УДК 343

ВРЕДОНОСНЫЕ ПРОГРАММЫ ДЛЯ МОБИЛЬНЫХ УСТРОЙСТВ В СФЕРЕ УГОЛОВНОГО ПРАВА

Нимченко Е.В, Кракова Д.В, студентки 3 курса специальности сетевое и системное администрирование
Научный руководитель – Сахибуллин Р.Н., преподаватель
Казанский национальный исследовательский технический университет имени А.Н. Туполева-КАИ, отделение СПО ИКТЗИ КИТ, РФ, г. Казань

Ключевые слова: *Вредоносные программы, мобильные устройства, уголовное право, киберпреступность, безопасность.*

В статье раскрывается понятие вредоносной программы и ее свойства. Рассмотрены функции, которые выполняет вредоносная программы. Кроме этого, также раскрыты виды уголовных наказаний назначаются за совершение киберпрестплений, связанных с созданием и распространением вредоносных программ (статья 273 УК РФ).

Введение. *В современном мире использование мобильных устройств стало неотъемлемой частью нашей повседневной жизни. Однако, наряду с увеличением популярности смартфонов и планшетов, становится все более актуальной проблема вредоносных программ для мобильных устройств. Киберпреступники все чаще используют мобильные устройства как цель для атак, в том числе и в сфере уголовного права. В данной статье мы рассмотрим виды вредоносных программ для мобильных устройств, их цели и последствия, а также меры (наказания) по защите от киберпреступлений в данной сфере.*

Согласно судебной статистике, в 2023 году в России к уголовной ответственности по ст. 273 УК РФ (создание, использование и распространение вредоносных компьютерных программ) было привлечено 3427 человек, в 2022 –137, в 2021 – 123, в 2019 – 225.

Термин «вредоносная программа» впервые введен в российское законодательство в уголовно - правовых целях. Так, в целях статьи 273 УК РФ [1] в редакции от 13 июня 1996 г. вредоносной понимается

«программа для ЭВМ, заведомо приводящая к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети» [2].

Вредоносные программы для мобильных устройств представляют серьезную угрозу для пользователей. Эти программы могут быть разработаны с целью кражи личных данных, вымогательства денег, шпионажа, а также уничтожения информации на устройстве. Кроме того, вредоносные программы могут использоваться для угрозы национальной безопасности, причинения ущерба бизнесу и многим другим негативным целям.

Исходя из данных подходов можно выделить ряд свойств, которые с точки зрения уголовно - правовой науки позволяют рассматривать определенные программы как вредоносные:

1) функциональное предназначение уничтожать, блокировать, модифицировать и копировать пользовательскую информацию, а также приводить к сбою в работе компьютерных систем и их сетей;

2) проведение операций скрытно или без явного одобрения пользователем;

3) несанкционированная пользователем установка программы или отсутствие информирования пользователя о наличии потенциально вредоносного функционала при установке легальной программы;

4) направленность на заведомо неправомерное и несанкционированное посягательство на пользовательскую информацию [3].

Вредоносные программы для мобильных устройств могут быть распространены различными способами. Это могут быть зараженные приложения, фишинговые сайты, вредоносные ссылки, а также через открытые сети Wi-Fi. Пользователи могут заразить свое устройство без своего ведома, что делает борьбу с вредоносными программами сложной и актуальной задачей.

Вредоносная программа способна выполнять ряд функций, в том числе:

- скрывать признаки своего присутствия в программной среде рабочей станции (сервера);

- обладать способностью к самодублированию, ассоциированию себя с другими программами и/или переносу своих фрагментов в иные области оперативной или внешней памяти;

- разрушать (искажать произвольным образом) код программ в оперативной памяти;

- сохранять фрагменты информации из оперативной памяти в некоторых областях внешней памяти прямого доступа (локальных или удаленных);

- искажать произвольным образом, блокировать и/или подменять выводимый во внешнюю память или в канал связи массив информации, образовавшийся в результате работы прикладных программ, или уже находящиеся во внешней памяти массивы данных [4].

Сфера уголовного права также затрагивается вредоносными программами для мобильных устройств. Преступники могут использовать вредоносные программы для осуществления мошенничества, кражи конфиденциальных данных, шпионажа, а также для организации кибератак на государственные и коммерческие системы. Такие действия являются преступными и наказуемыми по закону.

Для борьбы с вредоносными программами для мобильных устройств необходимо принимать ряд мер. В первую очередь, важно обеспечить безопасность своего устройства путем установки антивирусного программного обеспечения и регулярных обновлений операционной системы. Также следует избегать скачивания приложений из ненадежных источников, не открывать подозрительные ссылки и быть осторожными при подключении к открытым сетям Wi-Fi.

В уголовном праве существует ряд мер наказания для киберпреступлений, связанных с созданием и распространением вредоносных программ (статья 273 УК РФ). К таким мерам наказания относятся:

Штрафы за создание и распространение вредоносных программ могут быть назначены штрафы в зависимости от уровня ущерба, который они причинили.

Судебное преследование: лица, замешанные в создании и распространении вредоносных программ, могут быть подвергнуты уголовному преследованию и осуждены к тюремному заключению.

Конфискация имущества: в случае причинения значительного ущерба или вреда с помощью вредоносных программ, суд может принять решение о конфискации имущества виновного.

Запрет на занимание определенных должностей: лицо, осужденное за создание и распространение вредоносных программ, может быть лишено права занимать определенные должности или заниматься определенной деятельностью.

Экстрадиция: в случае, если лицо, замешанное в киберпреступности, находится за пределами страны, где было совершено преступление, может быть запрошена его экстрадиция для уголовного преследования.

Это лишь общие меры наказания, применяемые в отношении лиц, совершивших киберпреступления с использованием вредоносных программ. Конкретные санкции могут различаться в зависимости от законодательства конкретной страны.

Заключение. В целом, вредоносные программы для мобильных устройств представляют серьезную угрозу для пользователей и требуют внимательного внимания. Соблюдение основных правил безопасности и профилактические меры могут помочь предотвратить заражение устройства вирусами и минимизировать риски угрозы в сфере уголовного права.

Библиографический список:

1. Уголовный кодекс Российской Федерации" от 13.06.1996 N 63-ФЗ (ред. от 14.02.2024) // "Собрание законодательства РФ", 17.06.1996, N 25, ст. 2954.

2. Дремин, С. В. Анализ подходов к понятию вредоносной компьютерной программы в уголовном праве / С. В. Дремин // АКТУАЛЬНЫЕ вопросы РАЗВИТИЯ ПРАВОВОЙ ИНФОРМАТИЗАЦИИ в УСЛОВИЯХ ФОРМИРОВАНИЯ ИНФОРМАЦИОННОГО ОБЩЕСТВА : сборник статей Международной научно-практической конференции, Пенза, 15 июня

2021 года. – Уфа: Общество с ограниченной ответственностью "Аэтерна", 2021. – С. 28-31.

3. Россинская, Е. Р. Концепция вредоносных программ как способов совершения компьютерных преступлений: классификации и технологии противоправного использования / Е. Р. Россинская, И. А. Рядовский // Всероссийский криминологический журнал. – 2020. – Т. 14, № 5. – С. 699-709.

4. Приказ Росреестра от 29.01.2013 N П/31(ред. от 06.04.2016) "Об организации и проведении работ по обеспечению безопасности персональных данных при обработке в информационных системах персональных данных в Федеральной службе государственной регистрации, кадастра и картографии" // СПС Консультант Плюс.

MALWARE FOR MOBILE DEVICES DEVICES IN THE FIELD OF CRIMINAL LAW

Nemchenko E.V., Krakova D.V.
Scientific supervisor –Sahibullin R.N.
Kazan National Research Technical University named after A.N. Tupolev-KAI, Department of SPO ICTZI KIT, Russian Federation, Kazan

Keywords: *Malware, mobile devices, criminal law, cybercrime, security.*

The article reveals the concept of malware and its properties. The functions performed by the malware are considered. In addition, the types of criminal penalties are also disclosed for committing cybercrimes related to the creation and distribution of malware (Article 273 of the Criminal Code of the Russian Federation).