системи, призначені для накопичення та підбору документів. Фактографічні АІС оперують фактичними даними, представленими у формалізованому вигляді. Фактографічні АІС використовують для вирішення задач обробки даних. Завдання цього класу вирішуються при обліку товарів в магазинах, нарахування заробітної плати, управлінні виробництвом, фінансами. Розрізняють фактографічні АІС оперативної обробки даних,які передбачають швидке обслуговування відносно простих запитів від великої кількості користувачів, і фактографічні АІС аналітичної обробки, орієнтовані на виконання складних запитів. Усе це зроблено для швидкого одержання, накопичення, зберігання й обробки даних.

Основні висновки. Вся сучасна економіка базується на управлінні інформацією. Дані вирішують все, і дуже важливо ефективно їх обробляти. При вирішенні господарських, економічних і фінансових завдань доводиться мати справу з великими масивами даних. Вони різнорідні, та взаємопов'язані один з одним. Тому складні набори даних заведено називати БД, а програмне забезпечення, що здійснює операції над БД-СУБД.

ЛІТЕРАТУРА

1. Застосування СУБД в економіці [Електронний Ресурс] – Режим доступу до сайту: https://megalektsii.ru/s73378t3.html]

2. БД в економічних системах [Електронний Ресурс] – Режим доступу до сайту: http://helpiks.org/7-26402.html]

Антон Володченко,
Студент 2 курсу,
Гуманітарно-економічний факультет
Науковий керівник **І.С. Смоліна**
к.п.н., старший викладач (БДПУ)

КІБЕРЗЛОЧИННІСТЬ ТА ЗАСОБИ ЇЇ ПОДОЛАННЯ

Актуальність. У наші дні використання інформаційних технологій не має меж. Віртуальний простір переймає від реального все підряд, у тому числі й злочинність у її нових формах і проявах. Об'єктом кіберзлочинів є персональні дані, банківські рахунки, паролі та інша особиста інформація як фізичних осіб, так і бізнесу та державного сектору. Кіберзлочинність є загрозою не тільки на національному, а й на глобальному рівні.

Ступіть досліджуваності проблеми. Теоретико-методичні та науково-практичні основи попередження дій кіберзлочинців були закладені у дослідженнях науковців В. Голубєва, А. Долгової, К. Касперськи, М. Федотова, С. Орлова, М. Карчевського, Т. Кесарєвої, П. Андрушко.

Мета і методи дослідження. Метою дослідження є ознайомлення з поняттям «кіберзлочинність», з видами шахрайства у мережі Інтернет. У дослідженні були використанні такі методи: аналіз, індукція, узагальнення, порівняння.

Сутність дослідження. Кіберзлочинність – незаконні дії, які

здійснюються людьми, з використанням інформаційних технологій для злочинних цілей. На відміну від традиційних видів злочинів, історія яких налічує століття, таких як вбивство або крадіжка, кіберзлочинність явище відносно молоде і нове, яке виникло з появою мережі Інтернет.

Слід зауважити, що сама природа мережі Інтернет є достатньо сприятливою для вчинення злочинів.

Такі її властивсті, як глобальність, транснаціональність, анонімність користувачів, охоплення широкої аудиторії, розподіл основних вузлів мережі і їх взаємозамінність створюють кіберзлочинцям, які використовують Інтернет, переваги на всіх етапах скоєння злочину, а також дозволяють ефективно ховатися від правохоронних органів.

На відміну від традиційних видів злочинів, історія яких налічує століття, таких як вбивство або крадіжка, кіберзлочинність явище відносно молоде і нове, яке виникло з появою мережі Інтернет.

Слід зауважити, що сама природа мережі Інтернет є достатньо сприятливою для вчинення злочинів.

Такі її властивсті, як глобальність, транснаціональність, анонімність користувачів, охоплення широкої аудиторії, розподіл основних вузлів мережі і їх взаємозамінність створюють кіберзлочинцям, які використовують Інтернет, переваги на всіх етапах скоєння злочину, а також дозволяють ефективно ховатися від правохоронних органів.

Жодна держава сьогодні не в змозі протистояти кіберзлочинності самостійно. Нагальною є необхідність активізації міжнародної співпраці в цій сфері. Експерти впевнені: саме хакери в недалекому майбутньому стануть загрозою номер один, змістивши тероризм. Незважаючи на віртуальність злочинів, збиток вони завдають цілком справжній.

Кіберполіція – міжрегіональний територіальний орган Національної поліції України, який входить до структури кримінальної поліції Національної поліції та відповідно до законодавства України забезпечує реалізацію державної політики у сфері боротьби з кіберзлочинністю, організовує та здійснює відповідно до законодавства оперативно-розшукову діяльність. Спеціалізується на попередженні, виявленні, припиненні та розкритті кримінальних правопорушень, механізмів підготовки, вчинення або приховування яких, передбачає використання електронно-обчислювальних машин (комп'ютерів), телекомунікаційних та комп'ютерних інтернет-мереж і систем.

Розглянемо основні завдання Кіберполіції:реалізація державної політики у сфері протидії кіберзлочинності; завчасне інформування населення про появу новітніх кіберзлочинів; впровадження програмних засобів для систематизації та аналізу інформації про кіберінциденти, кіберзагрози та кіберзлочини; реагування на запити закордонних партнерів, що надходитимуть каналами Національної цілодобової мережі контактних пунктів; участь у підвищенні кваліфікації працівників поліції щодо застосування комп'ютерних технологій у протидії злочинності; участь у міжнародних операціях та співпраця в режимі реального часу. Забезпечення діяльності мережі контактних пунктів між 90 країнами світу; протидія кіберзлочинам.*У сфері використання платіжних систем*: скімінг (шимінг) — незаконне копіювання вмісту треків магнітної смуги (чипів)

банківських карток; кеш-трепінг — викрадення готівки з банкомату шляхом встановлення на шатер банкомату спеціальної утримуючої накладки; кардінг — незаконні фінансові операції з використанням платіжної картки або її реквізитів, що не ініційовані або не підтверджені її держателем; несанкціоноване списання коштів з банківських рахунків за допомогою систем дистанційного банківського обслуговування.*У сфері електронної комерції та господарської діяльності:* фішинг — виманювання у користувачів Інтернету їх логінів та паролів до електронних гаманців, сервісів онлайн аукціонів, переказування або обміну валюти, тощо; онлайн-шахрайство — заволодіння коштами громадян через інтернет-аукціони, інтернет-магазини, сайти та телекомунікаційні засоби зв'язку.*У сфері інтелектуальної власності:* піратство — незаконне розповсюдження інтелектуальної власності в Інтернеті; кардшарінг — надання незаконного доступу до перегляду супутникового та кабельного TV. *У сфері інформаційної безпеки:* соціальна інженерія — технологія управління людьми в Інтернет просторі; мальвер (англ. malware) — створення та розповсюдження вірусів і шкідливого програмного забезпечення; протиправний контент — контент, який пропагує екстремізм, тероризм, наркоманію, порнографію, культ жорстокості і насильства; рефайлінг — незаконна підміна телефонного трафіку.

Основні висновки. Існує декілька порад щодо того, як вберегти себе від кіберзлочинів: створення надійних паролів, захист інформації та періодична їх зміна; поінформованість про розповсюджені прийоми, які використовують злочинці для того, щоб розпізнавати їх; захист пристроїв, встановлення антивірусних програм; використання захищених мереж; перевірка своїх облікових записів;використання інструментів конфіденційності та безпеки браузерів.

ЛІТЕРАТУРА

1.[Кіберполіція та кіберзлочинність [Електронний ресурс] – Режим доступу до сайту: https://revolution.allbest.ru]

2. [Кіберзлочинність у всіх її проявах: види, наслідки та способи боротьби [Електронний ресурс] – Режим доступу до сайту: https://www.gurt.org.ua]

3. [Кіберполіція (Україна) [Електронний ресурс] – Режим доступу до сайту: https://uk.wikipedia.org]