

Cybercrime in the modern world
Cherkasov D.¹, Ivanov V.², Lubova E.³ (Russian Federation)

Киберпреступность в современном мире
Черкасов Д. Ю.¹, Иванов В. В.², Лубова Е. С.³ (Российская Федерация)

¹Черкасов Денис Юрьевич / Cherkasov Denis – студент;

²Иванов Вадим Вадимович / Ivanov Vadim – студент;

³Лубова Елена Сергеевна / Lubova Elena – студент,
кафедра компьютерной и информационной безопасности,
Институт кибернетики,

Федеральное государственное бюджетное образовательное учреждение высшего образования
Московский технологический университет,

Московский институт радиотехники электроники и автоматики, г. Москва

Аннотация: киберпреступность - незаконные действия людей, которые используют современные информационные технологии для достижения преступных целей. Актуальность данной темы заключается в острой проблеме, связанной с киберпреступностью в настоящее время.

Abstract: cybercrime is an illegal actions of people who uses modern information technologies to achieve criminal goals. The topicality of this topic is an acute problem associated with cybercrime now.

Ключевые слова: киберпреступность, взлом, данные.

Keywords: cybercrime, hacking, data.

Киберпреступностью обычно называются различные виды незаконной деятельности, которые используются в Интернете, в частной или публичной сетях либо внутренних компьютерных системах. В то время как большинство форм киберпреступности связано с похищением конфиденциальной информации для несанкционированного использования, существуют и другие формы, сосредоточенные на вторжении в частную жизнь. Киберпреступность становится большой проблемой во всем мире, поэтому многие страны приступают к принятию законов и других регламентирующих механизмов в попытке свести к минимуму число случаев киберпреступности [1].

Киберпреступность относится к электронным преступлениям. К основным видам киберпреступности относятся распространение вредоносного программного обеспечения, кража паролей, кража номеров кредитных карт и других банковских реквизитов. Одним из самых ярких примеров является использование сети и специально разработанного программного обеспечения с целью кражи личных данных, которые впоследствии преступник может использовать в корыстных целях. С помощью незаконно полученных данных злоумышленник может использовать чужие банковские счета. Таким образом, люди останутся с огромными долгами, к которым они не причастны [2].

Шантаж - давно установившийся незаконный акт, который является неотъемлемой частью современного мира. Шантажист угрожает выложить личную информацию жертвы в открытый доступ, если его требования не будут соблюдаться. Киберпреступления такого рода порой заходят так далеко, что мошенник переводит средства жертвы на несуществующий банковский счет при помощи некоторой платежной онлайн программы. Здесь можно сказать о полноценном использовании технологий для совершения преступлений.

К киберпреступности также относится незаконный доступ к данным компании. Как и в случае с физическими лицами, преступники могут украсть финансовую информацию и совершать покупки с использованием этих данных. В том числе мошенник может снять средства со счетов компании, а передача похищенных средств посредством различных счетов делает практически невозможным нахождение украденных активов. В других случаях преступник интересуется вовсе не деньгами или кредитной информацией - он стремится к получению сведений о патентах, которые продает конкурентам. Это является еще одним примером применения высоких технологий в преступной деятельности.

Во многих странах обсуждался вопрос киберпреступности, где упоминали о том, что и рассылка спама также является преступным деянием. Спам - это нежелательные сообщения, которые отправляются одновременно на тысячи или даже миллионы учетных записей электронной почты. Однако некоторые страны приняли конкретные законы, которые регламентируют ситуации, в которых спам не будет считаться актом киберпреступности. К таким случаям можно отнести ситуацию, в которой получателю предоставляется возможность отказаться от дальнейшего получения подобных писем. Поскольку данная проблема становится все более и более актуальной, большинство политиков стали продвигать идею о создании определенного национального или международного закона по борьбе с киберпреступностью, который бы касался использования спама либо его ограничения или ликвидации.

Получить статистику реальных данных о киберпреступности не так просто, как кажется. Как и в случае других преступных деяний, некоторые инциденты электронной преступности остаются незарегистрированными. Это делает невозможным сбор материалов о киберпреступности за определенный период времени. Однако многие правоохранительные органы во всем мире пытаются воссоздать наиболее

полную картину. Например, в США ФБР стремится выявить и задокументировать любые примеры электронной преступности, в том числе действия, которые относятся к террористической деятельности, мошенничеству, хищению личных данных или растрате.

Литература

1. *Волеводз А. Г.* - сост. Десятый Конгресс Организации Объединенных Наций по предупреждению преступности и обращению с правонарушителями. Сборник документов. Москва: Юристинформ, 2001 - с. 496.
2. *Леонов А. П.* [и др.]; под общ. Ред. А. П. Леонова. Компьютерная преступность и информационная безопасность. Минск: АРИЛ, 2000 - с. 552.