УДК 004 : 37.02

С. Д. Капустина,
факультет математики, информатики, физики и технологии,
Омский государственный педагогический университет
Научный руководитель: канд. пед. наук Т. В. Аршба

Основные виды киберпреступлений и инструменты для борьбы с ними

Аннотация. В статье рассмотрены основные виды современных киберпреступлений, степень их воздействия на киберпространство и людей. Автор приводит примеры актуальных и часто встречающихся схем киберпреступлений в цифровом мире, рассматривает способы, используемые злоумышленниками для незаконного доступа к компьютерным и мобильным устройствам, а также обобщает методы борьбы с ними.

Ключевые слова: цифровизация, киберпространство, киберпреступления, киберугрозы, информационнаяй цифровая среда.

Жизнь современного школьника невозможно представить без использования информационных технологий и интернета. Ежедневно ученики решают огромное количество задач в киберпространстве, «представляющем собой некоторое цифровое пространство, которое существует благодаря компьютеру и информационным технологиям» [2]. Таким образом, можно говорить о том, что часть жизни современного школьника осуществляется в информационной цифровой среде.

С каждым днем в киберпространстве увеличивается число киберугроз, с помощью которых злоумышленники могут затруднять работу пользователей, использовать ценную информацию в корыстных целях, а также осуществлять попытки разрушения целостности компьютерной системы. В связи с этим появляется необходимость в обучении школьников основам кибербезопасности. Зачастую в школьных учебниках информатики этот аспект не освещен полностью, и ученики не знают, какие новые виды опасностей могут быть в интернете, какие способы обмана существуют и какие средства защиты нужно использовать.

Киберпреступление всегда подразумевает под собой некоторую преступную деятельность, цель которой — кибератака на компьютеры с использованием вирусов и вредоносного программного обеспечения, а также персонального компьютера для совершения преступления [3].

Можно выделить несколько видов киберпреступлений: незаконный доступ к информации или компьютерным средствам, незаконный перехват данных, вмешательство в данные или систему [1].

Существует огромное количество схем мошенников, которые они используют для достижения цели. Рассмотрим некоторые из наиболее популярных мошеннических схем.

1. *Интернет-мошенничество с помощью сайтов-двойников*. Этот вид интернет-преступления является очень распространенным. Он представляет собой создание фишинговых сайтов — двойников официальных сайтов. Такой способ преступлений очень часто применяется для различных маркетплейсов, стриминговых сайтов и других приложений, где нужно вводить личные данные или оформлять подписку. С помощью обмана мошенники получают конфиденциальную информацию и могут использовать ее в корыстных целях.

2. *Письма помощи в социальных сетях.* Этот способ обмана в интернете является наиболее распространенным видом мошенничества. Он заключается в том, что злоумышленник осуществляет взлом страницы и с помощью писем с просьбой о помощи вымогает деньги или ценную информацию у знакомых пользователя.

3. *Преступления, связанные с онлайн-играми.* Многие подростки XXI в. очень много времени проводят в сети, играя в компьютерные игры. В данных играх присутствует система улучшений персонажа. Часто любители игр стремятся заполучить данные для улучшения более дешевым способом, для этого они ищут различные сайты, где услуга предоставляется за меньшую цену. Затем мошенник просит предоплату, а после не выполняет условия договора и обманным путем заполучает деньги.

4. *Интернет-преступления, связанные с мобильными устройствами.* Современные пользователи

мобильных устройств очень часто устанавливают различные приложения на свой телефон. Эти приложения могут понадобиться им для учебы, работы или личного пользования. Однако очень часто под видом обычного приложения пользователь может скачать вредоносную программу, с помощью которой злоумышленник воспользуется личными данными человека.

5. *Интернет-преступления, связанные с кражей онлайн-личности.* Зачастую кибермошенники могут использовать личные данные человека, полученные с помощью хакерской атаки, в корыстных целях. Например, злоумышленники, которые пользуются вашими конфиденциальными данными, могут получить доступ к информации о ваших налогах, заработной плате, месте работы. С помощью ваших данных они могут пользоваться различными государственными сайтами, где могут запросить государственные льготы или оформить кредит на ваше имя. Данный вид киберпреступлений очень опасен, поскольку мошенникам становятся доступны различные способы влияния на человека.

6. *Интернет-преступления, связанные с онлайн-покупками и доставкой.* В современном мире пользователи очень часто заказывают различные товары из интернета, что позволяет киберпреступникам придумывать новые схемы мошенничества. Одним из способов обмана в цифровом мире является поддельное письмо, отправляемое мошенниками от лица представителей онлайн-магазина, цель которого — проверка статуса доставки. В данном письме содержится ссылка на вредоносный ресурс или вредоносную программу, с помощью которой преступник может произвести хищение личной конфиденциальной информации.

7. *Интернет-преступления, связанные с размещением рекламы на сайте продаж.* В современном мире люди очень часто размещают рекламу о продаже каких-либо товарах на различных интернет-сайтах. Злоумышленники соглашаются на покупку товара и отправляют чек с суммой, которая превышает стоимость. Затем они требуют вернуть разницу и пропадают. Вскоре продавец понимает, что чек фальшивый, но деньги вернуть не может.

Существует огромное количество сценариев для совершения киберпреступлений, с каждым днем мошенники меняют свои схемы, улучшают их и продолжают обманывать пользователей. В связи с этим появляется необходимость в изучении различных способов защиты от данных киберугроз.

Для того чтобы не стать жертвой киберпреступления, необходимо соблюдать ряд мер: использовать лицензионное программное обеспечение, а также антивирусные программы; использовать сложные пароли и двухфакторную аутентификацию при работе в социальных сетях; проверять адрес сайта, не вводить личные данные при посещении подозрительных сайтов, не переходить по подозрительным ссылкам и не открывать вложенные файлы от неизвестных отправителей.

Подводя итоги вышесказанного, можно сделать выводы о том, что в условиях изменяющегося цифрового пространства необходимо знать способы обмана пользователей в интернете и уметь предотвращать данные киберугрозы.

1. *Вангородский С. Н.* Основы кибербезопасности : учеб.-метод. пособие. 5–11 классы. — М. : Дрофа, 2019. — 238 с.

2. *Цветкова М. С., Хлобыстова И. Ю.* Информационная безопасность. Кибербезопасность. 7–9 классы : учеб. пособие. — 2-е изд., пересмотр. — М. : БИНОМ. Лаборатория знаний, 2020. — 64 с.

3. Что такое кибепреступность? Защита от киберпреступности // Лаборатория Касперского : [сайт]. — URL: https://www.kaspersky.ru/resource-center/threats/what-is-cybercrime (дата обращения: 16.03.2023).