

УДК 343.92

ПРЕДУПРЕЖДЕНИЕ МОШЕННИЧЕСТВА С ИСПОЛЬЗОВАНИЕМ ВРЕДНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Д. Ю. Метченко

слушатель 4 курса

Барнаульского юридического института МВД России,

1856 учебная группа

Научный руководитель: М. А. Малетина,

старший преподаватель кафедры уголовного права и криминологии

Барнаульского юридического института МВД России,

кандидат юридических наук

В современном мире вместе с развитием технологий одновременно происходит появление новых приемов совершения мошеннических действий. Одним из них является заражение устройства вредоносной программой.

Так, основным способом заражения устройства вредоносными программами является скачивание носителя вируса из сети Интернет. В настоящий момент известны следующие вредоносные программы: программы-вымогатели и фишинговые приложения.

К программам-вымогателям относят программы, требующие определенную сумму за восстановление работоспособности устройства, получение контроля над ним. Указанные вредоносные программы можно разделить на два типа: *программы-шифровальщики*, шифрующие данные на устройстве случайно сгенерированным ключом, и *программы-блокировщики*, полностью блокирующие нормальную работу устройства.

Фишинговые приложения, в свою очередь, маскируемые под вид приложений банков, игр и прочих, используются для перехвата поступающей на устройство информации.

Следует сделать вывод о том, что человек, не обладающий достаточными знаниями, с трудом может распознать такое программное обеспечение (далее — ПО) и принять меры по недопущению его проникновения на устройство. Нами предлагается перечень мер, при соблюдении которых можно обезопасить свое устройство от заражения вредоносными программами: во-первых, скачивать приложения исключительно из официальных магазинов, таких как Google Play, AppStore и т. д.; во-вторых, не переходить по ссылкам от незнакомых номеров; в-третьих, необходимо обращать внимание на правильность написания ссылки, по которой предлагается перейти, — в большинстве случаев сайты с вредоносным ПО маскируются под сайты известных компаний; в-четвертых, обязательно использовать антивирусное ПО на устройстве. Такие программы

имеют собственную базу приложений, позволяя с большей вероятностью распознать и своевременно принять меры по нейтрализации угрозы.

Соблюдая перечисленные выше меры, возможно снизить риск заражения устройства вредоносным ПО, а соответственно, обеспечить безопасность как собственных данных, так и денежных средств.