НАВЧАЛЬНО-ВИРОБНИЧА ЛАБОРАТОРІЯ ВИХОВНОЇ ТА ПСИХОЛОГО-ПЕДАГОГІЧНОЇ РОБОТИ

НАВЧАЛЬНО-МЕТОДИЧНИЙ СЕМІНАР ДЛЯ СТУДЕНТІВ 1-4 КУРСІВ

Тема “Запобігання залучення здобувачів освіти до протиправної діяльності у кіберпросторі”

ілюстративно-презентаційний супровід циклу просвітницько-профілактичних семінарів для студентів усіх структурних підрозділів університету

2021 р.

Розробники та ведучі презентаційного заняття

Романкова Лілія Миколаївна

завідувач та засновник (2012 р.) навчально-виробничої лабораторії виховної та психолого-педагогічної роботи, кандидат психологічних наук, доцент

Петрошенко Сергій Іванович

провідний фахівець з питань забезпечення, підготовки, організації й проведення психолого-педагогічних та соціологічних обстежень

Кіберзлочинність у її проявах: види, наслідки та способи боротьби

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. Поняття кіберпростору, введеного письменником Вільямом Гібсоном у п'єсі «Le Neuromancer», описує віртуальний простір як такий, в якому циркулюють електронні дані всіх комп'ютерів світу.

Практично кожен чув про кіберзлочинність і, можливо, навіть особисто з нею зіштовхувався. Кіберзлочинність включає в себе різні види злочинів, що здійснюються за допомогою комп’ютера і в мережі Інтернет. 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.

Піратство та кіберзлочинність в Україні

Нормативне регулювання цієї сфери в Україні не встигає за розвитком технологій, що загострює проблему кіберзлочинності. На рівні фізичних осіб кіберзлочинність пов'язана з використанням піратського програмного забезпечення: зловмисники можуть отримати доступ до персональних даних користувача. Згідно з дослідженням Асоціації виробників програмного забезпечення (BSA) за 2011 р., рівень піратства в Україні становив 84%. За оцінками Міжнародного альянсу інтелектуальної власності (IIPA), Україну визнано «піратом №1» у світі.

Піратство створює сприятливі умови для розвитку кіберзлочинності. За словами начальника кіберполіції України Гринчака Олександра, збитки від кіберзлочинів в Україні тільки за 2020 рік становлять близько 37 млн гривень. Для прикладу: в 2019 році наслідки кіберзлочинів коштували українцям 39 млн гривень.

5 листопада 2015 року була створена нова Кіберполіція, як структурний підрозділ Національної поліції України.

Цей підрозділ займається розкриттям кримінальних правопорушень, що скоєні за допомогою комп'ютерів, телекомунікаційних та комп'ютерних інтернет-мереж і систем.

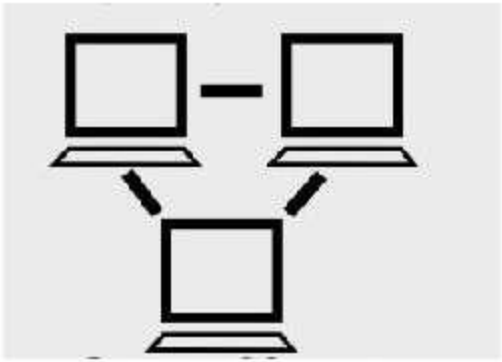
Детальніше ознайомитися з діями кіберполіції можна на їх сайті:

https://www.cybercrime.gov.ua/index.php .

Кіберзлочинність – одна з форм транснаціональної злочинності, що швидко розвивається у сучасному світі

Кіберзлочинність – це сукупність злочинів, що вчинюються у віртуальному просторі за допомогою комп'ютерних систем або шляхом використання комп'ютерних мереж та інших засобів доступу до віртуального простору, а також проти комп'ютерних систем, комп'ютерних мереж і комп'ютерних даних.

Кіберзлочинність швидко перетворилася на бізнес, доходи від якого перевищують $ 3 трлн на рік



Близько 80 млн хакерських атак відбувається кожного дня

Злочини з використання особистих даних -найбільш поширена форма обману онлайн-споживачів

1.Фішинг — виманювання у користувачів Інтернету їх логінів та паролів до електронних гаманців, сервісів онлайн аукціонів, переказування або обміну валюти, тощо;

Скимінг (шимінг) — незаконне копіювання вмісту треків магнітної смуги (чіпів) банківських карток;

Кеш-трепінг — викрадення готівки з банкомату шляхом встановлення на шатер банкомату спеціальної утримуючої накладки;

Кардшарінг — надання незаконного доступу до перегляду супутникового та кабельного TV;

Протиправний контент — контент, який пропагує екстремізм, тероризм, наркоманію, порнографію, культ жорстокості і насильства;

Кардинг — незаконні фінансові операції з використанням платіжної картки або її реквізитів, що не ініційовані або не підтверджен її держателем;несанкціоноване списання коштів з банківських рахунків за допомогою систем дистанційного банківського обслуговування.

Міжнародна класифікація та коди комп'ютерних злочинів

QA - Втручання або перехоплення
QAH - Незаконний доступ
QAI - Перехоплення
QAT - Викрадення часу
QAZ - Інші випадки несанкціонованого доступу або перехоплення
QD - Зміна або пошкодження інформації
QDL - "Логічна бомба"
QDT - "Троянський кінь"
QDV - Програми-віруси
QDW -"Черв'яки"
QDZ - Інші випадки пошкодження інформації
QF - Комп'ютерне шахрайство
QFC - Шахрайство з автоматами по видачі готівки
QFF - Комп'ютерна підробка
QFG - Шахрайство з ігровими автоматами
QFM - Шахрайство шляхом неправильного вводу/виводу або маніпуляції програмами
QFP - Шахрайство з платіжними засобами
QFT - Телефонне шахрайство
QFZ — Інші випадки комп'ютерного шахрайства
QR - Несанкціоноване копіювання
QRG - Несанкціоноване тиражування комп'ютерних ігор
QRS - Несанкціоноване тиражування програмного забезпечення
QRT - Несанкціоноване тиражування напівпровідникової продукції
QRZ - Інші випадки несанкціонованого копіювання
QS - Комп'ютерний саботаж
QSH - Саботаж технічного забезпечення
QSS - Саботаж програмного забезпечення
QSZ - Інші види комп'ютерного саботажу
QZ - Злочини, пов'язані з комп'ютерами
QZB - Незаконне використання дошки електронних оголошень (BBS)
QZE - Викрадення комерційної таємниці
QZS - Зберігання або розповсюдження матеріалів, які є об'єктом судово-І го переслідування
QZZ - Інші випадки вчинення злочинів, пов язаних з комп ютерами

Як вберегтися від кібершахраїв?

Банальні поради : не надавати нікому персональні дані, паролі і коди-підтвердження з смс для операцій з картками, не довіряти повідомленням про виграші в лотереях, перевіряти інформацію за офіційним номером банку, не скачувати в інтернеті сумнівні файли, не заходити на невідомі сайти, користуватись ліцензійним програмним забезпеченням, антивірусом тощо.

Більшість людей знають всі ці речі, але все одно потрапляють у пастки кіберзлочинців.

Небанальні. Сумнівний номер телефону чи картки можна перевірити на сайті кіберполіції, а також звернутися до спеціалістів із запитом.

Кіберполіція радить, як не стати жертвою **вірусу-вимагача**, як виявити, що злочинці **втручаються** в систему вашого онлайн-банкінгу, або як **захиститися** від телефонних шахраїв.

Проект Internet Freedom UA **навчає**, як не впустити кіберзлочинця у свій телефон, через який також можна отримати доступ до коштів на банківському рахунку.

Більшість кіберзлочинів розцінюються як шахрайство, за яке передбачена така відповідальність:

(Стаття 190 КК. Шахрайство)

Шахрайство, вчинене у великих розмірах, або шляхом незаконних операцій з використанням електронно-обчислювальної техніки, -

карається позбавленням волі на строк від трьох до восьми років.

Шахрайство, вчинене в особливо великих розмірах або організованою групою, -

карається позбавленням волі на строк від п'яти до дванадцяти років з конфіскацією майна.

Працівники правоохоронних органів настійно радять всім громадянам, стосовно яких вчинено шахрайські дії, звертатися із заявою до міліції.
Своєчасно отриманий сигнал допоможе оперативно розкрити злочин і повернути втрачене.

Відповідальність за кримінальні правопорушення у сфері використання комп'ютерів та комп'ютерних мереж

Стаття 361. Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку:

1. *Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, що призвело до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації*, – карається штрафом **від 600 до 1000** неоподаткованих мінімумів доходів громадян або обмеженням волі на **строк від 2 до 5 років**, або позбавленням волі на **строк до 3 років**, з позбавленням права обіймати певні посади чи займатися певною діяльністю на **строк до 2 років** або без такого.
2. *Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду*, – караються позбавленням волі на **строк від 3 до 6 років** з позбавленням права обіймати певні посади чи займатися певною діяльністю на **строк до 3 років**.

Примітка. Значною шкодою у статтях 361–363-1, якщо вона полягає у заподіянні матеріальних збитків, вважається така шкода, яка в 100 і більше разів перевищує неоподаткований мінімум доходів громадян.

Стаття 361-1. Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут

1. *Створення з метою використання, розповсюдження або збуту, а також розповсюдження або збут шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку*, – караються штрафом **від 500 до 1000** неоподаткованих мінімумів доходів громадян або виправними роботами на **строк до 2 років**, або позбавленням волі на той самий строк.
2. *Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду*, – караються позбавленням волі на **строк до 5 років**.

Стаття 361-2. Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації

1. *Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації, створеної та захищеної відповідно до чинного законодавства,* – караються штрафом **від 500 до 1000** неоподаткованих мінімумів доходів громадян або позбавленням волі на **строк до 2 років**.
2. *Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду,* – караються позбавленням волі на **строк від 2 до 5 років**.

Стаття 362. Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї:

1. *Несанкціоновані зміна, знищення або блокування інформації, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах чи комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї,* – караються штрафом **від 600 до 1000** неоподаткованих мінімумів доходів громадян або виправними роботами на строк **до 2 років**.
2. *Несанкціоновані перехоплення або копіювання інформації, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, якщо це призвело до її витоку, вчинені особою, яка має право доступу до такої інформації,* – караються позбавленням волі на строк **до 3 років** з позбавленням права обіймати певні посади або займатися певною діяльністю на той самий строк.
3. *Дії, передбачені частиною 1 або 2 цієї статті, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду,* – караються позбавленням волі на строк **від 3 до 6 років** з позбавленням права обіймати певні посади або займатися певною діяльністю на строк **до 3 років**.

Стаття 363. Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється

1. *Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється, якщо це заподіяло значну шкоду, вчинені особою, яка відповідає за їх експлуатацію,* – караються штрафом **від 500 до 1000** неоподаткованих мінімумів доходів громадян або обмеженням волі **на строк до 3 років** з позбавленням права обіймати певні посади чи займатися певною діяльністю на той самий строк.

Стаття 363-1. Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку

1. *Умисне масове розповсюдження повідомлень електрозв'язку, здійснене без попередньої згоди адресатів, що призвело до порушення або припинення роботи електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку*, – карається штрафом **від 500 до 1000** неоподаткованих мінімумів доходів громадян або обмеженням волі на строк **до 3 років**.
2. *Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, якщо вони заподіяли значну шкоду*, – караються обмеженням волі на строк **до 5 років** або позбавленням волі на той самий строк, з позбавленням права обіймати певні посади або займатися певною діяльністю на строк **до 3 років**.

Контактні данні навчально-виробничої лабораторії виховної та психолого-педагогічної роботи

Email: vvppr@pnu.edu.ua

Web: vvppr.pnu.edu.ua

Тел.: (0342) 75-23-56, (099) 310-78-08, (098) 009-23-48