«О профилактике преступлений в сфере высоких технологий»

В большинстве государств мира существует уголовная ответственность за преступления в сфере информационной и компьютерной безопасности. На сегодняшний день проблема преступности в информационных технологиях является актуальной, так как с развитием информационных технологий активно развивается и вредоносная вирусная база, и сети взломщиков. Сегодня неправомерное противозаконное распространение информации через глобальную сеть, взлом паролей, кража номеров кредитных карточек, фишинг стали очень популярными.

В уголовном кодексе Республики Беларусь выделен ряд преступлений против информационной безопасности. Уголовный Кодекс Республики содержит отдельную главу, которая предусматривает ответственность за преступления в сфере информационной безопасности и содержит 7 статей. К компьютерным преступлениям законодательства относится: ст.349 – несанкционированный доступ к компьютерной информации; ст. 350 – модификация компьютерной информации; ст. 351 – компьютерный саботаж; ст. 352 – неправомерное завладение компьютерной информацией; ст.353 – изготовление либо сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети; ст. 354 – разработка, использование либо распространение вредоносных программ; ст. 355 – нарушение правил эксплуатации компьютерной системы или сети.

Также в других разделах УК Республики Беларусь имеются составы преступлений, в которых предусмотрен способ совершения хищений с использованием компьютерной техники. Например, хищение путём использования компьютерной техники (ст.212 УК).

Глава 31 УК Республики Беларусь “Преступления против информационной безопасности” имеет своей целью охрану именно информационной безопасности – и только в силу этого защиту и аппаратно-технических средств, которые являются материальными носителями информационных ресурсов. Применительно к данной главе, под информационной безопасностью следует понимать совокупность общественных отношений, складывающихся в процессе защиты информационных ресурсов и охраны прав субъектов информатизации, а также обеспечения безопасности пользователей и пользования компьютерными системами и сетями.

Преступления в сфере компьютерной безопасности очень разнообразные. В большинстве составов преступлений против информационной безопасности предметом является компьютерная информация, т.е. информация, хранящаяся в компьютерной сети, системе, на компьютерных носителях либо передаваемая сигналами, распространяемыми по проводам, оптическим волокнам или радиосигналами.

Многим внушили, что если твой пароль никто не знает, то система в безопасности. Но это далеко не так. Сам пароль сейчас является маленькой крупинкой в процессе получения доступа к аккаунту в социальной сети,

электронному почтовому ящику и т.д. механическим подбором паролей злоумышленники занимаются в последнюю очередь.

Вот несколько самых популярных видов активности по взлому:

социальная инженерия – простые пароли, содержащие личную информацию о пользователе (дата рождения, ФИО и т.д.);

спам-рассылки – письмо, чаще всего о выигрыше ли выгодном предложении, со ссылкой, которая отсылает на сайт вредоносный сайт;

Фишинг – фальшивый копирующий оформление оригинала практически на 100% сайт, куда невнимательный пользователь вводит данные.

Распространение нелицензионного ПО с вирусами.

Проникновение за границу авторизации в социальных сетях чаще всего является следствием взлома почтовых ящиков. Помимо этого пользователи совершают много ошибок, что приводит к плачевным последствиям. В руки злоумышленников попадают личные фотографии, нежелательные сообщения и подробности из жизни и многое другое, что хотелось бы скрыть от глаз посторонних. Необходимо знать, что на данный момент взломать аккаунт социальной сети гораздо проще, чем обойти защиту достаточно известных сервисов электронной почты. Поэтому не достаточно защитить что-то одно, необходим комплекс мер. Лучшая защита – профилактика и бдительность.

Так как суть преступления по взлому ящика почты и аккаунта социальных сетей практически совпадает, то и уголовно-правовая характеристика у них одинаковая. В современном мире даже бизнес может быть организован через социальную сеть, поэтому нельзя сказать, что взлом того или иного объекта будет важнее, чем другого. Отметим важное – зачастую взлом является следствием банальной невнимательности пользователя, оставив открытый профиль в интернет кафе или у друга в гостях, уже сложно будет говорить вам об уголовном составе преступления.

Взлом аккаунта в социальной сети охватывается составом преступления предусмотренного статьей 349 УК Республики Беларусь (несанкционированный доступ к компьютерной информации).

Непосредственным объектом преступления, ответственность за совершение которого предусмотрена ст. 349 Уголовного кодекса Республики Беларусь, является информационная безопасность, под которой следует понимать совокупность общественных отношений, обеспечивающих состояние защищённости интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере.

Предметом указанного преступления является компьютерная информация.

К вышеперечисленным методам получения пароля можно добавить:

Незакрытые сессии в соц. Сетях;

Передача данных третьим лицам;

Использование непроверенных Wifi-сетей.

Вся сложность информационных преступлений состоит в доказательстве вины преступника. Крайне трудно привлечь конкретное лицо

к ответственности, особенно если оно совершенно незнакомо вам. Есть совсем немного способов доказать факт взлома профиля в социальной сети или электронного почтового ящика:

Отправить письмо управляющим почтового сервиса или социальной сети с просьбой предоставить список IP адресов, заходивших через ваш аккаунт;

Некоторые социальные сети в настройках позволяют проследить последние активности («ВКонтакте»);

Если от вашего лица приходит спам другим пользователям, профиль недоступен, к вам обратилась администрация ресурса, то вероятность взлома максимальная.

Обязательным признаком объективной стороны несанкционированного доступа к компьютерной информации является способ его совершения — нарушение систем защиты информации.

Нарушение системы защиты может быть осуществлено:

а) путем применения технических манипуляций (расшифровка кода, пароля, ключа доступа; маскировка под законного обладателя или пользователя информацией; изменение физических адресов технических средств; модификация компьютерных программных средств и т.п.);

б) без применения технических манипуляций, но посредством нарушения правового режима доступа к информации;

в) путем сочетания технических манипуляций и нарушения правового режима доступа к информации.

Уголовная ответственность за совершение преступления, предусмотренного ч. 2 ст. 349 УК, наступает при отсутствии общественно опасных последствий, предусмотренных ч. 1 ст. 349 УК (таких как нарушение прав, свобод и законных интересов граждан, например в разглашение информации о состоянии здоровья гражданина или членов его семьи и т.п.; нарушение общественных и государственных интересов; например, несанкционированный доступ к информационной сети с целью ознакомления с информацией, предназначенной исключительно для служебного пользования), но при наличии одного или нескольких обстоятельств, таких как:

а) корыстная или иная личная заинтересованность;

б) совершение группой лиц по предварительному сговору;

в) совершение лицом, имеющим доступ к компьютерной системе или сети.

Субъектом преступлений против информационной безопасности может стать, в принципе, любой человек, особенно если учесть возрастающую компьютерную грамотность населения. Ответственность за преступления против компьютерной безопасности наступает с 16 лет (ст. 27 УК Республики Беларусь). В ч.2.ст.349 и ст.355 предусмотрен специальный субъект – лицо, имеющее доступ к компьютерной системе или сети.

Таким образом, преступления против информационной безопасности являются обособленной в уголовном кодексе подгруппой более крупного явления – компьютерных преступлений.