Киберпреступность в сфере информационных технологий как современная угроза

Олег Сергеевич Баландин
Старший преподаватель кафедры оперативно-розыскной деятельности
Белгородский юридический институт МВД России имени И.Д. Путилина
Белгород, Россия
bos1975@yandex.ru
0000-0002-3584-4380

Юлия Владимировна Ветрова
Кандидат технических наук, доцент, старший преподаватель кафедры тактико-специальной подготовки
Волгоградская академия МВД России
Волгоград, Россия
vetrova2006@mail.ru
0000-0001-9513-130X

Александр Сергеевич Нерубенко
Старший преподаватель кафедры огневой подготовки
Белгородский юридический институт МВД России имени И.Д. Путилина
Белгород, Россия
asnspez@yandex.ru
0000-0002-1816-6450

Евгений Иванович Васильченко
Старший преподаватель кафедры огневой подготовки
Белгородский юридический институт МВД России имени И.Д. Путилина
Белгород, Россия
strelchamp@yandex.ru
0000-0002-3255-6586

Денис Валерьевич Олейник
Старший преподаватель кафедры огневой подготовки
Белгородский юридический институт МВД России имени И.Д. Путилина
Белгород, Россия
losicov@mail.ru
0000-0001-7312-8337

Поступила в редакцию 12.09.2021
Принята 10.10.2021
Опубликована 15.10.2021

10.25726/h5310-2360-2460-p

Аннотация

В данной статье рассматривается актуальная на сегодняшний день проблема киберпреступности, так как в современном обществе компьютеры, информационные технологии и телекоммуникационные системы проникли во все сферы деятельности человека и государства. Однако глобализация информационных технологий представляет огромную угрозу для человечества. За последнее столетие она приобрела особую актуальность. С годами информационные технологии становятся доступнее для пользователей. Безграничные возможности глобализации информационного

поля позволяют злоумышленникам беспрепятственно оказывать воздействие на личность, группу и общество в целом. Киберпреступность в настоящее время достигла беспрецедентного размаха. Все это не осталось без внимания президента Российской Федерации Владимира Путина, который назвал эту проблему вопросом государственной безопасности и предложил сформировать систему автоматизированного обмена информацией об угрозах в цифровом пространстве. В данной статье рассматриваются проблемы расследования преступлений в сфере информационных технологий, которые осложняются анонимностью, наличием «безграничного» пространства, открытостью потенциальных жертв. В заключение показываются пути разрешения проблемы киберпреступности как в России, так и в других странах на современном этапе, которые заключаются: в усилении Государственной системы предупреждения и обнаружения компьютерных атак на информационные ресурсы России, а также устранении их последствий; в усилении надёжности сети конфиденциальной связи силовых структур и органов власти; в укреплении международного сотрудничества в сфере борьбы с киберпреступностью.

Ключевые слова
Киберпреступность, информационные ресурсы, образование, государственная безопасность.

Введение

25 июня 2021 на совещании с постоянными членами Совбеза РФ по вопросам кибербезопасности президент В.В. Путин отметил, что «Сегодня у всех на слуху — по важности и по объемам решаемых задач в этой сфере — вопросы кибербезопасности, сотрудничество в этой сфере. Борьба с киберпреступностью, по словам президента Российской Федерации Владимира Путина, который выступил перед участниками совещания, является вопросом государственной безопасности.

Важно отметить, что совсем недавно преступления, связанные с компьютерными технологиями, были достаточно неординарным явлением. В настоящее время правоохранительные органы регулярно сталкиваются с преступлениями, осуществляемыми при помощи компьютерной техники, к ним относятся и онлайн-мошенничества, распространение детской порнографии, торговля предметов и вещей, изъятых из гражданского оборота, растрата, шпионаж, и киберпреследования и т.д (Ахтырская, 2014).

На современном этапе развития общества образовался достаточно большой пласт противоправной деятельности, а многие сотрудники правоохранительной системы имеют недостаточный уровень знаний и умений, необходимых для эффективного противодействия преступности в полном объеме (Быков, 2013). Такие преступления специфичны по способам и методам совершения и предполагают использование глобальной информационной сети, проникновение в электронные системы служб и организаций.

Задача расследования подобного рода преступлений осложняется анонимностью, наличием «безграничного» пространства, открытостью потенциальных жертв, а также законодательной неурегулированньстью. До настоящего момента кибератака не рассматривается как самостоятельная потенциальная угроза совершения актов незаконного вмешательства в деятельность объектов транспортной инфраструктуры и транспортных средств.

Материалы и методы исследования

Из приведенной выше статистики видно, что киберпреступность на сегодняшний день достигла беспрецедентного размаха (Карпова, 2014).

Под киберпреступлениями понимаются деяния, совершенные с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации.

Число компаний, столкнувшихся с APT, увеличилось в 2020 году почти вдвое. Одновременно с этим атаки прямо на глазах усложняются, в них активно применяются методы, затрудняющие расследование инцидентов.

Киберпреступление является результатом человеческих трудов, как и любое другое преступление. Не будь технологий – не было бы и этих составов, очередных способов преступить закон, чтобы достичь корыстных целей.

Майер Амшель Ротшильд отмечает: «Кто владеет информацией - тот владеет миром3 »[30], однозначно, он был прав. Информация всегда была двигателем процесса и на протяжении всей истории человечества4 являлась одним из основных ресурсов любой сферы деятельности человека. Ни для кого не секрет, что4 интересующую информацию можно с легкостью получить из информационных сетей, в том числе сети «Интернет» (Куява, 2016).

Глобализация информационных технологий представляет огромную угрозу для человечества. За последнее столетие она приобрела особую актуальность. С годами информационные технологии становятся доступнее для пользователей. И обойти закон не предоставляет труда, даже тому, кто не обладает определенным образованием или навыками. И именно эти безграничные возможности могут оказаться в руках злоумышленников, которые беспрепятственно смогут оказать воздействие на личность, группу и общество в целом.

Результаты и обсуждение

Термины «киберпреступность» и «компьютерная преступность» нередко употребляются как синонимы и их значения отождествляют. Но Номоконов В.А. и Тропина Т.Л. полагают, что эти термины не синонимичны, но близки друг другу. Они считают, что понятие «киберпреступность» шире и точнее термина «компьютерная преступность» (Номоконов, 2012).

Приходится признать их мнение, так как понятие «киберпреступность» подразумевает преступления, совершаемые в сфере информационных технологий, в связи с чем, является по смыслу шире, чем «компьютерная преступность». Компьютерная преступность ограничена использованием вычислительных машин, в то время как «киберпреступность» затрагивает и сеть «Интернет».

В большинстве развитых стран существует подразделение на типы правонарушений в сфере информационной безопасности, так к преступлениям в сфере компьютерных технологий относится:

1) техника как орудие совершения преступления;
2) выведение из строя носителей информации;
3) незаконный доступ к охраняемой информации.

Быстрое распространение компьютерных систем, телекоммуникационных сетей и других связанных с ними технологий, на которые мы полагаемся ежедневно, образовали очередные уязвимости в системе безопасности страны.

Поэтому, можно сказать, что на сегодняшний день жертвами киберпреступников становятся не только обычные люди, но и органы власти.

Современное развитие информационных технологий является распределенным процессом, который происходит параллельно по всему миру и вместе с тем характеризуется наличием определенных центров притяжения, которые аккумулируют научные мнения и практические наработки в этой сфере. В настоящее время такими центрами можно назвать США, мощные страны Европейского Союза, КНР, Японию, Индию, Австралию. Соответственно, в основном именно в этих странах происходит быстрое внедрение передовых технологий в правоохранительную деятельность, в частности по вопросам противодействия киберпреступности (Рязанов, 2017).

Учитывая изложенное, считается актуальным для правоохранительных органов России внедрение зарубежного опыта указанных стран не только непосредственно в практическую деятельность, но и в учебный процесс курсантов, студентов, слушателей высших учебных заведений, осуществляющих подготовку специалистов в сфере борьбы с киберпреступностью. Более того, внедрение такого опыта должно носить опережающий характер. Минимальным требованием должно стать, чтобы новейшие достижения в сфере борьбы с киберпреступностью параллельно внедрялись как в учебный процесс, так и в практическую деятельность. Программа максимум - чтобы такие технологии сначала отрабатывались во время обучения (Целуйко, 2017). Пока эти технологии дойдут до

«практиков», высшие учебные заведения уже смогут выпустить подготовленных специалистов в этой сфере. Поэтому они не будут нуждаться в дополнительном обучении.

В контексте исследуемой проблематики нужно отметить последние достижения университета по внедрению зарубежного опыта в учебный процесс курсантов.

Надо изучить внедрение опыта с использование анонимной помощи граждан для противодействия киберпреступности. На данный момент в РФ существует горячая линия, с помощью этой линии каждый гражданин может сообщить о наличии детской порнографии в интернет-пространстве. За последние 6 месяцев на горячую линию поступило 19 сообщений о совершении правонарушений, имеющих признаки распространения детской порнографии. Все они были внимательно проработаны и переданы правоохранительным органам по принадлежности (Шинкарецкая, 2017).

Горячая линия является мониторинговым инструментом для уборки (путем получения сообщений от граждан информации о фактах распространения детской порнографии в Интернете с целью дальнейшего блокирования этого негативного контента.

Каждый пользователь Интернета может сообщить о случаях детской порнографии в Интернете, отправив информацию с помощью формы на Главной странице сайта. Проверка сообщений будет осуществляться 1-2 раза в неделю экспертом центра «Ла Страда». Пользователи Интернета могут отправлять информацию о фактах детской порнографии в интернете анонимно. Если же пользователь желает получить ответ на свое сообщение и узнать о дальнейшей работе специалистов линии с полученной информацией, он может оставить свои контакты.

В связи с этим видится необходимость внедрения американского опыта по обмену информацией о фактах изготовления и распространения детской порнографии. С этой целью было бы полезно получить доступ к сервису secure.icaccops.com, аккумулирующий данные об IP-адресах, с которых происходит описанная противоправная деятельность. Эту задачу также сегодня пытается решить Харьковский национальный университет внутренних дел. Доступ к этому ресурсу облегчит работу функционирующего в университете с 2013 года На-учебно-тренировочного центра борьбы с киберпреступностью и мониторинга киберпространства на общественных началах. Кстати, благодаря работе данного центра в университете реализован уникальный проект обучения. В рамках функционирования указанного проекта происходит одновременное сочетание курсантами выполнения задач по охране правопорядка, отработка навыков правоохранителя на специальных учебно-тренировочных полигонах, разработка собственного программного обеспечения. Указанный процесс реализуется в непосредственном взаимодействии с территориальными подразделениями органов внутренних дел, о чем были составлены соответствующие договоры.

Подобный проект реализован в университете Пердью, также UCD Centre for Cybersecurity & Cybercrime Investigation - в ведущем европейском вузе по предоставлению образования в сфере противодействия киберпреступности Дублинском университетском колледже (University College Dublin). Вместе с тем, реализованный проект выгодно отличается тем, что курсанты привлекаются к работе правоохранительных органов не только во время проведения соответствующих экспертных исследований, но и для выявления, предупреждения, раскрытия преступлений и розыска лиц.

Феномен кибернетической безопасности заключается в ее бинарном характере. С одной стороны, она может рассматриваться как элемент национальной безопасности. С другой стороны, учитывая то, что информационное пространство является безграничным, для него не существует границ, поэтому преступления в этой сфере в основном квалифицируются как транснациональные, а следовательно, кибернетическую безопасность следует рассматривать как явление глобализированное. Это значит, что вопрос подготовки и повышения квалификации специалистов в указанной области является принципиально важным не только для России, но и для мирового сообщества в целом.

Наша научная позиция базируется на необходимости внедрения в интерпретации этого понятия двух подходов – узкого и широкого.

Итак, в узком смысле терминологического сочетания под специалистами по кибернетической безопасности можно понимать лиц, которые имеют профильное образование по специальности «Кибербезопасность» и работают по специальности. Если строго придерживаться юридических норм, то

есть основания относить к указанной категории лишь тех, кто осваивал отрасль «Информационные технологии» по этой специальности.

Мы предлагаем, употребляя терминологическое сочетание «специалист по кибербезопасности» в широком смысле именовать так лиц, которые по роду своей профессиональной деятельности могут использовать специальные знания для предупреждения потенциальных угроз, разоблачение/раскрытие, нейтрализации или минимизации последствий противоправного поведения правонарушителей в компьютерном пространстве. В таком контексте даже преподавателя информатики в школе или в высшем учебном заведении можно считать специалистом по кибербезопасности, поскольку в своей деятельности он призван не только дать знания из сферы информационных технологий, но и, осуществляя воспитательную работу, выполнять превентивные функции. Подобный пример означает, что кибернетическая безопасность может выступать не только как специальность, но и как специализация в пределах других специальностей или как отдельная компонента образовательной программы подготовки специалиста.

На основе концепции непрерывного образования возможны несколько вариантов работы в этом направлении, а именно:

1) предоставление второго высшего образования. Наиболее сложный (учитывая продолжительность, стоимость, требования к разносторонности задатков и способностей соискателя высшего образования), но и наиболее действенный путь. Например, выпускник технического высшего учебного заведения получает второе высшее образование по юридической специальности;

2) применение нелинейной схемы подготовки специалистов по разным степеням образования, что стало возможным благодаря новым нормам, закрепленным в Федеральном Законе «О высшем образовании». Например, бакалавр технического профиля поступает в магистратуру по экономической специальности с целью дальнейшей работы как специалиста по кибербезопасности в банковской сфере;

3) введение специализаций по кибернетической безопасности на других специальностях (юридических, экономических, управленческих и тому подобное);

4) переподготовка в контексте последипломного образования специалистов по близкородственным с кибернетической безопасностью специальностям;

5) использование потенциальных возможностей неформального образования для повышения квалификации действующих специалистов через проведение тренингов, круглых столов, международных стажировок и тому подобное.

Заключение

Направления подготовки и повышения квалификации специалистов по кибербезопасности, по нашему убеждению, целесообразно проектировать в соответствии с Конвенцией о киберпреступности, принятая Советом Европы 23 ноября 2001 г. Каждый из выделенных в ней аспектов может корреспондироваться с содержанием образования по специальностям, по которым в России осуществляется подготовка соискателей высшего образования.

Приведенный перечень не является исчерпывающим, хотя и достаточно полно демонстрирует, что объект и предмет кибербезопасности настолько многогранны, что обеспечить полноценную деятельность лишь специалистами по одной специальности практически невозможно. Отдельного внимания требует подготовка аналитиков в сфере кибернетической безопасности, на которых должны возлагаться обязанности по выявлению криминогенных факторов, способствующих распространению компьютерных преступлений, отслеживанию основных тенденций и прогнозированию потенциальных угроз. Несмотря на важность этой категории специалистов, такой специальности в России сегодня нет.

Список литературы

1. Ахтырская Н. Организованная преступность в сфере информационных технологий // Компьютерная преступность и кибертерроризм. Исследования, аналитика. Вып. 1. Запорожье, 2014. С. 30 - 35.

2. Быков В.М. Совершенствование уголовной ответственности за преступления, сопряженные с компьютерными технологиями // Уголовное право. 2013. № 3. С. 9-11.
3. Быков В.М., Новый закон о преступлениях в сфере компьютерной информации: ст. 272 УК РФ // Российский судья. 2012. №5. С. 14-19.
4. Голубев В.А., Угроза кибертерроризма: факторы и противодействие // Доклады ТУСУРа. 2004. №1 (21). С. 76 -86.
5. Грамматчиков А., Вандышева О. Идет кибервойна народная // Эксперт. 2017. № 5. С.12-19.
6. Гузеева О.С. Уголовная политика в отношении преступлений, совершаемых в российском сегменте сети Интернет // Законы России: опыт, анализ, практика. 2014. № 6. С. 74-77.
7. Завидов Б.Д., Ибрагимова З.А. Мошенничество в СВТ // Современное право. 2011. №4. С. 43-45.
8. Ибрагимов В. Кибертерроризм в Интернете до и после 11 сентября: оценка угроз и предложения по их нейтрализации // Компьютерная преступность и Кибертерроризм. Исследования, аналитика. Вып. 1. 2004. С. 56-61.
9. Карпова Д.Н. Киберпреступность: глобальная проблема и ее решение // Власть. 2014. №8. С.46-50.
10. Куява Т.Ю. Киберпреступность: проблемы уголовно-правовой оценки и организации противодействия // Молодой ученый. 2016. №29. С. 255-257.
11. Номоконов В.А., Тропина Т.Л. Киберпреступность как новая криминальная угроза // Криминология: вчера, сегодня, завтра. 2012. № 24. С.45-55.
12. Полякова Т.А. Базовые принципы правового обеспечения информационной безопасности // труды института государства и права РАН. 2016. №3 (55). С. 17-40.
13. Протасевич А.А., Зверянская Л.П. Криминалистическая характеристика компьютерных преступлений // Российский следователь. 2013. № 11. С. 45-47.
14. Рязанов Н.С. К вопросу о соотношении понятий «безопасность» и «транспортная безопасность» // Вестник Омской юридической академии. 2017. №3. С. 89-94.
15. Сидакова А.А. Система норм об обеспечении транспортной безопасности в уголовном законодательстве России и за рубежом // Транспортное право. 2018. №1. С 22-25.
16. Целуйко А.В., Петроченко В.В. Вопросы информационного обеспечения транспортной безопасности в условиях современности // Транспортное право. 2017. № 4. С. 28-31.
17. Шинкарецкая Г.Г. Атаки на компьютерные системы в мирное время и обеспечение безопасности государства // Труды Института государства и права РАН. 2016. №33. С. 127-132.

Cybercrime in the field of information technology as a modern threat

Oleg S. Balandin
Senior lecturer of the Department of Operational Investigative Activities
Belgorod Law Institute of the Ministry of Internal Affairs of Russia named after I.D. Putilin
Belgorod, Russia
bos1975@yandex.ru
0000-0002-3584-4380

Yulia V. Vetrova
Candidate of Technical Sciences, Associate Professor, Senior lecturer of the Department of Tactical and Special Training
Volgograd Academy of the Ministry of Internal Affairs of Russia
Volgograd, Russia
vetrova2006@mail.ru
0000-0001-9513-130X

Alexander S. Nerubenko
Senior lecturer of the Department of Fire Training
Belgorod Law Institute of the Ministry of Internal Affairs of Russia named after I.D. Putilin
Belgorod, Russia
asnspez@yandex.ru
0000-0002-1816-6450

Evgeny I. Vasilchenko
Senior lecturer of the Department of Fire Training
Belgorod Law Institute of the Ministry of Internal Affairs of Russia named after I.D. Putilin
Belgorod, Russia
strelchamp@yandex.ru
0000-0002-3255-6586

Denis V. Oleinik
Senior lecturer of the Department of Fire Training
Belgorod Law Institute of the Ministry of Internal Affairs of Russia named after I.D. Putilin
Belgorod, Russia
losicov@mail.ru
0000-0001-7312-8337

Received 12.09.2021
Accepted 10.10.2021
Published 15.10.2021

10.25726/h5310-2360-2460-p

Abstract

This article examines the current problem of cybercrime, since in modern society computers, information technologies and telecommunication systems have penetrated into all spheres of human activity and the state. However, the globalization of information technology poses a huge threat to humanity. Over the last century, it has become particularly relevant. Over the years, information technology has become more accessible to users. The limitless possibilities of the globalization of the information field allow attackers to freely influence an individual, a group and society as a whole. Cybercrime has now reached an unprecedented scale. All this did not go unnoticed by the President of the Russian Federation Vladimir Putin, who called this problem a matter of state security and proposed to form a system of automated information exchange about threats in the digital space. This article discusses the problems of investigating crimes in the field of information technology, which are complicated by anonymity, the presence of "limitless" space, and the openness of potential victims. In conclusion, the ways of solving the problem of cybercrime both in Russia and in other countries at the present stage are shown, which consist in strengthening the State system for preventing and detecting computer attacks on Russian information resources, as well as eliminating their consequences; strengthening the reliability of the confidential communication network of law enforcement agencies and authorities; strengthening international cooperation in the fight against cybercrime.

Keywords

Cybercrime, information resources, education, state security.

References

1. Ahtyrskaja N. Organizovannaja prestupnost' v sfere informacionnyh tehnologij // Komp'juternaja prestupnost' i kiberterrorizm. Issledovanija, analitika. Vyp. 1. Zaporozh'e, 2014. S. 30 - 35.

2. Bykov V.M. Sovershenstvovanie ugolovnoj otvetstvennosti za prestuplenija, soprjazhennye s komp'juternymi tehnologijami // Ugolovnoe pravo. 2013. № 3. S. 9-11.
3. Bykov V.M., Novyj zakon o prestuplenijah v sfere komp'juternoj informacii: st. 272 UK RF // Rossijskij sud'ja. 2012. №5. S. 14-19.
4. Golubev V.A., Ugroza kiberterrorizma: faktory i protivodejstvie // Doklady TUSURa. 2004. №1 (21). S. 76 -86.
5. Grammatchikov A., Vandysheva O. Idet kibervojna narodnaja // Jekspert. 2017. № 5. S.12-19.
6. Guzeeva O.S. Ugolovnaja politika v otnoshenii prestuplenij, sovershaemyh v rossijskom segmente seti Internet // Zakony Rossii: opyt, analiz, praktika. 2014. № 6. S. 74-77.
7. Zavidov B.D., Ibragimova Z.A. Moshennichestvo v SVT // Sovremennoe pravo. 2011. №4. S. 43-45.
8. Ibragimov V. Kiberterrorizm v Internete do i posle 11 sentjabrja: ocenka ugroz i predlozhenija po ih nejtralizacii // Komp'juternaja prestupnost' i Kiberterrorizm. Issledovanija, analitika. Vyp. 1. 2004. S. 56-61.
9. Karpova D.N. Kiberprestupnost': global'naja problema i ee reshenie // Vlast'. 2014. №8. S.46-50.
10. Kujava T.Ju. Kiberprestupnost': problemy ugolovno-pravovoj ocenki i organizacii protivodejstvija // Molodoj uchenyj. 2016. №29. S. 255-257.
11. Nomokonov V.A., Tropina T.L. Kiberprestupnost' kak novaja kriminal'naja ugroza // Kriminologija: vchera, segodnja, zavtra. 2012. № 24. S.45-55.
12. Poljakova T.A. Bazovye principy pravovogo obespechenija informacionnoj bezopasnosti // trudy instituta gosudarstva i prava RAN. 2016. №3 (55). S. 17-40.
13. Protasevich A.A., Zverjanskaja L.P. Kriminalisticheskaja harakteristika komp'juternyh prestuplenij // Rossijskij sledovatel'. 2013. № 11. S. 45-47.
14. Rjazanov N.S. K voprosu o sootnoshenii ponjatij «bezopasnost'» i «transportnaja bezopasnost'» // Vestnik Omskoj juridicheskoj akademii. 2017. №3. S. 89-94.
15. Sidakova A.A. Sistema norm ob obespechenii transportnoj bezopasnosti v ugolovnom zakonodatel'stve Rossii i za rubezhom // Transportnoe pravo. 2018. №1. S 22-25.
16. Celujko A.V., Petrochenko V.V. Voprosy informacionnogo obespechenija transportnoj bezopasnosti v uslovijah sovremennosti // Transportnoe pravo. 2017. № 4. S. 28-31.
17. Shinkareckaja G.G. Ataki na komp'juternye sistemy v mirnoe vremja i obespechenie bezopasnosti gosudarstva // Trudy Instituta gosudarstva i prava RAN. 2016. №33. S. 127-132.