ORES

Научно-практический электронный журнал
Оригинальные исследования (ОРИС), *ISSN 2222-0402*
www.ores.su
original-research.ru

УДК 343

КИБЕРПРЕСТУПНОСТЬ: БИЧ СОВРЕМЕННОГО ОБЩЕСТВА

Алиева Сабрина Нуриевна
магистрант юридического факультета
Казанский инновационный университет им. В.Г. Тимирясова
s8brina_888@mail.ru

Аннотация

В статье проанализировано современное состояние киберпреступности. Особое внимание уделено вопросам кибербезопасности несовершеннолетних в сети Интернет. Отмечено, что большинство преступлений, совершенных в отношении несовершеннолетних, носит сексуальный характер.

Ключевые слова: уголовное право, Интернет, несовершеннолетние, киберпреступность, кибербезопасность, развратные действия.

CYBERCRIME: THE SCOURGE OF MODERN SOCIETY

Sabrina N. Alieva
master's student of the Kazan Innovative University named after V. G. Timiryasov

ABSTRACT

The article analyzes the current state of cybercrime. Special attention is paid to the issues of cybersecurity of minors on the Internet. It is noted that the majority of crimes committed against minors are of a sexual nature.

Keywords: criminal law, Internet, minors, cybercrime, cybersecurity, debauchery.

За последние сто лет человечество сделало невероятный прыжок, перейдя в цифровой век своего развития. Наличие у каждого из нас собственного телефона с выходом в Интернет, персонального компьютера и других смарт-гаджетов упрощает нашу повседневную жизнь. Но вместе с этим, человека преследует и большая опасность.

Цифровизация различных процессов позволяет совершать общественно опасные деяния на удалении [1].

Казалось бы, любой взрослый человек понимает, что действия в сети оставляют свой цифровой след, а такие гиганты как Google, Yandex, Yahoo и другие компилируют и используют полученную информацию по своему усмотрению. Изначально целью сбора подобных данных было получение статистики для улучшения работы интернет-сервисов, понимания работы тех или иных технологических функций, но сейчас многие интернет-корпорации имеют доступ к личным данным людей, что, в свою очередь, может

приводить к разным рискам и угрозам. Например, Google Chrome имеет доступ к платежным системам пользователя, а также сохраняет в памяти персональные данные и пароли. Это не значит, что он имеет автономный доступ к этой информации, но злоумышленники способны воспользоваться этим в своих преступных целях.

В новостях [2] и научной литературе [3-10] постоянно появляется информация о хакерских атаках на стратегически важные объекты. Самой мощной на сегодняшний день считается NotPetya/ExPetya, которая нанесла ущерба на 10 миллиардов долларов. Это бы не стало таким уничижительным событием, если бы не пострадали финансовые организации, государственные ведомства и т.д. С одной эта беда постигла сначала Европу, а потом перешла и другие зарубежные страны.

Согласно данным, предоставленным Cybersecurity Ventures, в 2019 году каждые 14 секунд происходили кибератаки. При этом, больше 56 % компаний, принявших участие в данном опросе, заявили, что у них нет планов по предотвращению хакерских взломов, а также по быстрому реагированию [11].

Наибольшая опасность таких атак является их непредсказуемость. Во-первых, не сразу ясно, каким образом был произведен взлом (к примеру, NotPetya сработал как обновление для многих программ), что стало целью и как это остановить. Во-вторых, вирус или взломанный файл могут нанести локальный ущерб, а могут «перебросится» с одной страны на другую, создав колоссальную панику. В свое время много проблем принес и «червь» WannaCry, взламывающий и шифрующий информацию на компьютерах, требуя выкуп. Но, даже после проведения оплаты пользователь оставался ни с чем, так как вирус мог только шифровать файлы.

Иногда довольно сложно понять, откуда появляются все эти проблемы, ведь современное программное обеспечение создается с множеством уровней защиты. Здесь играет роль обыкновенная человеческая неосторожность. Ведь скачивая что-то из сети Интернет, легко не заметить дополнительный файл или же отказаться от предложения антивирусной программы перепроверить те или иные данные. Такую ошибку часто допускают дети, ещё не зная и не понимая, что нужно внимательно относиться к тому, что загружается на компьютер, или чему дается доступ. Огромное количество детей ежедневно выходят в сеть Интернет [12].

Говоря о детях, нужно понимать, что это – один из наиболее уязвимых слоев общества. Из-за неокрепшей психики и неполного понимания, что стоит, а что не стоит смотреть в Интернете, с кем можно общаться, и с кем нет, злоумышленники часто выбирают их как жертв. Поскольку собственного эмпирического опыта дети данной возрастной группы ещё не имеют, им сложно понимать и осознавать намерения человека. Интернет предоставляет возможность скрыть настоящую личность, чем часто пользуются преступники, особенно в преступлениях с сексуальным подтекстом. Недавним примером стало раскрытие социальной сети педофилов Elysium, где они имели возможность обмениваться информацией разного рода. К примеру, как подобраться к ребенку, кем прикинуться и как добиться получения от несовершеннолетнего непристойных видео- или фотоматериалов [13]. МВД России предоставляет неутешительную статистику – количество сайтов с детской порнографией увеличилось на треть, а самих материалов стало больше в 25 раз [14]. Именно такое большое количество ресурсов создает иллюзию «ненаказуемости» в связи с чем преступлений против несовершеннолетних осуществляется все больше и больше.

В зарубежных странах существует понятие «кибергруминг»/«онлайн груминг» (cybergrooming/online grooming), то есть, общение с ребенком в Интернете с целью совершения развратных действий и/или склонения детей к сексуальной связи. Т.В.

Чеботарева пишет о том, что существуют различные механизмы общения с детьми, целью которого является развращение [15].

Но, к сожалению, это не худшее, что может поджидать ребенка в сети Интернет. Отечественное сообщество уже не первый год волнует вопрос «групп смерти», то есть, сообществ, в которых дети получают разные задания. Иногда это может быть нечто относительно безобидное, но, в большинстве случаев это были инциденты с летальным исходом. В Российской Федерации отсутствует статистика о причинах подростковых суицидов [16].

Присутствует в Интернете и буллинг или же, как привычнее, издевательства, на что также указывает Т. В. Чеботарева [15]. Если взрослые уже сформированы и понимают разницу между обоснованной и необоснованной критикой, то для ребенка это воспринимается в разы сложнее, оставляя след на долгое время или даже формируя травму на всю жизнь.

С точки зрения взрослого человека, издевательства выглядят не так ужасно и решаются проще, по принципу «раз ты там не нравишься – не ходи туда». Но ребенок может ввязываться в споры, углубляя конфликт и получая ещё больше негатива в свою сторону. Поэтому здесь важно, чтобы родители помогали детям работать над самооценкой, поддерживая на должном уровне. Тогда ребенок будет осознавать, что критика не обоснована и реакция не станет столь острой.

Чтобы создать более комфортные условия для пребывания детей в Интернете, стоит работать над этим с самого детства. К примеру, родителям нужно использовать функцию «родительский контроль» на тех цифровых устройствах, что есть в доме (телефоны, смарт-телевизоры, часы, персональные компьютеры и т. д.), а также объяснить, что общение в сети должно происходить с теми людьми, которые более-менее знакомы. Если даже при соблюдении таких мер происходит что-то из ряда вон выходящее – дети должны сообщать взрослым.

Внедрение цифровой грамотности должно происходить и на уровне учебных заведений. Как присутствуют уроки безопасности жизнедеятельности, так и должны иметь место уроки кибербезопасности. Это должен быть полноценный курс об правильном использовании социальных сетей, сети в целом, а также отдельных программ.

Среди прочего, в каждой школе должен присутствовать кабинет психолога. Не всегда детям и подросткам хочется рассказывать о каких-то нюансах своей жизни своим близким, а квалифицированный специалист сможет дать совет и поддержать.

Кроме этого, стоит законодательно предусмотреть ответственность за интернет-травлю, а также действия педофилов в сети. Ст. 134 и 135 УК РФ должны быть дополнены обстоятельствами, изложенными выше.

Одним из радикальных предложений, вызывающих спор в многих странах, является химическая кастрация. Но, такие страны, как США, Великобритания и некоторые европейские страны практикуют этот вид наказания уже при первом случае, тогда как в России это предусмотрено в случае повторных действий развратного характера. Более действенно это было бы, если бы применялось тогда, когда человек впервые осуществил сексуальные действия по отношению к ребенку. Согласно данным МВД России, в странах, практикующих такие методы наказания, число подобных преступлений уменьшилось. Действенным механизмом защиты может стать и реестр педофилов, благодаря которому можно будет узнать, имел тот или иной человек судимость по этой статье.

Исходя из всего вышеизложенного, можно сделать несколько выводов:

1. Наиболее уязвимые пользователи сети Интернет – дети, ведь они могут

пострадать как от сверстников, так и от взрослых.

2. Большая часть преступлений, направленных на несовершеннолетних, носит сексуальный характер.

3. Российское уголовное законодательство имеет в своем составе механизмы наказания преступников, но не имеет механизмов предупреждения.

4. Современный опыт зарубежных стран может предложить действенные инструменты защиты несовершеннолетних в сети Интернет, особенно против преступлений, совершаемых в отношении на сексуальной почве.

Список литературы

1. Бегишев И.Р. Преступления в сфере обращения цифровой информации / И. Р. Бегишев, И. И. Бикеев. – Казань : Издательство «Познание», 2020. – 300 с.
2. Greenberg A. The Untold Story of NotPetya. The Most Devastating Cyberattack in History // The WIRED. URL: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world (дата обращения: 10.02.2021).
3. Бегишев И.Р. Информационное оружие как средство совершения преступлений // Информационное право. – 2010. – № 4. – С. 23-25.
4. Бегишев И.Р. Ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей // Вестник УрФО. Безопасность в информационной сфере. – 2012. – № 1(3). – С. 15-18.
5. Бегишев И.Р. Уголовная ответственность за приобретение или сбыт цифровой и документированной информации, заведомо добытой преступным путем // Актуальные проблемы экономики и права. – 2010. – № 1. – С. 123-126.
6. Бегишев И.Р. Проблемы ответственности за незаконные действия с информацией, заведомо добытой преступным путем // Безопасность информационных технологий. – 2010. – Т. 17. – № 1. – С. 43-44.
7. Бегишев И.Р. Ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей // Вестник УрФО. Безопасность в информационной сфере. – 2012. – № 1(3). – С. 15-18.
8. Бегишев И.Р. Проблемы уголовной ответственности за обращение со специальными техническими средствами, предназначенными для негласного получения информации // Следователь. – 2010. – № 5. – С. 2-4.
9. Бегишев И.Р. Безопасность критической информационной инфраструктуры Российской Федерации // Безопасность бизнеса. – 2019. – № 1. – С. 27-32.
10. Бегишев И.Р. Проблемы противодействия преступным посягательствам на информационные системы критически важных и потенциально опасных объектов // Информационная безопасность регионов. – 2010. – № 1(6). – С. 9-13.
11. Top 5 Cybersecurity Facts, Figures, Predictions, And Statistics For 2020 To 2021 // Cybersecurity Ventures. URL: https://cybersecurityventures.com/top-5-cybersecurity-facts-figures-predictions-and-statistics-for-2019-to-2021 (дата обращения: 10.02.2021).
12. Смирнов А.А. Виктимологическая профилактика преступлений против половой неприкосновенности несовершеннолетних, совершаемых с использованием сети интернет // Актуальные вопросы публичного права. – 2012. – № 11(11). – С. 37-46.
13. Вачедин Д. В Германии раскрыли сеть педофилов из 30 тысяч человек // Meduza. URL: https://meduza.io/feature/2020/07/06/v-germanii-raskryli-set-pedofilov-iz-30-

tysyach-chelovek-vlasti-priznayut-chto-lish-nemnogie-iz-nih-budut-naydeny-i-osuzhdeny (дата обращения: 10.02.2021).
14. Госдума ратифицировала международные договоры о защите детей // РИА-новости. URL: http://ria.ru/politics/20130426/934746783.html (дата обращения: 10.02.2021).
15. Чеботарева Т.В. Интернет-безопасность несовершеннолетних: миф или реальность // Сборник научных статей по материалам Всероссийской научной Интернет-конференции, посвященной 85-летию СГЮА 2-11 апреля 2016 г. «Информационные технологии и право». С. 258-264.
16. Лукашук А.В., Филиппова М.Д., Сомкина О.Ю. Характеристика детских и подростковых суицидов // Российский медико-биологический вестник имени академика И.П. Павлова. – 2016. – Т. 24. – № 2. – С. 137-143.

References

1. Begishev I. R. Crimes in the sphere of digital information circulation / I. R. Begishev, I. I. Bikeev. - Kazan: Publishing house «Cognition», 2020. - 300 p.
2. Greenberg A. The Untold Story of NotPetya. The Most Devastating Cyberattack in History // The WIRED. URL: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world (date accessed: 10.02.2021).
3. Begishev I. R. Information weapons as a means of committing crimes / / Information Law. - 2010. - No 4. - P. 23-25.
4. Begishev I. R. Responsibility for violation of the rules of operation of means of storage, processing or transmission of computer information and information and telecommunications networks // Bulletin of the Ural Federal District. Security in the information sphere. - 2012. - No 1(3). - P. 15-18.
5. Begishev I. R. Criminal liability for the acquisition or sale of digital and documented information, knowingly obtained by criminal means / / Actual problems of economics and law. - 2010. - No 1. - P. 123-126.
6. Begishev I. R. Problems of responsibility for illegal actions with information knowingly obtained by criminal means / / Security of information technologies. - 2010. - Vol. 17. - No 1. - P. 43-44.
7. Begishev I. R. Responsibility for violation of the rules of operation of storage, processing or transmission of computer information and information and telecommunications networks // Bulletin of the Ural Federal District. Security in the information sphere. - 2012. - No 1(3). - P. 15-18.
8. Begishev I. R. Problems of criminal liability for handling special technical means intended for secret receipt of information / / Investigator. - 2010. - No 5. - P. 2-4.
9. Begishev I. R. Security of critical information infrastructure of the Russian Federation / / Business Security. - 2019. - No 1. - P. 27-32.
10. Begishev I. R. Problems of countering criminal encroachments on information systems of critical and potentially dangerous objects / / Information security of regions. - 2010. - No 1(6). - P. 9-13.
11. Top 5 Cybersecurity Facts, Figures, Predictions, And Statistics For 2020 To 2021 / / Cybersecurity Ventures. URL: https://cybersecurityventures.com/top-5-cybersecurity-facts-figures-predictions-and-statistics-for-2019-to-2021 (date accessed: 10.02.2021).
12. Smirnov A. A. Victimological prevention of crimes against sexual inviolability of minors committed with the use of the Internet / / Actual issues of public law. - 2012. - No 11(11). - P. 37-46.

13. Vachedin D. In Germany, a network of pedophiles from 30 thousand people was revealed // Meduza. URL: https://meduza.io/feature/2020/07/06/v-germanii-raskryli-set-pedofilov-iz-30-tysyach-chelovek-vlasti-priznayut-chto-lish-nemnogie-iz-nih-budut-naydeny-i-osuzhdeny (date accessed: 10.02.2021).
14. The State Duma has ratified international treaties on the protection of children. URL: http://ria.ru/politics/20130426/934746783.html (date accessed: 10.02.2021).
15. Chebotareva, T. V., Internet child safety: myth or reality // Collection of scientific articles on the materials of all-Russian scientific Internet-conference dedicated to the 85th anniversary SHUA 2-11, 2016 «Information technology and law». P. 258-264.
16. Lukashuk A. V., Filippova M. D., Sakina O. Y. Characteristics of child and adolescent suicide // Rossijskij mediko-Biologicheskiy Vestnik imeni Akademika I. P. Pavlova. - 2016. - Vol. 24. - No 2. - P. 137-143.