Якимова Ульяна Алексеевна
студентка
Научный руководитель
Юн Лариса Владимировна
канд. юрид. наук, доцент
Казанский филиал ФГБОУ ВО «Российский государственный университет правосудия им. В.М. Лебедева»
г. Казань, Республика Татарстан

КОНСТИТУЦИОННО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ В УСЛОВИЯХ РАЗВИТИЯ ЦИФРОВИЗАЦИИ

Аннотация: *в статье рассматривается конституционно-правовое обеспечение кибербезопасности в условиях развития цифровизации. Автор в рамках проводимого исследования обращает свое внимание на ряд актуальных проблем, возникающих в ходе правового обеспечения кибербезопасности в цифровом пространстве и предлагает пути их решения.*

Ключевые слова: *кибербезопасность, цифровизация, кибер-угрозы, правовое обеспечение.*

В эволюции человеческой цивилизации наступила цифровая эпоха, в различной степени охватившая все континенты и страны земного шара. Тридцать лет назад интернет начал быть частью мира. Но только в начале XXI в. информатизация стала реализовываться в развитии развитых стран, что дало ученым и практикам возможность провозгласить начало четвертой промышленной революции, так называемой «Индустрии 4.0».

Данные показатели обусловливают тот факт, что потребность в информационно-коммуникационной сети на данный момент значительно велика в связи с повышением уровня правовой культуры [3; 10; 11], при оказании бесплатной юридической помощи или при последующем обращении в органы судебной власти [4; 6–9].

Content is licensed under the Creative Commons Attribution 4.0 license (CC-BY 4.0)

Отметим, что цифровизация и искусственный интеллект представляют собой основу современного бытия общества. Сейчас уже практически невозможно представить нашу повседневную жизнь без многочисленных инноваций. Но не стоит забывать о том, что вместе с развитием приходят и новые опасности. Так, например, может произойти вредоносное вмешательство в информационную систему другого человека, в том числе и в сфере трудовых отношений [10].

Кто владеет информацией, тот владеет миром – всеми известная фраза, смысл которой заключается в том, что при грамотном использовании определенных сведений человек способен сосредоточить всю власть в своих руках. При этом важно понимать, чтобы данная власть не повлекла за собой негативные последствия в виде преступлений. В этом случае важную роль играют следственные органы.

Р.А. Шарифуллин, Р.С. Бурганов, Р.Г. Бикмиев считают, что необходимо также ввести институт следственного судьи в уголовном процессе для разрешения уголовно-правовых споров либо о привлечении обвиняемого лица к ответственности либо о его освобождении [13].

«...В действительности, к сожалению, чаще всего информационная цифровизация усугубляет процессы социального и правового неравенства. Проблема цифрового равенства напрямую затрагивает уже существующие проявления расслоения граждан, усиливает риск злоупотребления тем или иным правом, появление которого непосредственно связано с цифровизацией. Все это актуализирует проблему обеспечения конституционного равенства в условиях становления информационно-цифрового пространства и его конституционализации...» [1, с. 27].

«...Под угрозой кибербезопасности понимаются различные действия, которые могут привести к нарушениям состояния защиты информации. Другими словами, это потенциально возможные события, процессы или действия, которые могут нанести ущерб информационной или киберсреде...» [2].

Содержимое доступно по лицензии Creative Commons Attribution 4.0 license (CC-BY 4.0)

Целью кибербезопасности является защита персональных данных российских граждан, а также предотвращение и смягчение последствий любых воздействий, причиняющих вред и наносящих ущерб информации (копирование, искажение, передача третьим лицам или вовсе ее удаление) [5].

К методам предотвращения угроз кибербезопасности относят меры, позволяющие защитить киберпространство от случайных или наоборот злонамеренных внешних и внутренних угроз. Методы предотвращения угроз кибербезопасности охватывают комплекс мер, направленных на защиту киберпространства от случайных либо намеренно вредоносных внешних и внутренних воздействий, причем эффективность таких мер определяется не столько их количеством, сколько системностью и согласованностью между собой. В науке и практике принято выделять несколько взаимодополняющих уровней: организационно-правовой (разработка политик безопасности, регламентов доступа, обучение персонала), технический (межсетевые экраны, системы обнаружения вторжений, антивирусная защита, шифрование данных) и процедурный (резервное копирование, аудит, реагирование на инциденты). Примечательно, что ни один из этих уровней в отдельности не способен обеспечить должный уровень защищенности, поскольку уязвимость, не устраненная на организационном уровне, рано или поздно проявится на техническом, и наоборот.

Особого внимания заслуживает разграничение превентивных и реактивных методов: если первые нацелены на недопущение угрозы (сегментация сетей, многофакторная аутентификация, контроль целостности), то вторые обеспечивают минимизацию последствий уже состоявшегося инцидента (изоляция зараженных узлов, восстановление из резервных копий, криминалистический анализ). Однако жесткое противопоставление этих групп было бы методологически неверным, поскольку граница между ними подвижна: хорошо выстроенная система реагирования сама по себе выполняет превентивную функцию, снижая привлекательность объекта для злоумышленника. В этом смысле кибербезопас-

Content is licensed under the Creative Commons Attribution 4.0 license (CC-BY 4.0)

ность следует рассматривать не как статичный набор инструментов, а как непрерывный процесс адаптации к меняющемуся ландшафту угроз, что требует постоянного пересмотра применяемых методов и их правового обеспечения.

Всевозможные угрозы кибербезопасности можно подразделить на несколько подгрупп: несанкционированный доступ, потеря информационных данных, кибератаки и кибервойны, мошенничество, утечка информации и нежелательный контент.

Помимо мошенничества наиболее акутальными киберпреступлениями являются «продажа» и «утечка» информации. Объективная сторона составов правонарушений отражает действие или бездействие. Оператор информации не обеспечил надлежащую защиту, т.е. кибербезопасность. Множество утечек информации с персональными данными наблюдается в страховых организациях, в банках, у сотовых операторов и в интернет-магазинах. В связи с этим недобросовестные работники таких организаций продают информационные базы мошенникам. Данные варианты злоупотреблений требуют новых вариативных методов решения проблемы, в том числе и в ходе помощи составления исковых заявлений в суд [12].

Резюмируя, подчеркнем, что несмотря на то, что цифровые технологии функционируют и активно развиваются во всех сферах жизнедеятельности нашего государства, киберузгрозы оказывают негативное воздействие и требуют более детального правового обеспечения.

Список литературы

1. Бондарь, Н. С. Информационно-цифровое пространство в конституционном измерении: из практики Конституционного Суда Российской Федерации / Н. С. Бондарь // Журнал российского права. – 2019. – № 11. – С. 25–42.

2. Курбанова, Н. Э. Методы предотвращения угроз кибербезопасности / Н. Э. Курбанова. – URL: https://cyberleninka.ru/article/n/metody-predotvrascheniya-ugroz-kiberbezopasnosti/viewer (дата обращения: 28.08.2026). – Текст : электронный.

Содержимое доступно по лицензии Creative Commons Attribution 4.0 license (CC-BY 4.0)

3. Юн, Л. В. Конституционное правопонимание как важный элемент конституционного судопроизводства / Л. В. Юн // Ученые записки Казанского филиала «Российского государственного университета правосудия». – 2023. – Т. 19. – С. 41–44.

4. Юн, Л. В. Судебная защита экологических прав человека и гражданина в национальном праве: актуальные проблемы / Л. В. Юн // Теория и практика социогуманитарных наук. – 2023. – № 3 (23). – С. 130–134.

5. Юн, Л. В. Обеспечение экологической безопасности в национальном и международном праве / Л. В. Юн // Вестник Московского государственного областного университета. Серия: Юриспруденция. – 2023. – № 1. – С. 110–118.

6. Шарифуллин, Р. А. Проблемы и перспективы создания института следственного судьи в уголовном процессе России / Р. А. Шарифуллин, Р. С. Бурганов, Р. Г. Бикмиев // Мировой судья. – 2020. – № 5. – С. 16–21.

Content is licensed under the Creative Commons Attribution 4.0 license (CC-BY 4.0)