УДК 005:343.23:621.395.721.5 **Т.М. Мужанова, Ю.М. Якименко**

КЛАСИФІКАЦІЇ ЗЛОЧИНІВ ІЗ ВИКОРИСТАННЯМ МОБІЛЬНОГО ТЕЛЕФОНУ

Проаналізовано передумови розширення масштабів злочинності у сфері мобільного зв'язку, розглянуто класифікації правопорушень із використанням мобільного телефону та охарактеризовано їх основні види. Представлено власну класифікацію, відповідно до якої правопорушення з використанням мобільного телефону поділено на телефонне хуліганство, телефонне шахрайство та інші злочини, в яких пристрій мобільного зв'язку є знаряддям неправомірних дій.

Ключові слова: правопорушення з використанням мобільного телефону, телефонне хуліганство, телефонний тероризм, телефонне шахрайство.

Постановка проблеми. Інтенсивний розвиток телекомунікаційних систем, засобів мобільного зв'язку та інших досягнень науки і техніки, їх проникнення в усі сфери життєдіяльності суспільства стали передумовою для швидкого зростання економіки, вирішення багатьох соціальних проблем і сприяли значному спрощенню життя людини.

Завдяки мобільним (стільниковим) телефонам зросли обсяги і швидкість комунікації, розширилися можливості спілкування незалежно від місцезнаходження співрозмовників. Мобільні телефони міцно увійшли в повсякденне життя суспільства, міжособистісні, професійні, соціально-політичні, господарські та інші відносини. Однак поряд із величезними перевагами їх використання несе і значну кількість загроз у сфері інформаційної безпеки. Все частіше мобільні телефони стають знаряддям вчинення правопорушень, а також об'єктом злочинних посягань.

Аналіз останніх досліджень і публікацій. Дослідження ґрунтується на вивченні публікацій вітчизняних та закордонних дослідників, присвячених проблемам злочинності у сфері телефонного зв'язку. Варто відзначити, що більшість публікацій розглядає питання правопорушень з використанням мобільного телефону в юридичному аспекті [3,4,9] або в контексті діяльності правоохоронних органів [1,2,5,8]. Значну увагу в роботах приділено висвітленню методики здійснення правопорушень, однак, не виявлено узагальненого підходу до класифікації злочинів із застосуванням мобільного телефону.

Метою дослідження є аналіз передумов розширення масштабів злочинності у сфері мобільного зв'язку, узагальнена характеристика основних видів правопорушень із використанням мобільного телефону та представлення власного підходу до їх класифікації, що визначає наукову новизну роботи.

Викладення основного матеріалу. Як показав огляд законодавства і джерел науково-практичного характеру на сьогодні не існує загальновизнаного визначення поняття «злочини у сфері мобільного зв'язку». Загалом злочини такого виду умовно можна віднести до визначеної в Кримінальному Кодексі України категорії злочинів у сфері використання ЕОМ (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Слід відзначити, що поява злочинів, пов'язаних з використанням сучасних технологій і засобів мобільного зв'язку, та розширення сфер злочинної діяльності безпосередньо обумовлені загальнодоступністю мобільних телефонів, недосконалістю законодавства в сфері регулювання надання послуг зв'язку, відсутністю профілактичної роботи та низькою правовою грамотністю населення з потенційно проблемних питань отримання послуг зв'язку [9].

Загалом, на думку фахівців, сьогоднішня ситуація, пов'язана із злочинністю у сфері телекомунікаційних систем, характеризується:

– великою латентністю, що спричиняє збільшення кількості скоєних злочинів;

– постійним ускладненням та модифікацією, появою нових видів правопорушень із використанням засобів мобільного зв'язку;

– відсутністю розроблених методів запобігання, виявлення, припинення і розкриття злочинів;

– міждержавним, міжрегіональним характером злочинів з використанням мобільного телефону;

– недостатньою налагодженістю взаємодії між телекомунікаційними компаніями і правоохоронними органами [4].

У сучасній науковій та професійній літературі представлено багато підходів до класифікації правопорушень з використанням мобільного телефону, однак доцільним є їх узагальнення і вироблення єдиної схеми (див.рис.1).

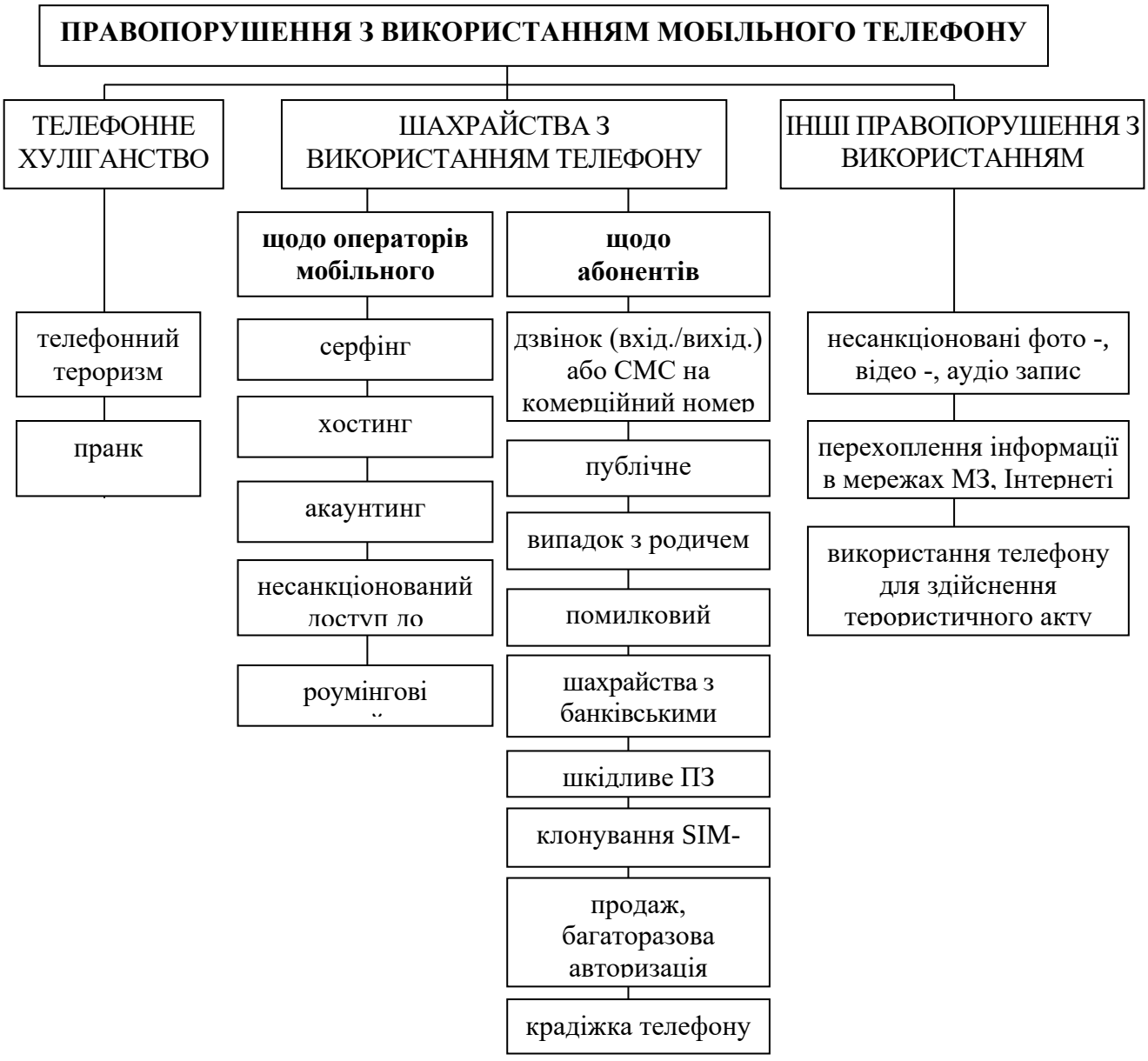

Рис.1. Види правопорушень із використанням мобільного телефону.

На нашу думку, усі правопорушення, в яких мобільний телефон виступає у якості знаряддя злочину, пропонується розділити на три групи: телефонне хуліганство, телефонні шахрайства та інші види злочинів із застосуванням мобільного телефону. Розглянемо їх детальніше.

Телефонне хуліганство. Телефонне хуліганство і телефонні розіграші, що включають як погрози злодіянь, злі образи по телефону, так і жарти та хитрощі різного характеру, називають пранком (від англ. prank - витівка, пустощі; жарт). Пранкери здійснюють телефонні дзвінки (зазвичай анонімні) своїм жертвам і шляхом провокацій і кепкування,

часто із використанням великої кількості нецензурної лайки, змушують жертву до яскравої реакції: гніву або істерики [7].

Сьогодні багато публічних осіб страждають від замовних атак телефонних хуліганів: внаслідок безперервних дзвінків на мобільний телефон з незареєстрованих номерів зловмисники фактично блокують жертві мобільний зв'язок, змушуючи її постійно відволікатися і роблячи неможливим налагодити з нею контакт по телефону.

За словами фахівців мобільного зв'язку, фізично телефонне хуліганство організовується з використанням спеціальних програмно-апаратних комплексів, які генерують дзвінки. При цьому існує можливість підставити будь-який телефонний номер як вхідний, тобто жертва телефонного хулігана буде бачити вхідний дзвінок, наприклад, від абонента вітчизняного оператора, а насправді дзвінок здійснюватиметься з «модуля», встановленого за кордоном. Боротися з цим явищем дуже важко, оскільки в мобільних операторів немає способу автоматичного блокування подібних атак.

До телефонного хуліганства відносять і телефонний тероризм. Під телефонним тероризмом розуміють завідомо неправдиве повідомлення по телефону про нещасні випадки або небезпечні ситуації (терористичний акт, вибуховий пристрій або злочин), які насправді не сталися, в спеціальні служби (поліцію, пожежну та газові служб, швидку допомогу).

Телефонний терорист переслідує різні цілі: відволікання спецслужб від реальних завдань, порушення роботи підприємств або організацій, провокування паніки в громадських місцях, а в окремих випадках порушник діє просто з хуліганських міркувань. Ще один фактор небезпеки - так званий ефект «Казки про брехливого пастушка», тобто спецслужби можуть не відреагувати на наступний виклик, який буде справжнім [7].

За статистикою, до скоєння таких злочинів здебільшого вдаються школярі або психічно не врівноважені особи. Майже 100% анонімних «терористів» встановлює СБУ у взаємодії з правоохоронними органами у досить стислі терміни.

Телефонні шахрайства. Окрему, очевидно найбільшу групу правопорушень з використанням телефону становить телефонне шахрайство. За даними фахівців, сьогодні доходи від мобільного шахрайства в світі оцінюються в $25 млрд. Європейські оператори щорічно передбачають у своїх бюджетах 5-10% на фінансові втрати від зловмисників. А згідно з дослідженнями російського оператора "Білайн" тільки за один рік жертвами обману ставали 10 мільйонів громадян, хоча фактично це число значно більше [2].

Об'єктивна сторона шахрайства полягає у заволодінні майном або придбанні права на майно шляхом обману чи зловживання довірою. Суб'єктивна сторона шахрайства характеризується прямим умислом і корисливим мотивом.

Обман як спосіб шахрайського заволодіння чужим майном чи придбання права на таке майно полягає у повідомленні жертві неправдивих відомостей або приховування певних відомостей, повідомлення яких мало б суттєве значення для поведінки потерпілого, з метою введення його в оману. Зловживання довірою полягає у недобросовісному використанні довіри з боку жертви: для заволодіння чужим майном чи правом на нього злочинець використовує особливі довірчі стосунки, які склалися між ним та власником майна. У результаті шахрайських дій потерпілий добровільно передає майно або право на майно правопорушнику [3].

Технологічна складова дає злочинцю можливість донести необхідну інформацію до потенційної жертви, забезпечити свою анонімність, безпеку, отримати від потерпілого гроші, не вступаючи з ним у безпосередній контакт.

Відповідно до запропонованої класифікації мобільні шахрайства можна об'єднати у дві основні групи відповідно до об'єкта посягань: злочини проти компаній мобільного зв'язку і злочини, що посягають на інтереси їхніх абонентів.

Шахрайства проти операторів мобільного зв'язку. Фактично основною метою злочинів проти операторів мобільного зв'язку є неправомірне використання ресурсів та користування послугами на значні суми з ухиленням від подальшої оплати. Часто такі

правопорушення називають фродом (від англ. fraud - «шахрайство»). Самі оператори мобільного зв’язку умовно поділяють види шахрайства на п'ять груп:

– серфінг - входження в мережу під чужим ім'ям: підроблені SIM-картки, паролі тощо;
– хостинг - використання технічних засобів для впливу на обладнання оператора;
– акаунтинг - втручання у систему рахунків і тарифів з метою їх зменшення;
– несанкціонований доступ до інформації: отримання паролів, кодів доступу тощо [2].

Серед найпоширеніших методів шахрайства проти операторів мобільного зв’язку фахівці зазначають переадресацію дзвінків, шахрайство з абонементом, перепрограмування, клонування. До цієї ж категорії відносять роумінгове шахрайство, яке базується на використанні затримки білінгової операції при роумінгових розрахунках між вітчизняним та іноземним стільниковими операторами.

У більшості випадків перелічені правопорушення мають на меті «торгівлю телефонними дзвінками», тобто надання третім особам можливості анонімно телефонувати за кордон за низьким тарифом. Компанії стільникового зв'язку змушені відшкодовувати компаніям міжрегіонального зв'язку вартість таких дзвінків.

Також до шахрайств проти операторів мобільного зв’язку відносять шахрайства з використанням комерційних номерів, при дзвінку або відправленні на які СМС-повідомлення з телефонного рахунку абонента знімається плата за товар або послугу, що перераховується на банківський рахунок власника номера. Привід може бути будь-яким: участь у неіснуючому телефонному соцопитуванні, повідомлення про вигаданий виграш у лотереї тощо.

Шахрайства проти абонентів мобільного зв’язку. Серед «мобільних» шахрайств найбільшу групу становлять шахрайства з метою виманювання грошей у пересічних громадян - абонентів мобільного зв’язку. Розглянемо найбільш поширені шахрайські схеми з використанням мобільного телефону.

Відома шахрайська схема, яка з'явилася в Японії – обірваний дзвінок або Wangiri - дзвінок на номер абонента з використанням комерційного номеру і миттєве скидання виклику. Вартість дзвінка у відповідь може сягати кількох десятків гривень за хвилину. Подібна схема діє, коли нічого не підозрюючий абонент відповідає на дзвінок з невідомого номера і з його рахунку списуються кошти.

Популярними видами злочинів з метою виманювання коштів є шахрайства шляхом публічного оголошення, зокрема повідомлення про різні псевдоакції мобільного оператора або Інтернет-провайдера, неіснуючий виграш у лотерею, прохання зробити благодійний внесок. Результатом таких зусиль має стати дзвінок або СМС-повідомлення на номер підвищеної тарифікації.

Часто шахраї телефонують жертві від імені служби підтримки оператора мобільного зв’язку:

– з повідомленням про накладення штрафних санкцій через не своєчасну оплату, зміну тарифу або використання послуг роумінгу без попередження оператора;

– з пропозицією підключити нову ексклюзивну послугу (в тому числі неіснуючі сервіси і програми, такі як "унікальний генератор кодів платіжних карток мобільного оператора", "читання чужих СМС тощо);

– із проханням перереєструватися, щоб уникнути відключення зв'язку внаслідок технічного збою, або для поліпшення якості зв'язку.

Подальші рекомендації злочинців включають здійснення дзвінка або відправлення СМС на короткий номер з підвищеною тарифікацією, також можливим є надання зловмиснику коду картки попередньої оплати.

Особи, які шукають роботу, можуть стати жертвами фіктивних кадрових агентств, що заманюють пропозиціями про стабільну роботу й високу заробітну плату, або псевдо-компаній, які нібито зацікавилися кандидатурою претендента. Жертві для одержання детальної інформації або проходження співбесіди необхідно відправити СМС або

зателефонувати на номер підвищеної тарифікації. Подібна схема тільки з використанням СМС діє у випадках СМС-знайомств та переписки, отримання віртуальної листівки.

Одним із способів телефонного шахрайства з метою поповнення рахунку правопорушників є схема «помилковий переказ коштів», коли абоненту надсилають фіктивне СМС-повідомлення про поповнення його рахунку, а потім у телефонній розмові просять повернути фактично не надіслані кошти назад тим же «мобільним переказом». Добровільне поповнення чужого рахунку може бути винагородою за загублену річ, яку шахраї обіцяють повернути.

Популярним способом цього виду шахрайств є дзвінок або СМС з повідомленням про проблеми з родичем і проханням перевести кошти на номер іншої особи або в інший спосіб передати їй гроші з метою залагодження проблеми.

Такі «мобільні» махінації проводяться, як правило, організованими групами, що спеціалізуються на вчиненні подібного роду злочинів, або особами, що утримуються в місцях позбавлення волі [1].

Шахрайства з картами передоплати включають продаж бракованих карт передоплати; багаторазову авторизацію карт передоплати [5].

Велику групу мобільних правопорушень становлять шахрайства з банківськими картками, матеріальні втрати внаслідок яких є найбільш суттєвими, а масштаби і способи їх реалізації розширюються з кожним днем.

Найпростіший спосіб заволодіти даними про картку користувача – це просто попросити жертву поділитися цими відомостями з метою перевірки безпеки або уточнення відомостей. Додатковим чинником, що полегшує завдання шахраїв, є введення жертви в стресовий стан, підштовхуючи до швидких і необдуманих дій.

Одне з примітивних шахрайств полягає у відправці абоненту СМС про заблокування його банківської карти (або необхідність термінового погашення кредиту) із зазначенням номера телефону, на який потрібно зателефонувати для уточнення подробиць.

Аналогічне шахрайство здійснюється шляхом здійснення телефонного дзвінка жертві і повідомлення, що з її картки зараз відбувається списання грошей, тому потрібно терміново перевірити інформацію щодо номера, терміну дії та коду верифікації користувача картки.

Складніша шахрайська схема, яка базується на зловживанні довірою, передбачає фіктивну перевірку картки через банкомат: Наприклад, жертва отримує СМС-повідомлення про переведення коштів зі своєї картки, якого вона, звичайно, не здійснює, але далі телефонує за вказаним номером (нібито «служби фінансового контролю»), де їй пояснюють, що сталася помилка, а для уникнення хибного переказу грошей необхідно звернутися до банкомату і виконати декілька дій з картою відповідно до вказівок «співробітника банку». Внаслідок таких дій жертва добровільно переводить гроші зі свого особистого банківського рахунку на чужий.

Сьогодні досить поширеним є шахрайства з використанням шкідливих комп'ютерних програм (вірусів), які блокують або в будь-який інший спосіб перешкоджають роботі програмного забезпечення телефону. Шкідливе програмне забезпечення може завантажуватися внаслідок переходу за посиланнями, вказаними в СМС або повідомленнях мобільної пошти, які прийшли з невідомих номерів або адрес. Для відновлення роботи пристрою необхідно поповнити баланс конкретного телефонного номера або надіслати на нього платне СМС-повідомлення, що на практиці не гарантує вирішення проблеми [6].

Іншим інструментом шахраїв є програми, установка яких здійснюється не з офіційного магазину PlayMarket, а зі сторонніх джерел. В результаті, на телефон завантажується вірус, а інфіковані телефони намагаються переводити кошти з електронних гаманців або з прив'язаних банківських карток на баланси шахраїв.

Окремим видом шахрайств із використанням мобільного телефону є клонування SIM-картки, дані з якої за допомогою спеціального апарату переносять на нову SIM-картку і в подальшому здійснюють дзвінки за рахунок жертви. Також шахраї можуть отримати доступ до її банківських карт, систем Інтернет-банкінгу, електронних гаманців, паролів до Інтернет-

сервісів. Таке правопорушення можливе, якщо жертва сама передає власний телефон іншій особі, наприклад, щоб відремонтувати його.

Втрати і крадіжки мобільних телефонів набули масового характеру і сьогодні є найпоширенішим видом злочинів. Цей вид розкрадання вражає величезною кількістю способів відбирання засобів зв'язку у власників. Як основні види можна виділити:

– обман (шахрай просить дати телефон, щоб передзвонити, і втікає);

– гру в довіру: злочинець, пославшись на розряджену батарею телефону, просить вставити в апарат жертви свою SIM-карту, щоб зробити терміновий дзвінок, потім залишивши свій телефон (насправді - муляж) у заставу, зникає;

– крадіжку (непомітне для жертви викрадення телефону, часто в громадському транспорті або в багатолюдних місцях) та розбій (вимагання телефону з використанням погроз та методів насильства).

Інші злочини з використанням мобільного телефону. Окрему, відносно невелику групу «мобільних» правопорушень становлять злочини, в яких неправомірні дії з використанням мобільного телефону не мають на меті отримання безпосередньої матеріальної вигоди. Серед них виділяють:

– несанкціонований запис розмови, відео-зйомка;

– розміщення в телефонному пристрої апаратури для перехоплення інформації в мобільних та комп’ютерних мережах;

– використання телефону як програмованого або дистанційно керованого пристрою для здійснення терористичного акту [8].

Висновки

Отже, правопорушення з використанням мобільного телефону доцільно поділити на такі групи: хуліганство, в тому числі телефонний тероризм; різноманітні види шахрайств, спрямовані проти операторів та абонентів мобільного зв’язку; інші злочини.

Розглядаючи способи неправомірного отримання грошових коштів з використанням мобільного телефону можна виділити такі найбільш поширені: здійснення дзвінка або відправлення СМС на номер підвищеної тарифікації; придбання карти передоплати і повідомлення шахраєві кодів для її активації; використання банківських переказів.

Література

1. Акопов С. Телефонная преступность – новый вызов правоохранительной системе / С. Акопов. [Электронный ресурс] – Режим доступа: https://pglu.ru/upload/iblock/5fc/16.pdf

2. Антонов Р. Мобильный телефон как орудие преступления / Р. Антонов. [Электронный ресурс] – Режим доступа: http://yvision.kz/post/290604

3. Коментар до статті 190. Шахрайство Кримінального кодексу України. [Електронний ресурс] – Режим доступу: http://yurist-online.com/ukr/uslugi/yuristam/ kodeks/024/187.php

4. Мезеря Д. Обстановка преступлений в сфере мобильных телекоммуникаций. / Д. Мезеря. [Электронный ресурс] – Режим доступа: http://teoria-practica.ru/rus/files/arhiv_zhurnala/2011/3/yurisprudentsiya/ mezerya.pdf

5. Пазиніч В. Мобільний як знаряддя злочину / В. Пазиніч. [Електронний ресурс] – Режим доступу: https://kyiv.npu.gov.ua/uk/publish/article/86163

6. Рєпін М. Характеристика злочинів шахрайського характеру, що здійснюються з використанням стільникового зв'язку / М. Рєпін // Молодий вчений - 2016. - №11. - С. 1335-1338.

7. Словари и энциклопедии на Академике. [Электронный ресурс] – Режим доступа: http://dic.academic.ru/dic.nsf/ruwiki/73748

8. Шорошев В. Суспільно небезпечні дії з використанням стільникових терміналів / В. Шорошев, М. Несторенко. [Електронний ресурс] – Режим доступу: https://kyiv.npu.gov.ua/uk/publish/article/86163

Яджин Н. Некоторые элементы криминалистической характеристики преступлений, совершаемых с использованием средств сотовой связи / Н. Яджин, В. Егоров // Научно-методический электронный журнал «Концепт». – 2014. – № 29. – С. 56–60. [Электронный ресурс] – Режим доступа: http://e-koncept.ru/2014/14848.htm.

Надійшла 10.02.2017 р. Рецензент: д.т.н., проф. Шевченко В.Л.