кафедри

Одарченко Р.С.
“_____”_____2021 р.

ЗАВДАННЯ
на виконання дипломної роботи

Гринчука Олександра Олександровича
(прізвище, ім'я, по батькові випускника в родовому відмінку)

1. Тема дипломної роботи (проекту): «Система оперативно розшукувальних заходів оператора мобільного зв' язку»
затверджена наказом ректора від « 06 » квітня 2021 р. №559 / ст.
2. Термін виконання роботи: з 17.05.2021 р. по 20.06.2021 р.
3. Вихідні дані до роботи: законодавча база України, вимоги до оперативно розшукувальних заходів.
4. Зміст пояснювавльної записки: теоретичні засади системи оперативно розшукувальних заходів, функціонування системи оперативно розшукувальних заходів оператора мобільного звязку, дослідження системи оперативно розшукувальних заходів оператора мобільного звязку.

5. Календарний план-графік

№ пор.	Завдання	Термін виконання	Відмітка про виконання
1	Розробити деталізований зміст розділів диплому	17.05.2021-21.05.2021	Виконано
2	Вступ	22.05.2021-23.05.2021	Виконано
3	Теоретичні засади системи оперативно розшукувальних заходів	24.05.2021-27.05.2021	Виконано
4	Функціонування системи оперативно розшукувальних заходів оператора мобільного звязку	28.05.2021-05.06.2021	Виконано
5	Дослідження системи оперативно розшукувальних заходів оператора мобільного звязку.	06.06.2021-15.06.2021	Виконано
6	Усунення недоліків дипломної роботи	16.06.2021-20.06.2021	Виконано

6. Дата видачі завдання: “26" квітня 2021 р.

Керівник дипломної роботи _____ Мачалін І. О.
(підпис керівника) (П.І.Б.)

Завдання прийняв до виконання _____ Гринчук О. О.
(підпис випускника) (П.І.Б.)

РЕФЕРАТ

Дипломна робота «Система оперативно розшукувальних заходів оператора мобільного зв' язку» містить 68 сторінок, 30 використаних джерел.

ОПЕРАТИВНО-РОЗШУКОВІ ЗАХОДИ, ОПЕРАТОРИ МОБІЛЬНОГО ЗВ'ЯЗКУ, ОПЕРАТИВНО-РОЗШУКОВА ДІЯЛЬНІСТЬ, ТЕХНІЧНІ ЗАСОБИ, ПРОВАЙДЕРИ ТЕЛЕКОМУНІКАЦІЙ.

Об'єкт дослідження – процес здійснення оперативно-розшукових заходів за допомогою технічних засобів, функціонування та захист від несанціонованого доступу яких забезпечують оператори та провайдери телекомунікацій.

Предмет дослідження – технічні засоби, які потрібні задля здійснення уповноваженими органами оперативно-розшукових заходів, встановлення, функціонування та захист від несанціонованого доступу яких забезпечують оператори та провайдери телекомунікацій.

Мета дипломної роботи – дослідити систему оперативно-розшукових заходів оператора мобільного зв'язку.

Матеріали дипломної роботи рекомендується використовувати при здійсненні оперативно-розшукової діяльності, зокрема при проведенні оперативно-розшукової діяльності.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ 6
ВСТУП 7
РОЗДІЛ 1 9
ТЕОРЕТИЧНІ ЗАСАДИ СИСТЕМИ ОПЕРАТИВНО-РОЗШУКОВИХ ЗАХОДІВ 9
1.1. Поняття оперативно-розшукових заходів 9
1.2. Основні засади застосування оперативно-розшукових заходів 11
РОЗДІЛ 2 14
ФУНКЦІОНУВАННЯ СИСТЕМИ ОПЕРАТИВНО РОЗШУКОВИХ ЗАХОДІВ ОПЕРАТОРА МОБІЛЬНОГО ЗВ'ЯЗКУ 14
2.1. Класифікація оперативно-розшукових заходів 14
2.2. Технічні засоби для здійснення оперативно-розшукових заходів 27
РОЗДІЛ 3 39
ДОСЛІДЖЕННЯ СИСТЕМИ ОПЕРАТИВНО-РОЗШУКОВИХ ЗАХОДІВ ОПЕРАТОРА МОБІЛЬНОГО ЗВ'ЯЗКУ 39
3.1. Розгляд системи перехоплення телекомунікацій 39
3.2. Перелік команд управління перехопленням, відповідей про результати їх виконання та повідомлень інтерфейсу управління та передачі. 45
3.3. Відповіді про підтвердження прийому команд управління перехопленням та про результати виконання команд управління перехопленням. 50
3.4. Повідомлення про службові дані сенсів зв'язку (СДСЗ), які відгалужені, та про події, пов'язані з діями абонентів спостереження. 53
3.5. Повідомлення про події, не пов'язані з дією команд управління перехопленням 55
ВИСНОВКИ 63
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 65

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ

АІС ЦБД ПН - Автоматизована інформаційна система "Централізована база даних перенесених номерів"

ЗІП - Запасні частини, інструмент та приладдя

ЗЗТМ - Засоби захищеної транспортної мережі

ЗТВ - Загальні технічні вимоги

ЗУСП - Засоби управління системою перехоплення

ІП - Інтерфейс перехоплення

ІПСЗ (СС) - Інформаційні повідомлення сеансу зв'язку (Content of Communication)

ІЗД - Інтерфейс запиту та доставки службових даних

ІУП - Інтерфейс управління та передачі

МК - Мережний комплект для здійснення перехоплення телекомунікацій

МКП - Мережа з комутацією пакетів

МЦК - Міжнародний центр комутації

ОВОП - Обладнання відбору об'єкта перехоплення

ОПТС - Опорно-транзитна телефонна станція

ОТВ - Окремі технічні вимоги

ПЗ - Програмне забезпечення

СКС-7 - Спільноканальна сигналізація № 7

СПТ - Система законного перехоплення телекомунікацій

ШМК - Шлюз мережного комплекту

AAA (Authentication Authorization Accounting) - автентифікація, авторизація та облік)

CB (Call Barring) - заборона виклику

CCBS (Completion of Calls to Busy Subscriber) встановлення з'єднання при зайнятості абонента

CD (Call Deflection) - відхилення виклику

ВСТУП

Актуальність теми дослідження. Нині в сучасному світі злочинність вирізняється високим рівнем професіоналізму та організованості. Для неї властивий транснаціональний характер, освоєння новітніх формам та методів протидії правоохоронним і судовим органам. Зокрема, певні злочинні групи та організації власною розвідкою і контррозвідкою, а також обладнані найновішими технічними засобами. Відповідно одержати необхідну інформацію про факт підготовки або вчинення кримінальних правопорушень такими угрупованнями та їх документування, зазвичай, є можливим тільки внаслідок проникнення у злочинне середовище із застосуванням відповідних оперативно-розшукових заходів.

Слід зазначити, що Законом України від 18 листопада 2003 року «Про телекомунікації» на операторів та провайдерів телекомунікацій покладається обов'язок за власний рахунок установлювати на своїх телекомунікаційних мережах технічні засоби, які потрібні задля проведення уповноваженими органами оперативно-розшукових, та обов'язок із забезпечування функціонування зазначених технічних засобів, а також у межах своїх повноважень сприяти проведенню оперативно-розшукових заходів та недопущенню розголошення організаційних і тактичних прийомів їх проведення. Крім того, оператори телекомунікацій зобов'язані забезпечувати захист зазначених технічних засобів від несанкціонованого доступу[1].

Наказом Служби безпеки України та Адміністрації Державної служби спеціального зв'язку та захисту інформації України № 1519/533 від 04 вересня 2018 року було затверджено «Технічні засоби для здійснення уповноваженими органами оперативно-розшукових заходів та негласних слідчих (розшукових) дій у телекомунікаційних мережах загального користування України», в якому розроблено загальні технічні вимоги до таких технічних засобів[2]. Необхідність розроблення таких вимог обумовлена розвитком систем телекомунікацій, які використовують нові сучасні телекомунікаційні технології.

Проте в науковому полі досить мала увага приділяється дослідженню даного питання, що й зумовлює актуальність теми дослідження.

Об'єкт дослідження – процес здійснення оперативно-розшукових заходів за допомогою технічних засобів, функціонування та захист від несанціонованого доступу яких забезпечують оператори та провайдери телекомунікацій.

Предмет дослідження – технічні засоби, які потрібні задля здійснення уповноваженими органами оперативно-розшукових заходів, встановлення, функціонування та захист від несанціонованого доступу яких забезпечують оператори та провайдери телекомунікацій.

Мета і завдання дослідження. Дослідити систему оперативно-розшукових заходів оператора мобільного зв'язку.

Задля досягнення окресленої мети потрібно виконати такі основні **завдання:**

1. Визначити теоретичні, зокрема правові, засади системи оперативно-розшукових заходів, а саме:

1.1. з'ясувати поняття оперативно-розшукових заходів;

1.2. з'ясувати основні засади застосування оперативно-розшукових заходів.

2. Дослідити функціонування системи оперативно-розшукових заходів оператора мобільного зв'язку, зокрема:

2.1. з'ясувати класифікацюя оперативно-розшукових заходів;

2.2. дослідити технічні засоби для здійснення оперативно-розшукових заходів.

Під час написання дипломної роботи використовувалися такі **методи**, як: аналіз, індукція, дедукція, метод порівняльного аналізу, формально-догматичний метод, системно-структурний та інституціональний методи.

Науково-теоретична основа виконання дослідження. Дане питання досліджували такі вчені як С. Тагієв, О.С. Сербінов, О. Хрущ, О. В. Грибовський, А. Ю. Шумилов, Т. В. Аверьянова та ін.

Структура та обсяг дипломної роботи зумовлені її метою та завданнями.

Робота складається зі вступу, трьох розділів, чотирьох підрозділів, висновку та списку використаних джерел.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ЗАСАДИ СИСТЕМИ ОПЕРАТИВНО-РОЗШУКОВИХ ЗАХОДІВ

1.1. Поняття оперативно-розшукових заходів

Слід зазначити, що нині існує правова невизначеність поняття оперативно-розшукових заходів (далі – ОРЗ) та відсутність їх законодавчого переліку, що негативно впливає на правозастосовний процес не тільки підрозділів, уповноважених на здійснення оперативно-розшукової діяльності (далі – ОРД), а й органів досудового розслідування, прокуратури та суду при використанні в ході досудового слідства чи судового розгляду кримінального провадження матеріалів ОРД, отриманих у ході проведення ОРЗ, здійсненні прокурорського нагляду і судового контролю за ОРД, поновленні прав громадян, порушених незаконним проведенням ОРЗ, тощо[3].

З огляду на те, яку роль поняття ОРЗ відіграє в теорії, законодавстві та практиці, йому в науковому полі присвячується низка наукових досліджень як вітчизняних, так і зарубіжних вчених, які працюють у сфері ОРД, контррозвідувальної діяльності, розвідки, криміналістики і кримінального процесу.

До прикладу, в навчальному посібнику «Оперативнорозшукова діяльність» зазначено, що оперативно-розшукові заходи є комплексом оперативно-технічних науково обґрунтованих, закріплених на законодавчому рівні, гласних і негласних, з точки зору тактики схожих між собою методів, прийомів і способів, за допомогою яких можна отримати, перевірити та реалізувати оперативну інформацію задля того, щоб вирішити задачі оперативнорозшукової діяльності [5, с. 107].

Такий неоднозначний підхід до розуміння поняття ОРЗ в науковому полі зумовлює те, що законодавством, відомчими нормативно-правовими актами зачасту до ОРЗ відносено ті заходи, котрі не є відповідними до їх змісту (до прикладу, ті організаційні заходи, котрі проводяться в рамках ОРД, оперативно-розшукові

операції, котрі з огляду на свою гносеологічну та правову природу наділені іншим змістовним значенням).

Тому, можна зазначити, що така невизначеність в науково-правовому полі щодо визначення поняття ОРЗ, зокрема й їх переліку підвищує актуальність теоретичної та законодавчої розробки даної проблеми, що, насправді, має практичне значення задля того, аби підвищити ефективність правозастосовного процесу органів, котрі здійснюють протидію злочинності у сфері економіки.

Слід зазначити, що нині ні чинним Кримінальним процесуальним кодексом України (далі – КПК України), ні Законом України «Про оперативно-розшукову діяльність» не закріплено визначення поняття «оперативно-розшуковий захід» (далі – Закон). Більше того, навіть саме слово «оперативно-розшуковий захід» не охоплюється законодавчим визначенням поняття «оперативно-розшукова діяльність», яке закріплено у ст. 2 даного Закону[3]. Така ситуація є незрозумілою, оскільки опертивно-розшуковий захід є невід'ємною складовом оперативно-розшукової діяльності.

Таким чином, оперативно-розшукові засоби є сукупністю узгоджених, взаємопов'язаних між собою, які мають єдину для всіх загальну мету та завдання дії уповноважених Законом України «Про оперативно-розшукову діяльність» суб'єктів, котрі проводяться здебільшого негласно за допомогою оперативних сил, спеціальних засобів, методів та форм.

Варто звернути увагу на те, що оперативно-розшукові засоби, які охоплюють собою і розвідувально-пошукові, і контррозвідувальні заходи, котрі реалізються суб'єктами ОРД, суттєві відрізняються від контррозвідувальних заходів, які реалізуються завдяки контррозвідувальних підрозділів Служби Безпеки України (далі – СБУ) задля того, аби отримати фактичні дані про розвідувально-підривну діяльність спеціальних служб іноземних держав і організацій. Порядок проведення останніх регламентовано Законом України «Про контррозвідувальну діяльність» від 26 грудня 2002 р. (статті 6, 7, 8) [4]. Крім того, вище зазначені заходи потрібно відрізняти й від розвідувальних заходів, які проводяться за допомогою розвідувальних органів України задля того, аби отримати інформацію, що потрібна

для забезпечення інтересів безпеки громадян, суспільства й держави. Поряд з тим, слід звернути увагу на те, що Законом України «Про розвідувальні органи України» порядок проведення даних оперативно-розшукових заходів не закріплюється, і визначено тільки правові основи організації та діяльності спеціальних органів державної влади, котрі займаються здійсненням розвідувальної діяльності задля того, аби захистити національні інтереси України від зовнішніх загроз: закріплює порядок контролю й нагляду за діяльністю таких органів, а також закріплює правовий статус працівників даних органів, та перелік їх соціальних гарантій [6].

1.2. Основні засади застосування оперативно-розшукових заходів

Слід зазначити, що стаття 4 Закону України «Про оперативно-розшукову діяльність» закріплює низку засад, на яких здійснюється вся ОРД. Проте, існують основні спеціальні засади, які властиві винятково застосуванню ОРЗ, до яких належать: конспірація; поєднання гласних та негласних методів, заходів та засобів; добровільніть конфіденційного співробітництва; забезпечення безпеки гласних і негласних позаштатних працівників[7,с.113].

Щодо засади конспірації, то вона полягає в тому, що має бути збережена таємниця здійснення негласних пошукових, розвідувальних і контррозвідувальних заходів та надання оперативно значущої інформації оперативному підрозділу повинно здійснюватись особами, котрі на конфіденційній основі співробітничають із ним. Варто зазначити, що будь-яка інформація про ОРЗ, які вже були проведені, або такі які проводяться або проведення яких є запланованим, а також конкретні факти конфіденційного співробітництва, мають зберігатися в таємниці як об’єктами оперативнорозшукової діяльності, так і працівниками самого оперативного підрозділу, котрим такі відомості не є необхідними задля виконання їх службових завдань.

В тому випадку, коли відповідно до ч. 5 ст. 8 Закону України «Про оперативно-розшукову діяльність» задля виконання окремих доручень в процесі оперативно-розшукової діяльності залучатимуться працівники інших підрозділів, то

їм також за відсутності обгрунтованої необхідності, не має бути надано доступу до інформації, котра безпосередньо не торкається їх участі у проведенні тих чи інших оперативно-розшукових заходів, кінцева мета заходу, сили й технічні засоби, котрі використовувалися, використовувалися або можуть бути використані під час проведення оперативно-розшукового заходу, а також відомості про всі ухвалені тактичні та стратегічні рішення[1]. Варто зазначини, що дана норма розповсюджується й на осіб, котрі на конфіденційній основі співпрацюють із оперативним підрозділом. Поряд з тим, відповідно до ч. 3 ст. 11 Закону України «Про оперативно-розшукову діяльність», ті особи, котрі можуть бути залучені до виконання завдань оперативно-розшукової діяльності, несуть обов'язок із збереження таємниці, яка стала їм відома, невиконання якого тягне за собою відповідальність, встановлену законодавством України[1]. Дана норма не розповсюджується на випадки, коли має місце розголошення інформації про незаконні дії, які порушують права людини.

Наступною є засада поєднання гласних і негласних методів, заходів, засобів оперативно-розшукової діяльності, яка випливає саме із ст. 2 Закону України «Про оперативно-розшукову діяльність» де надається визначення оперативно-розшукової діяльності як системи гласних і негласних пошукових, розвідувальних та контррозвідувальних заходів. Слід зазначити, що всі гласні та негласні методи, заходи, технічні засоби оперативно-розшукової діяльності, та їх поєднання, спрямовуються саме на те, аби вирішувати головне завдання такої діяльності – боротьбу зі злочинністю. Загалом, поєднання всіх цих технічних засобів, методів та заходів забезпечує швидке та ефективне отримання необхідного результату, за відсутності порушень положень чинного законодавства України [8, с.325].

Ще однією засадою проведення ОРЗ є наступальність, який полягає у безперервному ініціативному проведенні тих чи інших оперативно-розшукових дій, своєчасному одержанні та перевірці оперативно значущої інформації.

І досить важколивою засадою ОРЗ є гуманність в оперативно-розшуковій діяльності, яка полягає, насамперед, в спрямованості даної діяльності на те, аби захищати життя, здоров'я, конституційні права та свободи людини й громадянина,

та забезпечувати безпеку суспільства й держави в цілому [9, с. 117]. Слід зазначити про те, що задля отримання інформації та досягнення інших цілей ОРД заборонено використовувати технічні засоби, психотропні, хімічні та інші речовини, що можуть пригнічувати волю людей чи наносити шкоду їх здоров'ю і навколишньому середовищу.

РОЗДІЛ 2
ФУНКЦІОНУВАННЯ СИСТЕМИ ОПЕРАТИВНО РОЗШУКОВИХ ЗАХОДІВ ОПЕРАТОРА МОБІЛЬНОГО ЗВ'ЯЗКУ

2.1. Класифікація оперативно-розшукових заходів

Задля того, аби дослідити проблеми класифікації оперативно-розшукових заходів у розвідці потрібно розглянути ті підходи щодо їх розподілу, які склалися в науковому полі.

Зокрема своя точка зору на класифікацію оперативно-розшукових заходів у таких російських дослідників як К.К. Горяінов, В.С. Овчинський та О.Ю. Шумилов [10, с.276], адже вони поділяють ці заходи на наступні:

• ті, які пройшли адаптацію розшуком і є своєрідними криміналістичними методами: опитування, збирання відомостей, збір зразків з метою порівняльного дослідження, перевірочні закупівлі, дослідження предметів і документів, спостереження, ідентифікація особистості, огляд приміщень, будинків, споруд, ділянок місцевості й транспортних засобів, оперативний експеримент;

• розвідувальні методи, які притаманні тільки розшуку: контроль над поштовими відправленнями, телеграфними та іншими повідомленнями, прослуховування телефонних переговорів і зняття інформації з технічних каналів зв'язку;

• безпосередньо розвідувальні операції: оперативне впровадження і контрольована поставка.

В свою чергу, О.Ю. Шумилов вирізняє певні категорії оперативно-розшуковиз заходів [11, С. 9–10]. Першу категорію складають звичайні оперативно-розшукові заходи, котрими не передбачено обмеження конституційних прав людини. Такі заходи можуть бути проведені і в межах адміністративно-режимної оперативно-перевірочної роботи, і в рамках оперативно-розшукового процесу. До них належать: опитування, збирання відомостей, збір зразків для порівняльного дослідження (за винятком збору зразків, що передбачають проникнення у житло особи й збору

зразків голосу людини внаслідок здійснення контролю її телефонних переговорів), перевірочна закупівля, дослідження предметів і документів, спостереження (за винятком спостереження, яким передбачено проникнення у житло особи), ідентифікація особистості, оперативне впровадження, контрольована поставка, обстеження приміщень, будинків, споруд (за виняткомжитла), ділянок місцевості й транспортних засобів і зняття інформації з технічних каналів зв'язку (без втручання у приватне життя громадян).

Другу категорію, на думку дослідника, складають ті оперативно-розшукові заходи, якими передбачено обмеження конституційних прав людини, «…котрі проводяться лише під час оперативно-розшукового процесу задля того, аби вирішити завдання, які пов'язані з обмеженням деякого конституційного права людини й громадянина». Ця категорія озоплює собою всю решту оперативно-розшукових заходів, окрім оперативного експерименту, адже даний захід віднесений до третьої категорії заходів, що є спеціальними за своїм характером. До неї входять ті оперативно-розшукові заходи, котрі намправлені на здійснення протидіїї тяжких і особливо тяжких кримінальних правовопорушень. Наприклад, у Законі Російської Федерації «Про оперативно-розшукову діяльність» до спеціальних оперативно-розшукових заходів належить лише оперативний експеримент [10, с.280].

Слід зазначити, що О.Ю. Шумиловом здійснено багато дослідженнь у сфері ОРД в пошуках істини, і було також запропоновано дещо іншу класифікацію оперативно-розшуковиз заходів. Зокрема, автор поділив оперативно-розшукові заходи на дії, заходи та операції.

Дії охоплюють собою опитування, збирання відомостей, збір зразків з метою здійснення порівняльного дослідження, дослідження предметів і документів, спостереження, ідентифікація особистості.

До заходів належать: обстеження приміщень, будинків, споруд, ділянок місцевості й транспортних засобів, оперативний експеримент, контроль поштових відправлень, телеграфних та інших повідомлень, прослуховування телефонних переговорів і зняття інформації з технічних каналів зв'язку, оперативне впровадження й перевірочна закупівля.

Операція, на думку дослідника – це контрольована поставка.

В наступному своєму дослідженні «Краткая сыскная энциклопедия» О.Ю. Шумилов фактично дослідив ще одну класифікацію оперативно-розшукових заходів, і подлив їх на оперативно-технічні, спеціальні й інші оперативно-розшукові заходи [12, С. 79]. Проте, з огляду на таку кількість досліджень, присвячених опертивно-розшуковим заходам, автор так і висловив чітку прихильність до якоїсь певної їх класифікації.

Власна класифікація оперативно-розшукових заходів була запропонована і таким дослідником як В.М. Осипкін [13, с. 11.], котрий також виізняв три категорії оперативно-розшукових заходів.

Перша категорія, на думку автора, включає в себе ті оперативно-розшукові заходи, які не потребують винесення спеціальної постанови й одержання дозволу відповідного судді як обов'язкової підстави їх проведення. До таких оперативно-розшукових заходів належать: опитування; збирання відомостей; збір зразків з метою здійснення порівняльного дослідження, перевірочна закупівля предметів, речовин і продукції, вільна реалізація котрих не забороненяється законом чи оббіг яких так само не обмежується законом; дослідження предметів і документів; спостереження; ідентифікація особистості; контрольована поставка предметів, речовин і продукції, вільна реалізація яких не заборонена або їх обіг не обмежений; обстеження приміщень (за винятком житлових), будинків, споруд, ділянок місцевості й транспортних засобів.

Друга категорія, на думку дослідника, охоплює собою оперативно-рлзшукові заходи, підствою проведення якиї є спеціальна постанова, котра затверджена керівником органу, який провадить оперативно-розшукову діяльність. До таких заходів належать: перевірочна закупівля предметів, речовин і продукції, вільна реалізація яких забороненяється законом чи обіг яких так само обмежується законом; контрольована поставка предметів, речовин і продукції, вільна реалізація яких забороняється законом або обіг яких так само обмежується; оперативний експеримент; оперативне впровадження.

До третьої категорії В.М. Осипкін відносить ті оперативно-розшукові заходи, які можуть бути проведені не тільки на підставі спеціальної постанови керівника органу, який проводить оперативно-розшукову діяльність, а й на підставі наявного судового рішення. До таких оперативно-розшукових заходів належать обстеження житла; контроль поштових відправлень, телеграфних та інших повідомлень; прослуховування телефонних переговорів і зняття інформації з технічних каналів зв'язку.

Оперативно-розшуковій науці відомі й інші класифікації оперативно-розшукових заходів. Проте внаслідок детального аналізу даних класифікацій можна дійти висновку, що тдані класифікації мають певні недоліки.

Наприклад, К.К. Горяінов, В.С. Овчинський та О.Ю. Шумилов поділяють оперативно-розшукові заходи на адаптовані розшуком криміналістичні методи, розвідувальні методи, властиві тільки розшуку, і розвідувальні операції мають досить умовний та спірний характер. До приклуд, хибним є твердження зазначених дослідників про те, що контроль поштових відправлень належить до розвідувальних методів і властивий тільки розшуку. Накладення арешту на кореспонденцію й подальше дослідження листів є властивим і для криміналістики. Спірною є й думка про те, що спостереження є саме адаптованим криміналістичним методом, оскільки воно є ближчим саме до розшукових дій.

Не зовсім точною є одна із класифікацій, яку запропонував дослідник О.Ю. Шумилов. Як вважає вчений, опитування, збирання відомостей не обмежують за своїм характером конституційних прав людини і громадянина [10, с.282].Проте з даним твердженням можна не погодитись, адже під час проведення опитувань досить часто люди розкривають медичні, банківські чи будь-які інші особисті таємниці; обставини і зміст телефонних переговорів, переписки тощо, зміст якиї закріплюється й охороняється на рівні Основого Закону України. Поряд з тим, дійсно можна зазначити, що прослуховування телефонних переговорів не в будь-якому випадку може обмежувати права людини. Мова йде про ті випадки, коли соба задля своєї безпеки звертається з проханням здійснити контроль своїх телефонних переговорів.

Дослідник С.І. Захарцев проявляє сумніви стосовно того, чи варто надавати особливий статус такому оперативно-розшуковому заходу, як оперативний експеримент, посилаючись на те підставу, що він направлений здійснювати протидію вчиненню тяжких і особливо тяжких кримінальних правопорушень. Слід зазначити, що ще в 2000 році оперативний експеримент справді мав статус єдиного оперативно-розшукового заходу, котрий дозволялось проводити тільки розкриваючи тяжкі або особливо тяжкі кримінальні правопорушення. Проте впервше в 2001 році в Росії, коли був прийнятий Федеральний Закон «Про внесення змін і доповнень у деякі законодавчі акти Російської Федерації у зв'язку з ратифікацією Конвенції про захист прав людини й основних свобод» [14, Ст. 1132.] цей список поповнився й таким заходом як прослуховування телефонних переговорів. Враховуючи такі динамічні зміни законодавства у світі, не варто вважати, що класифікація оперативно-розшуковиз заходів перебуває у винятковій залежності від Закону Російської Федерації «Про оперативно-розшукову діяльність»[15, С. 282].

Крім того, незрозумілим залишається той факт, з якою метою дослідники класифікують оперативно-розшукові заходи на безпосередньо заходи, операції і дії, з огляду на те, що визначення «оперативно-розшукових дій» так і не існує ні на рівні законодавста, ні в науково-правовому полі. Як було зазначено вище, науковці відносять до оперативно-рошукових заходів-дій опитування, збирання відомостей, збір зразків з метою здійснення порівняльного дослідження, дослідження предметів і документів, спостереження, ідентифікація особистості. Проте кожна перелічена «дія» може бути і західом, і, залежно від організації, й операцією. Не ясно залишається чому саме такий оперативно-рошуковий захід як контрольована поставка віднесена О.Ю. Шумиловим до операції. і чому автор не наділяє таким же статусом оперативне впровадження чи оперативний експеримент [12, с. 80].

Задля того, аби вирішити проблему використання матеріалів оперативно-розшукової діяльності в кримінальному процесі досить вагоми критеріями класифікації оперативно-розшукових заходів, на думку дослідника М.А. Погорецького, є саме їх функціональне призначення, можливість обмеження конституційних прав людини, умови та специфіка проведення, характер закріплення

Законом України «Про оперативно-розшукову діяльність», документування та подальше використання їх результатів у кримінальному процесі [16, с. 65].

Слід зазначити, що М.А. Погорецький в межах оперативно-розшукової діяльності вирізняє саме оперативні організаційно-управлінські заходи й оперативно-розшукові заходи, такимчином розмежовуючи ці поняття [16, с. 66].

Оперативні організаційно-управлінські – це ті заходи, які здійснюються з метою самозабезпечити функціонування оперативнорозшукової діяльності як самостійної державної системи, а також здійснення оперативно-розшукових заходів (оперативно-забезпечувальних та інформаційно-пізнавальних заходів: використання допомоги гласних і негласних штатних та позаштатних працівників (п. 12 ст. 8 Закону України «Про оперативно-розшукову діяльність»); встановлення конфіденційного співробітництва з особами на засадах добровільності (п. 13 ст. 8 Закону України «Про оперативно-розшукову діяльність»); створення з метою конспірації підприємств, організацій, використання документів, якими зашифровано чи відомчу належність працівників, приміщень і транспортних засобів оперативних підрозділів (п. 16 ст. 8 Закону України «Про оперативно-розшукову діяльність»); створення і застосування автоматизованих інформаційних систем (п. 17 ст. 8 Закону України «Про оперативно-розшукову діяльність»).

Організаційно-управлінські, аналогічно як і оперативно-забезпечувальні заходи (операції), немають самостійного характеру, і є насамперед допоміжними, адже вони направлені на те, аби успішно провести інформаційно-пізнавальні заходи, і зрештою, на те, аби створити умови задля своєчасного отримання оперативної інформації [16, с. 66].

В свою чергу, оперативно-розшукові заходи автор поділяє на оперативно-забезпечувальні й інформаційно-пізнавальні [16, с. 67].

Оперативно-забезпечувальні – це ті заходи (операції), які направлені на те, аби успішно провести конкреті інформаційно-пізнавальні заходи щоб пізнати конкретні обставини злочинної діяльності, зокрема віднайти, виявити фактичні дані та їх джерела. Даною групою охоплюються заходи, які перелічені у ст. 8 Закону України «Про оперативно-розшукову діяльність», зокрема: контрольна та оперативна

закупівля й постачання, порушення питання про проведення перевірок фінансово-господарської діяльності підприємств, установ, організацій та осіб, котрі здійснюють підприємницьку діяльність чи інші види господарської діяльності індивідуально, та прийняття участі в їх проведенні (п. 3); проведення операцій по захопленню злочинців, припиненню кримінальних правопорушень, розвідувально-підривної діяльності спецслужб іноземних держав, організацій та окремих осіб (п. 5); проникнення в злочинну групу негласного працівника оперативного підрозділу або особи, яка співпрацює з останнім, із збереженням в таємниці достовірних даних щодо їх особистості (п. 8) [16, с. 64]

Інформаційно-пізнавальними є заходи, які безпосередньо направлені на те, аби отримати оперативну інформацію згідно з завданнями оперативно-розшукової діяльності. Оперативні інформаційно-пізнавальні заходи залежно від того, з якою метою передбачено їх проведння, поділяються на розвідувально-пошукові, розшукові й контррозвідувальні [16, с. 66]

Стаття 8 Закону України «Про оперативно-розшукову діяльність» відносить до оперативно-пізнавальних заходів наступні: опитування (п. 1); відвідування жилих та інших приміщень, згода на що надається їх власниками чи мешканцями з метою з'ясувати обставини вчиненого чи такого, яке перебуває на стадії готування, кримінального правопорушення, та зібрати відомості про протиправну діяльність підозрюваних або осіб, стосовно яких проводиться перевірка (п. 6); негласне виявлення та фіксування слідів тяжкого кримінального правопорушення, документів та інших предметів, які можуть виступати і якості доказів підготовки чи вчинення такогокримінального правпорушення, чи отримання розвідувальної інформації, зокрема внаслідок проникнення оперативного працівника в приміщення, транспортні засоби, на земельні ділянки (п. 7); зняття інформації з каналів зв'язку, застосування інших технічних засобів отримання інформації (п. 9); контроль шляхом відбору за окремими ознаками телеграфнопоштових відправлень (п. 10); проведення візуального спостереження в громадських місцях із застосуванням фото-, кіно- і відео них та радіоприладів, інших технічних засобів (п. 11) [16, с. 65]. М.А. Погорецький вважає, що формулювання окремих оперативно-розшукових заходів

даної категорії в чинній редакції Закону України «Про оперативно-розшукову діяльність» має бути уточнено законодавцем. До того ж, автор вважає, що слід закріпити у Законі України «Про оперативно-розшукову діяльність» і такі оперативно-розшукові заходи, як збирання відомостей про об'єкти оперативно-розшукової діяльності; оперативний експеримент; ідентифікація особистості тощо [16, с. 67]

З огляду на особливості, а також засоби, за допомогою яких проводяться оперативно-розшукові заходи можуть бути поділені на оперативні та оперативно-технічні.

З огляду на умови, за яких проводяться оперативно-розшукові заходи, їх можна поділити на ті, якими передбачене обмеення конституційних прав людини, зокрема такі проводяться виключно на підставі судового рішення (наприклад, негласне проникнення до житла чи до іншого володіння особи, зняття інформації з каналів зв'язку, контроль за листуванням, телефонними розмовами, телеграфною та іншою кореспонденцією, застосування інших засобів одержання інформації – передбачені ст. 8, ч. 2), та ті, якими не передбачено обмеження конституційних прав людини і відповідно проведення яких не потребує такого судового рішення [16, с.67].

Слід зазначити, що найбільш поширеною та загально відомою є класифікація оперативно-розшукових заходів на на гласні розшукові заходи та негласті. До першої групи належать такі як: опитування осіб, які надали на це згоду (ст. 8, п. 1), порушення в передбаченому законом порядку питання про проведення перевірок фінансово-господарської діяльності підприємств, установ, організацій (ст. 8, п. 3), витребування, збирання й вивчення документів та даних, які надають характеристику діяльності підприємств, установ, організацій, а також спосіб життя конкретно визначених осіб, які підозрюються у підготовці або вчиненні кримінального правопорушення, джерело та розміри їхніх доходів (ст. 8, п. 4); відвідування жилих та інших приміщень, за наявносі згоди власників чи мешканців з метою з'ясувати обставини вчиненого або такого, що перебуває на стадії готуваннння кримінального правопорушення, та зібрати відомості про протиправну

діяльність підозрюваних або осіб, стосовно котрих здійснюється перевірка (ст. 8, п. 6). В свою чергу, до другої групи належать наступні оперативно-розшукові заходи: негласне проникнення до житла чи до іншого володіння особи, зняття інформації з каналів зв'язку, контроль за листуванням, телефонними розмо- вами, телеграфною та іншою кореспонденцією, застосування інших засобів одержання інформації та ін.

Слід зазначити, що певні із вищезазначених оперативно-розшукових заходів можуть бути віднесені як до гласних, так і до негласних, зокрема такі як: наприклад, опитування, відвідування жилих та інших приміщень за наявності згоди їх власників чи мешканців з метою з'ясувати обставини вчиненого чи такого, що перебуває на стадії готування кримінального правопорушення, а та збирання відомостей про протиправну діяльність особі, які підозрюються чи осіб, стосовно яких здійснюється перевірка та ін.

З огляду на вимоги, які ставляться до документування і використання результатів оперативно-розшукових заходів у кримінальному процесі, оперативно-розшукові заходи поділяють на ті, які можуть використовуватися тільки з інформаційно-тактичною метою у кримінальному процесі, та ті, які за певних умов, згідно звимогами КПК України, можуть бути використані задля того, аби отримати фактичні дані, що можуть виступати і якості доказів у кримінальній справі.

Щоб визначити поняття та види оперативно-розшукових заходів потрібно виходити, перш за все, з з'ясування їх співвідношення з розшуковими заходами органу дізнання, про які йде мова у ч. 5 ст. 104, ч. 3 ст. 114 КПК України. Проводити такі заходи повинні й ті органи дізнання, які не мають повноваження на здійснення оперативно-розшукової діяльності. В даному випадку це капітани морських суден, які знаходяться у далекому плаванні, органи пожежного нагляду та ін. [17, с.485].

М.А. Погорецький вважає, що ті оперативно-розшукові заходи, які передбачені ст. 8 Закону України «Про оперативно-розшукову діяльність», можуть бути проведені виключно тими органами дізнання, які прямо зазначені у ст. 5 даного Закону.

Якщо говорити про розшукові заходи, котрі зазначені у ч. 5 ст. 104, ч. 3 ст. 114 КПК України, то вони можуть бути проведені будь-якими органами дізнання. Такі заходи не надалені статусом оперативно-розшукових [16, с.67].

З огляду на те, що оперативно-розшукова діяльність здійснює превентивну функцію щодо боротьби зі злочинністю, котра не регулюється чинним Законом України «Про оперативно-розшукову діяльність» а тільки передбачена у статті й, то необхіднонадати їй детальне визначення, і відповідно уповноважити оперативні підрозділи задля її реалізації на проведення тих оперативно-розшукових (розвідувально-пошукових заходів), котрими не обмежуються права громадян [18, с.38].

У процесі здійснення оперативно-розшукової діяльності оперативний підрозділ має право на те, щоб: 1) опитувати громадян; 2) збирати відомості про об'єкт оперативно-розшукової діяльності; 3) досліджувати предмети і документи; 4) збирати зразки з метою проведення порівняльного дослідження; 5) проводити оперативний експеримент; 6) проводити ототожнення особистості; 7) здійснювати візуальне спостереження в громадських місцях із застосуванням фото-, кіно- і відеозйомки, оптичних та радіоприладів, інших технічних засобів; 8) проводити оперативну закупівлю та контрольоване постачання; 9) проводити негласне проникнення до житла чи іншого володіння особи, обстеження приміщень, споруд, ділянок місцевості та транспортних засобів; 10) знімати інформацію з каналів зв'язку, застосувувати технічі засоби отримання інформації; 11) контролювати через відбір за окремими ознаками телеграфно-поштові відправлення [16, с. 67].

Варто зазначити, що запропоновані класифікації оперативно-розшукових заходів мають єдиний для всіх недолік, зокрема бажання дослідників здійснити систематизацію заходів стосовно назв та типових дій, хоча будь-який захід може бути проведено не лише за типовими планами. Найбільш уніфікована дія за певних умов може перетворитися на оперативну комбінацію. Таким чином, оперативно-розшукові заходи, перш за всЕ, варто поділити за іншими, більш вагомими підставами, а саме: обмеження конституційних прав людини, умови й особливості

проведення спеціальних оперативно-розшукових операцій, їх документування та використання результатів у кримінальному судочинстві [19, с.74].

Зважаючи на специфіку проведення оперативно-розшукових заходів потрібно вирізнити оперативно-розшукові заходи, котрі тільки припускають можливість використовувати спеціальні технічні засоби, і такі, які в обов'язковому порядку мають застосовувати такі заходи, зокерма мова йде про оперативно-розшукові заходи, як проводяться під час роботи у мережах зв'язку.

О.Ю. Шумилов у своєму дослідженні «Краткая сыскная энциклопедия» зазначив, що оперативно-розшукові заходи у мережах зв'язку є різновидом ОТЗ, які проводяться оперативнотехнічними підрозділами органу, який проводить оперативно-розшукову діяльність, і мета таких заходів – це одержання інформації, яка потрібна для конкретного завдання цієї діяльності [20, с. 129].

З огляду на документування, яке є необхідним у проведені оперативно-розшукових заходів, їх можна поділити на заходи, задля проведення котри потребується прийняття спеціального рішення чи надання дозволу суду, та заходи, задля проведення котрий обов'язкоко потрібне постновлення рішення керівника органу, який проводить оперативно-розшукову діяльність, і заходи, які можна проводити базуючись на судовому рішенні. Таку класифікацію розробив видатний вчений О. М. Бандурка у своєму дослідженні «Прокурорский надзор за оперативно-розыскной деятельностью» [21, с.251].

Проте, варто зазначити, що поряд з іншими науковцями, О.М. Бандурка здійснював класифікацію заходів за назвами та порядком впровадження. Зокрема спостереження він відносив до однієї групи, оперативний експеримент- до другої, прослуховування телефонних переговорів – до третьої групи. Однак таке твердження можна не підтримати, адже такий доволі конкретизований поділ є неприпустимим, адже задля того, аби провести прослуховування телефонних переговорів в певних ситуаціях за певних умов дозвіл судді не потребується, поряд з тим, спостереження в певних випадках може бути проведено тільки на підставі дозволу судді [21, с. 253]

Зважаючи на використання результатів оперативно-розшукової діяльності, проведені за кримінальними справами оперативнорозшукові заходи можна класифікувати на: заходи, котрі можуть бути використані в доказуванні, і заходи, результати яких не вважається за можливе використосувати в доказуванні. Перша група включає в тебе ті оперативно-розшукові заходи, результати яких зафіксовані й належним чином представлені під час встановлення причини вчинення кримінального правопорушення. Друга група охоплює собою оперативно-розшукові заходи, результати яких можуть мати інформативний, проте не нести при цьому ніякого доказового характеру.

Проводячи аналіз практичної діяльністі за реалізацією оперативно-розшукових заходів і використанням їх результатів у доведенні за кримінальними справами, можна дійти висновку, що наріжний камень у правовому регулюванні проведення оперативно-розшукових заходів – це обмеження прав людини й громадянина.

Виходячи з накового доробку видатних науковців, які займалися дослідженням оперативно-розшукової діяльності та згідно з нормами національного законодавства, можна запропонувати такі класифікацію оперативно-розшукових заходів, зокрема: оперативно-розшукові заходи з використанням оперативно-технічних засобів, оперативно-технічні заходи, котрі можуть бути проведені на підставі рішення суду, спеціальні оперативно-розшукові операції [22, с.420].

Оскільки наукові думки дослідників часто змінюються та вдосконалюються, можна запропонувати й таку класифікацію оперативно-розшукових заходів, зокрема: Захід-дія – що є дією одного працівника оперативного підрозділу, який уповноважений законодавством України, яке ґрунтується на галузевих принципах, спрямована на встановлення, уточнення, закупівлю, перевірку, дослідження, фіксацію та отримання оперативних, пошукових та оперативно-технічних даних, що передбачені функціональними обов’язками працівника та власним досвідом роботи, про ознаки протиправних, спеціально розроблених дій із застосуванням науково обґрунтованих, апробованих, найбільш ефективних способів і тактичних прийомів щодо вирішення організаційнотактичних завдань і використання їх результатів,

отриманих та зафіксованих відповідно до правил негласного провадження з розшуковою, розвідувальною та контррозвідувальною метою та у кримінальному судочинстві. Це заходи, до яких слід віднести: опитування, спостереження, засідку, переслідування, закупівлю, перевірку, збирання відомостей, отримання зразків та матеріалів, вивчення предметів, речей, документів, ідентифікацію особистості та психодіагностику.

Сукупність дій-заходів – це дії декількох працівників оперативного підрозділу, уповноважених законодавчими та нормативними актами, що спрямовані на встановлення, уточнення, перевірку, дослідження, фіксацію та отримання оперативних, пошукових та оперативно-технічних даних, які передбачені завданнями та функціями оперативного підрозділу із застосуванням науково обґрунтованих, апробованих, найбільш ефективних способів, тактичних прийомів з вирішення організаційно-тактичних розшукових, розвідувальних та контррозвідувальних завдань і використання їх результатів, отриманих та зафіксованих відповідно до правил негласного провадження з розшуковою, розвідувальною та контррозвідувальною метою та у кримінальному судочинстві.

Сукупність заходів-операцій є комплексним здійсненням адміністративних, кримінально-правових, організаційно-тактичних, оперативно-технічних та управлінських дій, які об’єднані єдиною ідеєю, мать єдиний план, узгоджені між собою за часом, місцем і цілями проведення оперативно-розшукових та інших, які передбачені законодавством України заходів, що засновані на використанні гласних та негласних сил, засобів і методів ОРД, які направлені на попередження і розкриття тяжких та особливо тяжких кримінальних правопорушень, та вирішення важких оперативно-тактичних завдань у боротьбі зі злочинністю.

В свою чергу, операції можна поділити на наступні: ініціювання, контроль, експеримент, упровадження, закупівля, постачання, затримання, супроводження тощо.

2.2. Технічні засоби для здійснення оперативно-розшукових заходів

Згідно з ч. 4 ст. 39 Закону України від 18 листопада 2003 року «Про телекомунікації» на операторів та провайдерів телекомунікацій покладений обов'язок за власний рахунок установлювати на своїх телекомунікаційних мережах технічні засоби, які потрібні задля проведення уповноваженими органами ОРЗ, та обов'язок із забезпечування функціонування зазначених технічних засобів, а також у межах своїх повноважень сприяти проведенню оперативно-розшукових заходів та недопущенню розголошення організаційних і тактичних прийомів їх проведення. Оператори телекомунікацій зобов'язані забезпечувати захист зазначених технічних засобів від несанкціонованого доступу[23]. Таким чином, законодавець поклав обов'язок із встановлення і функціонування таких технічних засобів саме на операторів та провайдерів телекомунікацій.

В свою чергу, слід зазначити про те, що 04 вересня 2018 року було видано Наказ Служби безпеки України та Адміністрації Державної служби спеціального зв'язку та захисту інформації України № 1519/533, яким затверджено «Технічні засоби для здійснення уповноваженими органами оперативно-розшукових заходів та негласних слідчих (розшукових) дій у телекомунікаційних мережах загального користування України»[2].

Даний нормативний документ базується на рекомендаціях Резолюції Ради Європи «Про законне перехоплення телекомунікацій» та «Про оперативні потреби правоохоронних органів стосовно телекомунікаційних мереж загального користування та послуг зв'язку» й закріплює загальні технічні вимоги (далі – ЗТВ) до технічних засобів, які використовують уповноважені органи при проведенні оперативно-розшукових заходів та негласних слідчих (розшукових) дій у телекомунікаційних мережах загального користування України[2].

Потреба в розробленні таких ЗТВ пов'язана безпосередньо з розвитком систем телекомунікацій, котрі використовують нові сучасні телекомунікаційні технології[24, с.58].

Варто зазначити, що базуючись на таких ЗТВ, та враховуючи специфіку призначення телекомунікаційної мережі, розробляються окремі технічні вимоги (далі – ОТВ) для таких технічних засобів, що по суті доповнюють та конкретизують ЗТВ.

Такі ЗТВ охоплюють собою технічні засоби, які використовують уповноважені органи для здійснення оперативно-розшукових заходів та негласних слідчих (розшукових) дій у телекомунікаційних мережах загального користування України в порядку, передбаченому законом.

ЗТВ застосовують оператори, провайдери телекомунікацій; проектувальники й виробники даних технічних засобі; проектувальники телекомунікаційних мереж і виробники обладнання телекомунікацій; органи, наділені повноваженнями здійснювати оперативно-розшукові заходи та негласні слідчі (розшукові) дії; органи, що проводять оцінку відповідності, випробувальними центрами (лабораторіями), які проводять діяльність, що стосується підтвердження відповідності технічних засобів; адміністратори Автоматизованої інформаційної системи «Централізована база даних перенесених номерів»[25, с.37].

Слід зазначити, що технічні засоби для здійснення уповноваженими органами оперативно-розшукових заходів та негласних слідчих (розшукових) дій у телекомунікаційних мережах загального користування України охоплюють собою:

1) мережний комплект (далі – МК), який покликаний здійсненювати перехоплення телекомунікацій;

2) засоби управління системою перехоплення телекомунікацій (тобто сервери, станції, термінали та інші – ЗУСП);

3) засоби захищеної транспортної мережі (далі – ЗЗТМ);

4) програмне забезпечення (далі – ПЗ) технічних засобів;

5) експлуатаційну й програмну документацію технічних засобів;

6) комплект запасних частин, інструменту та приладдя (далі – ЗІП).

Слід зазначити, що поєднання даних засобів із функціональної точки зору зумовлбє створення системи перехоплення телекомунікацій (далі – СПТ).

Для того, аби розуміти зміст вище зазначених технічних засобів, необхідно розглянути призначення кожного з них.

По-перше, МК покликаний перехоплювати телекомунікації, які потрібні для розпізнавання й відгалуження об’єктів перехоплення, відбору та передачі даних до ЗУСП.

Складається МК з обладнання відбору об’єкта перехоплення (далі – ОВОП) та шлюзу, котрі встановлюються на сегменті телекомунікаційної мережі загального користування України. Організація взаємодії зазначених елементів МК відбувається по інтерфейсу перехоплення. В свою чергу, шлюз повинен здійснювати взаємодію із ЗУСП по інтерфейсу управління та передачі.

Задля того, аби забезпечити доступ до будь-яких об’єктів перехоплення, враховуючи технічні характеристики та особливості побудови телекомунікаційної мережі, можуть бути використані технологічні можливості мережі при відгалуженні об’єктів перехоплення.

Варто зазначити, що МК, здійснюючи перехоплення телекомунікацій не можуть погіршувати якість послуг, які надаються абонентам телекомунікаційної мережі. Саме тому МК, що входить до складу телекомунікаційного обладнання ма відповідати стандартам та цим ЗТВ, що підтверджується у встановленому законом порядку.

Призначення ЗУСП полягає в тому, що вони покликані здійснювати управління МК задля того, аби забезпечити гарантоване перехоплення об’єктів перехоплення, прийому даних від МК та їх обробки, підготовки копій об’єктів перехоплення, а також для того, аби організувати незалежне використання одержаної інформації кожним із суб’єктів перехоплення[26].

Якщо говорити про ЗЗТМ , то їх покликанням є забезпечення взаємодії технічних засобів СПТ між собою, а також між ЗУСП та віддаленими терміналами суб'єктів перехоплення по захищених каналах електрозв’язку.

ПЗ СПТ забезпечує функціонування технічних засобів СПТ згідно з цими ЗТВ.

В свою чергу, ЗІП забезпечують підтримання та відновлення працездатності, справності складових частин СПТ при технічному обслуговуванні.

Варто зазначити, що законодавець встановив функціональні вимоги стосовно кожного із технічних захосіб СПТ.

Наприклад, щодо МК, то вій має забезпечувати реалізацію гарантованого перехоплення об'єктів перехоплення в телекомунікаційній мережі незважаючи на те, які технології в ній застосовуються, а також незалежно на її структуру та топології, і передбачати локальну чи розподілену структуру МК на площах оператора, провайдера телекомунікацій.

Таким чином МК повинні:

1) розпізнавати та відгалужувати об'єкти перехоплення, відгалуження та фіксувати вміст сеансів зв'язку абонентів спостереження протягом усього періоду здійснення перехоплення;

2) перетворювати дані задля взаємодії із ЗУСП з формату інтерфейсу перехоплення на формат інтерфейсу управління та передачі і здійснювати зворотне перетворення;

3) забезпечувати можливість адаптації до модифікацій обладнання телекомунікаційної мережі та версій його ПЗ, що в свою чергу, забезпечує функціонування СПТ за призначенням;

4) передавати до ЗУСП вміст сеансів зв'язку абонентів спостереження в форматі, котрий використовувався операторами, провайдерами телекомунікацій до використання кодування, стиснення та шифрування телекомунікаційного трафіку;

5) недопускати виявлення факту того, що мало місце перехоплення телекомунікацій абонентами та персоналом оператора, провайдера телекомунікацій.

Щодо ОВОП, то воно має:

1) забезпесувати взаємодію з обладнанням телекомунікаційної мережі, щоб отримати доступ до інформації про телекомунікаційні послуги цієї мережі, які надані абонентам спостереження;

2) прийняти від шлюзу згідно з інтерфейсом перехоплення команд взаємодії з телекомунікаційною мережею;

3) розпізнавати та відгалужувати об’єкти перехоплення у реальному часі;

4) передавати об’єкти перехоплення до шлюзу через інтерфейс перехоплення;

5) захищати від несанкціонованого доступу до інформації, котра має відомості про його взаємодію з телекомунікаційною мережею та відібрані об’єкти перехоплення.

Щодо шлюзу, то він повинен:

1) узгоджувати сигнали автоматичного управління роботою ОВОП та його (їх) адміністрування;

2) підключатися до точок доступу телекомунікаційних мереж за інтерфейсами, базуючись на протоколах СКС-7; DIAMETER та SIP;

3) підключатися до апаратно-програмних засобів, котрі, в свою чергу, покликані забезпечувати аналіз, обробку та фільтрацію трафіку в каналах сигналізації від/до інших телекомунікаційних мереж стосовно функціонування мереж рухомого (мобільного) зв’язку та кінцевого обладнання абонентів;

4) приймати від ЗУСП команди управління з метою здійснення гарантованого перехоплення вмісту об’єктів перехоплення;

5) перетворювати команди управління в команди взаємодії з телекомунікаційною мережею (зокрема й ознаки об’єктів перехоплення);

6) передавати в автоматичному режимі команди взаємодії (зокрема й ознаки об’єктів перехоплення) до всіх ОВОП, що можна було розпізнати та відгалузити об’єкти перехоплення;

7) приймати від ОВОП згвдно з інтерфейсом перехоплення відгалуженв об’єкти перехоплення;

8) отримувати від ЗУСП підтвердження про отримання об’єктів перехоплення після того, як вони були прийняті;

9) приводити інформаційні повідомлення до вигляду, який придатний для передавання через інтерфейс управління та передачі;

10) зберігати ідентифікатори абонентів спостереження в незмінному вигляді протягом терміну, який потрібний для того, аби здійснити перехоплення телекомунікацій та передати до ЗУСП об’єктиперехоплення;

11) передавати до ЗУСП повідомлення про підтвердження прийому та виконання команд управління (якщо є така технічна можливість);

12) передавати до ЗУСП вміст відібраних об’єктів перехоплення;

13) передавати до ЗУСП певні, визначені законом повідомлення;

14) передавати до ЗУСП ідентифікаційні властивості об’єктів перехоплення, які визначаються зі службових даних об’єктів перехоплення та покликані забезпечувати формування ознак об’єктів перехоплення;

15) захищати від несанкціонованого доступу до інформації, що має риси об’єктів перехоплення, дані взаємодії з телекомунікаційною мережею та об’єкти перехоплення;

16) забезпечувати буферизацію, тобто тимчасове проміжне зберігання інформації для запобігання її втрати, вмісту об’єктів перехоплення у разі пошкодження каналу зв’язку між шлюзом та ЗУСП не менше чотирьох годин;

17) створювати, редагувати та видаляти групи обладнання ОВОП;

18) ініціювати процедуру проведення аудиту/синхронізації таблиць спостереження, як окремого ОВОП, так і груп ОВОП, відображення результатів аудиту та синхронізації у табличному вигляді, їх сортування за часом та типом події відповідно до графічного інтерфейсу ШМК з ЗУСП. Слід зазначити, що вимоги до графічного інтерфейсу ШМК з ЗУСП визначаються в ОТВ.

19) забезпечувати підключення до систем (сервісів) визначення місцезнаходження рухомої (мобільної) станції, зо застосовуються на телекомунікаційній мережі. Слід зазначити, що порядок підключення ШМК до систем (сервісів) визначення місцезнаходження рухомої (мобільної) станції визначається в ОТВ[2].

МК мають бути забезпечені засобами функціонального контролю, які здатні своєчасно здійснювати контроль стану обладнання МК, фіксувати (локалізувати) пошкодження з точністю до одного елементу заміни та забезпечувати автоматичний збір і передачу на ЗУСП діагностичної інформації (наприклад, по протоколу SNMP)[2; 26], що охоплює собою такі параметри як:

а) стан виконання програмних додатків, процесів (виконується, не виконує ніяких обчислень, не працює);

б) ступінь завантаження системних ресурсів;

в) відображення черги для передачі інформації.

Слід зазначити, що вплив МК на стан з'єднання, в якому здійснюється перехоплення вмісту об'єктів перехоплення, не має бути вищим за:

1) середню затримку з'єднання/роз'єднання, тобто бути не більше ніж 20 мс;

2) рівень зваженого псофометричного шуму в з'єднанні з підключеним МК, тобто бути не більше ніж мінус 63 dBmOp;

в) кількість відмов робочих з'єднань у зв'язку з негативним впливом МК – не більше одного на 1x106 .

В свою чергу, вимогами до ЗУСП є те, що вони мають:

1) приймати від віддалених терміналів суб'єктів перехоплення звернення стосовно здійснення перехоплення відповідно до вимог, встановлених законодавством України;

2) підтверджувати цілісність звернень та авторизацію користувача СПТ;

3) формувати ознаки об'єктів перехоплення згідно з рисами відбору та передавання їх до МК;

4) формувати та автоматично передавати до МК команди управління задля того, аби гарантовати перехоплення вмісту об'єктів перехоплення, а саме - для їх розпізнавання, відгалуження, відбору та передачі;

5) приймати від МК відгалужені об'єкти перехоплення в режимі реального масштабу часу та їх оброблення;

6) проводити буферизацію, тобто тимчасове проміжне зберігання інформації для запобігання її втрати, вмісту об'єктів перехоплення в тому разі, коли пошкоджується канал зв'язку між ЗУСП і віддаленими терміналами суб'єктів перехоплення;

7) передавати до віддалених терміналів суб'єктів перехоплення об'єкти перехоплення після того, як вони пройдуть автоматичну перевірку на відповідність

ознакам відбору відповідно до зверненб на здійснення перехоплення телекомунікацій;

8) отримувати від віддалених терміналів суб'єків перехоплення підтвердження про те, щ обуло отримано вміст об'єктів перехоплення;

9) формувати ознаки наступних об'єктів перехоплення разом із додатковими особливостями ідентифікації (йде мова про особливості відбору або ідентифікаторів), що виділені при обробці вмісту об'єктів перехоплення;

10) передавати до віддалених терміналів суб'єктів перехоплення повідомлення щодо виконання режиму спостереження стоосовно об'єктів перехоплення;

11) приймати від МК та ЗЗТМ дані (до прикладу, по протоколу SNMP), що можуть дозволити локалізувати порушення у роботі СПТ з точністю до одного елементу заміни для відновлення несправних апаратних і програмних засобів СПТ;

12) забезпечувати автоматичний збір (до прикладу, по протоколу SNMP), обробки та відображення діагностичної інформації, що охоплює собою такі параметри:

а) стан робочих станцій та серверів у локальній обчислювальній мережі;

б) стан виконання програмних додатків, процесів (виконується, не виконує ніяких обчислень, не працює);

в) ступінь завантаження системних ресурсів;

г) відображення черги для обробки інформації;

13) приймати від МК повідомлення стосовно підтвердження прийому та, за можливістю, виконання команд управління, а також сигналів аварій;

14) встановлювати та своєчасно змінювати режимми роботи СПТ щоб забезпечити гарантоване перехоплення вмісту об'єктів перехоплення;

15) зберігати копії діючих конфігурацій СПТ та властивостей об'єктів перехоплення задля того, аби відновити роботу СПТ у випадку перезавантаження обладнання телекомунікаційної мережі та/або СПТ;

16) розмежовувати доступ суб'єктів перехоплення до СПТ і забезпечувати незалежне отримання інформації кожним із суб'єктів перехоплення;

17) складати протокол у разі кожного використанням СПТ, коли здійснюється перехоплення телекомунікацій;

18) зберігати протоколи використання СПТ та дані про звернення за дозволами на перехоплення з електронними цифровими підписами протягом усього часу та у формі, яка дозволяє здійснити перевірку їх цілісності посадовими особами при здійсненні контролю за користувачами СПТ відповідно до закону;

19) документування даних щодо передачі та виконання команд управління перехопленням шляхом запису в окремому файлі захищеному від несанкціонованого доступу спеціальним паролем, а також зберігання цього файлу протягом заданого часу;

20) захищати від несанкціонованого доступу до інформації, що має відомості про взаємодію з МК та відгалужений вміст об’єктів перехоплення;

21) приймати від МК буферизоваі об’єкти перехоплення після того, як буде відновлено функціонування каналу зв’язку між шлюзом і ЗУСП та їх оброблення;

22) одержувати від АІС ЦБД ПН дані стосовно того, які номери перенесені та здійснювати їх обробку. Варто зазначити, що ЗУСП також покликані забезпечувати отримання від операторів, провайдерів телекомунікацій службові дані телекомунікацій та збережені ними дані про надані телекомунікаційні послуги, зокрема й службові дані сеансів зв’язку абонентів телекомунікаційних мереж.

Якщо говорити про вимоги, які встановлюються до, то огляду на них ЗЗТМ мають:

1) забезпечувати взаємодію технічних засобів СПТ як на фізичному, так і логічному рівнях інтерфейсу управління та передачі;

2) передавати між технічними засобами СПТ, а також між ЗУСП та віддаленими терміналами суб'єктів перехоплення вміст зафіксованих об’єктів перехоплення та повідомлень, які захищені каналами електрозв’язку, додержуючись при цьому вимог щодо захисту інформації;

3) передавати по захищених каналах електрозв’язку від ЗУСП до МК команди управління щодо виконанням вимог із захисту інформації;

4) забезпечувати пропускну спроможність каналів електрозв’язку, яка потібна, щоб забезпечити гарантовану та своєчасну передачу в реальному часі вмісту зафіксованих об’єктів перехоплення та повідомлень між технічними засобами СПТ, а також між ЗУСП та віддаленими терміналами суб'єктів перехоплення;

5) передавати дані з приводу вмісту об’єктів перехоплення, додержуючись при цьому визначеного рівня якості;

6) резервувувати маршрути передачі даних між технічними засобами СПТ, а також між ЗУСП та віддаленими терміналами суб'єктів перехоплення з можливістю зміни маршрутів при виникненні збоїв у функціонуванні або виходу з ладу елементів ЗЗТМ;

7) підтримувати мережну служби якості обслуговування (йде мова про сукупність технологій, що забезпечують у мережі певний рівень якості обслуговування потоку даних з точки зору пропускної спроможності, тимчасового розкиду затримки відгуку, загальної затримки, а також продуктивність та надійність мережі), що дозволяє уникнути втрати інформації в той момент, коли існує максимальне навантаження в мережі;

8) захищати інформацію, яка передається по захищених каналах електрозв’язку, сертифікованими чи допущеними до експлуатації засобами згідно з грифом обмеження доступу до цієї інформації;

9) забезпечувати конфіденційність, цілісність та відсутність можливості блокування інформації, яка передається. Слід додати, що додаткові вимоги до ЗЗТМ визначаються в ОТВ.

Якщо говорити про вимоги до ПЗ технічних засобів СПТ[2], то слід зазначити, що ПЗ технічних засобів СПТ має охплювати своїм складом операційні системи та додаткове спеціальне ПЗ, що, в свою чергу, повинно:

1) забезпечуватий те, аби технічні засоби СПТ здійснювали свої напрямки діяльності за призначенням;

2) реалізовувати процедури, пов’язані з ініціалізацією та перезавантаженням;

3) забезпечувати автентифікацію суб’єктів перехоплення та розподіляти доступ згідно з наданими їм правами;

4) автоматично відновлювати функції після будь-яких збоїв;

5) забезпечувати антивірусний захист даних. Варто зазначити, що при створенні ПЗ технічних засобів СПТ потрібно застосовувати лише ліцензійні програмні продукти.

Якщо говорити про вимоги до контролю працездатності технічних засобів СПТ[2], то слід зазначити, що під час експлуатації технічних засобів СПТ повинно бути передбачено автоматичний контроль функціонування СПТ без будь-яких втручань у процес роботи її технічних засобів, а також забезпечено передачу сигналів до ЗУСП про будь-які несправності МК і ЗЗТМ.

Під час технічного обслуговування СПТ повинна бути передбачена можливість здійснювати локальний контроль працездатності технічних засобів СПТ до їх складових частин.

Якщо говорити про вимоги до ініціалізації та перезавантаження ПЗ технічних засобів СПТ[2], то слід зазанчити, що при аварійному перезавантаженні ПЗ відповідних технічних засобів телекомунікаційної мережі, МК або ЗЗТМ забезпечує передачу інформації про даний факт в ЗУСП.

Крім того, у випадку аварійної зупинки технічних засобів МК риси об’єктів перехоплення не мають зберігатися у МК. Коли відбувається наступний запуск, вищезгадані дані повинні бути предані в МК із ЗУСП через передбачені команди управління.

Необхідно звернути увагу й на те, що технологічний режим перезавантаження технічних засобів СПТ повинен мати у собі процедури перезавантаження кожної зі складових частин (тобто і МК, і ЗЗТМ, і ЗУСП). Таке перезавантаження технічних засобів СПТ повинно відбуватися за відсутності будь-яких втручань у процес функціонування обладнання телекомунікаційної мережі. Необхідно знати, що під час перезавантаження ПЗ МК функції режиму спостереження не можуть бути підтримані. Крім того, таке перезавантаження ПЗ технічних засобів СПТ відбуватися в автоматичному режимі.

Варто зазначити ще той факт, що законодавець закріпив і вимоги до надійності технічних засобів СПТ. До прикладу, в кліматичних умовах

експлуатування (температура середовища від 15°С до 35°С, відносна вологість повітря від 45% до 80% та атмосферний тиск від 84,0 кПа до 106,7 кПа) СПТ має бути відповідною до таких показників:

По-перше, наробіток до відмови має складати не менше ніж 10 000 годин;

По-друге, час відновлення має складати не більше ніж 30 хвилин за використання одиночного ЗІП;

По-третє, термін служби має складати не менше ніж 8 років.

СПТ повинна забезпечувати цілодобове спостереження за об’єктами перехоплення[2].

РОЗДІЛ 3
ДОСЛІДЖЕННЯ СИСТЕМИ ОПЕРАТИВНО-РОЗШУКОВИХ ЗАХОДІВ ОПЕРАТОРА МОБІЛЬНОГО ЗВ'ЯЗКУ

3.1. Розгляд системи перехоплення телекомунікацій

Слід зазначити, що призначенням системи перехоплення телекомунікацій (СПТ), згадуваною нами раніше, є оперативне одержання інформації щодо об'єкта перехоплення. Тому з огляду на це, СПД повинна[2]:

1) забезпечувати можливість доступу до будь-якого об'єкту перехоплення таким чином, щоб зберегти якість телекомунікаційних послуг, які надаються абонентам спостереження, і не внесячи зміни і перешкоди до роботи телекомунікаційної мережі;

2) забезпечувати відповідність функціональних можливостей СПТ згідно з рівнем розвитку телекомунікаційних технологій, що застосовуються у телекомунікаційних мережах;

3) забезпечувати можливість здійснювати модернізацію СПТ згідно з розвитком телекомунікаційної мережі, що зумовлюється впровадженням нових телекомунікаційних технологій і послуг;

4) забезпечувати можливість ініціювати перехоплення телекомунікацій і незалежне використання отриманої інформації будь-яким суб'єктом перехоплення;

5) забезпечувати технічні можливості, пов'язані з контролем використання СПТ за призначенням до національного законодавства.

Слід зазнчити, що законодавець передбачив вимоги документації СПТ. Зокрема, якщо говорити про вимоги до експлуатаційної документації СПТ, то комплект експлуатаційної документації, призначенням якого є вивчення конструкції технічних засобів і правил їх експлуатування, повинен мати у своєму складі наступне:

1) паспорти чи формуляри на технічні засоби СПТ;

2) настанову стосовно експлуатування технічних засобів СПТ;

3) відомості ЗІП для технічних засобів СПТ;

4) настанову операторів робочих місць технічних засобів СПТ.

Стосовно вимог, які встановлені до програмної документації СПТ, то слід зазначити, що програмна документація в обов'язково повинна включати в себе сукупність програмних документів, які мають дані, потрібні для того, аби експлуатувати та супроводжувати ПЗ. Також програмна документація обладнання вітчизняного виробництва додатково має включати в себе документи з даними для створення ПЗ та з описом програм.

Варто зазначити, що досить важливим питанням при дослідженні СПТ є режими роботи цієї системи. Категорії режимів та пріоритети спостереження можна поділити за об'єктами перехоплення[2].

Наприклад, спостереження за об'єктами перехоплення повинно здійснюватися:

1) відповідно до властивостей кожного об'єкта перехоплення;

2) при перехопленні телекомунікацій одночасно декількома суб'єктами перехоплення;

3) при незалежному протоколюванні процедури спостереження для кожного із суб'єктів перехоплення.

Загалом, СПТ повинна встановлювати та знімати ознаки об'єкта перехоплення та визначати наступні такі категорії режимів спостереження як повна й статистична.

Якщо говорити про першу категорію режиму спостереження, тобто повну, то об'єкти перехоплення від ОВОП до виходу шлюзу мають передаватися із затримкою не більше ніж 1 секунди відносно часу передачі інформації у каналі зв'язку абонента спостереження.

Якщо ж говорити про другу категорію режиму спостереження, тоюто статичну, то тут від ОВОП до виходу шлюзу передаються службові дані сеансів зв'язку із затримкою не більше ніж 1 секунди стосовно часу передачі інформації у каналі зв'язку абонента спостереження.

Досить важливим є той факт, що СПТ повинна забезпечувати можливість зміни категорії режимів спостереження. У випадку такої зміни категорії режиму спостереження під час поточного сеансу зв'язку абонента спостереження перехоплення за зміненим режимом має здійснюватися з його наступного сеансу зв'язку.

Встановлення ознак об'єктів перехоплення відбувається за нормальним або вищим пріоритетами (як опція). Слід зазначити, що, перш за все, під спостереження підпадають службові дані та інформаційні повідомлення, які належать до об'єктів перехоплення з вищим пріоритетом.

Якщо відбувається передача на віддалений термінал суб'єкта перехоплення інформаційних повідомлень сеансів зв'язку абонентів спостереження, то СПТ має забезпечити якість, відповідну нульовому чи першому класу мережного QoS протоколу IP[27].

Будь-яка часова затримка початку передачі до віддаленого терміналу суб'єкта перехоплення інформаційних повідомлень сеансів зв'язку абонентів спостереження по закінченню перехоплення телекомунікацій має бути погоджена суб'єктом перехоплення з підрозділом перехоплення.

Якщо говорити про визначення місцезнаходження термінала (географічного, фізичного, геодезичного або логічного) абонента спостереження, то таке визначення місцезнаходження абонента спостереження здійснюється у телекомунікаційних мережах (підсистемах мереж), де абонент спостереження може здійснювати переміщення або користується послугами «персональний номер» та «перенесення номера».

Залежно від того, який тип телекомунікаційної мережі має місце, визначення місцезнаходження термінала абонента спостереження може бути поділено на[2]:

1) географічне місцезнаходження (ідентифікатори країни, міста або оператора телекомунікацій, зони приймання для мереж рухомого (мобільного) зв'язку тощо);

2) фізичне місцезнаходження (номер абонентської лінії; абонентський номер кінцевого обладнання у мережі фіксованого зв'язку, доступ до якої здійснюється із його використанням);

3) логічне місцезнаходження (IP адреси для мереж передачі даних тощо);

4) геодезичні координати місцезнаходження.

Слід зазначити, що визначення місцезнаходження абонента спостереження здійснюється при повному і при статистичному режимах спостереження, як при здійснені сеансу зв'язку, наданні додаткових послуг, так і незалежно від цього[28].

Визначення географічного, геодезичного, фізичного або логічного місцезнаходження абонента спостереження може мати місце в діяльності ЗУСП у разі:

1) успішної або неуспішної спроби встановлення сеансу зв'язку для вихідного виклику від абонента спостереження та успішної спроби встановлення сеансу зв'язку для вхідного виклику до абонента спостереження;

2) обміну службовими повідомленнями між терміналом та обладнанням телекомунікаційної мережі;

3) надання абоненту спостереження додаткових послуг;

4) передачі спеціального запиту від ЗУСП щодо визначення місцезнаходження абонента спостереження.

Законодавцем встановлено також вимоги щодо здійснення взаємодії технічних засобів СПТ, оскільки лише в їх функціональній взаємодії утворюється сама система СПТ. Тому виникає необхідність розглянути порядок взаємодії технічних засобів СПТ приздійсненні перехоплення телекомунікацій.

Спершу ЗУСП мають сформувати та передати до МК команди управління[2].

В свою чергу, МК формують та передають ЗУСП повідомлення про отримання та виконання команд управління (якщо є така технічна можливість).

МК здійснює розпізнавання та відгалуження об'єктів перехоплення, оформлює їх вміст згідно з форматом інтерфейсу управління і передачі.

Результати перехоплення вмісту сеансів зв'язку абонентів спостереження передаються на ЗУСП, де вони підлягають обробці та реєстрації.

Інформаційні повідомлення сеансів зв'язку, які відгалужені, мають передаватися від ОВОП до ЗУСП опосередковано шлюзом МК або безпосередньо від ОВОП до ЗУСП. У випадку, коли передаються інформаційні повідомлення

сеансів зв’язку, які є відгалуженими, безпосередньо від ОВОП до ЗУСП повинна забезпечуватися кореляція інформаційних повідомлень сеансів зв’язку із технічними ознаками, за якими здійснюється перехоплення телекомунікацій. Порядок взаємодії ЗУСП і ОВОП визначається в ОТВ[2].

Якщо має має місце несанкціоноване втручання у роботу МК та/або ЗЗТМ, яке було виявлено за допомогою засобів функціонального контролю, на ЗУСП повинно бути передано повідомлення про те, що відбулось таке втручання.

Загалом, процес перехоплення здійснюється ще до часу початку та часу, коли закінчується спостереження, котрі визначаються в командах управління перехопленням.

При цьому, технічні засоби ОВОП та шлюз МК мають бути синхронізовані за часом між собою та з обладнанням телекомунікаційної мережі з точністю до 1 секунди[2].

Крім того, у ефективному функціонуванні СПТ відіграють значну роль інтерфейси. Зокрема у СПТ повинні застосовуватися такі інтерфейси як: 1) інтерфейс перехоплення (далі – ІП); 2) інтерфейс управління та передачі (далі – ІУП)[2].

Якщо характеризувати перший інтерфейс, то його призначенням є передача[2]:

а) від шлюзу до ОВОП команд управління (ІП1);

б) від ОВОП до шлюзу сигналів аварії (ІП1);

в) від ОВОП до шлюзу відгалужених об’єктів перехоплення (ІП2 та ІП3).

Якщо ж характеризувати друзий інтерфейс, то його призначенням є передача:

а) у першій частині (ІУП1) від ЗУСП до МК:

- команд управління (таблиця 1);

- відповідей про те, що підтверджений прийом повідомлень про події, які не пов’язуються з дією команд управління перехопленням;

б) у першій частині (ІУП1) від МК до ЗУСП:

- відповідей про підтвердження прийому команд управління перехопленням та про результати виконання команд управління перехопленням;

- повідомлень про події, не пов’язані з дією команд управління перехопленням;

в) у другій частині (ІУП2) від МК до ЗУСП повідомлень про службові дані сеансів зв’язку (СДСЗ), які відгалужені, та про події, що пов’язуються з діями абонентів спостереження;

г) у другій частині (ІУП2) від ЗУСП до МК відповідей про підтвердження прийому повідомлень про події, які пов’язуються з діями абонентів спостереження;

д) у третій частині (ІУП3) від МК до ЗУСП інформаційних повідомлень сеансів зв’язку (ІПСЗ), які відгалужені.

Законодавцем закріплено також вимоги до інтерфейсів СПТ, зокрема вони повинні:

1) здійснювати передачу інформації стосовно визначеного об’єкта перехоплення;

2) передавати інформацію задля незалежного використання одержаної інформації кожним суб’єктом перехоплення;

3) використовувати типові протоколи зв’язку з використанням для цього стандартизованих форматів повідомлень, стандартних методів кодування інформації та захисту інформації від несанкціонованого доступу;

4) забезпечувати цілісність даних, коли звідбувається інформаційний обмін.

Варто зазначити про те, що інтерфейси СПТ при передачі повинні зберігати і якість інформації відгалужених сеансів зв’язку[29].

Загалом же, конфігурація інтерфейсу перехоплення спрямована на:

1) забезпечення взаємодії шлюзу з різновидами ОВОП через сегмент телекомунікаційної мережі загального користування в Україні;

2) здійснювати забезпечення саме незалежної взаємодії шлюзу з одним чи кількома ОВОП;

3) забезпечувати збереження цілісністі вмісту сеансів зв’язку, коли вони передаються від ОВОП до шлюзу;

4) сприяти пристосуванню до модифікацій складових обладнання телекомунікаційної мережі та версій ПЗ,котрі використовуються.

Крім того, дана конфігурація інтерфейсу управління та передачі повинна сприяти незалежній взаємодії ЗУСП з кількома МК.

Варто звернути увагу на той факт, що інтерфейс управління та передачі СПТ в жодному разі не має перебувати в залежності від типу обладнання телекомунікаційної мережі, засобів транспортування інформації та ПЗ, що застосовуються у мережі.

3.2. Перелік команд управління перехопленням, відповідей про результати їх виконання та повідомлень інтерфейсу управління та передачі.

В рамках дослідження необхідно розглянути й перелік команд управління перехопленням, відповідей про результати їх виконання та повідомлень інтерфейсу управління та передачі.

Кожна команда повинна мати у своєму складі загальні параметри такі як: ідентифікатор МК, до якого адресована команда; ідентифікатор ОВОП; порядковий номер команди; пароль для роботи з МК та системний час передачі команди[2].

Першою командою управління перехопленням є «Запуск МК (ініціалізація)». Під час цієї команди виконується включення та ініціалізація МК. За МК має бути закріплений конкретний номер. Початковий пароль команди вводиться розробником МК та повідомляється замовнику.

Наступною командою управління є «Зупинка МК (відключення)». Під час цієї команди мають бути знищені всі дані, котрі пов’язуються з роботою системи перехоплення. Обладнання МК перебуває пасивному стані, вміст таблиці спостереження знищується.

Третьою командою управління є «Зміна пароля», що полягає у здійсненні зміни (встановлення нового) пароля. Команда має містити новий пароль.

Четвертою командою є «Запит на надання даних про перелік ОВОП». Тобто по суті здійснюється запит на надання даних про перелік усіх ОВОП.

Наступною командою управління є «Створення групи ОВОП», під час якої має бути забезпечене формування групи ОВОП. Команда повинна мати також дані про ідентифікатори ОВОП, які входять в групу.

Шостою командою управління перехопленням є «Видалення групи ОВОП» Відміняється дія команди №5 Забезпечується розформування групи ОВОП. Команда повинна включати також дані про ідентифікатори ОВОП, що входять у групу.

Сьомою командою управління перехопленням виступає «Закріплення ОВОП за групою ОВОП», під час якої має бути забезпечено включення ОВОП в групу. Команда повинна включати також дані про ідентифікатор ОВОП.

Восьмою командою є «Вилучення ОВОП із групи ОВОП», яка полягає у вилученні ОВОП із групи. Команда повинна включати також ідентифікатор ОВОП.

Наступною командою є «Запит на надання даних про перелік груп ОВОП», під час якої здійснюється запит на надання даних про перелік груп ОВОП.

Десятою командою управління перехопленням є «Запит на надання даних про перелік ОВОП в окремий групі ОВОП». Тобто здійснюється запит на надання даних про перелік ОВОП, які закріплені за окремою групою ОВОП. Команда повинна включати також ідентифікатор окремої групи ОВОП.

Одинадцятою командою управління є «Постановка ознаки об’єкта перехоплення на спостереження». Тут вносяться дані про ознаку об’єкта перехоплення і таблицю спостереження, встановлюється категорія спостереження та рівень пріоритету. Команда повинна мати також дані про об’єкт перехоплення (ознаку об’єкта перехоплення та її умовний номер, тип об’єкта перехоплення); режим спостереження (суміщений чи роздільний, як опція); категорію спостереження; рівень пріоритету (як опція); час початку та закінчення спостереження; номер групи КЗЛ (як опція).

Наступною командою є «Зняття ознаки об’єкта перехоплення з спостереження», під час якої видаляються дані про ознаку об’єкта перехоплення із таблиці спостереження. Команда повинна мати також умовний номер ознаки об’єкта перехоплення, щодо якого вилучаються зазначені дані.

Тринадцятою командою є «Запит на надання даних про ознаку об’єкта перехоплення», на якій відбувається запит про те, аби надати дані про ознаку об’єкта перехоплення згідно з її умовним номером. Команда має містити також і умовний номер ознаки об’єкта, який перехоплюється.

Чотирнадцятою командою є «Зміна даних про об’єкт перехоплення», на якій піддаються зміні дані про об’єкт, який перехоплюється (ці дані описуються у команді №11). Зазаначенена команда повинна включати також умовний номер ознаки об’єкта, що перехоплюється, дані, на котрі потрібно здійснити зміни: категорію спостереження, рівень пріоритету (як опція) і час, коли закінчується спостереження.

Далі йде така команда як «Переривання видачі відповідей на запит про вміст таблиці спостереження», під час якої припиняється видача даних на всі активні на момент відправлення даної команди запити в МК про те, що містить таблиця спостереження. Слід зазначити, що при виконанні команди ті дані, які містить таблиця спостереження, які були непередані втрачаються.

Шістнадцятою командою є «Очищення таблиці спостереження», під час якої здійснюється відмова від усіх замовлень на спостереження. МК залишає перебувати в активному стані.

Наступною є «Перевірка працездатності каналів зв’язку». Така перевірка працездатності каналів зв’язку між МК та ЗУСП реалізовується через передачу тестового повідомлення. Слід зазаначти, що в тому разі, коли команда протягом 10 хвилин не надходить до МК від ЗУСП по будь-якому з організованих каналів зв’язку, то МК повинна забезпечити перехід на зарезервовані канали зв’язку із ЗУСП.

Наступною командою є «Заборона з’єднання», яка здійснюється на вхідні або/та вихідні сеанси зв’язку абонента спостереження. Команда повинна включати також умовний номер ознаки об’єкта перехоплення та код події (заборона на вхідні та вихідні сеанси зв’язку, на вхідні сеанси зв’язку, на вихідні сеанси зв’язку).

Далі йде команда під назвою «Відміна усіх видів заборон». Під час цієї команди має бути відмінена дія попередньої команди №18, а також має бути

здійснена відміна заборон на вхідні та вихідні сеанси зв'язку абонента спостереження. Команда повинна включати також умовний номер ознаки об'єкта перехоплення.

Двадцятою за порядком здійснення є така команда як «Запит версії програмного забезпечення пункту доступу». Йде мова про запит інформації про версію (редакцію) програмного забезпечення пункту доступу (центрів комутації, шлюзових вузлів та інших). Така команда повинна включати в себе й ідентифікатор пункту доступу.

Двадцять першою є така команда як «Запит часу», тобто запит системного часу, який функціонує в МК.

Наступною командою управління перехопленням є «Закріплення контрольної з'єднувальної лінії за групою (як опція)», під час якої забезпечується включення контрольної з'єднувальної лінії (КЗЛ) в групу. Дана команда має містити також дані про номер та тип групи КЗЛ, номери КЗЛ-А, КЗЛ-В. Максимальна кількість груп визначається максимальною кількістю КЗЛ між МК та ЗУСП. Кількість КЗЛ у групі може бути від однієї до максимальної кількості КЗЛ між МК та ЗУСП.

Двадцять третьою є команда під назвою «Підключення до розмовного тракту», під час якої має бути забезпечене підключення КЗЛ до розмовного тракту з'єднання абонента спостереження, що визначається номером виклику. Ця команда повинна включати також умовний номер ознаки об'єкта перехоплення; номер виклику (число, яке надається кожному виклику, що перехоплюється) та номер групи КЗЛ (як опція).

Наступною командою є «Вивільнення контрольної з'єднувальної лінії (як опція)», під час якої забезпечується примусове вивільнення КЗЛ між МК та ЗУСП. Ця команда повинна включати також умовний номер ознаки об'єкта перехоплення; номери КЗЛ-А та КЗЛ-В.

Далі йде «Вилучення контрольної з'єднувальної лінії з групи (як опція)», під час якої має бути відмінена дія команди №22. Забезпечується вилучення КЗЛ з групи. Дана команда має включати також номер групи КЗЛ, номери КЗЛ-А та КЗЛ-В.

Наступною командою є «Запит на передачу інформації про відповідність між контрольними з'єднувальними лініями та групами (як опція)», під час якого забезпечується видача від МК до ЗУСП інформації про входження КЗЛ до групи. Від ЗУСП до МК передаються дані про номер та тип групи КЗЛ, номери КЗЛ-А та КЗЛ-В.

Наступною командою є «Запит на передачу списку додаткових видів обслуговування», під час якого має бути забезпечена видача повної інформації стосовно додаткових видів обслуговування, що надаються абоненту спостереження. Ця команда повинна включати також умовний номер ознаки об'єкта перехоплення.

Далі відбувається «Запит ідентифікації кінцевого обладнання абонента спостереження», під цією командою розуміється запит щодо ідентифікації кінцевого обладнання абонента спостереження та визначення його місцезнаходження. Зазначена команда повинна включати також умовний номер ознаки об'єкта перехоплення. Слід зазначити, що у разі відсутності абонента в мережі, має бути передане його останнє місцезнаходження.

Далі відбувається «Запит завантаження МК», що полягає у запиті на передачу від МК даних про кількість втрачених МК пакетів та про обсяг вільного місця в пам'яті МК.

Передостанньою командою є «Включення фільтра» (як опція), під час якої зазначається умовний номер ознаки об'єкта перехоплення, а також протокол транспортного рівня та порти вузла МПД, по яким відміняється перехоплення телекомунікацій. Дана команда повинна включати і протоколи транспортного рівня та порти вузла МПД, по яким відміняється перехоплення телекомунікацій.

І останньою командою є «Відключення всіх фільтрів» (як опція), під час якої має бути відмінена дія попередньої команди №30. Ця команда повинна включати і умовний номер ознаки об'єкта перехоплення.

Варто зазначити, що перелічені команди управління перехопленням від №1 до №29 функціонують в СПТ для тих мереж, які застосовують технологію комутації каналів. Команди від №1 до №21 та від №27 до №31 функціонують в СПТ для тих мереж, які застосовують технологію комутації пакетів.

Крім того, інтерфейс управління та передачі повинен забезпечувати передачу від МК до ЗУСП відповідей про підтвердження прийому команд управління перехопленням та про результати виконання команд управління перехопленням.

Всі відповіді повинні включати в себе загальні параметри, тобто ідентифікатор МК; ідентифікатор ОВОП; порядковий номер команди, на яку дається відповідь; порядкове значення відповіді; системний час передачі відповіді.

Таким чином, необхідно розглянути й відповіді про підтвердження прийому команд управління перехопленням та про результати виконання команд управління перехопленням.

3.3. Відповіді про підтвердження прийому команд управління перехопленням та про результати виконання команд управління перехопленням.

Першою відповіддю на команди є «Інформація про прийом або відхилення команди із ЗУСП». Тобто має бути надана відповідь про те, що підтверджено прийом будьякої команди та здійсненна перевіра її параметрів на коректність або про відхилення команди. Така відповідь повинна включати в себе і код прийому до виконання або код помилки в разі відхилення команди. Слід зазначити, що відповідь не передається у разі прийому команди №17 «Перевірка працездатності каналів зв’язку».

Наступною відповіддю є «Інформація про виконання команди із ЗУСП» (якщо наявна технічна можливість). Тобто має бути надана відповідь про підтвердження виконання будь-якої команди або про неможливість її виконання. Відповідь має містити також код виконання команди або код помилки. Сід зазначити, що відповідь не передається у разі прийому команди №17.

Далі відповіддю є «Інформація про перелік ОВОП», що за своєю суттю є відповіддю на команду №4.

Наступною відповіддю є «Інформація про створення групи ОВОП та її виддалення». Вона являє собою відповідь на команди №5 та №6. Зазначена

відповідь повинна включати в себе ідентифікатор групи, що створена або видалена, та ідентифікатори ОВОП, котрі є або були закріплені за групою.

Наступною відповіддю є «Інформація про закріплення ОВОП за групою ОВОП або вилучення ОВОП із групи». Це відповідь на команди №7 та №8, яка повинна включати в себе ідентифікатор групи ОВОП та ідентифікатор ОВОП, що закріплений або вилучений із нею.

Насупною є «Інформація про перелік груп ОВОП», що є відповіддю на команду №9, і повинна включати в себе ідентифікатори груп ОВОП.

Далі йде «Інформація про перелік ОВОП в окремий групі ОВОП», що є відповіддю на команду №10, і повинна включати в себе ідентифікатор окремий групи ОВОП та ідентифікатори ОВОП, що закріплені за нею.

Наступна відповідь – це «Інформація про постановку ознаки об’єкта перехоплення на спостереження», що є відповіддю на команду №11 і повинна включати в себе умовний ознаки об’єкта перехоплення; результат постановки ознаки об’єкта перехоплення на кожне ОВОП та ідентифікатор групи ОВОП.

Наступною є «Інформація про ознаку об’єкта перехоплення», що є відповіддю на команду №13 і повинна включати в себе інформацію про ознаку об’єкта перехоплення, а також встановлені ознаку об’єкта перехоплення та її умовний номер, тип об’єкта перехоплення; режим спостереження (суміщений чи роздільний, як опція); категорію спостереження; рівень пріоритету (як опція); стан (активний або неактивний); місцезнаходження (за наявності даних) абонента спостереження; системний час початку та кінця перехоплення та ідентифікатор окремий групи ОВОП.

Наступна відповідь – це «Інформація про результати заборони з’єднання та відміни усіх видів заборон», що є відповіддю на команди №18 та №19 і повинна включати в себе умовний номер ознаки об’єкта перехоплення; код результату події (заборона встановлена на всі види сеансів зв’язку, заборона встановлена на вхідні сеанси зв’язку, заборона встановлена на вихідні сеанси зв’язку, ознака відсутня в таблиці спостереження, заборона встановлена раніше, відміна усіх видів заборон).

Да, відповіддю є «Інформація про версію програмного забезпечення пункту доступу» що являє собою відповідь на команду №20, яка повинна включати в себе також ідентифікатор пункту доступу; дані про версію (редакцію) програмного забезпечення пункту доступу та інше (як опція).

Наступною є «Інформація про системний час», що є відповіддю на команду №21, і повинна включати в себе поточний системний час обладнання пункту доступу.

Далі йде відповідь під назвою «Інформація про список додаткових видів обслуговування», що є відповіддю на команду №27 і повинна включати в себе умовний номер ознаки об'єкта перехоплення; список кодів додаткових послуг, які надаються абоненту спостереження.

Наступною відповіддю є «Інформація про ідентифікацію кінцевого обладнання абонента спостереження», що являєсобою відповідь на команду №28. Така відповідь повинна включати в себе умовний номер ознаки об'єкта перехоплення; дані щодо ідентифікації кінцевого обладнання, стан активності обладнання.

Далі йде «Інформація про завантаження МК», що є відповіддю на команду №29 і повинна включати в себе дані щодо завантаження МК (кількість активних сеансів зв'язку, кількість доставлених пакетів, кількість втрачених пакетів, об'єм вільної пам'яті).

Переостанньою відповіддю є «Інформація про працездатність каналів зв'язку», що є відповіддю на команду №17 і повинна включати в себе дані щодо працездатності каналів зв'язку.

І останньою є «Інформація про відповідність між контрольними з'єднувальними лініями та групами» (як опція), що є відповіддю команду №26. Така відповідь повинна включати в себе дані про номер та тип групи КЗЛ, номери КЗЛ-А, КЗЛ-В.

Слід зазначити, що відповіді від №1 до №17 діють в СПТ у мережах, які застосовують технологію комутації каналів. Відповіді від №1 до №16 діють в СПТ у

мережах, які застосовують технологію комутації пакетів. Опис вказаних відповідей наведено у додатку В.

3.4. Повідомлення про службові дані сенсів зв'язку (СДСЗ), які відгалужені, та про події, пов'язані з діями абонентів спостереження.

Інтерфейс управління та передачі повинен забезпечити передачу від МК до ЗУСП повідомлень про службові дані сенсів зв'язку (СДСЗ), які відгалужені, та про події, пов'язані з діями абонентів спостереження.

Кожне з таких повідомлень повинно включати в себе загальні параметри: ідентифікатор МК, де відбулася подія; порядкове значення; ідентифікатор ОВОП та час події.

Відповідно виникає необхідність дослідження детальніше повідомлень про службові дані сенсів зв'язку (СДСЗ), які відгалужені, та про події, пов'язані з діями абонентів спостереження.

Першим повідомленням є «Початок сеансу зв'язку (з'єднання)», яке має бути передано на початку сеансу зв'язку абонента спостереження. Повідомлення повинно включати в себе номер виклику (число, яке надається кожному виклику, що перехоплюється); умовний номер ознаки об'єкта перехоплення; дані щодо ідентифікації кінцевого обладнання.

Наступним повідомлення є «Кінець сеансу зв'язку (роз'єднання)», котре має бути передано при завершенні сеансу зв'язку абонента спостереження. Повідомлення має містити також номер виклику; умовний номер ознаки об'єкта перехоплення; код завершення сеансу зв'язку; дані щодо ідентифікації кінцевого обладнання та інше.

Третім повідомлення є «Використання додаткових видів обслуговування», котре передається при замовленні, перевірці, використанні і відміні послуг додаткових видів обслуговування. Таке товідомлення повинна включати в себе умовний номер ознаки об'єкта перехоплення; код послуги, що надається абоненту спостереження; дані щодо ідентифікації кінцевого обладнання. Слід звернути увагу

на той факт, що перелік кодів послуг повинен базуватися на відповідних міжнародних рекомендаціях. Якщо абоненту спостереження надаються послуги, які не вказані в міжнародних рекомендаціях, то їх коди повинні надавати виробники обладнання пунктів доступу.

Наступним повідомленням є «Інформація про результати підключення до розмовного тракту», котре передається при підключенні КЗЛ до розмовного тракту з'єднання абонента спостереження. Таке повідомлення повинно включати в себе номер виклику; умовний номер ознаки об'єкта перехоплення та номер групи КЗЛ (як опція).

Наступне повідомлення – це «Інформація про результати вивільнення контрольної з'єднувальної лінії», що передається при вивільненні КЗЛ між МК та ЗУСП. Таке повідомлення повинно включати в себе також код вивільнення КЗЛ (в результаті виконання команди №17 «Вивільнення КЗЛ», по пріоритету абонента спостереження, в результаті несправності МК).

Наступним повідомленням є «Зміна статусу абонента спостереження», що передається при реєстрації і перереєстрації абонента спостереження в телекомунікаційній мережі. Таке повідомлення повинна включати в себе умовний номер ознаки об'єкта перехоплення; код статусу абонента спостереження; дані щодо ідентифікації кінцевого обладнання.

Далі передається зміст короткого повідомлення SMS, яке повинно включати умовний номер ознаки об'єкта перехоплення; зміст SMS; дані щодо ідентифікації кінцевого обладнання.

Насупним повідомленням є «Зміна місцезнаходження», котре передається при зміні місцезнаходження абонента спостереження. Зазанчене повідомлення повинно включати в себе умовний номер ознаки об'єкта перехоплення; код події, що викликала передачу повідомлення; дані щодо ідентифікації кінцевого обладнання.

Передостаннім повідомленням є «Сеанс зв'язку встановлено», що має бути передано відразу після того, як буде встановлено сеанс зв'язку абонента спостереження. Таке повідомлення повинно включати в себе номер виклику;

умовний номер ознаки об’єкта перехоплення; дані щодо ідентифікації кінцевого обладнання та інше.

Останнім є «Повідомлення мережі». Тобто передається зміст повідомлення мережі, яке має включати в себе умовний номер ознаки об’єкта перехоплення; зміст повідомлення мережі та інше.

Варто зазначити, що повідомлення від №1 до №10 функціонують в СПТ у мережах, які застосовують технологію комутації каналів. Повідомлення №7 та №8 функціонують лише в СПТ у мережах рухомого (мобільного) зв’язку. Повідомлення від №1 до №3, №6, від №8 до №10 фенкціонують в СПТ у мережах, які застосовують технологію комутації пакетів.

В свою чергу, інтерфейс управління та передачі повинен забезпечити передачу від МК до ЗУСП повідомлень про події, які не пов’язуються з дією команд управління перехопленням. Кожне таке повідомлення, повинно включати в себе загальні параметри: ідентифікатор МК, де відбулася подія; ідентифікатор ОВОП; порядкове значення здійснення події; системний час події.

Відповідно виникає необхідність розглянути повідомлення про події, не пов’язані з дією команд управління перехопленням детальніше.

3.5. Повідомлення про події, не пов’язані з дією команд управління перехопленням

Перше повідомлення має назу «Аварія» і передається у разі виходу з робочого стану обладнання або програмного забезпечення, що впливають на роботу СПТ чи обслуговування абонентів спостереження. Таке повідомлення повинно включати в себе ідентифікатор пункту доступу (як опція) та код аварії. Коди аварій надаються виробниками обладнання пунктів доступу. Рекомендований перелік можливих аварійних ситуацій наводиться в додатку В.

Наступним повідолменням є «Перезавантаження програмного забезпечення пункту доступу», котре передається у разі готовності пунктів доступу до функціонування, після первинного їх запуску або усунення аварії, або

перезавантаження програмного забезпечення. Таке повідомлення повинно включати в себе ідентифікатор пункту доступу та код обладнання, в якому відбулася подія.

Далі йде повідомлення під назвою «Статистичні дані протоколу, що реалізує функції ААА». Мова йде про передачу статистичних даних протоколу, що реалізує функції ААА. Таке повідомлення повинно включати в себе ознаки об'єкта перехоплення та статистичні дані.

Наступним повідомленням є «Несанкціонований доступ до МК», що передається у випадку несанкціонованого доступу до МК. Таке повідомлення повинно включати в себе код несанкціонованого доступу (апаратного та/або програмного).

Наступним повідомленням є «Заповнення пам'яті МК» (при наявності технічних можливостей), що має бути переданим у випадку, коли об'єм вільної пам'яті МК, що залишилася, складає не більше ніж 10% від об'єму пам'яті для даних, що призначені для передачі до ЗУСП. Слід зазначити, що таке повідомлення повинно включати в себе з інтервалом в 1 хвилину до тих пір, поки об'єм вільної пам'яті не збільшиться до вказаної межі.

Наступним повідомленням є «Порушення/ відновлення функціонування МК», яке передається у разі виявлення порушень у функціонуванні МК або після відновлення його працездатності Таке повідомлення повинно включати в себе опис причини порушення функціонування МК.

Останнім повідомленням є «Зняття ознаки об'єкта перехоплення в МК із спостереження», що передається у разі закінчення терміну спостереження за ознакою об'єкта перехоплення та зняття її в МК із спостереження. Таке повідомлення повинно включати в себе умовний номер ознаки об'єкта перехоплення.

Варто зазначити, що повідомлення № 3 може мати місце лише у СПТ у мережах, які застосовують технологію комутації пакетів.

Інтерфейс управління та передачі повинен забезпечити передачу відповідей від ЗУСП до МК про підтвердження прийому повідомлень про події, пов'язані з

діями абонентів спостереження, та про події, які не пов’язуються з дією команд управління перехопленням.

Підтвердження прийому повідомлення повинне включати в себе ідентифікатор МК та порядковий номер повідомлення, на яке дається відповідь (квитанція).

Слід зазначити, що в рамках дослідження, потрібно звернути увагу на той факт, що законодавець закріпив й низку вимог до захисту інформації.

Зокрема, програмне забезпечення, обладнання технічних засобів СПТ, команди управління та відповіді на зазначені команди управлнні, дані, що містяться в таблиці спостереження, повідомлення і об’єкти перехоплення повиння обов’язково захищатися від несанкціонованого доступу.

Програмне забезпечення обладнання телекомунікаційної мережі, зокерма що стосується комутаційних систем, центрів комутації, шлюзових вузлів по забезпеченню послуг та інших, повинно забезпечувати те, щоб в системних журналах (каталогах, файлах) була відсутнія інформація щодо змісту команд управління взаємодії МК з ЗУСП і відповідно відповідей на ці команди.

Загалом же, захист інформації стосовно здійснення перехоплення інформації в телекомунікаційних мережах покликані забезпечувати відповідні 33 технічні засоби. Комплекс засобів захисту СПТ повинен бути сумісним з комплексом засобів захисту телекомунікаційної мережі. Заходи щодо захисту інформації об’єктів перехоплення мають забезпечувати її конфіденційність та цілісність.

На ЗУСП повинні передаватися повідомлення про будь-які спроби несанкціонованого втручання у роботу МК, ЗЗТМ та захищених каналів електрозв’язку у випадку технічної можливості виявлення факту втручання.

Крім того, захист інформації, яка передається по захищених каналах електрозв’язку СПТ, повинна забезпечуватися сертифікованими чи допущеними до експлуатації у відповідному порядку апаратнопрограмними засобами.

Всі апаратні та програмні засоби, які використовують технологію віртуалізації функцій мережі (NFV) та в яких циркулює інформація, що пов’язується з перехопленням телекомунікацій, мають бути захищеними від несанкціонованого

доступу. Інформація, котра стосується перехоплення телекомунікацій, в жодному разі не має бути доступною суб'єктам, котрі займаються оркестрацією сервісів, управлінням та адмініструванням рішень базуючись на технологіях NFV.

У звязку з вищезазначеним, було закріплено вимоги до захищених каналів електрозв'язку СПТ, згідно з якими останні мають:

1) здійснювати забезпечення гарантованої передачі об'єктів перехоплення з визначеними показниками надійності, необхідної пропускної спроможності та належним рівнем якості;

2) бути у відповідності з вимогами нормативних документів сфери телекомунікацій;

3) застосовувати стандартні протоколи зв'язку та методи кодування інформації.

Варто зазначити, що надійність захищених каналів ЗЗТМ повинна бути досягнути шляхом резервуванн, побудовою кільцевих і багатозв'язаних з'єднань. При цьому, додаткові вимоги до ЗЗТМ визначаються в ОТВ.

Також важливим питанням в рамках дослідження є службові дані телекомунікацій та збережені службові дані сеансів зв'язку, а також інтерфейс запиту та доставки службових даних.

Слід зазначити, що службові дані телекомунікацій операторів, провайдерів телекомунікацій (далі – СДЕЗ) і ті, які були збережені ними в період строку позовної давності згідно з п.7 ч.1 та ч. 2 ст. 39 Закону України «Про телекомунікації» записи про надані телекомунікаційні послуги, зокрема й службові дані сеансів зв'язку абонентів телекомунікаційних мереж (далі –СДСЗ), мають надаватися в ЗУСП підрозділу перехоплення уповноваженого органу.

Вищезазаначена інформація застосовується в ЗУСП з метою організації перехоплення телекомунікацій та кореляції технічних ознак, до яких відбувається перехоплення телекомунікацій з ознаками, котрі охоплюються службовими даними відгалужених сеансів зв'язку абонентів спостереження.

В ЗУСП відповідно у відповідь на запит повинні бути надані такі службові дані телекомунікацій операторів, провайдерів телекомунікацій[2]:

1) персональні дані абонентів, (фізичних осіб та інформація про юридичних осіб), котрі отримують телекомунікаційні послуги на умовах договору;

2) дані про фізичне та логічне місцезнаходження абонентів (і фізичних, і юридичних осіб);

3) профіль послуг, що надаються абонентам, та їх технічні характеристики;

4) MSISDN, PSTN та MNP номери абонентів;

5) ідентифікатори абонентів (user ID, SIP-URL);

6) ідентифікатори обладнання абонентів (MAC address, IP address);

7) географічні координати та адміністративні адреси розташування базових станцій, коди зони розташування, ідентифікатори стільників, азимути секторів базових станцій, ширину секторів, радіуси зони покриття;

8) дані про відповідність внутрішніх та зовнішніх (публічних) IP – адрес та портів в конкретний проміжок часу, які перетворюються обладнанням з функцією NAT/PAT.

Крім того, в ЗУСП за запитом мають бути доставлені такі збережені службові дані сеансів зв’язку абонентів телекомунікаційних мереж:

1) дані, за допомогою яких можна ідентифікувати сторону сеансу зв’язку, що викликає;

2) дані, за якими можна ідентифікувати сторону сеансу зв’язку, котру викликають;

3) дані (абонентський номер), за якими можуть ідентифікувати третю сторону сеансу зв’язку при наданні послуги з переадресації виклику;

4) дані, необхідні для визначення дати, часу початку, закінчення та тривалості сеансу зв’язку;

5) дані, за якими визначаються спроби встановити з’єднання, зокрема й виклики з нульовою тривалістю та короткі текстові повідомлення з відображенням їх типів;

6) дані, за якими визначаються надана телекомунікаційна послуга, спроби її замовлення, відміни та тип сеансу зв’язку;

7) дані, за допомогою яких можна ідентифікувати обладнання (термінал) абонента;

8) дані (за наявності), що можуть охарактеризувати географічне (фізичне) місце розташування та логічне місцезнаходження термінала абонента;

9) дані, за допомогою яких можна ідентифікувати країну, іноземного оператора телекомунікацій при міжнародному роумінгу абонентів та дані, за якими можна ідентифікувати оператора телекомунікацій, при національному міжмережному роумінгу.

У СПТ для отримання даних, повинен використовуватися інтерфейс запиту та доставки службових даних (далі – ІЗД), призначенням якого є передача[2]:

1) від ЗУСП до технічного засобу оператора, провайдера телекомунікацій запитів про службові дані телекомунікацій та збережені службові дані сеансів зв'язку абонентів телекомунікаційних мереж;

2) від ЗУСП до технічного засобу оператора, провайдера телекомунікацій відповідей про те, що підтверджено прийом службових даних;

3) від технічного засобу оператора, провайдера телекомунікацій до ЗУСП відповідей про те, що підтверджено прийом запитів;

4) від технічного засобу оператора, провайдера телекомунікацій до ЗУСП відповідей на запити;

5) від технічного засобу оператора, провайдера телекомунікацій до ЗУСП повідомлень про порушення/відновлення функціонування технічного засобу оператора, провайдера телекомунікацій та про несанкціонований доступ до технічного засобу оператора, провайдера телекомунікацій.

Крім того, повинен ІЗД забезпечувати:

1) передання службових даних з тією метою, аби незалежно використати одержану інформацію кожним суб'єктом перехоплення;

2) використання типових протоколів зв'язку завдяки стандартизованим форматам повідомлень, стандартним методам кодування інформації і також захисту інформації від несанкціонованого доступу;

3) цілісність даних процесі обміну інформації.

Крім того, кожний запит повинен включати в себе загальні параметри, зокрема: код запиту, котрим визначається формат та саме призначення запиту; ідентифікатор пріоритету запиту, він може бути вищим або нормальним; критерій запиту, тобто мається на увазі одиночний параметр чи їх сукупність, що виступають підставою, за якою можна провести оцінку збережених службових даних, щоб в подальшому здійснити їх відбір; ідентифікатор ЗУСП, до якого має бути передана відповідь на запит; порядкова роль запиту; пароль, призначений для роботи з технічним засобом оператора, провайдера телекомунікацій, системний час та дата, коли був переданий даний запит [30].

Застосовуються одиночний та множинний запити. Одиночний запит грунтується на одиночному критерії запиту, а множинний запит – на сукупності одиночних критеріїв запиту.

Варто зазначити, що в якості критеріїв запиту повинні бути застосованітакі параметри як[2]:

1) MSISDN, PSTN номери абонента;

2) перенесений номер абонента;

3) ідентифікатор споживача (абонента) user ID, MAC – address;

4) ідентифікатор SIP-URL;

5) IP address, IP порт;

6) дані, за якими можна ідентифікувати фізичну або юридичну особу, котрі одержують телекомунікаційні послуги відповідно до умов договору;

7) дані, що ідентифікують електронне листування;

8) час, протягом якого потрібно відібрати службові дані;

9) інформація про місцеперебування;

10) ідентифікатор видів послуг.

Критерії запиту мають бути однозначно ідентифіковані технічним засобом оператора, провайдера телекомунікацій задля того, аби чітко і точно визначити перелік службових даних, які повинні бути доставлені в ЗУСП.

Запити в технічному засобі оператора, провайдера телекомунікацій обробляються у поряду надходження [2; 30]. Кожна відповідь на такий запит

повинна включати в себе загальні параметри, а саме: свій код, яким встановлюється взаємозв’язок відповіді з конкретним запитом (з визначеним порядковим значенням); ідентифікатор технічного засобу оператора, провайдера телекомунікацій, від якого передана відповідь; порядкове значення відповіді; код причини відмови на надання даних (у разі її наявності); системний час, дату передачі відповіді, та службові дані, що були запитані (у разі наявності причини відмови на надання даних, дані не надаються).

Зміст самих запитів службових даних та відповідей на запит не мають зберігатися в технічному засобі оператора, провайдера телекомунікацій.

Технічний засіб оператора, провайдера телекомунікацій повинен забезпечувати запобігання виявлення фактів здійснення запитів службових даних та передачі відповідей до ЗУСП персоналом оператора, провайдера телекомунікацій.

Будь-яка відповідь про підтвердження прийому службових даних або запитів повинна включати в себе загальні параметри, зокрема: свій код, який встановлює взаємозв’язок відповіді з конкретними службовими даними або запитом (з визначеним порядковим значенням); ідентифікатор технічного засобу оператора, провайдера телекомунікацій; порядкове значення відповіді; системний час та дату передачі відповіді.

Будь-яке повідомлення чи те, яке містить інформацію про порушення, чи те, яке має інформацію про відновлення роботи технічного засобу оператора, провайдера телекомунікацій, про несанкціонований доступ до технічного засобу оператора, провайдера телекомунікацій повинен включати в себе загальні параметри,зокрема: власний код; ідентифікатор технічного засобу оператора, провайдера телекомунікацій, котрий власне передавав повідомлення; порядкову роль повідомлення; код, який описує чому відбулося порушення чи функціонування, чи відновлення функціонування технічного засобу оператора, провайдера телекомунікацій; код несанкціонованого доступу до нього , зокрема, апаратного та/або програмного; системний час та дату, коли було передано дане повідомлення [2].

ВИСНОВКИ

Отже, в дипломній роботі здійснено детальний аналіз технічних засобів, а також вимог до таких технічних засобів, які потрібні задля проведення уповноваженими органами оперативно-розшукових заходів. Встановлено, що згідно з ч. 4 ст. 39 Закону України від 18 листопада 2003 року «Про телекомунікації» саме на операторів та провайдерів телекомунікацій покладається обов'язок за власний рахунок установлювати на своїх телекомунікаційних мережах технічні засоби, які потрібні задля проведення уповноваженими органами ОРЗ, та обов'язок із забезпечування функціонування зазначених технічних засобів, а також у межах своїх повноважень сприяти проведенню оперативно-розшукових заходів та недопущенню розголошення організаційних і тактичних прийомів їх проведення. Крім того, на операторів телекомунікацій покладено обов'язок із забезпечення захисту даних технічних засобів від несанкціонованого доступу.

Зокрема, визначено теоретичні, зокрема правові, засади системи оперативно-розшукових заходів, а саме: з'ясувано поняття оперативно-розшукових заходів;з'ясувати основні засади застосування оперативно-розшукових заходів. Попри відсутність законодавчо визначеного поняття оперативно-розшукових заходів, встановлено, що найбільш розповсюдженим його варіантом серед науковців є наступний: «оперативно-розшукові заходи виступають комплексом оперативно-технічних, обґрунтованих з наукової точки зору, закріплених на законодавчому рівні, гласних і негласних, з точки зору тактики схожих методів, прийомів і способів отримання, перевірки і реалізації оперативної інформації, які покликані вирішувати задачі оперативнорозшукової діяльності».

Крім того, визначено, що основними спеціальними засадами, які властиві винятково здійсненю ОРЗ єконспірація; поєднання гласних та негласних методів, заходів та засобів; добровільніть конфіденційного співробітництва; забезпечення безпеки гласних і негласних позаштатних працівників.

Досліджено функціонування системи оперативно-розшукових заходів оператора мобільного зв’язку, зокрема: з’ясувано класифікації оперативно-розшукових заходів, які існують в науковому полі; досліджено технічні засоби для здійснення оперативно-розшукових заходів. Зокрема, з’ясовано, що видано Наказ Служби безпеки України та Адміністрації Державної служби спеціального зв’язку та захисту інформації України № 1519/533 від 04 вересня 2018 року, яким було затверджено перелік технічних засобів задля проведення уповноваженими органами оперативно-розшукових заходів у телекомунікаційних мережах, призначениз для загального користування. Зазначений документ визначає загальні технічні вимоги (ЗТВ) до технічних засобів з метою проведення спеціальними органами, упровноваженими на це законом оперативно-розшукових заходів у телекомунікаційних мережах загального користування України. Слід зазначити, що до таких технічних засобів належать мережний комплект (МК), який призначений перехоплвати телекомунікації; засоби управління системою перехоплення телекомунікацій (сервери, станції, термінали та інші - ЗУСП); засоби захищеної транспортної мережі (ЗЗТМ); програмне забезпечення (ПЗ) технічних засобів; експлуатаційна та програмна документація технічних засобів;

Встановлено, що систему перехоплення телекомунікаці (СПД) утворює сукупність технічних засобів у їх функціональній взаємодії. Власне, призначенням такої системи є оперативне одержання інформації щодо об’єкта перехоплення.

В дипломній роботі здійснено детальне дослідження та розбір вимог, які висуваються до технічних засобів, зокрема слід зазанчити, що необхідність розроблення аких вимог обумовлена розвитком систем телекомунікацій, які використовують нові сучасні телекомунікаційні технології. Попри це, в науковому полі увага дослідженню даному питанню майже не приділяється, тому на сьогодні необхідно розширити наукову базу з даної тематики.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про оперативно-розшукову діяльність: Закон України від 18 лютого 1992 р. № 2135-XII. URL: https://zakon.rada.gov.ua/laws/show/2135-12#Tex
2. Технічні засоби для здійснення уповноваженими органами оперативно-розшукових заходів та негласних слідчих (розшукових) дій у телекомунікаційних мережах загального користування України: Наказ від 04 вересня 2018 року № 1519/533/ /Служба безпеки України, Адміністрація Державної служби спеціального зв'язку та захисту інформації України. URL: https://ssu.gov.ua/uploads/documents/2020/05/27/p-140-70438355.pdf
3. Грибовський О.В. Оперативно-розшукові заходи та негласні слідчі (розшукові) дії під час виявлення й фіксації одержання неправомірної вигоди. Юридичний часопис Національної академії внутрішніх справ. 2015. № 1. С. 180-190
4. Про контррозвідувальну діяльність [Електронний ресурс] : Закон України від 26 груд. 2002 р. – Режим доступу : http://zakon1.rada.gov.ua/laws/show/2341-14
5. Оперативно-розшукова діяльність : [навч. посіб.] / [Є. М. Моісеєв, О. М. Джужа] ; ред. Д. Й. Никифорчук [та ін.]. – К. : Прав. єдність, 2009. – 309 с, с. 107
6. Про розвідувальні органи України [Електронний ресурс] : Закон України від 22 берез. 2001 р. – Режим доступу : http://zakon1.rada.gov.ua/laws/show/2341-14
7. Основи оперативно-розшукової діяльності: навчальний посібник / О. Ю. Анциферов, О. М. Чистолінов, С. В. Єськов та ін. / за ред. С. М. Гусарова; Харків. нац. ун-т внутр. справ. – Харків: Золота міля, 2015. – 312 с
8. .Оперативно-розшукова діяльність органів внутрішніх справ. Загальна частина : підручник / С. В. Албул, К .І. Бєляков, А. І. Берендєєва та ін.; за ред. М. П. Водька, О. Ф. Долженкова, С. П. Черних. Київ: Відділ редакційно-видавничої діяльності МВС України, 2012. 884 с.

9. Оперативно-розшукова діяльність: посібник для вищих навчальних закладів за заг. редакцією генерала поліції першого рангу, кандидата юридичних наук, Заслуженого юриста України С. М. Князєва; академіка Академії Наук Вищої школи України, доктора юридичних наук, професора А. М. Кислого. Київ: «Видавництво Людмила», 2019. 240 с.
10. Оперативно-розыскная деятельность: учебник / под ред. К.К. Горяинова, В.С. Овчинского, А.Ю. Шумилова. – М., 2001. – С. 305
11. Шумилов А.Ю. Юридические основы оперативно-розыскных мероприятий: учеб. пособие / А.Ю. Шумилов. – М., 1999. – С. 9–10
12. Шумилов А.Ю. Краткая сыскная энциклопедия: Деятельность оперативно-розыскная, контрразведывательная, частная сыскная (детективная) / А.Ю. Шумилов. – М., 2000. – С. 79–81
13. Осипкин В.Н. Прокурорский надзор за оперативно-розыскной деятельностью: учеб. пособие / В.Н. Осипкин. – СПб., 2001. – С. 11–12
14. Собрание законодательства Российской Федерации. – 2001. – № 13. – Ст. 1140
15. Захарцев С.И. Оперативно-розыскные мероприятия. Общие положения / С.И. Захарцев. – СПб., 2004. – 286 с
16. Погорецький М.А. Оперативно-розшукові заходи: поняття і види / М.А. Погорецький // Державна безпека України: наук.-практ. зб. НАН України і СБ України. – К., 2005. – № 1(3). – С. 62–67
17. Аверьянова Т.В. Криминалистика: учебник для вузов / Т.В. Аверьянова, Р.С. Белкин, Ю.Г. Корухов, Е.Р. Россинская; под ред. Р.С. Белкина. – М.: Изд. группа НОРМА-ИНФРА-М, 1999. – 900 с. – С. 482–490
18. Погорецький М.А. Проблеми правового регулювання превентивних заходів в оперативно-розшуковій діяльності / М.А. Погорецький // Методологічні проблеми теорії та практики ОРД в сучасних умовах: Вісник Луганської академії МВС ім. 10-ти річчя незалежності України. – Ч. 1. – 2004. – Спец. вип. № 2. – С. 35–44.

19. Сервецький І.В. Поняття спеціальної оперативно-розшукової операції / І.В. Сервецький, В.В. Гелетей // Наук. вісн. Нац. акад. внутр. справ України. – 2005. – Ч. 2. – № 1. – С. 73–82
20. Албул С. В. Основи оперативно-розшукової діяльності / С. В. Албул, С. В. Андрусенко, Р. В. Мукоіда та ін.; за заг. ред. С.В. Албула. Одеса : ОДУВС, 2016. 270 с.
21. Бандурка О. М. Оперативно-розшукова компаративістика: монографія / О. М. Бандурка, М. М. Перепелиця, О. В. Манжай, В. В. Шендрик. Харків: Золота міля, 2013. 352 с.
22. Водько Н П. Формирование политики противодействия уголовным правонарушениям в Украине (оперативно-розыскной аспект): монография / Н. П. Водько. Одесса: Феникс, 2015. 572 с.
23. Про телекомунікації: Закон України від 18 листопада 2003 року № 1280-IV [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/1280-15
24. Використання можливостей операторів стільникового (мобільного) зв'язку для розкриття та розслідування злочинів [Текст]: метод. реком. / [Чернявський С.С., Татаров О.Ю., Алексєєва-Процюк Д.О. та ін.]. – К.: Нац. акад. внутр. справ, 2012. – 58 с.
25. Сербінов О.С. Окремі види інформації про абонента, яка знаходиться у користуванні операторів мобільного зв'язку та може бути отримана у ході проведення оперативнорозшукових заходів або слідчих дій / О.С. Сербінов // Адвокат. – 2009. – № 1. – С. 36–39.
26. Про законне перехоплення телекомунікацій: Резолюція Ради Європи від 17 січня 1995 року [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/ show/994_235
27. Про затвердження Правил надання та отримання телекомунікаційних послуг: постанова Кабінету Міністрів України від 11 квітня 2012 року № 295 [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/295-2012-%D0%BF

28. Тагієв С. Тимчасовий доступ до інформації, яка знаходиться в операторів і провайдерів телекомунікацій, у кримінальному провадженні / С. Тагієв // Слово Національної школи суддів. – 2013. – № 2 (3). – С. 13–24.
29. Хрущ О. Порядок доступу до інформації, яка знаходиться в операторів і провайдерів телекомунікаційних послуг, у кримінальному провадженні / О. Хрущ // Науковий часопис Національної академії прокуратури України. – 2017. – № 1(13). – С. 209–216 [Електронний ресурс]. – Режим доступу: http://www.chasopysnapu.gp.gov.ua/chasopys/ua/pdf/1-2017/hrusch. pdf
30. Про оперативні запити правоохоронних органів стосовно громадських телекомунікаційних мереж та послуг: Резолюція Ради Європи від 20 червня 2001 року [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/994_234