**Барабинская транспортная прокуратура**

**Использование информационных технологий в качестве способов совершения преступлений**

По данным Генеральной прокуратуры РФ, на деяния, совершенные с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, приходится одно из четырех регистрируемых в текущем году преступлений (363 тыс.).

Ранее отмечавшиеся практически двукратные темпы их увеличения

несколько замедлились и составляют 77 %. Отмечается, что больше половины всех киберпреступлений совершается с использованием сети Интернет (209,7 тыс.), свыше 42 % – при помощи средств мобильной связи (155,2 тыс.)3.

Однако даже эти показатели не отражают объективную картину киберпреступности в РФ, поскольку используемое в отчетности понятие «преступление, совершенного с использованием информационно-телекоммуникационных технологий» охватывает около 10 составов преступлений (ст. 158, 159, 1593, 1596, 183, 272–274 УК РФ), а ряд преступлений против личности, например доведение до само- убийства (ст. 110 УК РФ), склонение к совершению самоубийства или содействие совершению самоубийства (ст. 1101 УК РФ), организация деятельности, направленной на побуждение к совершению самоубийства (ст. 1102 УК РФ), угроза убийством или причинением тяжкого вреда здоровью (ст. 119 УК РФ), принуждение к изъятию органов и тканей человека для трансплантации (ст. 120 УК РФ), клевета (ст. 1281 УК РФ), понуждение к действиям сексуального характера (ст. 133 УК РФ) и иные преступления, совершаемые дистанционным способом в отчет не попадают

Самая распространения категория способов противоправной деятельности с использованием информационных технологий – это применение вредоносных программ. Такое программное обеспечение позволяет получить доступ к банковским счетам, иным данным потерпевших. Назначение вредоносного программного обеспечения зависит от характера информации, которую требуется получить злоумышленнику. Так, определенные вредоносные программы осуществляют сбор и передачу информации о реквизитах входа в систему дистанционного банковского обеспечения либо выполнение несанкционированных законным пользователем функций как в тайне от последнего, так и в явном виде. Некоторые программы предполагают дестабилизацию деятельности ранее установленного программного обеспечения.

Вредоносные компьютерные программы находят свое применения в фишинговой деятельности. «Фишинговые» сайты или рассылаемые электронные письма, содержащие вредоносные эксплойты, активируясь через действия пользователя, открывают доступ преступникам в информационную систему, вследствие чего у преступников появляется возможность перехватывать данные, осуществлять переводы денежных средств на подконтрольные им банковские счета.

Отдельно следует выделить использование вредоносного программного обеспечения для операционных систем современных смартфонов. Внедрение такого программного обеспечения на смартфон, где хранятся конфиденциальные сведения о привязанной к номеру телефона банковской карте, имя и пароль входа в систему банковского обслуживания, SMS-сообщения, подтверждающие совершение транзакций и др.), дают большой простор для преступной деятельности.

Информационные технологии играют существенную роль в преступлениях, связанных с незаконным распространением объектов, изъятых из гражданского оборота. Для данной категории преступлений первостепенное значение имеет дистанционный способ реализации таких предметов. В частности, такая деятельность предполагает использование социальных сетей, специализированных сайтов на серверах вне юрисдикции государства, возможности которых используются для распространения информации о наличии у продавцов соответствующего запрещенного товара, а также для информирования покупателя о способах и порядке расчетов, времени и месте получения товара.

Существуют и иные виды программного обеспечения, позволяющего скрыть все данные о преступнике, и, что особенно важно, указанные способы совершенствуются с каждым днем. Быстро развивающаяся динамика преступности с использованием информационных технологий свидетельствует о необходимости совершенствования системы противодействия указанным преступлениям со стороны как законодательных, так и правоохранительных органов. Поскольку появление новых способов противоправной деятельности с использованием высоких технологий требует не только быстрого реагирования правоохранительных органов, но и своевременного правового обеспечения, создающего необходимую правовую базу противодействия киберпреступности.