УДК 343.9

АКТУАЛИЗАЦИЯ МЕР ПРОТИВОДЕЙСТВИЯ КОМПЬЮТЕРНЫМ ПРЕСТУПЛЕНИЯМ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ ОБЩЕСТВА

Савотченко С.Е.,
доктор физико-математических наук, доцент;
Акапьев В.Л.,
кандидат педагогических наук
(Белгородский юридический институт МВД России имени И.Д. Путилина)

Аннотация: сформулированы правила поведения, позволяющие не стать жертвой мошенника в компьютерной сети Интернет. Приведены советы для осуществления безопасной работы в Интернете. Описаны основные меры предупреждения преступлений с использованием телекоммуникационных средств и информационных технологий. Сформулированы предложения для эффективной реализации рассмотренных мер.

Ключевые слова: информационные технологии, телекоммуникационные средства, компьютерные сети, киберпреступность.

ACTUALIZATION OF MEASURES TO COUNTERACT COMPUTER CRIMES IN THE CONTEXT OF THE DIGITALIZATION OF SOCIETY

Savotchenko S.E.,
Doctor of Physical and Mathematical Sciences, Associate Professor;
Akapev V.L.,
Candidate of Pedagogical Sciences
(Putilin Belgorod Law Institute of Ministry of the Interior of Russia)

Abstract: the rules you need to know in order not to become a victim of a fraudster on the Internet computer network are formulated. Some tips to help you surf the Internet safely are derived. The main measures for the prevention of crimes using telecommunications and information technologies are described. Proposals for the effective implementation of the considered measures are formulated.

Keywords: information technology, telecommunications facilities, computer networks, cybercrime.

Интернет стал выгодной платформой для киберпреступников [1]. Более того, пандемия и самоизоляция в 2020 году выступили особым катализатором этих процессов, произошло увеличение числа пользователей Интернета, что стимулировало высокий рост преступности. Количество пользователей Интернета с каждым днем увеличивается. Как следствие растет и оборот денег, а так-

же незаконный оборот, в частности, наркотических средств [2]. Учитывая вышеизложенное, мошенники и преступники понимают, что Интернет – это легкое место для наживы, позволяющее каким-то образом обогатиться.

В настоящее время в эпоху Интернета люди стали меньше общаться вживую, отдавая предпочтение социальным сайтам, где пользователи помещают огромное количество персональной информации, которой мошенники могут воспользоваться для совершения различных преступлений. К примеру, на сервисы платежных систем направляются реквизиты банковских карт; посредством электронной почты пересылаются копии документов, удостоверяющих личность; в социальных сетях размещается информация о личной жизни, с помощью мессенджеров передается иная конфиденциальная информация. Кроме этого, системы поиска на основе анализа запросов пользователя с хорошей точностью формируют его социальный портрет, включая его увлечения, профессию, уровень доходов, точное местоположение, круг знакомых и другое. Эти и другие новшества в сфере информационных технологий не могли не сказаться на состоянии преступности. Несомненно, развитие информационных технологий открывает новые границы для совершения перечисленных и иных киберпреступлений, что обусловлено постоянным развитием технических средств [3].

Вследствие этого, чтобы избежать осложнений для себя и своих близких, нужно быть предельно внимательными, знать меры профилактики и помнить основные правила безопасного поведения и общения в Интернете.

Итак, рассмотрим, какие же правила нужно знать, чтобы не стать жертвой мошенника:

1. Если вам звонят по телефону и представляются сотрудником Сбербанка, то знайте, что настоящий сотрудник банка никогда не станет просить данные с вашей карты, так как у них есть эти данные.

2. Храните пин-код отдельно от карты, его не следует писать на самой банковской карте, так как при потере преступники смогут этим воспользоваться. Лучше всего пин-код запоминать, так мошенники никогда его не узнают, если вы сами его им не скажете.

3. Берегитесь телефонных мошенников, они будут пытаться ввести вас в заблуждение. Лучше всего избегать с ними контакта, ни в коем случае не говорить слово «Да», так как в настоящее время в Сбербанке есть функция распознавания голоса, следовательно, мошенники смогут снять денежные средства с вашего счета. Таким образом, если представляются сотрудником банка, просто закончите разговор и сами сходите в Сбербанк, узнайте, есть ли у сотрудников к вам вопросы.

4. Пристально читайте сообщения, приходящие от банковских структур. Ни под каким предлогом не сообщайте никому пароли и секретные коды, которые приходят вам, в частности, от Сбербанка.

5. Знайте, если вас просят пройти с банковской картой к банкомату, то это несомненно мошенники, так как сотрудники Сбербанка никогда не будут просить вас об этом.

6. Никогда не покупайте в интернет-магазине товар по очень низкой цене, так как это явно мошенники.

7. Никогда не переводите деньги, если об этом вас просит сделать ваш друг в социальной сети. Скорее всего преступники взломали его аккаунт. Сначала позвоните вашему другу и узнайте, на самом ли деле он просит у вас материальной помощи. Чаще всего мошенники, взывая о помощи от имени вашего знакомого, просят перевести деньги на банковскую карту, которую присылают вам в личном сообщении, где указана фамилия и имя вашего друга. Но это не так, мошенники с помощью приложения для обработки фотографий Adobe Photoshop подделали фото и вместо своих инициалов написали инициалы жертвы, оставив номер карты неизменной, либо просят скинуть деньги на мобильный телефон.

8. В Интернете не переходите по неизвестным ссылкам на незнакомые сайты.

9. Никогда не перечисляйте по просьбе иных лиц деньги на различные нужды органов государственной власти – это мошенники.

10. Не следует присылать фото банковской карты даже в личных сообщениях в социальных сетях, а также авиабилеты, паспорт и другие документы, которые включают персональные данные человека, так как ими могут воспользоваться мошенники. В настоящее время в связи с развитием информационных технологий развивается и мошенничество. Так, хакерам уже не составляет труда просматривать ваши переписки.

Советы для безопасного нахождения в Интернете:

1. Установите или обновите проверенный и надежный антивирус на своем устройстве. К примеру, на 2022 год лучшими антивирусниками являются McAfee, Norton и Kaspersky.

2. Используйте официальное программное обеспечение для защиты от заражения вирусами при скачивании различных программ.

3. Не скачивайте файлы из подозрительных сайтов, а только с официальных.

4. Не сообщайте никому свои личные данные. Лучше всего закрывать свою страницу в социальной сети и не писать никакой личной информации, с помощью которой мошенники смогут взломать вашу страницу и совершить неправомерные деяния.

5. Используйте сложные пароли из различных комбинаций символов, цифр, различных знаков, но не следует использовать в пароле дату рождения, чтобы минимизировать взлом страницы.

Таким образом, зная несложные правила нахождения в информационной среде, можно избежать столкновения с мошенниками. При этом главным критерием является хранение личных данных в тайне.

Какие же методы в современном мире используются для борьбы с преступлениями в информационной среде? Современные ученые выделяют три основные меры предупреждения преступлений с использованием телекоммуникационных устройств: правовые, организационно-управленческие, технические [4; 5]. Так, к правовым мерам предупреждения относятся нормы законодательства, устанавливающие уголовную ответственность за преступные деяния в сфере информационных технологий.

Юридическая ответственность за преступления, совершенные в сфере информационных технологий, предусмотрена Уголовным кодексом Российской Федерации от 1996 года (ред. от 05.04.2021) в главе 28, в статьях 272-274, где указаны меры наказания за преступления в сфере компьютерной информации.

В наше время российское законодательство недостаточно разработано и более лояльно относится к преступникам, так как если рассматривать Соединенные Штаты Америки, то у них за киберпреступления предусмотрено до 25 лет лишения свободы, тогда как в Российской Федерации максимальный срок достигает 10 лет. Также можно отметить несоответствие уровня проработки УК РФ на примере ст. 274 о неправомерном доступе к защищенной информации, где сказано, что никто не вправе каким-либо образом уничтожать, изменять или копировать информацию. Но ведь преступник может не вносить изменения в эту информацию, а просто может прочитать и изучить ее.

Таким образом, в современном мире за преступления в информационной среде предусмотрены уголовные наказания в виде лишения свободы, но, к сожалению, киберпреступников это не останавливает и поэтому правоохранительным органам и всей структуре МВД в целом необходимо разрабатывать действующие меры по борьбе с киберпреступлениями.

Другим направлением предупреждения преступлений в информационной среде являются организационно-управленческие меры:

1. Устранение хищения, изменения и подделывания защищенной информации. Выражается это в том, что такие органы власти, как Федеральная служба безопасности, Роскомнадзор каждый день в Сети следят за тем, чтобы не похищалась конфиденциальная информация.

2. Устранение незаконных действий по уничтожению, изменению, копированию информации и другого незаконного вмешательства в информационные системы. Правоохранительные органы по геолокации отыскивают и задерживают киберпреступников, но если найти их не удается, блокируют их в Интернете. Так ФСБ использует СОРМ – комплекс мер, направленных на проведение оперативно-розыскных мероприятий в Сети и СОРМ-1 – для прослушивания телефонных переговоров.

3. Защита государственной тайны и конфиденциальной информации. Поддерживают защиту этой информации следующие государственные органы: межведомственная комиссия по защите государственной тайны и иные федеральные органы исполнительной власти.

4. Гарантия прав и свобод граждан в информационном пространстве в сфере информационных технологий. Государство гарантирует соблюдение прав и свобод человека не только в реальной жизни, но и в Интернете.

5. Проведение агитации и мероприятий, направленных на распространение сведений о дающей успешные результаты борьбе с преступлениями в сфере информационных технологий. Это делается для того, чтобы преступники знали, что они могут быть пойманы и заключены под стражу, следовательно, это может оказать влияние на снижение количества преступлений в сфере информационных технологий.

6. Проведение разъяснительных бесед с подрастающим поколением. Так, на национальном уровне проводятся различные диалоги назначаемых лиц от правоохранительных органов с молодежью. Эти беседы проводятся в школах, университетах, колледжах для объяснения подросткам, что Интернет – это не место для развлечения, это место повышенной социальной опасности, где в любой момент смогут украсть ваши персональные данные, снять деньги с вашего счета, а также выложить ваши личные фото или переписку с друзьями в Интернет. Поэтому нужно быть осторожным в информационной среде, чтобы не попасться на уловки мошенников. Также необходимо пояснить молодежи, что ждет мошенников за такие деяния, ознакомить подростков со статьями 272, 273 и 274 УК РФ, так как по статистике мошенниками в современное время, к несчастью, становится молодое поколение.

Помимо этого, чтобы снизить тенденцию у молодежи совершать противоправные деяния в информационной среде, нужно вводить в учебные занятия дополнительные часы по такой дисциплине как «Информатика». Благодаря этому подростки не только не будут совершать преступления в Интернете, но и будут знать, как противостоять этому.

Следовательно, организационно-управленческие меры позволяют значительно снизить преступления в информационной среде, благодаря действиям правоохранительных органов проводятся различные мероприятия, профилактические беседы, а также в самом Интернете органы ФСБ ведут борьбу с кибертерроризмом. Все это пресекает неправомерные действия киберпреступников и мошенников в сетевом пространстве.

Следующим вариантом предупреждения преступлений являются технические меры – это меры, направленные на предотвращение преступлений в информационной среде за счет осуществления мероприятий технического характера, обеспечивающих безопасность, а также формирование материально-технической базы по борьбе с киберпреступностью.

Они подразделяются на аппаратные и программные методы:

1. Аппаратные методы служат для того, чтобы защищать телекоммуникационные технологии от нежеланных физических воздействий и закрытия возможных каналов утечки личной информации. К ним относятся устройства идентификации личности, источники бесперебойного питания и устройства экранирования аппаратуры.

2. Программные методы нужны для того, чтобы при передаче информации никакая информация не была похищена либо искажена кем-либо. Для этого используются различные методы шифрования данных.

Для эффективной реализации рассмотренных мер необходимо:

1. Разработать порядок взаимодействия правоохранительных органов с международными организациями для обмена информацией о киберпреступности и для совместного взаимодействия.

2. Благоприятствовать проведению ежегодных научных конференций по проблемам выявления, пресечения и расследования киберпреступности.

3. Подготовить методические рекомендации по предупреждению, выявлению и пресечению преступлений в информационной среде.

4. Создавать организации, либо иные подразделения, направленные на борьбу с киберпреступностью.

5. Разработать программу подготовки специализированных кадров для работы по защите информационных технологий от угроз киберпреступников.

Таким образом, все эти меры являются уникальными и довольно трудоемкими, так как вводить их достаточно затратно по времени и по ресурсам для государства, но это необходимо делать, так как именно государство и все общество в целом с помощью данных мер сможет справиться с такой серьезной проблемой, как киберпреступность.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Журавленко Н.И., Шведова Л.Е. Проблемы борьбы с киберпреступностью и перспективные направления международного сотрудничества в этой сфере // Общество и право. 2015. № 3(53). С. 65–73.

2. Баринов В.Б. Сущность оперативно-розыскной профилактики преступлений // Пробелы в российском законодательстве. 2020. № 2. С. 173–198.

3. Тишутина И.В. Новые возможности раскрытия и расследования преступлений в условиях глобальной цифровизации // Юридические науки. 2020. № 3. С 39–47.

4. Даненьян А.А. Международное правовое регулирование киберпространства // Наука и право. 2020. № 2. С. 239–268.

5. Эмиров М.Б. Борьба с преступлениями в глобальных компьютерных сетях // Юридический вестник Белгородского государственного университета. 2018. № 3. С. 49–56.