УДК 004.056

Ерошова Екатерина Алексеевна
студентка
Институт магистратуры и заочного обучения
Саратовская государственная юридическая академия
Россия, Саратов
e-mail: panther02102000@mail.ru

Научный руководитель: Варламова Елена Владимировна
кандидат педагогических наук, доцент
Саратовская государственная юридическая академия
Россия, Саратов

ПРОБЛЕМЫ ПРАВОВОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЭКОСИСТЕМЕ ЦИФРОВОЙ ЭКОНОМИКИ

Аннотация: *В статье автор рассматривает понятие информационной безопасности цифровой экономики, способы ее защиты. Рассматриваются причины развития угроз для цифровой экономики, анализируются мнения разных учёных. Производится анализ зарубежного опыта. Даются некоторые советы для защиты цифровой экономики. Дается теоретический анализ понятийного аппарата и основных признаков киберугроз.*

Ключевые слова: информационная безопасность, цифровая экономика, информационные технологии, киберугрозы.

Yeroshova Ekaterina Alekseevna
student
Institute of Master's Degree and Distance Learning
Saratov State Law Academy
Russia, Saratov

Scientific adviser: Varlamova Elena Vladimirovna,
candidate of pedagogical sciences, associate professor
Saratov State Law Academy
Russia, Saratov

PROBLEMS OF LEGAL PROVISION OF INFORMATION SECURITY IN THE ECOSYSTEM OF THE DIGITAL ECONOMY

Abstract: *In the article, the author examines the concept of information security of the digital economy, ways to protect it. The reasons for the development of threats to the digital economy are considered, the opinions of various scientists are analyzed. The analysis of foreign experience is carried out. Some tips are given to protect the*

digital economy. A theoretical analysis of the conceptual apparatus and the main signs of cyber threats is given.

Key words: information security, digital economy, information technologies, cyber threats.

В условиях бурного развития цифровых технологий с каждым годом появляется множество новых рисков и угроз для цифровой экосистемы. Эти угрозы связаны с обуславливаются не только быстрыми темпами развития цифровых технологий, но и масштабной цифровизации общественной жизни путём повсеместного использования цифровых средства и методы обработки информации. Организации уже не могут обеспечить свою информационную безопасность в условиях новейших технологий, а государство в свою очередь с опозданием даёт юридическую оценку новых технологий. И даже способ стратегического регулирования права в данной сфере не успевает за столь быстрыми изменениями, это связано со сложностью прогнозирования развития технологий на несколько лет вперёд. Только некоторые футурологи рискуют делать долгосрочные прогнозы в данной сфере, так как дать точный прогноз практически нереально. Государство в свою очередь в вопросах информационной безопасности цифровой экономики базируется на первоочередных задачах, срок выполнения этих задач вуалируется разбит на 3-5 летние периоды. Но это не все причины развития угроз в данной сфере к более ярким можно отнести ещё ряд причин [1]:

1. Несовершенство законодательства;
2. Неспособность или не желание бизнеса оперативно реагировать на необходимость развития систем обеспечения информационной безопасности;
3. Низкий уровень образовательных программ в сфере информационной безопасности.

Хотя выше перечисленные причины требуют срочного их устранения для обеспечения цифровой безопасности, но не являются единственными, причины развития угроз в сфере цифровой безопасности экосистемы [2].

Большинство проблем в данной сфере связано с отсутствием целостно политики в вопросах цифровой безопасности на международном уровне, о чем писалось выше. Глобализация общественных отношений не только создает новые тенденции развития общества, но и несёт с собой риски и угрозы безопасности частным и национальным интересам. Для предотвращения этих угроз необходимо не просто реакция отдельного государства, но и разработки международных принципов и подходов, основанных на всестороннем, комплексном правовом, политическом, экономическом, социологическом, психологическом анализе указанных явлений.

Проанализировав мнения учёных поданному вопросу, можно выделить тенденцию поиска альтернативных праву регуляторов именно в цифровой среде. В таком случае большое значение отводится механизмам организационного регулирования и саморегулирования, данный механизм обусловлен самостоятельностью цифровых платформ в обеспечение информационной безопасности в сети Интернет и защиты людей от негативной информации. Для этого данный механизм имеет следующие средства регулирования:

1. Нанесения тех или иных пометок, указаний на новостях как «сомнительные», «спорные» и т.п.;
2. Возможность блокировки аккаунтов в сети Интернет, социальных сетях, блокировки введения информации в чатах за нарушения правил цифровой платформы;
3. Включение отдельных ресурсов в черные списки, отражение данного факта при обращении пользователей к данным ресурсам.

Особая роль в таком саморегулирование цифровой платформы отводится СМИ и иным субъектам информационной сферы. На них возлагаются полномочия по борьбе с распространением негативной информации в сети Интернет. Для этого они наделены разными способами борьбы с такой информацией к ним относятся: информирование общественности о механизмах распространения и распознания негативной информации, опровержение уже имеющейся информации, опровержения с детальным разбором и приведением

доказательств, составление базы данных негативных сообщений и их распространителей.

Важным элементом информационной безопасности цифровой экосистемы является цифровой профиль. Для ответа на вопрос что такое цифровой профиль нужно понять откуда пошло профилирование личности и кому оно выгодно. Изначально организации получали персональные данные о физических лицах из различных источников — результаты интернет-поиска, покупательские привычки, образ жизни и поведенческие данные, собранные с мобильных телефонов, социальных сетей, систем видеонаблюдения и Интернета вещей. После получения этих данных они анализируются, через специальные цифровые платформы чтобы классифицировать людей по различным группам. Этот анализ выявляет корреляции между различными моделями поведения и характеристиками для создания профилей отдельных людей. В итоге такого анализа эти профили будут содержать новые персональные данные об этом человеке.

Государственный цифровой профиль работает по похожим алгоритмам и является совокупностью цифровых записей о физических лицах и юридических лицах, которые содержатся в государственных информационных системах предоставление этих данных обеспечивается использованием технологической инфраструктуры, которая позволяет использовать данные пользователя с согласия, предоставляемого в цифрового носителя цифрового профиля в цифровом виде.

Ярким примером страны, в которой активно используют цифровой профиль, является Китай. Там работает система социального кредита, основывающаяся на цифровом профиле граждан, она учитывает многие факторы экономической и социальной активности человека. К таким факторам относятся: уплата налогов, поведение в обществе, оплата кредитов вовремя, поведения граждан в социальных сетях и многое другое. Все эти данные находят свое отображение в государственной информационной системе и создают рейтинговую систему человека, на основе данного рейтинга граждане имеют или

не имеют расширенные возможности использования услуг. Тем самым социальный рейтинг, отображенный в цифровом профиле гражданина является посредником между государством и гражданином и мотивирует второго на благие действия и поступки, достигать. Однако следует сказать о том, что данный рейтинг имеет ряд минусов и рисков основной риск заключается во вхождении в частную жизнь гражданина. Также при использование данного рейтинга без разрешения гражданина происходит нарушения права на защиту персональных данных.

В России цифровой профиль изначально появился в виде эксперимента, который планировали провести с 1 июля 2019 г. по 31 марта 2020 г. [2]. Согласно данному эксперименту цифровая платформа, на базе которой будет работать цифровой профиль, должная включать в себя сервисы по хранению информации о гражданине и сервис регистрации цифровых согласий. Благодаря сервису цифровых согласий у граждан будет возможность узнать какие системы собирают персональные о них и прежеланные отозвать своё согласие на обработку персональных данных. В 2020 году данный эксперимент решили продлить и расширить перечень собираемых цифровых данных о гражданах информацией из электронной трудовой книжке [3]. Данная информация поможет работодателям удаленно принимать сотрудников на работу.

Банком после продления данного эксперимента было дано разрешение на анализ цифровых профилей с целью заключения любых сделок, а не только кредитных договоров.

Одной из причин возможного сбоя в работе цифровой экосистемы является возможность DDOS атаки на цифровую платформу. DDOS атака представляет собой распределённую атаку, которая создаёт нагрузку на сервер и приводит к отказу системы. При таких условиях пользователи не могут получить доступ к сайту или веб-сервису, а владельцы проектов могут потерять прибыль. Для предотвращения таких атак необходимо рассмотреть проблемы в правовом регулирование данной сферы [3]. Паровое регулировании в данной сфере осуществляется на уровне Конституции РФ, Российской Федерации. Так, в п. «и»

ст. 71 Конституции РФ в число вопросов федерального ведения включены дополнительно информационные технологии [4]; п. «М» расширен за счет включения вопросов обеспечения безопасности личности, общества и государства при применении информационных технологий, обороте цифровых данных. Кибербезопасности в данном случае полностью включается в последний блок отношений, поскольку внешние и внутренние киберугрозы всегда связаны с применением информационных технологий.

Проведя анализ правового обеспечения кибербезопасности на современном этапе его развития, можно с уверенностью сказать о том, что развитие правовых средств, которые должны обеспечивать цифровую безопасность России сильно отстаёт от развития технических, организационных, программно-аппаратных и иных средств. Одной из проблем которая влияет на эффективность правовых средств является отсутствие специального стратегического регулирования по данному вопросу, вследствие чего невозможно создать единый понятийный аппарат. К данной проблеме можно отнести и отсутствия, сформулированных на государственном уровне принципов правового регулирования кибербезопасности в связи с чем, неэффективно применяется система правовых запретов, ограничений в киберпространстве и не развивается система сетевого государственного суверенитета. В России на данном этапе правовые средства связаны с отдельными институтами развития, а не создают единую систему правовых средств, в целом направленных на обеспечение функционирования института кибербезопасности на государственном уровне с учетом единой системы публичной власти в Российской Федерации. К отдельным институтам можно отнести — обеспечения защиты информации ограниченного доступа, в том числе государственной тайны, коммерческой тайны, персональных данных; института критически важной инфраструктуры; противодействия преступлениям в сфере компьютерной информации и другие.

Изучив опыт других стран в области системы современных киберугроз, можно сделать вывод о том, что такие угрозы присущи и России. Просто в нашем

государстве есть свои специфические факторы из-за которых появляются особенные угрозы, к ним можно отнести отсталость оборудования на предприятиях, низкий уровень внедрения программно-аппаратных средств и инноваций в сфере кибербезопасности, и главное нехватка государственных программ и специальной поддержки от государства в данной сфере. Ещё из анализа современных мировых киберугроз следует схожесть и стандартизация большинства правонарушений в сфере киберпространства из этого следует, что важным элементом борьбы в данной сфере является изучения правового опыта зарубежных стран.

Основными мировыми тенденциями в этой сфере являются:

1. Активное развитие правового регулирования данной сферы путём издания нормативно правовых актов в сфере кибербезопасности;
2. Закрепление на государственном уровне системы средств обеспечения кибербезопасности, разработка планов, дорожных карт по реализации установленных средств;
3. Приоритет принципа государственного суверенитета в сфере кибербезопасности при разработке новых правовых актов;
4. системный подход к ограничениям и запретам в киберпространстве с установлением системы органов, осуществляющих контроль и надзор в данной сфере;
5. Внедрения новых государственных программ в сферу образования с целью обучении профессиональных кадров по обеспечению кибербезопасности;
6. Развитие института юридической ответственности в сфере кибербезопасности;
7. Грамотное использование искусственного интеллекта в целях борьбы с киберугрозами;
8. Активная борьба с фейками в сфере цифровой безопасности;

Анализ киберугроз позволил выделить явную тенденцию в последние годы на рост инцидентов, связанных с различными DDOS-атаками. Рост киберугроз и киберпреступности за последний год связывается с пропорциональным ростом

инцидентов, связанных с различными DDOS-атаками. Таким образом, сегодня явно существует необходимость системного правового обеспечения кибербезопасности в России в связи с активным использованием дистанционных технологий электронного взаимодействия.

Список литературы:

1. Вайпан В.А., Егорова М.А. Проблемы создания цифровой экосистемы: правовые и экономические аспекты. М.: Юстицинформ, 2021. 274 с.

2. Соловьева Л.Н. Цифровая идентичность как новый вид идентичности человека информационной эпохи // Общество: философия, история, культура. 2018. № 12 (56). С. 44.

3. Сергеев Л. И. Цифровая экономика. М.: Юрайт, 2022. 332 с.

4. Конституция Российской Федерации (принята всенародным голосованием 12 декабря 1993г.) (с учетом поправок, внесенных Федеральным конституционным законом «О поправках к Конституции РФ» от 30 декабря 2008 г. № 6-ФКЗ, от 30 декабря 2008 г. №7-ФКЗ, от 5 февраля 2014 г. №2-ФКЗ, от 21 июля 2014 г. № 11-ФКЗ, от 14 марта 2020 № 1-ФКЗ)) // Российская газета. 1993 25 дек.; Собрание законодательства РФ. 2020. № 11. Ст. 1416.