ОБЛАСТНЫЕ МАТЕРИАЛЫ
для членов информационно-пропагандистских групп
(март 2020г.)
Дополнительная тема

ПРЕДУПРЕЖДЕНИЕ СОВЕРШЕНИЯ НЕСОВЕРШЕННОЛЕТНИМИ ПРЕСТУПЛЕНИЙ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ

Количество пользователей сети интернет в Республике Беларусь и их сетевая активность имеют устойчивую тенденцию роста.

Сегодня информационные технологии задействованы везде: в промышленности, в авиатранспорте, железнодорожном транспорте, науке, образовании, социальных структурах, государственном управлении, экономике и культуре.

Состояние криминогенной обстановки в сфере высоких технологий в 2019 году в сравнении с 2018 годом свидетельствует о значительном увеличении в Республике Беларусь количества зарегистрированных киберпреступлений (*более чем в 2 раза; с 4741 до 10539*)**.**

В Гомельской области в прошлом году зафиксировано 1781 киберпреступление (*в 2018 году – 563*), из них совершено преступлений несовершеннолетними или при их участии 42 (*14 в 2018 году*).

В законодательстве Республики Беларусь предусмотрена ответственность, в том числе уголовная за совершение противоправных деяний в сфере высоких технологий.

Самыми распространенными преступлениями, совершенными несовершеннолетними лицами, являются преступления, предусмотренные статьей 212 Уголовного кодекса Республики Беларусь (далее – УК).

Необходимо отметить, **что ответственность** за деяния, предусмотренные ст.212 УК, **наступает с 14-летнего возраста**.

Наиболее распространенными схемами преступлений ст. 212 УК, совершенных несовершеннолетними лицами, являются:

1) Хищение денежных средств со счета найденной либо похищенной банковской платежной карточки (далее – БПК) с использованием банкомата, платежного терминала. В последнее время наиболее актуальны факты хищений с использованием реквизитов карт при осуществлении интернет-платежей (*покупки в интернет магазинах «JOOM», «Aliexpress», оплата подписок на различных сайтах, оплата различных бонусов в онлайн-играх и т.д.*), а также завладение денежными средствами, хранящимися на счетах различных

электронных платежных систем и сервисов (когда логин и пароль от электронной платежной системы стал известен несовершеннолетнему лицу).

2) Хищение денег абонентов сотовой связи через мобильный банкинг. Схема базируется на услуге «А1- banking», предоставляющей доступ к электронному кошельку «А1-кошелек» унитарного предприятия «А1». Пользователям этого сервиса оператор связи предлагает 100 рублей в качестве беспроцентного кредита.

Злоумышленники просят у человека телефон, чтобы позвонить, а на самом деле стремительно выполняют преступные манипуляции.

Так, в 2019 году несовершеннолетний просил у прохожих телефон, чтобы якобы позвонить домой маме. На самом деле после того, как телефон оказывался у него в руках, за короткое время он активировал на смартфоне потерпевших услугу А1-banking, по которой компания предоставляла кредит в сумме 100 рублей, а затем переводил деньги, полученные при подключении, на свой лицевой счет абонентского номера СООО «Мобильные ТелеСистемы». После этого, как ни в чем не бывало, возвращал телефон владельцу и удалялся.

Многие даже не сразу понимали, что пострадали от ловких действий преступника. Спустя какое-то время потерпевшим поступали смс-сообщения от унитарного предприятия «А1» с информацией о задолженности по номеру телефона и граждане понимали, что стали жертвой преступника.

В настоящее время в отношении несовершеннолетнего задокументировано 24 эпизода противоправной деятельности, материалы уголовных дел формируются для направления в суд.

Статья 349 УК. Несанкционированный доступ к компьютерной информации. **Ответственность** за деяния, предусмотренные ст. 349-355, наступает **с 16-летнего возраста**.

Например, несанкционированный доступ (*открытие и просмотр файлов, писем, переписки личных данных пользователя и т.п., в нарушение установленного законодательством порядка*) к электронной почте, учетным записям на различных сайтах, в том числе в социальных сетях, к информации, содержащейся на компьютере, в смартфоне и защищенной от доступа третьих лиц.

Статья 350 УК. Модификация компьютерной информации.

В качестве примера можно привести произведенные изменения компьютерной информации в системе либо сети, которые затрудняют либо исключают ее дальнейшее использование.

Статья 351 УК. Компьютерный саботаж.

Здесь мы говорим об умышленном уничтожении (*удалении, приведении в непригодное состояние, шифровании*) компьютерной информации либо ее блокировании (*например, путем смены пароля доступа, изменении графического ключа и т.д.*).

Так, в 2019 году несовершеннолетний с использованием своей учетной записи, зарегистрированной в социальной сети «ВКонтакте», осуществлял переписку с различными пользователями, которые хотели продать или обменять свои игровые аккаунты игры «Битва Замков». После, договорившись о покупке, несовершеннолетний получал от продавца логин и пароль игрового аккаунта. Затем, осуществив доступ к указанному игровому аккаунту, умышленно изменял пароль доступа к нему, тем самым блокировал доступ к указанному игровому аккаунту и связанной с ней компьютерной информацией правомерному пользователю. Никаких денежных средств за игровой аккаунт несовершеннолетний продавцу не перечислял.

О данной преступной деятельности стало известно после обращения потерпевшего гражданина Российской Федерации в правоохранительные органы Республики Беларусь, так как злоумышленник не единожды обращал внимание в переписке, что он из Беларуси. По результатам проведенной проверки несовершеннолетний привлечен к уголовной ответственности по ст. 351 УК Республики Беларусь и осужден к наказанию в виде 3-х лет ограничения свободы без направления в исправительное учреждение открытого типа.

Статья 352 УК. Неправомерное завладение компьютерной информацией.

В данном случае учитываются действия, связанные с копированием какой-либо значимой информации (*в обязательном порядке не находящейся в открытом доступе, т.е. защищенной паролем, либо содержание логинов и пароле от учетных записей полученные путем их «взлома»*), повлекшие причинение существенного вреда, к примеру копирование писем из электронной почты, личной переписки из социальных сетей, закрытых для просмотра третьими лицами.

Статья 353 УК. Изготовление либо сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети.

Статья достаточно специфична и применяется при разработке, изготовлении и сбыте специальных программ и устройств, предназначенных для осуществления несанкционированных доступов. Примером может служить изготовление и сбыт средств (*смарт-карт,*

чипов и т.п.) для неправомерного просмотра зашифрованных телевизионных каналов.

Статья 354 УК. Разработка, использование либо распространение вредоносных программ.

К уголовной ответственности по данной статье могут быть привлечены лица за разработку вредоносного программного обеспечения, а также разработку и использование вирусов, например блокирующих смартфоны либо шифрующих компьютерную информацию на серверах.

Статья 355 УК. Нарушение правил эксплуатации компьютерной системы или сети.

Указанная статья может быть применена к лицам, имеющим доступ к компьютерным сетям (*в том числе к абонентам интернет-провайдеров*) и системам, в которых хранится значимая информация, халатные действия которых привели к нарушению функционирования таких систем либо нарушению правил их использования.

Кодексом об административных правонарушениях Республики Беларусь также предусмотрена ответственность за совершение несанкционированного доступа к компьютерной информации, не повлекшего существенного вреда.

Управление внутренних дел облисполкома
Главное управление идеологической работы, культуры и по делам молодежи облисполкома