УДК 342.7(476)

БОРЬБА С КИБЕРУГРОЗАМИ И ЗАЩИТА ПРАВ ГРАЖДАН РЕСПУБЛИКИ БЕЛАРУСЬ В ЦИФРОВОМ ПРОСТРАНСТВЕ

Д.В. Берёзко
ВГУ имени П.М. Машерова, Республика Беларусь

Аннотация. В статье рассматриваются вопросы, связанные с кибербезопасностью и защитой прав граждан в условиях современного цифрового мира. Обозначены киберугрозы, с которыми сталкиваются граждане Беларуси ежедневно, включая фишинг, вредоносное программное обеспечение и DDoS-атаки. Анализируется законодательство и политика в области кибербезопасности, а также роль государства в борьбе с киберугрозами. Подчеркивается важность образования и информированя граждан в сфере кибербезопасности. Рассматриваются вопросы защиты прав граждан в цифровом пространстве, включая защиту личных данных и конфиденциальности.

Ключевые слова: киберугрозы, кибербезопасность, цифровое пространство, защита прав граждан, кибератаки, концепция национальной безопасности

Тема исследования является актуальной и важной в современном мире. С развитием информационных технологий и интернета киберугрозы стали серьезной проблемой, которая может негативно сказываться на безопасности и правах граждан.

В цифровом пространстве граждане Республики Беларусь сталкиваются с различными видами киберугроз, такими как: хакерские атаки, фишинг, кибершпионаж, распространение вредоносного программного обеспечения и многие другие. Эти угрозы могут привести к утечке личной информации, финансовым потерям, нарушению прав на приватность и даже к угрозе национальной безопасности.

Для борьбы с киберугрозами и защиты прав граждан в цифровом пространстве Республика Беларусь принимает ряд мер и разрабатывает соответствующие нормативные правовые акты (например, Министерство связи и информатизации Республики Беларусь, которое занимается координацией действий по защите информации и борьбе с киберпреступностью).

Также реализуются образовательные программы и кампании, направленные на повышение информированности граждан о кибербезопасности. Гражданам рекомендуется быть внимательными при обращении с личной информацией в интернете, использовать надежные пароли, устанавливать антивирусное программное обеспечение, регулярно обновлять программы и операционные системы.

Однако, несмотря на предпринимаемые меры, киберугрозы постоянно эволюционируют, и необходимо постоянно совершенствовать методы защиты и борьбы с ними. Поэтому важно, чтобы граждане Республики Беларусь знали о последних трендах в кибербезопасности и принимали соответствующие меры предосторожности.

Цель статьи – повысить осведомленность о киберугрозах и предложить рекомендации по защите прав граждан в цифровом пространстве Республики Беларусь. Статья позволяет лучше понять значение борьбы с киберугрозами и принять меры для защиты своих прав и конфиденциальности в цифровом пространстве.

Материал и методы. Материалом для исследования послужили нормативные правовые акты: Указы Президента Республики Беларусь от 9 ноября 2010 г. № 575 «Об утверждении Концепции национальной безопасности Республики Беларусь», от 14 февраля 2023 г. № 40 «О кибербезопасности»; Закон Республики Беларусь от 07.05.2021 № 99-З «О защите персональных данных», Постановление Совета безопасности Республики Беларусь от 6 марта 2023 г. №1 «О рассмотрении проекта новой Концепции национальной безопасности Республики Беларусь».

При проведении исследования использовались следующие методы: анализа, синтеза, логико-юридический, сравнительно-правовой и др.

Результаты и их обсуждение. Киберугрозы представляют серьезную опасность для Беларуси, также как и для многих других стран. В последние годы наблюдается значительное увеличение случаев кибератак, включая хакерские атаки, фишинг, вредоносные программы и другие виды киберпреступности.

Одна из основных угроз – это хакерские атаки на государственные организации, критическую инфраструктуру и крупные компании. Такие атаки могут привести к утечке конфиденциальной информации, нарушению работы систем и серьезным экономическим потерям. Также существует угроза для отдельных пользователей, включая фишинговые попытки получить личную информацию, вредоносные программы, направленные на кражу финансовых данных или шантаж, и другие виды мошенничества.

Для борьбы с киберугрозами в Беларуси были приняты меры по улучшению законодательства, расширению сотрудничества с международными организациями, проведение широкомасштабной информационно-просветительской кампании. Кроме того, в соответствии с Указом Президента Республики Беларусь от 14 февраля 2023 г. № 40 «О кибербезопасности» в стране будет создана национальная система обеспечения кибербезопасности, элементами которой станут:

– Оперативно-аналитический центр при Президенте Республики Беларусь;

– Национальный центр обеспечения кибербезопасности и реагирования на киберинциденты;

– центры обеспечения кибербезопасности и реагирования на киберинциденты объектов информационной инфраструктуры государственных органов и иных организаций;

– оператор электросвязи по взаимодействию Национального центра кибербезопасности, центров кибербезопасности, а также государственных органов и иных организаций;

– объекты информационной инфраструктуры государственных органов и иных организаций;

– сети передачи данных, используемые для взаимодействия элементов национальной системы обеспечения кибербезопасности [2].

Тем не менее, это постоянно развивающаяся область, и важно, чтобы государство, субъекты хозяйствования и отдельные пользователи принимали меры для защиты своей информации и сетевых ресурсов.

Так, Концепция национальной безопасности Республики Беларусь 2010 г., утвержденная Указом Президента Республики Беларусь от 9 ноября 2010 г. № 575 «Об утверждении Концепции национальной безопасности Республики Беларусь» (далее – Концепция), не содержит упоминания о киберпреступности. В пункте 34 главы 5 Концепции в качестве внутреннего источника угрозы национальной безопасности в информационной сфере указывается рост преступности с использованием информационно-коммуникационных технологий [1].

Постановлением Совета безопасности Республики Беларусь от 6 марта 2023 г. № 1 предложен к рассмотрению проект новой Концепции национальной безопасности Республики Беларусь (далее – проект Концепции). В данном проекте Концепции значительное внимание уделяется вопросам кибербезопасности и киберпреступности. В проекте Концепции кибербезопасность критической инфраструктуры определяется как условие обеспечения устойчивости всех сфер жизнедеятельности [4].

Кроме того, в качестве одной из основных угроз национальной безопасности выделяется нарушение киберустойчивости национального сегмента сети Интернет, критически важных объектов информатизации и государственных информационных систем [4]. Это свидетельствует о том, что вызовы новейшего времени требуют от Республики Беларусь сосредоточения особого внимания на проблемах, вызванных развитием современных технологий. Если ранее данное направление не выделялось как самостоятельное, то бурное развитие информационных технологий, происходящее в последнее десятилетие, заставляет принимать ответные меры.

В этой связи в качестве одного из важнейших направлений нейтрализации внутренних источников угроз национальной безопасности в информационной сфере в проекте Концепции указывается развитие национальной системы обеспечения кибербезопасности [4]. В проекте Концепции уделено особое внимание расширению сотрудничества с другими странами и международными организациями в области кибербезопасности. Вместе с тем, представляется целесообразным дополнить пункт 59 главы 8 проект Концепции мерами по укреплению защиты информационных систем и повышению осведомленности о киберопасности в обществе.

Борьба с киберугразами осуществляется на различных уровнях, в том числе путем проведения профилактических и образовательных мероприятий. Всплеск таких проявлений противоправной деятельности злоумышленников как фишинг, распространение вредоносного программного обеспечения и совершение DDoS-атак, направленных на физические и юридические лица, которые ранее не сталкивались с такого рода угрозами, потребовал оперативного привлечения внимания общественности к проблеме. В качестве наиболее эффективных способов информирования населения о киберугрозах можно выделить размещение информационных материалов в СМИ, проведение работниками банков и сотрудниками правоохранительных органов встреч с трудовыми коллективами и обучающимися учреждений образования различного уровня.

Поскольку злоумышленники постоянно совершенствуют способы и методы совершения киберпреступлений важно уделять внимание формированию общей культуры поведения населения в виртуальном пространстве, понимания важности и необходимости упорядочения распространения персональных данных.

Так, Закон Республики Беларусь от 07.05.2021 № 99-З «О защите персональных данных» заложил основы правового регулирования вопросов защиты персональных данных, прав и свобод физических лиц при обработке их персональных данных. Несмотря на определенные трудности с практической реализацией данного нормативного акта, в целом можно отметить его позитивное влияние на цифровое информационное пространство. Граждане и юридические лица все больше внимания обращают на важность недопущения бесконтрольного распространения персональных данных, поскольку ряд киберперступлений совершается исключительно благодаря получению доступа к персональным данным со стороны злоумышленников.

Чаще всего киберпреступники выдают себя за людей из действующих на законных основаниях организаций и учреждений, чтобы обманом вынудить граждан раскрыть личную информацию и предоставить преступникам деньги, товары и/или услуги. Мишенью киберпреступников становятся информационные ресурсы, принадлежащие банковскому сектору, государственным органам и коммерческим организациям, а также конфиденциальная информация, персональные данные, имущество и денежные средства граждан.

Ограничения свободного доступа к персональным данным, а также создание ограничений к распространению и обработке такого рада информации, в значительной степени позволяет сократить количество противоправных действий злоумышленников.

Заключение. Таким образом, уровень безопасности информационного пространства государства непосредственно влияет на возможность реализации прав и свобод граждан, на сохранение суверенитета и обеспечение стабильного развития экономики. В связи с распространяющимися киберугрозами и угрозами кибертерроризма важно проводить целенаправленную работу по эффективному обеспечению кибербезопасности цифрового и информационного пространства государства и недопущению деструктивных кибератак, краж цифровых данных и распространения фейков. Противостоять киберугрозам – одна из важнейших комплексных задач обеспечения информационной безопасности личности, экономики и государства.

Список использованных источников

1. Об утверждении Концепции национальной безопасности Республики Беларусь [Электронный ресурс]: Указ Президента Республики Беларусь от 9 ноября 2010 г. № 575: в ред. Указа Президента Республики Беларусь от 24.01.2014 № 49 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

2. О кибербезопасности [Электронный ресурс]: Указ Президента Республики Беларусь от 14 февраля 2023 г. № 40 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

3. О защите персональных данных [Электронный ресурс]: Закон Республики Беларусь от 07.05.2021 № 99-З: в ред. Закона Республики Беларусь от 01.06.2022 № 175-З // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

4. О рассмотрении проекта новой Концепции национальной безопасности Республики Беларусь [Электронный ресурс]: Постановление Совета безопасности Республики Беларусь от 6 марта 2023 г. № 1 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2023.

УДК 340

ПРОБЛЕМНЫЕ ВОПРОСЫ ДЕЯТЕЛЬНОСТИ ОРГАНОВ ПРОКУРАТУРЫ РЕСПУБЛИКИ БЕЛАРУСЬ

Ю.С. Бутримова

ВГУ имени П.М. Машерова, Республика Беларусь

Аннотация. В статье приводиться анализ различных точек зрения на вопросы конституционно-правового регламентации деятельности органов прокуратуры Республики Беларусь. Автор делает выводы о необходимости формулирования единой позиции в понимании и раскрытии содержания важных категорий для прокурорского надзора.

Ключевые слова: прокуратура, деятельность прокуратуры, конституционно-правовое регулирование, направления деятельности, надзор, осуществление полномочий.

Статус прокуратуры регламентируется на высшем конституционном уровне. Так правовому статусу данного органа посвящена целая глава Конституции Республики Беларусь. Закон «О прокуратуре Республики Беларусь» установил фундаментальную отрасль прокурорского надзора – надзор за соблюдением законодательства Республики Беларусь, приоритетом которого является защита прав и свобод человека и гражданина.

В юридической науке традиционным является вопрос о месте данного государственно-правового института в системе разделения властей. Однако мало внимания уделено вопросам законодательного закрепления понятий «направление деятельности прокуратуры» и «отрасль прокурорского надзора», а также их четкой дифференциации. Мнения авторов по данному вопросу существенно отличаются, а отсутствие единой позиции в понимании и раскрытии содержания таких принципиальных, с точки зрения прокурорского надзора, категорий приводит к теоретической путанице, что, безусловно, негативно отражается впоследствии и в правоприменительной деятельности.

Цель исследования – исследование основной сферы деятельности отечественной прокуратуры – прокурорского надзора, его правовых основ, видов и содержания, отражения роли и места прокурорского надзора в становлении правового государства.

Материалы и методы. Методологическую основу исследования составляют общенаучный диалектический метод, частнонаучные методы: системный, логический, сравнительно-правовой, статистический, социологический методы познания, а также методы наблюдения и анализа документов.