КИБЕРПРЕСТУПНОСТЬ В ОТНОШЕНИИ НЕСОВЕРШЕННОЛЕТНИХ

Бурова Азалия Ильдаровна

студент, Елабужский институт (филиал) федерального государственного автономного образовательного учреждения высшего образования Казанский (Приволжский) федеральный университет, РФ, г. Елабуга

Нуриева Алеся Радиевна

научный руководитель, старший преподаватель, Елабужский институт (филиал) федерального государственного автономного образовательного учреждения высшего образования Казанский (Приволжский) федеральный университет, РФ, г. Елабуга

Аннотация. Какая киберпреступность совершается в отношении несовершеннолетних? Какие виды защиты существуют от данного преступления? Разберем поставленные вопросы и изучим данную тему в деталях. Киберпреступность один из самых популярных видов преступлений на сегодняшний день. Виды существующих киберпреступлений в отношении несовершеннолетних.

Ключевые слова: киберпреступление, кибербезопасность, дети.

1. Виды совершаемых киберпреступлений.

В настоящее время мы часто становимся свидетелями киберпреступлений которые совершаются в отношении детей и людей преклонного возраста. Для того чтобы найти истину мы должны определиться с термином «киберпреступность».

Термин киберпреступность означает любую преступную активность, где объектом в качестве цели и инструмента является компьютер или любое сетевое устройство. Достаточно много различных видов преступления на просторах интернета, которые так или иначе имеют схожести в манерах преступления. Сейчас расскажем о основных видах и категориях киберпреступлениях.

Киберпреступность, бесспорно, занимает в современном криминальном мире одно из лидирующих видов преступлений.

Целью киберпреступлений является получение прибыли. Получение прибыли делиться на 2 категории. Первое извлечение прибыли с продажи той или иной информации (баз данных), или получения. Второе похищение денежных средств со счетов и карт. Путей обоих видов бессчётное множество.

Киберпреступления можно разделить на две категории:

Первая категория	Вторая категория
Криминальная деятельность, целью которой являются сами	Киберпреступления в которых использу

компьютеры. В данном случае преступники используют вирусы и другие типы вредоносных программ, чтобы заразить компьютеры и таким образом повредить их или остановить их работу. Также с помощью троянов можно удалять или похищать данные.	или сети для распространения вредоно нелегальной информации или нера изображений.

Киберпреступления, в результате которых владельцы устройств не могут пользоваться своими компьютерами или сетью, а компании - предоставлять интернет-услуги своим клиентам, называется атакой отказа в обслуживании (DoS).

В европейской конвенции о киберпреступности названы виды деятельности с использованием компьютеров, которые считаются киберпреступлениями, к ним относятся: социальные и политически мотивированные киберпреступления, преступления на почве ненависти и домогательств, кибертерроризм, кибербуллинг, незаконный перехват или кража данных, компрометация компьютерных систем и сетей, продажа незаконных продуктов.

Теперь, когда ознакомились с термином «киберпреступления», вернемся к теме статьи. И опишем категории преступлений, которым наиболее подвержены несовершеннолетние.

2. Социальные и политически мотивированные киберпреступления.

Этим видом преступления направлен на изменения настроений в политической сфере, чтобы поднять общество к тем или иным действиям или поднять влияние тех или иных людей, партий, стран. В последнее время часто слышим, что несовершеннолетние граждане попали под вражескую агитацию в силу своего возраста, неопытности и отсутствия информированности от попечителей, они распространяют фейки *((англ. **fake** — подделка) — что-либо ложное, недостоверное, сфальсифицированное, выдаваемое за действительное)* в социальных сетях в отношении нашего государства.

Из-за данного преступления в большинстве своем ответственность несут законные представители ребенка в виде: лишения родительских прав, административных и уголовных преследований.

3. Преступления на почве ненависти и домогательств. Кибербуллинг.

Также дети часто становятся жертвами преступлений на почве ненависти по отношению к личности или группе людей, которым относятся их родители и они сами. Обычно совершаются на основе гендерной, расовой, религиозной, национальной принадлежности, сексуальной ориентации и других отличительных признаков. Примеры: домогательства и рассылка оскорбительных сообщений и взброс ложных новостей, касающихся определенной группы или определенного лица.

Из-за данного преступления многие дети начинают иметь проблемы с психологическим здоровьем, замыкаются в себе, начинают стыдиться себя.

Самый популярный вид киберпреступления в отношении детей, который часто совершается самими детьми. Интернет-травля или кибербуллинг — намеренное оскорбления, угрозы, диффамации и сообщение другим компрометирующих данных с помощью современных средств коммуникации, как правило, в течение продолжительного периода времени незаконный перехват или кража данных.

Как упомянуто выше одно из самых опасных видов киберпреступлений в отношении детей, способное не просто сломить дух и психологическое здоровье ребенку, но и довести до летального исхода, как саму жертву, так и его окружающих, которых потерпевший воспримет как его личных обидчиков.

4. Методы борьбы с киберпреступностью. Борьба с киберпреступностью с стороны Государства.

Борьба с киберпреступностью в наши дни - не миф, а суровая реальность, с которой нужно бороться. Уже давно прошли те времена, когда спецслужбы не знали каким способом подступиться к данным правонарушениям. Да, конечно, они не дошли до того, чтобы полностью контролировать киберпреступность, поэтому число киберпреступлений, с каждым днем растет, но все эти преступления мелочные, а все весомые преступления не остаются безнаказанными.

В нашей стране за киберпреступлениями следит отдел «К».

Управление «К» отдел МВД России, осуществляющий борьбу с компьютерными преступлениями и незаконным оборотом РЭС (радиоэлектронных средств). Управление «К», находясь в составе ГУВД субъекта РФ, выявляет, предупреждает, пресекает и раскрывает преступления в сфере информационных технологий, незаконного оборота РЭС, специальных технических средств СТС и детской порнографии.

Задачи управления «К»:

- борьба с нарушением авторских и смежных прав (ст. 146 УК РФ,ст. 7.12 КоАП РФ);
- выявление незаконного проникновения в компьютерную сеть (ст. 272 УК РФ), борьба с распространителями вредоносных программ (ст. 273 УК РФ);
- выявление нарушений правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 274 УК РФ);
- выявление использования подложных кредитных карт (ст. 159 УК РФ);
- борьба с распространением порнографии посредством сети Интернет и Компакт-дисков (ст. 242 УК РФ);
- выявление незаконного подключения к телефонным линиям (ст. 165 УК РФ, ст. 13.2 КоАП РФ);

5. Рекомендации по борьбе с киберпреступностью.

1. Рекомендация по борьбе с киберпреступностью с стороны опекунов несовершеннолетних.

Для того чтобы осуществлять контроль над детьми, нужно самим разбираться в данной теме. На сегодняшний день имеется много книг и методических указаний, соответствующих ФГОС.

Для ограждения ребенка от киберпреступлений нужно установить на всех устройствах, которыми пользуется он родительский контроль. Безусловно, данная программа не способна защитить ребенка от всех опасных факторов, поэтому нужно лично проверять материалы, которые изучает несовершеннолетний.

Очень важно уделять ребенку свое время и научить выявлять опасный контент, делиться опытом из жизни.

2. Рекомендация по борьбе с киберпреступностью с стороны педагогов.

Для предотвращения появления пострадавших от киберпреступлений среди обучающихся. Нужно проводить тесты по информационной грамотности подопечных в период указанном в ФГОС. Так же проводить открытые уроки, игры для повышения информационной грамотности детей. В случае неудовлетворительных результатов сообщить родителям и объяснить серьезность ситуации. В случае появления пострадавших среди обучающихся, необходимо связаться с родителями и решить проблему совместными усилиями.

Вывод:

Киберпреступность и кибертерроризм являются объективным следствием глобализации информационных процессов и появления глобальных компьютерных сетей. С ростом

использования информационных технологий в различных сферах деятельности человека растет и использование их в целях совершения преступлений.

Необходимость защиты детей от киберпреступников очевидна. Желательно, чтобы совместными усилиями решалась данная проблема, на доверительных отношениях с ребёнком, чтобы он знал, что родитель поможет в данной ситуации. А также на уровне государства решались проблемы борьбы с киберпреступлениями, а повсеместно преподаватели проводили работу с обучающимися по разъяснению опасности от киберпреступников, по умению определять возможную угрозу.

Кибербезопасность детей в наших руках! Мы за безопасность использования информационного пространства.

Список литературы:

1. «Информационно-коммуникационные технологии в дошкольном образовании», Комарова Тамара Семеновна, Туликов Алексей Викторович, 2013г.

2. «Как противостоять хакерским атакам. Уроки экспертов по информационной безопасности», Роджер Граймс, 2023г.

3. «Линия защиты: как Минцифры хочет развивать кибербезопасность в России до 2035 года», Роман Рожков и Анастасия Гаврилюк, Редакция Forbes, 2023г.

4. Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации: «Информационная безопасность», 2021г, https://digital.gov.ru/ru/activity/directions/874