Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

Усова В.В., Шульга А.В. Киберпреступления и способы их совершения // Академия педагогических идей «Новация». Серия: Студенческий научный вестник. – 2019. – №4 (апрель). – АРТ 346-эл. – 0,3 п.л. - URL: http: //akademnova.ru/page/875550

РУБРИКА: ЮРИДИЧЕСКИЕ НАУКИ

УДК 343.9

Усова Валерия Владимировна
студентка 2 курса факультет юриспруденции
Шульга Андрей Владимирович
к.ю.н., доцент, зав. кафедрой уголовного права
ФГБОУ ВО «Кубанский государственный аграрный
Университет им. И.Т. Трубилина»
г. Краснодар, Российская Федерация
E-mail: valera_us1701@mail.ru

КИБЕРПРЕСТУПЛЕНИЯ И СПОСОБЫ ИХ СОВЕРШЕНИЯ

Аннотация: в статье рассматривается такая проблема современного общества, как киберпреступность. Каждый год во всём мире значительно увеличивается число киберпреступлений. Это связано с непрерывным техническим развитием компьютерных и информационных технологий.

Ключевые слова: киберпреступления, компьютерный вирус, виртуальное пространство, кибероружие, кибербезопасность.

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

Usova Valeriya
2nd year student, faculty of law
Shulga Andrey Vladimirovich
Ph.D. assistant professor
Head of the Department of Criminal Law
FGBOU VO «Kuban state agrarian University
named after I. T. Trubilin»
Krasnodar, Russian Federation

CYBER CRIMES AND METHODS OF THEIR IMPLEMENTATION

Abstract: The article deals with such a problem of modern society as cybercrime. Every year throughout the world, the number of cybercrimes increases significantly. This is due to the continuous technical development of computer and information technology.

Keywords: cybercrime, computer virus, virtual space, cyber weapon, cyber security.

Прежде чем начать говорить о кибпреступности, следует разобраться, что же такое преступность. Преступность — это исторически изменчивое социальное и уголовно-правовое негативное явление, представляющее собой систему преступлений, совершённых на определённой территории в тот или иной период времени. Что касается киберпрестпуности, то это одна из существенных проблем уголовного преследования настоящего времени. Под данным понятием подразумевается совершение преступлений в сфере высоких технологий. Это весьма обширный термин, включающий в себя множество незаконных деяний. Таким образом, киберпреступность - это преступность в виртуальном пространстве.

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

Виртуальное пространство можно определить, как моделируемое с помощью компьютера информационное пространство, в котором находятся сведения о лицах, предметах, фактах, событиях, явлениях и процессах, представленные в математическом, символьном или любом другом виде и находящиеся в процессе движения по локальным и глобальным компьютерным сетям.

Глава 28 УК РФ посвящена киберпреступности (Глава 28 УК РФ «Преступления в сфере компьютерной информации»). Указанная нами глава содержит всего 4 статьи, предусматривающие уголовную ответственность за преступления, совершенные с использованием компьютерной техники и инновационных технологий. Особенности главы в том, что, во-первых, она завершает раздел IX УК РФ, посвященный общественно опасным деяниям против общественного порядка и безопасности. Глава включает преступления, в состав которых входит общий субъект (ответственность наступает с 16 лет), а специального не предусмотрено. Гл. 28 включает наименьшее количество статьей по сравнению с другими гл. разделе IX УК РФ. Она считается относительно новой, в ней указываются составы преступлений, которые до 1996 года не были известны уголовному законодательству.[1]

Но все же выясним, какие виды киберпреступлений бывают и как обезопасить себя от них.

Рассмотрим способы совершения киберпреступлений: «фишинг», «спам», «инсайдинг», «хакерство», похищение цифровой личности, телекоммуникационные преступления.

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

Одним из распространенных киберпреступлений является «Фишинг» - это один из способов интернет мошенничества, когда всеми возможными правдами и неправдами пытаются узнать различные персональные данные (пароли, логины, номера банковских карт и счетов). Смысл заключается в том, чтобы побудить перейти по «фишинговой» ссылке на поддельную страницу, визуально похожую на настоящую, например, банка, где под различными предлогами выудить персональную информацию.[2]

Следующим в перечне киберпреступлений выступает «спам». К нему относятся нежелательные рекламные объявления, мистификации и сообщения, предназначенные для распространения рекламных объявлений или вредоносных программ. Доставляемые пользователю неудобства и опасность увеличиваются из-за того, что стоимость рассылки минимальна, а в распоряжении авторов «спама» есть множество средств получения новых адресов электронной почты и способов нелегально рассылать сообщения.

Также существует такое понятие как «Инсайдинг». «Инсайдер» (работающий или освобожденный сотрудник компании) является потенциальным преступником. Знакомый с тонкостями компьютерной системы компании, он имеет неограниченный доступ к системе с целью незаконного вмешательства в работу автоматизированных электронно-вычислительных машин, их систем или компьютерных сетей, или с целью незаконного завладеет информацией, которая является собственностью компании.

Рассмотрим такой способ совершения киберпреступления как «Хакерство». «Хакер»» - чрезвычайно квалифицированный IT-специалист, человек, который понимает самые глубины работы

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

компьютерных систем. Изначально хакерами называли программистов, которые исправляли ошибки в программном обеспечении каким-либо быстрым и далеко не всегда элегантным или профессиональным способом. Однако большинство людей считают, что хакер компьютерный взломщик, проникающий в закрытые информационные сети, банки данных и тому подобное с целью получения доступа к секретной информации, а также заражения их вирусами.

Следующий метод это – похищение цифровой личности - неправомерное завладение, например, профилем в социальной сети, с целью рассылки спама, использования личных данных, шантажа, выманивания денежных средств и другое.

А также существуют «телекоммуникационные преступления» - преступления, совершаемые через СМИ и средства связи. Наиболее известным из них является атака с целью перегрузить оборудование жертвы и помешать его нормально использовать.[3]

Для того чтобы обезопасить себя от киберпреступлений достаточно придерживаться следующих правил: обязательно удаляйте «скриншоты» и сообщения с паролями, не сохраняйте пароли в браузерах, не переходите по подозрительным ссылкам, пользуйтесь приложениями, а не сайтами каких-либо магазинов, они безопаснее, не пересылайте фотографии своих банковских карт. Для получения перевода, достаточно шестнадцати цифр расположенных на лицевой стороне карты, а срок действия и код на обратной стороне карты рекомендуется держать при себе.[4]

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

Исходя из правовой статистики, можно привести пример, что в 2012 году МВД выявило 11 тыс. киберпреступлений, из которых 20% в отношении детей. Младшее поколение — это наименее защищенная категория пользования сетью Интернет, а также данный ресурс требует дополнительных средств для противодействия сетевым злоумышленникам.

Согласно исследованию американской компании «Norton» в 2012 году в России киберпреступники нанесли ущерб в размере 12 млрд. долларов, а количество жертв составило 30 млн. человек.

В частых случаях жертвами таких киберпреступлений как: интернет - мошенничество, «спам», негативный «контент» – становятся именно дети. В 2018 году полиция зарегистрировала более 206 тысяч преступлений, связанных с телекоммуникационной и компьютерной информацией. Об этом ТАСС сообщили в пресс-службе МВД России. Как сообщили в полиции, киберпреступления совершались «с использованием или применением расчетных карт, компьютерной техники, программных средств, фиктивных электронный платежей, сети интернет и средств мобильной связи». Всего полиции удалось выявить более 24 тысяч человек, которые совершили преступления в киберпространстве.

Чтобы обезопасить гражданина от интернет - мошенничества необходимо, в первую очередь, проинформировать его о всевозможных угрозах. Установить персональную программу по обнаружению вирусов, иными словами «антивирус», и активизировать «брандмауэр» (как вспомогательное средство при фильтрации проходящей через него информации), который оградит личность от потенциально вредоносных сайтов. Для предотвращения

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

заражения компьютера так называемыми «вирусами» и «троянскими программами», следует установить на ПК специализированный почтовый фильтр.

2018 год ознаменовался большим количеством киберпреступлений. Эксперты считают, что кибератаки в нынешнем году будут распространены в еще большем объеме. Становится все труднее противостоять киберпреступлениям, так как вредоносное программное обеспечение постоянно совершенствуется. Кроме того, крупные компании оцифровывают свою деятельность для повышения эффективности, тем самым делая свою работу более уязвимой. По мере расширения цифровой экономики, деятельность киберпреступников увеличивается в тождественном коэффициенте. Ситуация усугубляется в связи с развитием возможностей технического обучения и искусственного интеллекта. С каждым днем растет количество вредоносных программ, а также различных «чат-ботов», которые способствуют совершению кибератак. Кроме того, развивается «криптография» — еще один способ кражи личных данных, при котором жертвы даже не подозревают о взломе и утечке конфиденциальной информации.

Следует указать на тенденции развития киберпреступности в 2019 году.

Во-первых, это - «Чат-боты»: в 2019 году хакеры начнут активно внедрять вредоносных «чат-ботов», которые помогут пользователям загружать зараженные файлы, делиться личной информацией, а также переходить на подозрительные сайты по ссылкам. Возможно, что мошенники смогут внедрять такие «чат-боты» даже на проверенных сайтах.

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

Во-вторых, кибератаки как новый компонент теневой экономики: злоумышленники будут использовать новые инструменты, которые смогут выводить из строя компьютеры. После такой кибератаки необходимо будет полностью заменить оборудование. Вероятно, что в этом будут замешаны террористические организации.

Киберпреступления со стороны государства: ожидается значительное увеличение числа нападений со стороны государства. Известно, что Россия была лидером в использовании целенаправленных кибератак для достижения определенных целей. Другие государства могут последовать ее примеру.

Растущая милитаризация данных: несмотря на попытки технологических компаний обезопасить своих пользователей, их конфиденциальная информация все еще находится в зоне риска. Социальная сеть «Facebook» не скрывает того, что использует личные данные пользователей для увеличения своих доходов. В большинстве случаев пользователи сами предоставляют информацию о своих интересах и предпочтениях социальным сетям. Этим активно пользуются рекламодатели.

Программы-вымогатели: программы-вымогатели стали все чаще использоваться после массовых атак вируса «WannaCry», который вымогает деньги у его жертв. По данным ФБР, общая сумма денег, отданная вымогателям, в США превысила 1 млрд. долларов. В последнее время практически ничего не слышно о таких атаках, однако это не исключает вероятности того, что в 2019 году они снова станут актуальными.

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

Диверсия против разработки ПО: вредоносное ПО уже было обнаружено в некоторых библиотеках программного обеспечения с открытым исходным кодом. Когда клиенты загружают и устанавливают обновления, они добровольно внедряют вредоносное ПО в свою систему. Вероятно, что в 2019 году такая тенденция продолжится.

Спутники под угрозой: в июне 2018 «Symantec», компания по разработке ПО, сообщила, что группа хакеров атаковала спутниковую связь телекоммуникационных компаний Юго-Восточной Азии, занимающихся созданием геопространственных карт и съемкой изображений. Также «Symantec» сообщала о нападениях на военные спутники Китая. В августе 2018 года на ежегодной конференции по информационной безопасности «Black Hat» стало известно, что спутниковая связь, используемая судами, самолетами и военными для подключения к Интернету, очень уязвима.[5]

Исходя из анализа понятия «киберпреступление» проведенного в нашей статье, необходимо указать, что человек является первостепенной целью работы киберпреступников, тем самым, обостряя такое новое направление в уголовно-наказуемых деяниях, и обеспечивающее активную деятельность органов государственной власти в данном направлении.

Список используемой литературы:

1. Уголовный Кодекс Российской Федерации от 13.06.1996 63-ФЗ (с изм. и доп., вступ. в силу с 11.01.2015) // Собрание законодательства РФ.- 17.06.1996.- N 25, ст. 2954.

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

2. Шульга А.В. Интеллектуальная собственность как предмет хищения // Государство и прав. 2012. №2. С.29-32.

3. Вехов В. Б. Компьютерные преступления: способы совершения и раскрытия / В.Б. Вехов; Под ред. акад. Б.П. Смагоринского. - М.: Право и закон, 2014.- 182 с.

4. Авчаров И.В. Борьба с киберпреступностью / И.В. Авчаров. // Информатизация и информационная безопасность правоохранительных органов. XI межд. конф. - М., 2012. - С. 191-194.

5. https://psm7.com/security/kiberprestupnost-v-2019-godu.html.

Дата поступления в редакцию: 11.04.2019 г.
Опубликовано: 11.04.2019 г.