ПЗ будь-якого рівня складності для UNIX-подібних систем та Windows.

**Список використаних джерел:**

1. Краткая история развития Qt. URL: https://www.opennet.ru/docs/RUS/qt3_prog/f71.html (дата звернення: 01.11.2020).
2. Qt Designer Manual. URL: https://doc.qt.io/qt-5/qtdesigner-manual.html (дата звернення: 01.11.2020).
3. Qt Documentation. URL: https://doc.qt.io (дата звернення: 01.11.2020).

**Ключові слова**: Qt, інструментарій розробки програмного забезпечення, кросплатформне ПЗ, графічний інтерфейс користувача.

**Ключевые слова**: Qt, инструментарий разработки программного обеспечения, кроссплатформенное ПО, графический интерфейс пользователя.

**Keywords**: Qt, software development toolkit, cross-platform software, graphic user interface.

***Науковий керівник**: к.т.н., доц. Трофименко О. Г.*

***Стаднік Денис Андрійович***
Національний університет «Одеська юридична академія», студент 3-го курсу факультету кібербезпеки та інформаційних технологій

## ПРОТИДІЯ ЗЛОЧИНЦЯМ В МЕРЕЖІ DARKNET

DarkNet – прихована мережа, з'єднання якої встановлюються тільки між довіреними бенкетами, з використанням нестандартних протоколів і портів. Анонімна мережа являє собою систему не зв'язаних між собою віртуальних тунелів, що надає передачу даних в зашифрованому вигляді. Даркнет відрізняється від інших розподілених тимчасових мереж, так як файлообмін відбувається анонімно, і, отже, користувачі можуть спілкуватися без особливих побоювань і державного втручання.

Зброя, фальшиві гроші, наркотики, крадений кредитки – Це не повний перечнь всього наявного. Це справжнє дно інтернету, де щодня покидьки порушують закон. Вони настільки небезпечні тільки через те, що навчилися використовувати і комунікувати між собою за допомогою Darknet.

Всі адреси, через які вони працюють використовують домен. onion, а такого по суті не існує. ICANN (американська корпорація), без якої не виникне ні один домен першого рівня, нічого подібного не санкціонувала. Однак ці правила не поширюються в DarkNet. Вони не замінюють звичайний інтернет, але створюють поверх публічного Інтернету замасковані, огорожі від зовнішнього світу мережі передачі даних з криптографічним захистом трафіку і своїми методами адресації ресурсів. Використовувати Darknet можна тільки за допомогою технології Tor. Пакет даних, який передається по вузли Tor-мережі, багаторазове шифрується. Ланцюжок з'єднань між двома користувачами будується випадковим чином. Перехоплення даних в одній з ланцюжків не дасть потрібної інформації про користувача або про дані. За допомогою криптографічного захисту всіх даних, це дає можливість сховатися від спостереження.

Як тільки слідчі виявлять активність, пов'язану з наркотиками в реальному світі, вони зацікавляться тим, що робиться онлайн. Спостереження і таємні операції дозволяють визначити ті точки, де зустрічаються реальний і віртуальний світ.

Торговці наркотиками і іншими забороненими засобами використовують свої замасковані сайти тільки як магазини, а шукають клієнтів у відкритому интеренете. Через це торговці забороненим є досить вразливою мішенню. Відповідно до закону, адміністратори сайтів зобов'язані співпрацювати з поліцією і передавати їм необхідну інформацію.

Для боротьби з продажами наркотиків в інтернеті використовується метод знаходження та перевірки інформації про сайтах, на яких можна купити наркотики. Обчислення злочинців в TOR займає багато часу. Спершу за підозрюваним ведуть спостереження, паралельно перевіряючи всіх з ким він

спілкується і його клієнтів. Буває що вже на цьому етапі злочинець робить помилку, за допомогою якої обчислюють його справжній IP-адресу. Після цього його місце розташування стає відомо і його можна успішно затримати. Злочинців в TOR ловлять і за допомогою підставних ресурсів, форумів та посилань. На них розміщують зображення і відео, частина яких розташовується в іншій доменній зоні – наприклад.com або. ru. Картинки відкриваються поза TOR-браузера, і поліцейські відразу дізнаються справжню IP-адресу зловмисника. Часто агенти спец.служб входять в довіру до адмінам заборонених сайтів і уявляють себе в ролі торгашів і споживачів. Боротися з фінансовими шахраями допомагають банківські сервера. Коли злочинець входить в акаунт, який він вкрав або електронний гаманець, що надходить трафік на сервер починає сповільнюватися. Навіть якщо злочинець захищає своє з'єднання, ці затримки будуть у в його зашифрованому трафіку – Таким способом можна довести його провину. Самий вразливий момент для злочинця це висновок грошових коштів, так як для цієї операції потрібно знайти спеціально навченого людини, якими можуть виявитися ті самі агенти спец служб. «Більшість таких випадків разові, і правоохоронці постійно повинні шукати особливий підхід для злочинця».

Зараз в світі задаються питанням, як забезпечити більш ефективний і швидкий спосіб пошуку злочинців. Це війна білого і чорного, і як в будь-якій сучасній війні, щоб її закінчити мало однієї тактики, хитрощів і вивертів. Потрібно мати нову, сучасну зброю, яка зможе поставити крапку в цій війні. Якщо уявити технологію, яка могла б зчитувати дані користувача навіть через Onion посилання, або створити масштабний штучний інтелект, який буде сам відслідковувати незаконні дії користувачів на всіх сайтах і передавати інформацію до відповідних органів, це б змінило все. Однак для створення цих технологій потрібні великі кошти, а так само необхідно щоб люди зрозуміли всю небезпеку даркнета і кинули більше сил для боротьби. Але як можна було помітити, анонімність користувачів в самому даркнета переоцінена. Зловмисники

з DarkNet залишаються безкарними лише до тих пір, поки правоохоронні органи не починають приймати контрзаходи, які найчастіше бувають засновані не на новітніх технологіях машинного навчання, а на класичних методах розслідування.

**Список використаних джерел:**

1. Что такое Даркнет [Електронний ресурс] – Режим доступу до ресурсу: https://ru.wikipedia.org/wiki/%D0%94%D0%B0%D1%80%D0%BA%D0%BD%D0%B5%D1%82.

2. Как ловят преступников в DarkNet [Електронний ресурс] – Режим доступу до ресурсу: https://habr.com/ru/company/wirex/blog/400723/

**Ключові слова:** Даркнет, протидія, злочинці
**Ключевые слова:** Даркнет, противодействие, преступники
**Keywords:** Darknet, anti-action, criminals
***Науковий керівник**: к.т.н., доцент Бойко В. Д.*

***Трєгубов Нікіта Олександрович***
Національний університет «Одеська юридична академія»,
студент 3 курсу факультету кібербезпеки
та інформаційних технологій

## МЕТОДЫ ОБЕСПЕЧЕНИЯ АНОНИМНОСТИ ПОЛЬЗОВАТЕЛЯ

Все мы сталкивались с небольшим оповещением на сайте о том, что надо принять «cookie» файлы, принять условия соглашения конфиденциальности, о сборе данных и так далее, и просто дальше пользовались сетью Интернет. Но задумывались ли вы на что именно соглашаетесь? Были ли у вас мысли что именно за данные вы отдаёте компаниям, чьими услугами вы пользуетесь?

Возьмем, например, компанию Google. Данная компания собирает данные обо всём что вы делаете, когда вы пользуетесь любым из предлагаемых продуктов или асоциированных