ЮРИДИЧЕСКИЕ НАУКИ

ПРОТИВОДЕЙСТВИЕ КИБЕРПЕСТУПНОСТИ[1]

Антонян Елена Александровна
Доктор юридических наук, профессор кафедры криминологии и уголовно-исполнительного права Московского государственного университета имени О.Е. Кутафина (МГЮА)
Бархатова Елена Валерьевна
пеподаватель кафедры криминологии и уголовно-исполнительного права Московского государственного университета имени О.Е. Кутафина (МГЮА)
DOI: 10.31618/ESU.2413-9335.2019.4.64.239

АННОТАЦИЯ

В статье рассматриваются вопросы информационной безопасности в условиях угроз, которые несет киберпреступность. Немсмотря на то, множество информации в киберпространстве представляет огромное значение для индивидов, организаций, компаний, стран и способна изменить будущее, судьбы и жизни, необходимо охрана такой информации с использованием для этого всех возможных форм защиты. В статье отражены промежуточные результаты исследования, выполненного при финансовой поддержке РФФИ в рамках научного проекта № 18-29-16175

Метод. Диалектический, логический (анализ и синтез, индукция и дедукция). Также использовались частно-научные методы познания (формально-юридический, сравнительно-правовой, исторический) и специальные методы исследования (статистический метод).

Результат. Изучение законодательства, практики его применения показывает, что ведущие страны мира, ведущие борьбу с кибепреступностью, остаются все еще уязвимыми в плане обеспечения национальной безопасности от киберугроз.

Выводы. Основные меры противодействия кибепреступности на национальном уровне: принятие законов, стратегий противодействия киберпреступности, эффективное руководство, развитие потенциала органов уголовного правосудия и правоохранительных органов, информационно-просветительская деятельность, создание прочной базы знаний, сотрудничество между органами государственного управления и частным сектором.

Цель. Изучить и дать оценку отдельным аспектам борьбы с кибепреступностью на примере практики применения законодательства в данной сфере в России и США.

ANNOTATION

The article discusses information security issues in the face of threats posed by cybercrime. Despite the fact that a lot of information in cyberspace is of great importance for individuals, organizations, companies, countries and is able to change the future, destiny and life, it is necessary to protect such information using all possible forms of protection. The article reflects the interim results of a study carried out with the financial support of the Russian Foundation for Basic Research in the framework of the research project No. 18-29-16175

Method. Dialectical, logical (analysis and synthesis, induction and deduction). Also used private-scientific methods of knowledge (formal legal, comparative legal, historical) and special methods of research (statistical method).

Result. A study of the legislation and the practice of its application shows that the leading countries in the world fighting cybercrime are still vulnerable in terms of national security from cyber threats.

Findings. Basic cybercrime responses at the national level: adoption of laws, strategies to counter cybercrime, effective governance, capacity building of criminal justice and law enforcement agencies, awareness-raising activities, building a solid knowledge base, cooperation between government and the private sector.

Purpose. To study and assess individual aspects of the fight against cybercrime on the example of the practice of applying legislation in this field in Russia and the United States.

Ключевые слова: киберпреступность, меры противодействия киберпреступности, хакер, предупреждение, меры противодействия.

Keywords: cybercrime, countermeasures to cybercrime, hacker, prevention, countermeasures.

В современном мире информация представляет собой один из самых ценных ресурсов. Но, среди терабайтов данных находится и множество информации, представляющей весомое значение для индивидов, организаций, компаний, стран, способной изменить будущее,

[1] Исследование выполнено при финансовой поддержки РФФИ в рамках научного проекта № 18-29-16175 «Блокчейн технологии противодействия рискам кибертерроизма и киберэкстремизма: криминолого-правовое исследование»

судьбы и жизни. Возникает вопрос об охране такой информации, о использовании для этого всех возможных форм защиты.

Сегодня ни государства, ни компании, ни пользователи не используют большинство доступных способов защиты данных. Чтобы проанализировать ситуацию, стоит рассмотреть существующие меры защиты информации на примерое известных кибератак.

Вопросами поиска оптимальных мер в области предупреждения киберпреступности занимаются правоохранительные органы практически всех стран мира. Мы видим, наблюдающийся в последние годы, высокий уровень активности в принятии международных и национальных документов, направленных на противодействие киберпреступности, что связано с повышением количества преступлений в данной сфере, в особенности, кибертерроризма.

На национальном уровне предупреждение преступности состоит из стратегий и мероприятий, направленных на снижение риска совершения преступлений и нейтрализацию потенциально вредных последствий для частных лиц и общества. Так, в Доктрине информационной безопасности РФ особое внимание уделяются тому факту, что информационные технологии приобрели глобальный трансграничный характер и стали неотъемлемой частью всех сфер деятельности личности, общества и государства[1].

К числу основных мер относятся: принятие законов, стратегий противодействия киберпреступности, эффективное руководство, развитие потенциала органов уголовного правосудия и правоохранительных органов, информационно-просветительская деятельность, создание прочной базы знаний, сотрудничество между органами государственного управления и частным сектором. Безусловно, немаловажным фактором является надлежащее отношение к соответствующей компьютерной информации, которая представляет собой определенный интерес для другого субъекта, ограничение доступа к такой информации при помощи использования лицензированных компьютерных программ и антивирусных софтов для защиты компьютера от незаконного взлома.

Возрастающие масштабы компьютерной преступности, прежде всего в кредитно-финансовой сфере, увеличивает число преступлений, связанных с нарушением конституционных прав и свобод человека и гражданина, в том числе, в части, касающейся неприкосновенности частной жизни, личной и семейной тайны, при обработке персональных данных с использованием информационных технологий. При этом методы, способы и средства совершения таких преступлений становятся более изощренными[1].

Изучение ситуацию показывает, что основной мерой противодействия киберпреступности на государственном уровне является именно правовое регулирование: совершенствование законодательства, криминализация новых деяний, ужесточение ответственности за уже существующие преступления в сфере кибепространства.

Несмотря на существующее законодательство разных стран, для киберпреступников не существует границ и юрисдикций. Киберпреступники совершают преступления исходя из совершенно различных мотивов и преследуя различные цели. Однако стоит отметить, что киберпреступники, получив доступ к конфиденциальным данным или управлению ИТ-системами, иногда даже не понимают, что делать с полученной информацией[3].

Пользователям и компаниям особенно важно соблюдать хотя бы базовые правила обеспечения безопасности информации, ведь, если определенные данные попадут к преступникам, это может отразиться на будущем граждан и корпораций.

Так, И. Сачков, президент компании Group-IB, занимающаяся расследованием компьютерных преступлений, отмечает необходимость соблюдения правил технической самозащиты для обеспечения собственной безопасности. Его компанией разработаны специальные памятки, для предотвращения возможности использования кибермошенниками информации.

Путём обобщения самых доступных способов был получен список базовых действий пользователей:

1. Использование лицензированных компьютерных программ и антивирусных софтов.
2. Использование электронного почтового адреса по конкретному назначению: для регистрации на сайтах, для оплаты услуг, для передачи важной информации (лучше защищенный).
3. Открытие вложений только от известных отправителей, если есть сомнения необходимо связаться с отправителем иным способом.
4. Проверка вложения на наличие вирусов.
5. Нежелательность указания в полученных по электронной почте формах и анкетах личные данные, так как их безопасную передачу могут гарантировать только защищенные сайты.
6. Проверка запросов персональных данных из деловых и финансовых структур, путём обращения в эти структуры по контактам, указанным на официальном сайте, но не в электронном письме.
7. При общении с клиентами банки не осуществляют как правило массовую рассылку. Поэтому лучше связаться с офисом банка по контактным данным на его официальном сайте, чтобы прояснить ситуацию.
8. Требования немедленных действий в чрезвычайных ситуациях с высокой степенью вероятности являются мошенничеством. Преступники вызывают ощущение тревоги, чтобы заставить пользователя действовать в критической ситуации быстро и неосмотрительно. Необходимо

оценивать ситуацию и принимать взвешенное решение.

9. Выпуск дополнительной карты для оплаты товаров в интернете.

10. При взломе вашей страницы, если вами был скачен какой-либо файл, заходите на сайт для восстановления страницы с незараженного устройства. После выполните процедуру восстановления пароля, перед этим сменив учетные данные во всех сервисах, где они совпадали со скомпрометированными: для защиты других аккаунтов.

11. Никогда не открывайте фалы, запрашивающие использование компонентов ActiveX в браузере Internet Explorer, так как они позволяют JavaScript'ам, выполняющимся в контексте браузера IE, осуществлять доступ к объектам операционной системы, в том числе загружать на нее исполняемые файлы, которые с высокой вероятность могут оказаться вредоносными объектами и запускать их [4].

Угрозе незаконного завладения данными, подвергаются не только индивидуальные пользователи, но и организации. В исследовании международной консалтинговой компании PwC отмечается, что большинство российских компаний не способны успешно противостоять кибератакам. Половина российских респондентов (и 44% в мире) отмечает, что в их компаниях нет общей стратегии информационной безопасности: в 48% компаний нет программы обучения, направленной на повышение уровня осведомленности сотрудников в вопросах безопасности; 56 % компаний указали, что у них не отработан процесс реагирования на кибератаки. А в способности найти хакеров полностью уверены лишь 19% участников исследования в России и 39% респондентов во всем мире [5].

По данным Национального Отделения ФБР по компьютерным преступлениям, от 85% до 97% нападений на корпоративные сети не то, что не блокируются, но и не обнаруживаются. Испытания, проведенные в США, показали следующие результаты: в 88% случаев проникновение специальных групп экспертов в военные информационные системы было успешным, в 4,36% случаев атаки были обнаружены, и только в 5% о таких атаках сообщили системные администраторы. Другая группа экспертов обследовала около 8 тыс. компьютеров Министерства обороны США и обнаружила 150 тыс. уязвимых мест. В среднем 80% успешных компьютерных вторжений в федеральные компьютерные системы происходит из-за ошибок в программном обеспечении или из-за его низкого качества [6].

По данным Генеральной Прокуратуры РФ число киберпреступлений в России с 2 013 года увеличилось в шесть раз, на что Генеральный прокурор Ю.Чайка обратил внимание в августе 2017 года на встрече Генеральных прокуроров стран БРИКС в Бразилии. По оценке Сбербанка, количество киберпреступлений к 2020 году в сравнении с 2018 может вырасти ещё в четыре раза, при этом возможные потери России составят около двух триллионов рублей.

Если рассматривать случаи самих кибератак в последние годы, то ответные действия на них нельзя оценить, как профессиональные.

Возьмем только примеры за 2017 год.

В мае масштабная атака вируса WannaCry затронула более пятисот тысяч компьютеров по всему миру. Лидерами по количеству заражений стали Россия, Украина и Индия. Программа шифровала практически все файлы на компьютере и требовала выкуп за возврат доступа.

В июне вирус-вымогатель NotPetya поразил IT-системы компаний в нескольких странах мира, в большей степени затронув Украину. Программа шифровала файлы и данные, необходимые для загрузки системы. Для восстановления доступа вирус требовал выкуп в биткойнах.

В октябре ряд российских СМИ, а также банки из первой двадцатки атаковал вирус-шифровальщик BadRabbit. За разблокировку одного компьютера программа требовала 0,05 биткойнов (около 16 тысяч рублей) в течении 48 часов. Также вирус затронул Турцию и Германию.

Количество преступлений, совершаемых в киберпространстве, растет пропорционально числу пользователей компьютерных сетей, и, по оценкам Интерпола, темпы роста преступности в глобальной сети Интернет, являются самыми быстрыми на планете. Поэтому государства прибегают к самым разнообразным методам борьбы, одним из которых является привлечение хакеров для борьбы с киберугрозами.

Так, в 2013 году в Японии были налажены условия для привлечения «этичных» хакеров для борьбы с киберпреступностью. Кроме того, японская полиция начала налаживать контакты с учебными заведениями и компаниями, занимающимися IT-технологиями для привлечения к сотрудничеству экспертов по киберпреступности. Министерство обороны Японии в свою очередь заявило, что в целях создания новых методов киберзащиты, они начали заниматься сбором и анализом информации о компьютерных вирусах, что опять же связано с налаживанием взаимодействия с разработчиками вирусов [7].

США продолжает активно внедрять свои меры борьбы с киберпреступностью. Об этом свидетельствуют данные исследования Zecurion Analytics, согласно которым финансирование этого направления в США составляет около $7 млрд. в год, а численность хакеров, сотрудничающих с государством – около 9 тыс. человек [9]. Ещё в 2015 году США решили привлечь для борьбы с киберпреступностью подростков: иначе таланты могли попасть в частный сектор на высокооплачиваемую работу или увлеклись бы наркотиками и не смогли бы пройти отбор на работу в спецслужбу, поэтому необходимо было разработать программу привлечения подростков. Программа стартовала весной 2016 года, в ходе которой ФБР приступило к установлению

контактов со школами около Питсбурга, предложив им проводить занятия по компьютерной безопасности для старшеклассников и с местными университетами, чтобы те принимали самых перспективных студентов.

Генеральный директор по кибербезопасности компании ZoneFox Джейми Грейвс высказал по поводу привлечения хакеров очень чёткое мнение, согласно которому несмотря на то, что киберпреступность продолжает приносить урон компаниям, и более двух третей предприятий не имеют достаточно способностей для защиты своей компании от киберугроз, необходимо задаться вопросом, как можно заставить талантливых молодых хакеров бороться с преступностью, а не способствовать ей»[11]. Данная позиция была высказана в ответ на исследование Национального агентства по борьбе с преступностью (NCA), которое затрагивало исследование личности преступника-хакера из числа подростков. В процессе исследования было установлено, что уважение и популярность среди сверстников – одни из основных мотивирующих факторов для молодых киберпреступников. Правонарушители начинают свою незаконную деятельность с участия в игровых чат-сайтах и форумных играх, и только потом переходят к хакерским форумам или вовлекаются в преступную деятельность.

Киберпреступность представляет повышенную опасность именно потому, что направление в области кибернетики и защиты данных в образовании не является не только просто приоритетным направлением, но и вообще развивается медленнее, чем развитие технологий. Также в компаниях существует множество внутренних угроз из-за недобросовестности сотрудников: самовольная установка и использование нерегламентированного программного обеспечения (до 78% внутренних происшествий), увеличение случаев использования оборудования и ресурсов в личных целях (на 10%) делает рабочие сети более уязвимыми. Известны случаи серьезных нарушения правил информационной безопасности даже в серьезных структурах, отвечающих за безопасность государства, которые проявляются в распространении практика так называемых неучтенных программ и программ с просроченными сертификатами, что несет в себе потенциальную угрозу для безопасности и национальной инфраструктуры в целом[6].

Чтобы избежать случаев несоблюдения информационной безопасности, подростку нужно прививать культуру работы с компьютерными приборами, интернетом с ранних лет. В рамках школ такие занятия возможно проводить на уроках безопасности жизнедеятельности.

Список литературы:

1. Большинство российских компаний не устойчивы к кибератакам, заявили в PwC. [Электронный ресурс]. URL: https://ria.ru/technology/20171109/1508453887.html.

2. Киберпреступность и отмывание денег. [Электронный ресурс]. URL:http://www.cbr.ru/today/anti_legalisation/evraz/Tipologiya_kiber_EAG_2014.pdf.

3. Кончена А. Реальные опасности виртуального мира: есть ли защита от киберпреступлений? [Электронный ресурс]. URL: https://rb.ru/opinion/virtual-world/.

4. 11 правил сетевой безопасности: как защититься от кибермошенников 27.01.2016 / Марина ЛЕПИНА [Электронный ресурс]. URL: https://www.miloserdie.ru/article/11-pravil-setevoj-gigieny-kak-zashhititsya-ot-kiberprestupnosti/.

5. Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ от 5 декабря 2016 г. № 646) // СПС «КонсультантПлюс» // http://www.consultant.ru.

6. Проблемы противодействия компьютерной преступности. [Электронный ресурс]. URL: http://www.securitylab.ru/contest/382194.php?ref=123.

7. Японская полиция просит помощи у "этичных" хакеров. [Электронный ресурс]. URL: https://hitech.newsru.com/article/25jan2013/jpplchckrs.

8. Киберспецслужба: Сбербанк предложил создать штаб борьбы с хакерами. [Электронный ресурс]. URL: http://www.rbc.ru/technology_and_media/01/09/2017/59a9799f9a7947375702db15.

9. Zecurion: Россия — в числе пяти стран с лучшими кибервойсками. [Электронный ресурс]. URL: http://www.tadviser.ru/index.php

10. Осипов А.: ФБР привлечет тинейджеров к борьбе с киберпреступностью. [Электронный ресурс]. URL: https://www.vedomosti.ru/management/articles/2015/10/06/611541-fbr-privlechet-tineidzherov-borbe-kiberprestupnostyu.

11. Если вы не можете победить их, вербуйте: привлекайте молодых хакеров к борьбе с киберпреступностью. [Электронный ресурс]. URL: https://www.security-news.today/esli-vy-ne-mozhete-pobedit-ih-verbujte-privlekajte-molodyh-hakerov-k-borbe-s-kiberprestupnostyu/