НОМІНАЦІЯ:
ОПЕРАТИВНО -РОЗШУКОВА ТА СПЕЦІАЛЬНА ДІЯЛЬНІСТЬ
ПРАВООХОРОННИХ ОРГАНІВ

Никифорчук Вадим Дмитрович,
слухач магістратури навчально -наукового інституту заочного навчання НАВС
Науковий керівник: кандидат юридичних наук, викладач кафедри оперативно-розшукової діяльності НАВС **Лизогубенко Є.В,**

ОСОБЛИВ ОСТІ В ЧИНЕНИХ МЕРЕЖЕВИХ КОМП'ЮТЕРНИХ ЗЛОЧИНІВ

Процеси глобалізації, характерні для сучасного етапу розвитку суспільства, тісно пов'язані з удосконаленням інформаційних технологій і багато в чому підтримуються впровадженням світових інформаційних систем, що функціонують на основі глобальних комп'ютерних мереж. Єдиний світовий інформаційний простір, у якому постійно циркулює різна інформація, відбувається її накопичення, обробка, зберігання, перестало бути чимось теоретичним, перетворилося в цілком відчутну реальність.

У прийнятій лідерами провідних світових держав Хартії глобального інформаційного суспільства відзначається, що інформаційно-комунікаційні технології увійшли до числа найбільш істотних факторів, що впливають на формування сучасного суспільства. Вони стають важливою складовою суспільного розвитку, позначаються на способі життя людей, характері їх освіти і роботи, відбиваються на взаємодії урядів і громадянського суспільства. Сучасні інформаційні технології в значній мірі змінюють не тільки структуру економіки, але і механізми функціонування багатьох суспільних інститутів, інститутів державної влади, стають важливою складовою розвитку світової економіки.

Однак удосконалювання технологій приводить не тільки до зміцнення індустріального суспільства, але й до появи нових, раніше невідомих джерел небезпеки для нього. Економіка і обороноздатність провідних держав світу все більшою мірою залежать від нормального функціонування глобальних комп'ютерних мереж. Порушення їхньої працездатності може спричинити серйозні наслідки, а національні і міжнародні правові інститути та організаційні структури практично не готові до адекватної протидії новим загрозам.

Так поняття "комп'ютерний злочин" представляється в наш час не цілком визначеним, що не має чітких меж, але широко використовуваним у спеціальній літературі. Найбільш вдалим у зазначеному відношенні представляється вживання поняття "мережевий комп'ютерний злочин", тобто передбачені кримінальним законодавством суспільно небезпечні діяння, вчинені шляхом віддаленого доступу до об'єкта зазіхання з використанням глобальних комп'ютерних мереж як основний засіб досягнення мети

Можна помітити, що вся сукупність мережевих злочинів розділяється на чотири основних типи:

1. Несанкціоноване проникнення в комп'ютерну систему, що має підключення до глобальної комп'ютерної мережі. Пов'язане з порушенням конфіденційності інформації.

2. Порушення нормального функціонування мережевої комп'ютерної системи. Приводить до блокування доступу до інформації.

3. Несанкціоноване внесення змін у комп'ютерні дані (маніпулювання даними). Порушує цілісність і вірогідність інформації.

4. Публікація в глобальних комп'ютерних мережах матеріалів протиправного характеру. Пов'язана з неналежним поширенням інформації.

Представлена типологія дозволяє виділити загальні, найбільш істотні риси досліджуваного явища, знання яких дає можливість далі розвивати аналіз за допомогою строго формальних методів. Такий

підхід може бути корисний при виборі організаційно-тактичних підходів протидії злочинності в глобальних комп'ютерних мережах

Також можна виділити основні особливості «мережевих комп'ютерних злочинів»:

1. Латентність мережевих злочинів

Встановити справжні масштаби нових видів злочинної діяльності, в основному, набагато складніше, ніж будь-яких інших. По оцінках фахівців, від 85 до 97 % мережевих комп'ютерних вторгнень навіть не виявляється

2. Транснаціональний характер мережевих злочинів

Розуміється злочини, вчинені на території і за межами певної держави з порушенням охоронюваних міжнародним і державним законодавством інтересів двох або більше країн.

3. Організований характер мережевих злочинів

Організованість проявляється як у координованості дій технічного характеру, так і в розподілі ролей у групах і навіть участі в діяльності організованої злочинності.

Так можна виділити кілька основних етапів підготовки і реалізації мережевого злочину. Умовно їх можна визначити в наступному узагальненому виді.

1. Підготовка до злочину.
2. Проникнення в мережеву систему.
3. Знищення слідів.
4. Використання результатів.

Отже, цілком очевидно, що сучасні глобальні комп'ютерні мережі є новим об'єктом правоохоронної діяльності. На це вказують присутність кримінальної складової в процесах, пов'язаних з їхнім функціонуванням, наявність у глобальних мережах джерел оперативно - значимої інформації, розвинені механізми забезпечення анонімності при використанні мережею, вплив нормального функціонування мережевих об'єктів на безпеку суспільства, наддержавний характер глобальних мереж, що сприяє вчиненню транснаціональних злочинів.

Більше того, глобальні комп'ютерні мережі можуть бути віднесені до специфічних криміногенних об'єктів, що підтверджується присутністю в них значних обсягів оперативної інформації, функціонуванням каналів обміну інформацією між учасниками злочинних груп, вчиненням з використанням глобальних мереж латентних злочинів, концентрацією навколо них кримінально спрямованих осіб.

У той же час важливо підкреслити, що неприпустимо розглядати глобальні комп'ютерні мережі як інформаційне середовище негативної девіантної спрямованості. Натомість це позитивне явище, здатне принести сучасному суспільству масу переваг. Саме тому на перший

план виходить важливе завдання - знайти рівновагу між створенням умов для безперешкодного розвитку глобальних комп'ютерних мереж і послуг, що надаються з їх допомогою, з одного боку, і забезпеченням безпеки суспільства, держави і особи за допомогою правоохоронних органів, з іншої сторони.