www.esa-conference.ru

УДК 343.9

Хищения, совершенные с помощью информационных технологий: вопросы теории, законодательного регулирования и практики

Шава Эмма Васильевна, студент,
направление «Право и организация социального обеспечения»
Самитов Эльдар Оскарович, кандидат юридических наук, старший преподаватель
кафедры правовой информатики, информационного права
и естественнонаучных дисциплин, научный руководитель
Казанский филиал Российского государственного университета правосудия

Аннотация. *Статья посвящена изучению преступлений, совершенных с помощью "информационных технологий" или "высоких технологий". Существуют различные типы киберпреступности, некоторые из них даже не требуют использования интернета, например, кража личных данных, но в основном любое преступление с помощью выхода в Интернет. Список наиболее распространенных преступлений составляют: взлом, кража, кибер-выслеживание, вредоносное программное обеспечение, вымогательство, жестокое обращение с детьми и мошенничество.*

Ключевые слова: *преступления, киберпреступления, информационные технологии.*

Theft, committed with the help of information technologies: theoretical issues, legislative regulation and practice.

Shawa Emma Vasilievna, student, direction "The right of social security"
Samitov Eldar Oskarovich, Candidate of Law, Senior Lecturer
of the Department of Legal Informatics, Information Law and Natural Sciences
The Kazan Branch of the Russian State University of Justice

Annotation. *The article is devoted to the study of crime issues with the help of "information technology" or "high technology". There are various types of cybercrime, some of them do not even require the use of the Internet, such as identity theft, but basically any crime with access to the Internet. The list of the most common crimes are: hacking, theft, cyber-tracking, malware, extortion, child abuse and fraud.*

Keywords: *crimes, cybercrime, information technology.*

Актуальность.

Существуют различные типы киберпреступности, некоторые из них даже не требуют использования интернета, например, кража личных данных, но в основном любое преступление с помощью выхода в Интернет. Список наиболее распространенных преступлений составляют: взлом, кража, кибер-выслеживание, вредоносное программное обеспечение, вымогательство, жестокое обращение с детьми, мошенничество. Обычный человек сказал бы что-то о хакерстве, пиратстве или распространение вирусов. Это явление имеет множество названий, среди них известны такие как "преступление с помощью клавиатуры", преступления "информационных технологий" или "высоких технологий".

Результаты исследования. Теперь нужно разобрать эту проблему изнутри, а именно выяснить, кто же такие киберпреступники, их цели и жертвы. Адам Андерсон, психолог преступников, сказал, что "киберпреступность это проблема не компьютера и развития технологий, это проблема нашего поведения и отношения", поэтому давайте рассмотрим эту проблему как поведение со стороны.

Первый вопрос описан в работе Камини Дашоры под названием "Кибер преступность в обществе". Она разделила всех преступников на 4 группы:

1. Дети и подростки в возрасте от 6 до 18 лет

Простая причина такого типа поведения у детей выражена в основном из-за желания знать и исследовать новые вещи. Другой, связанной с первой, причиной может быть самоутверждение себя и желание быть лучшим в своей социальной группе.

2. Организованные хакеры или киберпреступления белых воротничков (должных лиц, чиновников)

Эти виды хакеров в основном организованы в группы для достижения определенной цели, обычно такие цели связаны с государственными ценными бумагами, конфиденциальной информацией или даже терроризмом. Причины могут быть различными: политическими, религиозными, идеологическими и тд. В данном случае, стоит рассказать о «Пакистанцах», организованная группа, которая является одной из лучших хакерский группировок в мире. НАСА, а также пользователи Microsoft чаще всего становятся жертвами данной группы..

3. Профессиональные хакеры/взломщики

Их мотивы просто: желание обогатиться. Эти виды хакеров в основном занимаются взломами сайтов конкурентов, кражей персональных данных, мошенничеством в интернете и тд.

4. Сотрудников, которые были уволены

В этом случае, человек желаем отомстить работодателю, поэтому с чувством мести он всегда собирает информацию только под одну фирму и ее филиалы.

ЕВРАЗИЙСКОЕ НАУЧНОЕ ОБЪЕДИНЕНИЕ
EURASIAN SCIENTIFIC ASSOCIATION
www.esa-conference.ru

Что мы должны знать о жертвах?

Это именно тот случай, когда отношение человека играет важную роль. Жертвами киберпреступности обычно становятся люди с низкой самооценкой и с неверными убеждениями. Стоит обратить ваше внимание на три основные убеждения, разделяемые большинством жертв:

1. Я не важен и никто не ищет меня.
2. У меня нет ничего, чего бы кто-либо хотел.
3. Я не могу остановить их, даже если бы хотел.

Чтобы предотвратить киберпреступность, мы не должны полагаться только на конкретную программу безопасности, но мы также должны осознавать угрозу и быть более уверенными в своих действиях в Интернете.

Например, есть куча сайтов с наживкой, созданных для мошенничества или отмывание денег, но не все программы видят опасность в обычной кнопке или веб-сайте, но если человек знает о проблеме, я уверена, что он никогда не перейдет по ссылке на сайт, которая внезапно появилась на экране компьютера. Виктимология - очень важная отрасль криминальной психологии. Это так же важно знать на кого преступник, скорее всего, нацелится. Все преступники – по крайней мере, умные будут только нападать только на тех, кто проявляет определенную уязвимость. Так же, как грабитель никогда не подумает об ограблении кто-либо, заведомо зная, что он вооружен, поэтому киберпреступники осторожны с личностями тех, они выбирают в роли жертвы.

Выделяют четыре уровня жертв киберпреступности:

1. Излишне доверчивые люди.
2. Отчаянные или жадные люди.
3. Неопытные (в силу возраста) люди.
4. Несчастные люди.

1. Доверчивые жертвы не сомневаются, что киберпреступники больше всего любят тех, кого легко обмануть. Спамеры отправляют несколько сообщений по электронной почте и доверчивые становятся жертвами содержимого электронной почты. Как правило, пожилые люди склонны быть жертвами мошенничества, поскольку они более доверчивы и не осознают возможного риска. В противопоставление, молодое поколение также часто становится жертвами данной категории, так как дети считают, что люди, с которыми они знакомятся по сети, так же дружелюбны и достойны доверия, как и реальные люди. Почти все жертвы киберпреследователи склонны доверять людям и легко заводить друзей.

2. Отчаянные и жадные пользователи интернета нуждаются в простых способах делать деньги. Следовательно, они легко попадают на электронные письма, которые говорят "Быстро разбогатеть - это возможно!", "Поздравляем с победой в лотерее" и тому подобное.

Обычные люди обычно подумают, если они не принимали участия в какой-либо лотерее, то почему кто-то поздравляет Вас с победой? Жадные и отчаявшиеся люди будут всегда попадать на этот уровень мошенничества, и следовать инструкциям в электронных письмах. Есть другие люди, которых привлекают рекламные объявления, связанные с улучшением личного имиджа. Например: «Пластика дешево», «как стать успешным в один клик». Чаще всего такие объявления служат отличной возможностью для хакера узнать номер банковской карты или определённую личную информацию человека, как средний заработок, место проживания, вредные привычки, часто посещаемые сайты и запросы в поисковых системах.

3. Неопытных людей очень много, их знания о сети ограничиваются простым общением со своими друзьями и, возможно, поиском информации в Google. Они не знают о том, что большинство людей, которых они встречают в интернете, являются преступниками, которые прячутся под тенью интернета, чтобы совершать различные преступления. Они так же не знают о мошенничестве через клик-бейт, поэтому, увидев рекламу, быстро перейдут по ней.

4. Есть люди, которые не подходят ни под одну из этих категорий, но которым просто не повезло оказаться не в том месте, не в то время, то есть в киберпространстве. Кроме того, полномасштабная атака или самовоспроизводящийся и высокоразвитый вирус может нанести большой ущерб сетям или ПК.

Предупреждение хищений, совершенных с использованием информационных технологий.

Пользователь сети должен помнить о следующих вещах:

1. Чтобы предотвратить хищения, совершенных с использованием информационных технологий, избегайте раскрытия любой информации, относящейся к вашему "я".

2. Всегда избегайте отправки любых фотографий в интернете, особенно незнакомым людям и друзьям чата, поскольку были случаи неправильного использования фотографий.

3. Всегда используйте последнюю версию и обновляйте антивирусное программное обеспечение для защиты от вирусных атак.

4. Всегда сохраняйте резервные копии, чтобы не допустить потери данных в случае заражения вирусом

5. Никогда не отправляйте номер своей кредитной карты на любой сайт, который не защищен, чтобы защитить себя от мошенничества.

6. Всегда следите за сайтами, к которым обращаются ваши дети, чтобы предотвратить любые преследования или развращение детей.

Литература:

1.Криминалистика: учебник/С.Я. Казанцев, А.В. Варданян, Э.О.Самитов. -Москва: Юстиция, 2020. -326 с.

2.Казанцев С.Я., Самитов Э.О. Тактические особенности проведения обыска при расследовании хищений, совершенных с использованием интернет-технологий. Вестник Московского университета МВД России. 2016. № 8. С. 145-147

3.Самитов Э. О. Роль допроса в расследовании хищений, совершенных с использованием интернет-технологий / Э.О. Самитов, И.Е., Мазуров// Судебная экспертиза: прошлое, настоящее и взгляд в будущее:

Материалы ежегодной научно-практической конференции (4-5 июня 2015 г.) СПб.: Изд-во СПб ун-та МВД России, 2015.С.295-298

4.Самитов Э.О. Особенности коммуникативного взаимодействия первоисточника и потребителя информации /Монография.-Казань:Изд-во "Магариф-Вакыт",2014.-207с.

6.Самитов Э.О., Мазуров И.Е. Роль криминалистической характеристики в расследовании хищений, совершенных с использованием интернет-технологий. В сборнике: криминалистика: актуальные вопросы теории и практики: сборник трудов участников XIII Всероссийской научно-практической конференции. 2016. С. 143-146.

7.Facts On File, Incorporated “Cybercrime” - Infobase Publishing, 2009, p.14

8.Kamini Dashora “Cyber in Society” – India, 2011

9.Sylvester, Linn (2001): The Importance of Victimology in Criminal Profiling. Available online at: http://isuisse.ifrance.com/emmaf/base/impvic.html

10.Vannesa Pitts “Cyber Crimes: History of World’s Worst Cyber Attacks” - Vij Books India Pvt Ltd, 2017

11.Cybercrime and the Law: Challenges, Issues, and Outcomes Авторы: Susan W. Brenner

12. Cybercrime: Criminal Threats from Cyberspace Авторы: Susan W. Brenner

13.International Guide to Combating Cybercrime Авторы: Jody R. Westby