Е. В. Зыкина
кандидат юридических наук,
доцент кафедры государственно-правовых дисциплин и теории права
М. В. Ахтырская
студент
Псковский государственный университет

ОХРАНА ПРАВ ГРАЖДАН В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

В научной статье рассмотрено влияние информационных технологий на правовое положение граждан. Рассмотрены особенности информационно-коммуникационных форм обеспечения доступа к информации. В связи с этим становится актуальным наиболее точный и глубокий анализ положения, которое занимает наша страна в мировом информационном пространстве, международной политике и международном законодательстве об интернете. Угроз со стороны Всемирной паутины множество, так как с развитием интернет-технологий параллельно развиваются и различного рода интернет угрозы.

Глобальная сеть Интернет – главной ресурс опасностей информационной защищенности, который нацелен на ликвидирование трёх ключевых инцормационных данных: ее единства, конфиденциальности, а также доступности. Все без исключения атаки киберпреступников ориентированы в несоблюдение одного из этих качеств, либо все одновременно. По этой причине главная цель информативной защищенности – охрана сведений. Большое количество граждан относят сферу информативной защищенности только лишь с информативными технологиями либо со сетью интернет. Однако это не так. Угрозам подвергается не только информация, хранящаяся в сети или на электронных носителях, но и любые ее виды.

Развитие ИТ в мире и их проникновение в различные отрасли и сферы деятельности человека предполагает также и параллельное развитие систем обеспечения информационной безопасности. Это неудивительно – ведь чем больше технологий появляется, тем стремительнее развитие угроз и уязвимостей информационной безопасности. За последние несколько лет этот прогресс стал намного заметней и интенсивней.

Главное желание киберпреступника – извлечь выгоду от реализации угроз, а чем большие возможности предоставляют современные технологии, тем больше вероятности у киберпреступников осуществить свои намерения.

Интенсивность борьбы с интернет-угрозами в России. С процессом развития всемирной сети буквально каждый пользователь ежедневно пользуется интернет-возможностями. Известно, что масштабная сеть, в большинстве своём, является неиссякаемым источником информации и возможностью для виртуального общения. Однако далеко не многим известно, какие потери и ущерб может быть нанесен персональному компьютеру пользователя. Безопасность в интернете требует принятия необходимых мер, обеспечивающих защиту от компьютерных вирусов различной сложности, а также от взлома ПК злоумышленниками с целью овладения частной или корпоративной информацией. Безопасность в сети интернет является злободневной проблемой, которую целиком разрешить почти невозможно, так как вредоносные программы и сайты совершенствуются [1, 59–61].

В России система защиты граждан от интернет-контента требует усовершенствования. В связи с этим актуальным является принятие следующих общественно-полити-

ческих мер: создание безопасного интернет-пространства; просветительская деятельность и реклама, направленная на повышение уровня осознания проблемы агрессивного контента в зоне Рунета в органах государственной власти, интернет-сообществе, гражданском обществе; образовательная деятельность, направленная на повышение культуры пользования Интернетом.

Также обширно обсуждается вопрос прав гражданина в Интернете, а именно рассматривается право на допуск к Интернету с разных точек зрения, например в возможности права на видеоинформацию и связь, обеспеченных конституцией в государствах или закрепленного в специальном судопроизводстве.

Дополнительные возможности, которые предоставляет использование электронных ресурсов, ставят под угрозу безопасность и конфиденциальность сведений о пользователях огромного интернет-пространства. Должны быть корреспондирующие обязанности лиц, ведущих процесс по разработке защитных мер, направленных на защиту рассматриваемых прав, реализация которых возможна посредством использования информационных технологий [1].

Проблемы в сфере информационной безопасности в России являются только частью общемировых задач и проблем. Общее количество угроз в мире показывает, что Россия находится на втором месте по количеству кибер-атак. В современных геополитических условиях угрозы в «мире технологий» все более актуальна, и в связи с этим целесообразным является введение набора знаний и навыков в области информационной безопасности граждан [2, с. 243–248].

Последние достижения в области информационных и коммуникационных технологий позволили впустить Интернет во все сферы общественной жизни и даже в органы государственной власти. Однако правовая природа Интернета вообще не закреплена на законодательном уровне. До сих пор нормативное регулирование отношений между пользователями Интернета не носит правового характера. Несмотря на множество регламентов и технических стандартов к Интернету применимы нормы, которые относятся к традиционным, корпоративным или даже этическим, но и данные правовые отношения подвергаются нерегуриуемому воздействию с другой стороны интернет-пространства. Воздействие заключается в том, что в информационном обществе значительная часть общественных функций переходит в сеть в «Даркнет», в виртуальную сферу, что позволяет говорить о совершенно новых вопросах защиты и реализации прав человека. В российском законодательстве данная категория прав введена федеральным законом от 18.03.2019 г. № 34-ФЗ с 1 октября 2019 г. Под цифровым правами признаются названные в таком качестве в законе обязательственные и иные права, содержание и условия осуществления которых определяются в соответствии с правилами информационной системы, отвечающей установленным законом признакам.

Даркнет (или теневой интернет), – это закрытая группа веб-сайтов, которая доступна лишь через специальные браузеры. Они используются для сохранения анонимности и приватности действий, совершаемых в интернете, – в большинстве своём незаконных. В Даркнете всё конфиденциально – создатели сайтов анонимно создают их, пользователи имеют возможность анонимного посещения таких сайтов. Всё потому, что предмет обсуждения и сделок на теневых сайтах – это запрещённые законами многих стран товары, услуги и контент [4].

Многие аналитики считают, что доля Даркнета от основного Интернета составляет около 1%.

Несмотря на это, преступность в Даркнете как негативное социальное явление, обретает все большие масштабы по мере проникновения интернет-технологий в повседневную жизнедеятельность граждан РФ.

Очевидно, что тяготение к криминальной модели применения Даркнета заложено в анонимности сети, что привлекает различного рода злоумышленников, избегающих идентификации и привлечения к юридической ответственности.

Однако и государственные защитные меры требуют совершенствования, о чем говорят участившиеся взломы правительственных серверов в разных странах мира и «теневой интернет». Возьмем приговор Ленинского суда г. Чебоксары, когда в июле 2017 г. россиянин получил 4 года условного срока за покупку на одном из сайтов Даркнета наркотических средств.

Пакет с психотропным веществом в виде заказного письма был отправлен продавцом из Германии, но на таможне во Внуково был вскрыт и запротоколирован. В Чебоксары посылка отправилась с сопровождением сотрудниками МВД. Поскольку письмо шло из Германии в Россию, в качестве противоправного действия в приговоре фигурирует контрабанда наркотиков.

Проблема осложняется тем, что преступники чаще всего не попадают под юрисдикцию государства, подвергшегося кибернападению. Преступники являются либо иностранцами, либо лицами без гражданства – «гражданами мира», которые способствуют развитию. Все это вынуждает искать общемировой консенсус в борьбе с угрозами и создавать общую систему информационной безопасности. Ведутся предварительные переговоры о возможности не только признавать кибератаки преступлениями, но и приравнивать их к вооруженным нападениям, когда целью являются государственные институты.

Но Правительство России принимает меры по искоренению кибер-преступников, в частности участников теневого Интернета. 12 февраля 2019 года, депутаты Госдумы в первом чтении приняли законопроект по обеспечению устойчивой работы российского сегмента интернета (Рунета) в случае кибератак и других агрессивных действий из-за рубежа. Авторами инициативы выступили глава комитета Совета Федерации по конституционному законодательству Андрей Клишас из «Единой России», его первый заместитель и однопартиец Людмила Бокова, а также депутат от ЛДПР Андрей Луговой. Законопроект об устойчивом интернете предполагает создание национальной системы получения данных о доменных именах и сетевых адресах. Данный документ закрепляет правила маршрута трафика, задача которого — свести к минимуму передачу за рубеж данных, которыми обмениваются российские пользователи. Кроме того, провайдеры должны установить технические средства, благодаря которым будет определяться источник передаваемого трафика. Законопроект поставил задачу непрерывного подключения к Сети россиян, как отмечал Андрей Клишас. Однако больше всего депутатов беспокоит принятая в сентябре прошлого года Стратегия национальной кибербезопасности. Она подразумевает введение санкций на информационные активы для усмирения страны-агрессора.

Законопроект позволит сформировать условия для устойчивой работы российского сегмента интернета. Ожидается, что контролем новой системы займется Роскомнадзор. Законопроект обяжет интернет-провайдеров установить в своих сетях технические средства противодействия угрозам. В спокойное время работа сети будет осуществляться в стандартном режиме, и пользователи даже не заметят изменений. Однако ведомство будет управлять Рунетом в случае возникновения опасности, а также будет блокировать запрещенные в России сайты [2].

Дополнительным аргументом, который подтверждает важность создания международной нормативно-правовой базы по борьбе с кибер-угрозами, служит риск ущерба

репутации государства. Информационная безопасность и защита репутации государства должны стать одним из инструментов в геополитическом противоборстве. Все это укрепляет идею сосредоточить усилия мирового сообщества на выстраивании системы превентивных мер, одной из которых может стать криминализация преступлений в сфере информационной безопасности на максимально высоком уровне.

Применительно к качеству государственного или корпоративного управления уровень информационной безопасности определяется способностью государства или компании: обеспечить функционирование информационных ресурсов и потоков, достаточное для нормальной жизнедеятельности и развития; защитить в полном объеме коммерческую или государственную тайну от незаконных посягательств; противостоять техническим и психологическим угрозам, оградить систему и пользователей от негативного воздействия с использованием информационных технологий [2];

поддерживать эффективность работы, возможность «саморазвития» и адекватные реакции системы на возрастающие вызовы; использовать такие методы и средства защиты информационного суверенитета государства или корпоративных ценностей, которые не посягали бы на целостность прав и свобод других государств и граждан.

Защита прав человека в условиях информационной среды. С процессом формирования современных технологий и использованием информационного пространства для осуществления противоборства стран в новой форме изменяется сама цель этого рода конфронтации. Осуществляется отход от идеи физического уничтожения врага к управлению его сознанием, изменению его ценностных ориентаций и внутренних мотивов, психологическому влиянию на его поведение, что показывает явное неисполнение права на свободу мнений и убеждений, а также их свободного выражения. Одним из нормативных документов, закрепляющих данные права и свободы, является Всеобщая декларация прав человека, принятая Генеральной Ассамблеей ООН в 1948 г. Так, ст. 19 устанавливает право каждого человека на свободу убеждений и свободу их выражения. Кроме того, такая статья также закрепляет свободу на определение, получение и распространение информации и идей любыми средствами и вне зависимости от государственных границ [5, с. 35–38].

Для киберпреступников, работающих в глобальном масштабе, не имеется границ между странами. Как отметил Г. Греф, «Киберпреступность имеет, к сожалению, мировые корни. Как правило, нас атакуют не из Российской федерации. Проблеме информационной (компьютерной) безопасности в государствах должно уделяться особое внимание. Стоит отметить, что государства принимают меры к объединению усилий в сфере борьбы с киберпреступниками. Так, в 2009 г. в Эстонии открылся Центр коллективной кибербезопасности под руководством НАТО. 25 января 2018 г. начал работу Глобальный центр по вопросам кибербезопасности под эгидой Всемирного экономического форума в Давосе, где Сбербанк стал одним из соучредителей. Как уточнил заместитель председателя правления «Сбербанка» С. Кузнецов, «Центр возьмет на себя роль уникальной платформы по взаимодействию государственного и частного секторов, развитие которой будет происходить по трем ключевым направлениям. Эти направления — установление взаимовыгодного сотрудничества между государственными и частными компаниями, развитие которых необходимы условий для предприятия неизменного обмена информацией и формирование надежного исследовательского центра, осуществляющего независимую оценку и анализ текущей обстоятельства в области безопасности в интернете на мировой арене».

Вывод. Таким образом, полагаю, что с целью противодействия преступлений, совершаемых с использованием сегодняшних информационных технологий в нашем

государстве необходимо регулярно увеличивать безопасность информационных систем, развивать сегодняшние информационные технологии, совершенствовать законодательство в сфере информационных преступлений, развивать конкурентоспособные средства информатизации, расширять международное партнёрство Российской федерации в сфере безопасного использования информационных ресурсов.

Эффективная координация поступков в некоторых субъектах мира позволит сформировать единое информационное пространство в целом.

ЛИТЕРАТУРА

1. Базовая информация о информационной безопасности [Электронный ресурс] // Интернет-портал – URL: https://elar.urfu.ru/bitstream/10995/73899/3/978-5-7996-2677-8_2019.pdf (Дата обращения: 13.04.2021). С. 59–61.
2. Федерального закона от 1 мая 2019 г. N 90-ФЗ «О внесении изменений в Федеральный закон „О связи“.
3. Бородкина Татьяна Николаевна Павлюк Альберт Валентинович Киберпреступления: понятие, содержание и меры противодействия // Киберпреступления: понятие, содержание и меры противодействия. - М.: Российская газета, 2017. С.2-3.
4. Иванов М.Г. О роли уголовного наказания в предупреждении служебно-экономической преступности и коррупции в современной России // Юридическая наука и практика. Вестник Нижегородской академии МВД России. 2017. № 3 (39). С. 243–248.
5. Райтман М.А. Искусство легального, анонимного и безопасного доступа к ресурсам Интернета. Екатеринбург, 2017. С. 35-38.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

УЧРЕЖДЕНИЕ ОБРАЗОВАНИЯ
«ПОЛОЦКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ТРАНСФОРМАЦИЯ ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ И МЕСТНОГО САМОУПРАВЛЕНИЯ В УСЛОВИЯХ РАЗВИТИЯ ИНФОРМАЦИОННОГО ОБЩЕСТВА

Электронный сборник статей
Международного круглого стола
(Новополоцк, 16 апреля 2021 г.)

Текстовое электронное издание

Новополоцк
Полоцкий государственный университет
2021

Об издании – 1, 2

1 – дополнительный титульный экран – сведения об издании

УДК 342.5
ББК 67.400

Рекомендован к изданию методической комиссией юридического факультета
Полоцкого государственного университета (протокол № 6 от 02.06.2021 г.)

ТРАНСФОРМАЦИЯ ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ И МЕСТНОГО САМОУПРАВЛЕНИЯ В УСЛОВИЯХ РАЗВИТИЯ ИНФОРМАЦИОННОГО ОБЩЕСТВА [Электронный ресурс] : электрон. сб. ст. Междунар. круглого стола, Новополоцк, 16 апреля 2021 г. / Полоц. гос. ун-т ; редкол.: И. В. Шахновская, П. В. Соловьев. – Новополоцк : Полоц. гос. ун-т, 2021. – 1 электрон. опт. диск (CD-R).

ISBN 978-985-531-782-2.

В сборник включены научные статьи профессорско-преподавательского состава юридических факультетов Республики Беларусь, Польши, Российской Федерации и Узбекистана по результатам проведенного международного круглого стола на базе юридического факультета Полоцкого государственного университета (16 апреля 2021 г., Новополоцк).

Издание адресуется научным сотрудникам, преподавателям средних специальных и высших учебных заведений, аспирантам, магистрантам, и иным специалистам в области конституционного права. Ответственность за содержание статей несут авторы.

Сборник включен в Государственный регистр информационного ресурса.
Регистрационное свидетельство № 3102126804 от 03.11.2021.

№ госрегистрации 3102126804
ISBN 978-985-531-782-2

2 – дополнительный титульный экран – производственно-технические сведения

Для создания текстового электронного издания «Трансформация государственного управления и местного самоуправления в условиях развития информационного общества» под редакцией И. В. Шахновской, П. В. Соловьева использованы текстовый процессор Microsoft Word и программа Adobe Acrobat XI Pro для создания и просмотра электронных публикаций в формате PDF.

ТРАНСФОРМАЦИЯ ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ И МЕСТНОГО САМОУПРАВЛЕНИЯ В УСЛОВИЯХ РАЗВИТИЯ ИНФОРМАЦИОННОГО ОБЩЕСТВА

Электронный сборник статей
Международного круглого стола
(Новополоцк, 16 апреля 2021 г.)

Техническое редактирование и верстка: *А. А. Прадидова.*
Компьютерный дизайн *М. С. Мухоморовой.*

Подписано к использованию 25.11.2021.
Объем издания: 1,96 Мб. Тираж 3 диска. Заказ 791.

Издатель и полиграфическое исполнение:
учреждение образования «Полоцкий государственный университет».

Свидетельство о государственной регистрации
издателя, изготовителя, распространителя печатных изданий
№ 1/305 от 22.04.2014.

ЛП № 02330/278 от 08.05.2014.

211440, ул. Блохина, 29,
г. Новополоцк,
Тел. 8 (0214) 59-95-41, 59-95-44
http://www.psu.by