КИБЕРПРЕСТУПНОСТЬ КАК УГРОЗА НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ И НОРМАТИВНЫЕ ПРОБЕЛЫ В СФЕРЕ КИБЕРБЕЗОПАСНОСТИ

Кучеренко А.С.

«Южный институт менеджмента» (ЮИМ)

e-mail:super.azhela943985@ya.ru

Аннотация: Киберпреступность - это любое незаконное действие в электронной сфере, которое совершено с помощью компьютерных технологий, либо против них.

Существует 5 разновидностей киберпреступлений: 1)преступление направлен2) Фишинг, одним словом преступления с помощью технологий, с целью извлечения экономической выгоды ное на базу данных пользователя ПК.3) Право4) Нарушение авторских прав нарушения, связанные с содержанием контента5) Кибертерроризм. Таким словом называют особо серьезные преступления, связанные с жестокостью и совершением актов насилия по средствам высоких технологий.

В действующем УК РФ существует только одна глава, которая предусматривает ответственность за киберпреступления «Преступления в сфере компьютерной информации» и содержит три статьи определяющие ответственность по вредоносным программно-техническим действиям. (ст. 272-274 УК РФ). Однако, если обратиться к ст. 272 УК РФ то в ней четко предусмотрена ответственность за неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло ее уничтожение, блокирование, модификацию либо копирование. Следует отметить, что физическое повреждение компьютера, повлекшее уничтожение информации, хранящейся в нем, не влечет за собой последствий, предусмотренных ст. 272УК РФ поскольку объектом преступного посягательства является компьютерная информация, а не носители таковой.

На данный момент государство принимает различные меры по борьбе с киберпреступностью, однако не стоит забывать, что для того чтоб эта борьба была эффективной, пользователям стоит соблюдать правила безопасности в сети интернет. Не пользоваться подозрительными сайтами, не переходить по различным ссылкам, которые пользуются популярностью в инстаграмм и т.д.

Ключевые слова: киберпреступность, фишинг, кибертерроризм.

CYBERCRIME AS A THREAT TO NATIONAL SECURITY AND REGULATORY GAPS IN CYBERSECURITY

Kucherenko A.S.

Southern Management Institute (SMI)

e-mail: super.azhela943985@ya.ru

Abstract: Cybercrime is any unlawful action in the electronic sphere that improves with the help of computer technology, or against them.

There are 5 types of cybercrime: 1) the crime is directed 2) The right 4) copyright infringement related to content content 5) Cyberterrorism. This word refers to particularly serious crimes related to cruelty and the commission of acts of violence by means of high technology.

In the current Criminal Code of the Russian Federation there is only one chapter that will be responsible for cybercrime "Crime in the field of computer information" and contains three articles defining the liability for malicious software and hardware actions. (Article 272-274 of the Criminal Code of the Russian Federation). However, if we refer to Art. 272 of the Criminal Code in accordance with the law on intellectual property, if this act entailed its destruction, blocking, modification or copying. It should be noted that physical damage to the computer, which caused the destruction of information stored in it, does not entail consequences, 272UK RF for the object of criminal assault is computer information, and not carriers of that.

At the moment, the state takes various measures to combat cybercrime, but do not forget that in order for this fight to be effective, users should follow the security rules on the Internet. Do not use suspicious sites, do not navigate through various links that are popular in instagrams, etc.

Keywords: cybercrime, phishing, cyberterrorism.

Киберпреступность - это любое незаконное действие в электронной сфере, которое совершено с помощью компьютерных технологий, либо против них.

Довольно часто специалисты в области компьютерных технологий используют свитч. С его помощью можно подключить несколько компьютеров в сеть.

Существует 5 разновидностей киберпреступлений: 1)преступление направленное на базу данных пользователя ПК. К примеру, это взлом базы данных мобильных операторов, с целью получения паспортных данных пользователей. 2) Фишинг, одним словом преступления с помощью технологий, с целью извлечения экономической выгоды (данные банковских карт, электронных кошельков и т.д.) 3) Правонарушения, связанные с содержанием контента (распространение порнографии) 4) Нарушение авторских прав (распространение видеоролика (с целью получения выгоды) с присваиванием его авторства). 5) Кибертерроризм. Таким словом называют особо серьезные преступления, связанные с жестокостью и совершением актов насилия посредством высоких технологий. Также к этому виду относят

деяния, которые ставят под угрозу общественную безопасность. Пример – взлом NASA. Такое происходило однажды, и к счастью виновник не имел злого умысла, в противном случае он мог бы поставить под угрозу национальную безопасность США (например, если продать засекреченные государственные сведения враждебным государствам или террористическим группировкам).

Обычные сотрудники полиции не обладают должными знаниями в области компьютерной техники, поэтому власти нашей страны были вынуждены создать отдельный отдел по выявлению и борьбе преступлений в сфере компьютерных технологий. Задачи данного подразделения следующие: борьба с нарушением авторских прав; обнаружение незаконных проникновений в базы данных; выявление создания поддельных кредитных карт; борьба с незаконными подключениями к АТС; обнаружение неправильной эксплуатации систем ЭВМ; борьба с распространением порнографии в интернете и через съемные носители.

В действующем УК РФ существует только одна глава, которая предусматривает ответственность за киберпреступления «Преступления в сфере компьютерной информации» и содержит три статьи определяющие ответственность по вредоносным программно-техническим действиям. (ст. 272-274 УК РФ). Однако, если обратиться к ст. 272 УК РФ то в ней четко предусмотрена ответственность за неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло ее уничтожение, блокирование, модификацию либо копирование. Следует отметить, что физическое повреждение компьютера, повлекшее уничтожение информации, хранящейся в нем, не влечет за собой последствий, предусмотренных ст. 272УК РФ поскольку объектом преступного посягательства является компьютерная информация, а не носители таковой.

На данный момент государство принимает различные меры по борьбе с киберпреступностью, однако не стоит забывать, что для того, чтобы эта борьба была эффективной, пользователям стоит соблюдать правила

безопасности в сети интернет. Не пользоваться подозрительными сайтами, не переходить по различным ссылкам, которые пользуются популярностью в инстаграмм и т.д.

Библиографический список:

1. Уголовный кодекс Российской Федерации" от 13.06.1996 N 63-ФЗ (ред. от 19.02.2018). – Режим доступа: http://www.consultant.ru/
2. Приказ Генпрокуратуры России от 14.09.2017 N 627 "Об утверждении Концепции цифровой трансформации органов и организаций прокуратуры до 2025 года". - Режим доступа: http://www.consultant.ru/