КИБЕРПРЕСТУПЛЕНИЯ В СОЦИАЛЬНЫХ СЕТЯХ

Викулина Д.Д.,
студентка 3 курса ВГУ имени П.М. Машерова, г. Витебск, Республика Беларусь
Научный руководитель – Сухарев А.А., канд. пед. наук, доцент

Киберпреступления в социальных сетях стали одной из наиболее актуальных проблем в современном мире. С развитием интернета и социальных медиаплатформ количество преступлений, связанных с ними, значительно выросло. Киберпреступники используют социальные сети для различных видов атак, в том числе для кражи личной информации, мошенничества и даже террористической пропаганды. Цель данной научной работы – исследовать виды киберпреступлений в социальных сетях, их влияние на дестабилизацию информационной безопасности и правовую культуру населения и способы их предупреждения и пресечения.

Материал и методы. Материалом для исследования являются нормативные правовые акты Республики Беларусь; статистические данные МВД Республики Беларусь в данной области. При этом использовались общенаучные методы, а также формально-юридический и метод конкретного правового анализа.

Результаты и их обсуждение. С развитием технологий и доступности интернета, социальные сети стали неотъемлемой частью жизни многих людей. Однако, с ростом популярности социальных сетей, также растет и число киберпреступлений, совершаемых через них, ведь новые технологии порождают и новые преступления. Согласно исследованиям Государственного комитета судебных экспертиз сегодня 1/4 часть всех преступлений совершается с использованием IT-технологий [1]. Общая статистика МВД Республики Беларусь говорит о том, что из года в год регистрируется все большее количество киберпреступлений. Так, на момент 2019 года количество зарегистрированных преступлений, совершенных в сети Интернет, составляло около 10 тысяч, позже в 2020 году выросло в 2,5 раза (в том числе из-за нахождения общества в условиях пандемии). В последние 2-3 года статистика также остается неизменной и, несмотря на все действия правоохранительных органов, количество преступлений возрастает (в 2022 году число киберпреступлений составляло 14,8 тысяч, а на момент 2023 года – 15,7 тысяч) [2].

Кибербуллинг, кибермошенничество, кража личных данных – лишь некоторые из видов преступлений, которые процветают в социальных сетях. Некоторые из разновидностей киберпреступлений (фишинг, смишинг, фарминг, брутфорс) и вовсе непонятны простому обывателю, что ещё больше повышает риск обычных граждан стать жертвой мошенников и способствует распространению преступлений с использованием компьютерных систем и информационных технологий [3]. Последствия таких преступлений могут быть катастрофическими для жертв – от утраты денежных средств и личной информации до психологических проблем и суицидов. Именно поэтому сотрудники правоохранительных органов в ходе различных профилактических встреч с гражданами рекомендуют оставаться бдительными и всеми способами следить за сохранностью своих данных в социальных сетях (не сообщать конфиденциальную информацию по телефону, не отвечать на звонки с трансграничных номеров, не переходить по незнакомым ссылкам и не доверять подозрительным и непроверенным интернет-источникам) [1].

Острой проблемой для разрешения вопросов, связанных с кибербезопасностью, является недостаточный уровень изученности самого понятия «киберпреступление», ведь ни в одном документе оно не закреплено на официальном уровне. Так, система оценки МВД предусматривает преступления, которые подлежат учету по линии подразделения по раскрытию преступлений в сфере высоких технологий. Это относительно узкое направление, поэтому перечень статей, предусмотренных УК Республики Беларусь в их отношении не так велик: хищение имущества путём модификации компьютерной ин-

формации (ст. 212), несанкционированный доступ к компьютерной информации (ст. 349), уничтожение, блокирование или модификация компьютерной информации (ст. 350), неправомерное завладение компьютерной информацией (ст. 352), разработка, использование, распространение либо сбыт вредоносных компьютерных программ или специальных программных или аппаратных средств (ст. 354), нарушение правил эксплуатации компьютерной системы или сети (ст. 355). Помимо этого, в УК содержатся статьи, предусматривающие ответственность за оскорбление и клевету Главы государства и представителя власти (ст. 367-369), распространение заведомо ложных сведений о политическом, экономическом, социальном, военном или международном положении Республики Беларусь, правовом положении граждан в Республике Беларусь, деятельности государственных органов, Вооруженных Сил Республики Беларусь и др. (ст. 369^1), размещенные в том числе в сети интернет [4]. На наш взгляд, можно использовать правовой опыт Российской Федерации, в УК которой отдельными составами преступлений против информационной безопасности являются неправомерное воздействие на критическую информационную инфраструктуру государства, нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования на территории России.

Помимо этого, актуальной является проблема обеспечения электорального суверенитета во время избирательных кампаний, так как в настоящее время активно для агитационной деятельности используются и соцсети, в том числе для вброса фейковой информации. В связи с вышесказанным, тема киберпреступлений в социальных сетях и сети интернет в современных условиях является актуальной для изучения и представляет собой научный и практический интерес. Представляется необходимым детальное исследование механизмов, используемых киберпреступниками, с целью обеспечения наиболее эффективных способов защиты в интернет-пространстве.

В настоящее время эффективными методами борьбы с киберпреступлениями в социальных сетях является обучение пользователей основам кибербезопасности, регулярные семинары и курсы по защите личной информации в интернете, развитие технологий и программных средств для обнаружения и предотвращения подобных преступлений.

Заключение. Таким образом, киберпреступления – правонарушения, непосредственно связанные с использованием компьютерных технологий и сети интернет – приобрели транснациональный характер, так как они подпадают под все критерии, предусмотренные Конвенцией ООН против транснациональной организованной преступности от 15.11.2000 года, участницей которой является и Республика Беларусь. Постоянный рост киберпреступлений в социальных сетях – серьезная проблема, которая требует комплексного подхода к решению. Обучение пользователей кибербезопасности, развитие технологий для предотвращения атак и сотрудничество социальных сетей с правоохранительными органами – все эти меры необходимы для борьбы с этим явлением, поскольку именно так граждане смогут повысить свой уровень осведомленности в данной сфере, а также противостоять кибермошенникам.

1. Киберпреступность в Беларуси [Электронный ресурс]. – Режим доступа: https://brest.mvd.gov.by/ru/news/126. – Дата доступа: 15.03.2024.

2. В Беларуси с начала 2023 года зафиксировано 15,7 тыс. киберпреступлений [Электронный ресурс]. – Режим доступа: https://www.belta.by/society/view/v-belarusi-s-nachala-2023-goda-zafiksirovano-157-tys-kiberprestuplenij-605224-2023/. – Дата доступа: 14.03.2024.

3. Как судебные эксперты помогают раскрывать киберпреступления [Электронный ресурс]. – Режим доступа: https://www.belta.by/interview/view/najdem-sledy-dazhe-esli-ih-zametali-kak-sudebnye-eksperty-pomogajut-raskryvat-kiberprestuplenija-7759/. – Дата доступа: 14.03.2024.

4. Уголовный кодекс Республики Беларусь [Электронный ресурс]: 9 июля 1999 г. № 275-З: в ред. от 09.03.2023 № 256-З // ЭТАЛОН. Законодательство Республики Беларусь / Национальный центр правовой информации Республики Беларусь. – Минск, 2024.

5. Козел, А. Н. Криминалистическая характеристика киберпреступлений [Электронный ресурс] / Козел А. Н.; науч. рук. Алхимина И. А. // XVII Машеровские чтения: материалы международной научно-практической конференции студентов, аспирантов и молодых ученых, Витебск, 20 октября 2023 г.: в 2 т. – Витебск: ВГУ имени П. М. Машерова, 2023. – Т. 1. – С. 297-299. – URL: https://rep.vsu.by/handle/123456789/40580 (дата обращения: 15.03.2024).