Режим доступа: https://www.mos.ru/mgi/documents/normativno-pravovie_akty/regionalniy_gosudarstvenniy_zilishniy_nadzor/view/218747220/. – Дата доступа: 16.11.2024.

УДК 004

И.О. Кузнецова[1,2], Ю.В. Шляпина[1,2], С.Л. Шабоха[1]
[1]Омский институт водного транспорта – филиал «Сибирский государственный университет водного транспорта»
[2]АНО ВО Сибирский институт бизнеса и информационных технологий
Омск, Россия

НОВЫЕ ВИДЫ ПРЕСТУПЛЕНИЙ - КИБЕРПРЕСТУПЛЕНИЯ

Аннотация. *Цифровизация процессов стремительно развивается во всех сферах деятельности человека. Вместе с этим появляются и новые виды мошенничества и преступлений – киберпреступления. Российское государство на законодательном уровне стремится обезопасить страну от киберпреступников.*

I.O. Kuznetsova[1,2], Yu.V. Shlyapina[1,2], S.L. Shabokha[1]
[1]St Institute of Water Transport – branch of the Siberian State University of Water Transport
[2]Siberian Institute of Business and Information Technologies
Omsk, Russia

NEW TYPES OF CRIMES - CYBERCRIME

Abstract. *Digitalization of all processes is rapidly developing in all spheres of human activity. Along with this, new types of fraud and crimes are emerging – cybercrime. At the legislative level, the Russian state seeks to protect the country from cybercriminals.*

Экономики всего мира быстрыми темпами под воздействием повсеместного внедрения цифровых технологий модернизируются. Абсолютно все области деятельности человека трансформируются под влиянием информационно-коммуникационных технологий. Громадные возможности цифровых устройств способствуют онлайн решению множеству вопросов – поиск необходимой литературу в электронной библиотеке, запись на прием к врачу при помощи портала электронной записи в поликлинике, электронная карта у врача, электронный заказ продуктов питания, электронное меню в кафе ресторане, электронные салоны мебели, электронные магазины одежды, электронная продажа авиа и железнодорожных билетов,

электронный личный кабинет в банке, ФСС, Госуслуги. Многочисленные сферы обыденной жизни обыкновенного гражданина преображается в цифровую [1].

Однако вместе с молниеносным развитием электронного благоустройства в нашей жизни появляются и электронные преступления. И с каждым днем преступники становятся гораздо образованнее и опытнее. Совершают преступления не просто мошенники, а мошенники с высокой квалификацией и серьезным образованием.

Еще двадцать лет назад, чтобы находиться в безопасности достаточно было в темное время суток не выходить на улицу, не посещать сомнительные заведения, не ходить по безлюдным местам, закрывать двери на крепкие замки, то теперь все эти предосторожности совершенно не имеют смысла и абсолютно не гарантируют нам безопасной, спокойной жизни и того, что наше имущество, наше здоровье, наши финансы и наши персональные данные будут надежно защищены.

Одновременно с появлением благ цифровизации возникли и новые типы преступления, а именно - киберпреступления [3], причем рост их с геометрической прогрессией увеличивается с каждым годом и теперь это не только воровство персональных данных, но и более серьезные преступления, которые требует от нас применение более эффективных и действенных мер защиты. Цифровая безопасность и покой с каждым днем становится все более уязвимыми и зыбкими, возникает глобальная потребность обеспечения высококачественной безопасности в цифровом мире.

Что следует считать к киберпреступлением? – всевозможные типы атак, например, хакерские, фишинговые, вредоносные программы и др. Эти методы используют киберпреступники для незаконного доступа к системам и украденным данным. В организации, правительственных учреждениях и у индивидуальных пользователей очень часто возникает проблема цифровой безопасности. Необходимо предпринять меры по защите информации и противодействию кибератакам [4].

В современном мире увеличились объемы юридической значимости хранения персональных и данных различной этиологии, параллельно этому увеличился риск их утечки. Нарушение безопасности и отступление от мер защиты может способствовать утечке личных данных, а именно имя, фамилия, адрес, паспортные данные, финансовая информация и иные конфиденциальные данные. Утечка данных может иметь серьёзные последствия в отношении

индивидуума и организации, в том числе в связи с финансовыми потерями и в связи с угрозами конфиденциальности. Для тех, кто использует цифровые технологии, приоритет защищать персональные данные.

Низкая информированность пользователей об уязвимостях кибербезопасности – одна из основных проблем. Многие не знают, как защитить свои данные. Недостаток грамотности цифрового образования и подготовки к кибербезопасности приводит к тому, что пользователи становятся менее защищенными от киберугроз. Образовательная программа и информационная кампания должны проводиться в целях повышения информированности и подготовки пользователей к мерам безопасности в цифровой среде.

Самым главным из методов обеспечения безопасности в киберпространстве является использование современных технологий защиты данных и криптографии. Это предполагает использование сильных паролей, двухфакторную аутентификацию, шифрование данных в хранилищах и передачу информации. Организациям и пользователям необходимо принимать регулярные меры по обновлению ПО для устранения уязвимостей и обеспечения безопасности своих систем и данных.

Государственный аппарат и управленческие структуры, производственные предприятия играют и частные компании играют особую и очень важную роль в защите кибербезопасности, защите персональной информации. Необходимо строгое регулирование обработки данных и хранения персональной информации. Важно, чтобы организации вкладывали средства в защиту информации и обучение персонала по кибербезопасности.

Но только этих мер недостаточно, необходимо, чтобы сами граждане нашей страны помнили, что беспечность способствует совершению преступлению, в первую очередь по отношению к ним самим. Необходимо быть бдительными и не поддаваться на провокационные действия различных мошенников. Всегда помнить, что нас защищает наше законодательство и правовые акты.

В нашей стране мощная законодательная база, благодаря которой защищены права граждан Российской Федерации и наказываются преступники за нарушение этих законов и совершение цифровых преступлений. В России уже много лет существуют такие законы и нормативно-правовые акты. Самые важные и основные из них представлены на рисунке 1.

Кроме вышеперечисленных проблем, еще одна угроза нашей цифровой безопасности, на которую пока не обращают недостаточно

внимания – это спам. Достаточно неприятная и надоедливая массовая рассылка рекламы, которая происходит, совершенно без согласования с получателем. Для этого используются всевозможные цифровые адреса, спам приходит в смс на номер телефона, на электронную почту в различные социальные сети и различные форумы.

Сегодня очень часто мы слышим о том, что происходит обсуждение необходимости конкретной криминализации спама. В 2004г. Были попытки создания ФЗ «О внесении изменений в Федеральный закон «О рекламе», Уголовный кодекс Российской Федерации и Кодекс Российской Федерации об административных правонарушениях (о рекламе в сети электросвязи)», предусматривающий дополнение УК РФ статьёй об уголовной ответственности за спам. Он даже был вынесен на заседание Государственной думы, однако вскоре законопроект отозвали сами авторы данной юридической инициативы.

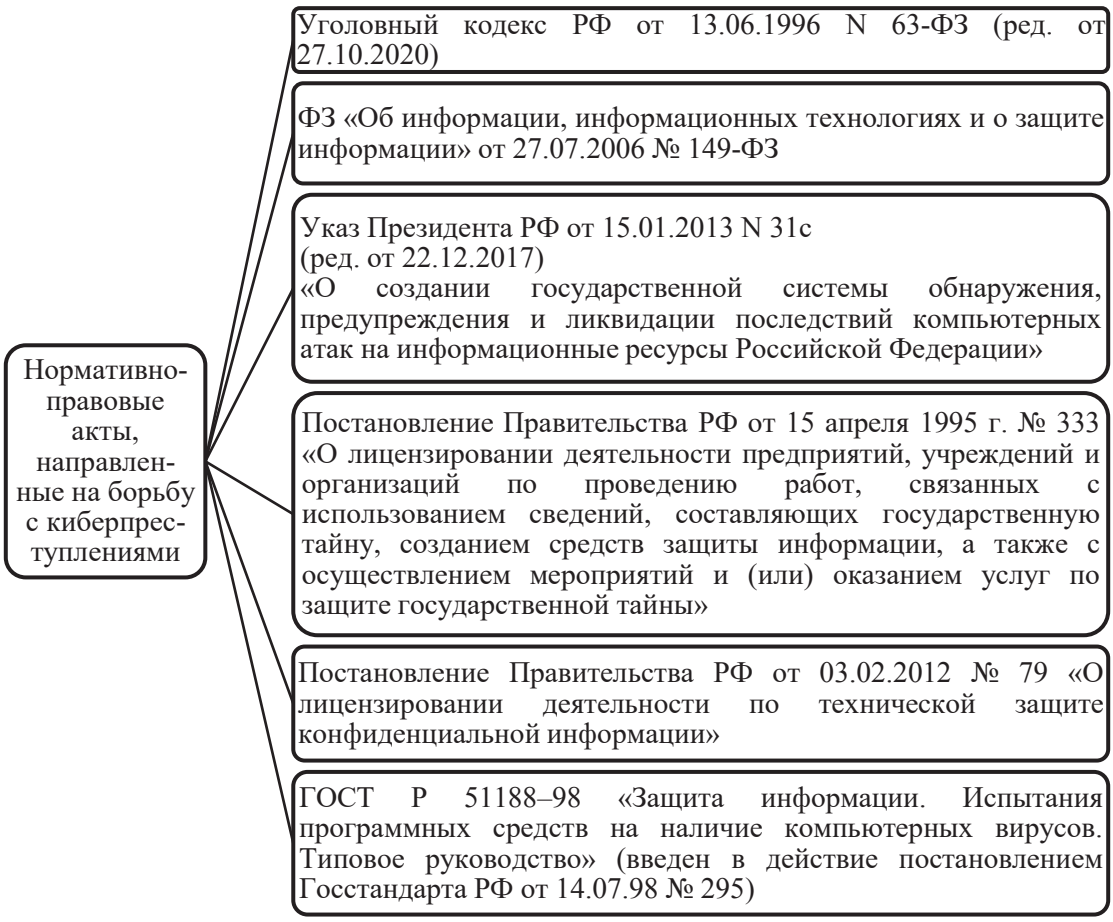

Рис. 1 - Российская законодательная база, направленная на предупреждение киберпреступлений

Спамом, это действие, с которым бороться не только нужно, но и необходимо, его опасность – является одной из главных основ чтобы

криминализировать спам. Скорее всего возможно обойтись и без уголовной ответственности. Достаточно внести в Кодекс Российской Федерации административную ответственности за незапрашиваемую рассылку.

Нам всем следует помнить, о том, что цифровой мир несет реальные опасности, гораздо проще предупредить их нежели потом преодолевать последствия.

Список использованных источников

1. Елохина, Э. Э. Цифровизация современного социума: достоинства и угрозы / Э. Э. Елохина. — Текст: непосредственный // Молодой ученый. — 2023. — № 24 (471). — С. 187-189. — URL: https://moluch.ru/archive/471/104131/ (дата обращения: 04.12.2023).
2. Кузнецова И.О. ИНФОРМАЦОННЫЕ УГРОЗЫ АКТУАЛЬНАЯ ПРОБЛЕМА БЕЗОПАСНОСТИ ВО ВРЕМЯ ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА В РЕЗУЛЬТАТЕ ВЕДЕНИЯ СВО. XXX Апрельские экономические чтения: материалы Всерос. науч.-практ. конф. (Омск, 18 апр. 2024 г.) / Финансовый ун-т при Правительстве РФ (г. Омск) ; под общ. ред. А. И. Ковалева, О. В. Фрик. – Омск : Изд-во ОмГТУ, 2024. –ISBN 978-5-8149-3786-5.
3. Шляпина Ю. В., Кузнецова И. О. НЕОБХОДИМОСТЬ РАЗВИТИЯ И ВНЕДРЕНИЯ ЭКОНОМИЧЕСКОЙ КИБЕРБЕЗОПАСНОСТИ СРЕДИ ГРАЖДАН СТРАНЫ. XXX Апрельские экономические чтения : материалы Всерос. науч.-практ. конф. (Омск, 18 апр. 2024 г.) / Финансовый ун-т при Правительстве РФ (г. Омск) ; под общ. ред. А. И. Ковалева, О. В. Фрик. – Омск : Изд-во ОмГТУ, 2024. –ISBN 978-5-8149-3786-5.
4. Крицкая, Е. В. Цифровое мошенничество: современные тенденции, способы защиты и превенции / Е. В. Крицкая, Т. А. Коновалова. — Текст: непосредственный // Молодой ученый. — 2020. — № 50 (340). — С. 258-263. — URL: https://moluch.ru/archive/340/76549/ (дата обращения: 06.12.2023).