УДК 4414

Осипов Георгий Дмитриевич,
студент магистратуры
Юридический факультет,
Российский государственный университет правосудия
Россия, г. Москва
e-mail: sheismylife@ya.ru

ПРОБЛЕМАТИКА В СФЕРЕ КИБЕРБЕЗОПАСНОСТИ

Аннотация: *В статье рассматриваются вопросы кибербезопасности как инструмента минимизации финансовых рисков хозяйствующих субъектов. В исследовании освещены основные принципы кибербезопасности, нарушение которых может привести к негативным последствиям.*

Ключевые слова: кибербезопасность, кибератаки, гиберугрозы, аудит.

Osipov George Dmitrievich,
master student
Faculty of Law,
Russian State University of Justice
Russia, Moscow

THE ISSUES OF CYBERSECURITY

Abstract: *The article addresses cybersecurity issues as a tool to minimize the financial risks of business entities. The study highlights the basic principles of cybersecurity, the violation of which can lead to negative consequences*

Key words: cybersecurity, cyber attacks, hiberrosis, audit.

Актуальность исследования обусловлена быстрым развитием информационных и коммуникационных технологий (ИКТ), которые усиливают свое влияние во всех ключевых сферах личности, общества и государства; рост числа кибератак на системы управления критическими технологиями; кража активов банка; утилизация энергосистем и атомной промышленности; повышение эффективности средств деструктивного информационного воздействия как следствие увеличения возможностей информационных систем; необходимость обновления и пересмотра сегодняшних правовых норм, выступающих в качестве основного средства регулирования информационных отношений [4, с. 90].

Анализ динамики зарегистрированных преступлений на территории Российской Федерации, совершенных в сфере телекоммуникаций и компьютерной информации, за период 2017-2019 гг. Показывает, что их количество ежегодно увеличивается. Так, если в 2015 году было зарегистрировано 43657 5 (+ 298,5%) преступлений, в 2017 году - 65949 (+ 50,5%), в 2018 году - 90587 (+ 37,4%), то за 9 месяцев 2019 года - 121247 (+ 93,9%).

Наше общество все больше осознает вопросы безопасности как одну из важнейших проблем своего существования. Современные государства все больше зависят от безопасности технологий, которые они используют, в первую очередь компьютерной информации и кибертехнологий. Большое количество и сложность вызовов кибербезопасности требует глубокого научного изучения. Институт системного анализа РАН - один из ведущих исследовательских центров, занимающихся проблемами управления кибербезопасностью. В последнее время в России все чаще используется термин «кибербезопасность» [1, с. 43].

Примеров более чем достаточно:

- хакеры ИГИЛ взламывают аккаунты Министерства обороны США в социальных сетях и активно развивают социальные сети;

- смерть французских карикатуристов из Charlie Hebdo разоблачает конфликт между традиционной исламской и современной постхристианской культурами в Европе;

- полномасштабная информационная война в связи с событиями на Украине, СМИ с российским участием становятся объектами воздействия.

Следовательно, они являются ключевым компонентом системы защиты киберпространства. Если не вдаваться в нюансы терминологии, то кибербезопасность - это безопасность информации и поддерживающей инфраструктуры в цифровой среде.

Также необходимо учитывать, что существует несколько уровней проблем и решений: от частных, связанных с защитой граждан и конкретного человека,

от различных типов злоумышленников до государственных и наднациональных, где решаются вопросы национальной безопасности и информационных войн. Фактически, вопросы информационной безопасности, включая кибербезопасность, решаются всеми ветвями власти: законодательной, исполнительной и судебной. Это предусмотрено Федеральным законом от 28 декабря 2010 г. № 390-ФЗ «О безопасности». Закон гласит, что общее руководство 61 органом государственной безопасности в Российской Федерации осуществляется Президентом. Помимо государственных органов и институтов управления безопасностью, в обществе сформирована и действует система неправительственных организаций, общественных объединений, движений граждан, коммерческих структур, объединений юридических и физических лиц. Ключевое событие и диск Информационную платформу по кибербезопасности в России смело можно назвать Форумом по кибербезопасности (в 2019 году он проводился в июне с темой «Безопасный Интернет будущего») [3, с. 88].

Помимо проблем информационной безопасности, они также обсуждают безопасность коммуникаций в СМИ, вредоносные технологии распространения информации, а также возможность влияния на людей через СМИ. Важно, что во время таких встреч участники обсуждают и разрабатывают законодательные решения, которые напрямую влияют на работу СМИ на базовом, инфраструктурном уровне, и устанавливают пределы возможностей и ответственности авторов публикаций.

Примечательно, что стратегии национальной безопасности в Сети появились относительно недавно. Соединенные Штаты, как один из лидеров в развитии этого направления, приобрели национальную стратегию кибербезопасности только в 2003 году. Например, Франция разработала собственные правила и положения только в 2011 году, а общая стратегия для Европейского Союза появилась только в Февраль 2013 г. Другими словами, проблемы кибербезопасности выросли из частных проблем до межгосударственного уровня всего за пару десятилетий. Таким образом, поощряется межведомственное сотрудничество и государственно-частное

партнерство внутри стран и межгосударственное сотрудничество за пределами страны.

Гражданское общество и журналистика как публичный институт должны способствовать поддержанию этого баланса: использование гибкой стратегии со стороны государства должно способствовать развитию фактов и практики принятия решений (на основе массивов знаний, мониторинга киберугроз и схемы реагирования). В 2015 году контроль и борьба с кибертерроризмом явно усилились, но более активное участие граждан и СМИ в построении системы сетевой безопасности принесет пользу всем участникам.

Не случайно революции получили название «Твиттер» или «информационные» революции из-за колоссальной роли социальных сетей в механизме беспорядков [2, с. 50]. Именно поэтому слова президента РФ Владимира Путина, сказанные 7 апреля 2014 года на расширенной коллегии ФСБ, сегодня чрезвычайно актуальны. Президент особо отметил рост числа межэтнических провокаций с использованием современных информационных средств и технологий, в том числе Интернет и социальные сети. «Я считаю, что сегодня, как никогда раньше, гражданское общество должно не только обращать внимание на эту проблему, но и помогать государству эффективно и быстро решать ее», - подчеркнул Владимир Путин. Основано в основном на выполненном по прогнозам аналитиков РАЭК, GROUPIB и «Лаборатории Касперского» на прошедший год можно выделить несколько ключевых тенденций в области кибербезопасности:

1. Тенденции регулирования Интернета во всех сферах будут только усиливаться. Активно продолжится разработка новых законопроектов и поправок к действующему законодательству в области ИКТ и компьютерной информации.

2. Актуальность Тема цифрового суверенитета Российской Федерации будет и дальше расти, особенно в связи с обострением отношений с Западом и санкциями против России.

3. Значение органов государственной власти и их влияние на интернет-индустрию и телекоммуникационные компании возрастет, но также будет активизироваться встречное движение со стороны бизнеса и профессионального сообщества, институтов гражданского общества в виде инициатив, совместных проектов и решений.

Основные направления межгосударственного и международного сотрудничества, включая институты гражданского общества в сфере противодействия высокотехнологичному терроризму, могут быть рассмотрены в контексте правовых и управленческих решений.

В целом необходимо отметить, что действующее законодательство, основанное на нормах Конституции РФ и международного права, предоставляет государству ряд возможностей противодействия киберпреступности уголовно-правовыми, административными и гражданско-правовыми методами.

Наиболее острым инструментом регулирования отношений в борьбе с этими преступлениями является уголовное право. Закон предусматривает применение суровых наказаний к лицам, ущемляющим интересы личности, общества и государства. Однако эта тема недостаточно изучена в юридической науке и, в частности, в уголовном праве.

В отечественной литературе отсутствует определение понятия «кибербезопасность» во всех его проявлениях, в том числе в криминальном и судебно-медицинском аспектах, недостаточное исследование политико-правовых проблем обеспечения национальной безопасности Российской Федерации в сфере кибербезопасности. , анализ основных проблем государственной политики в области кибербезопасности показал, что существует необходимость выделения кибербезопасности в отдельный вид безопасности; Предлагаются меры по совершенствованию нормативно-правовой базы обеспечения кибернетической безопасности Российской Федерации. Автор формулирует определение кибербезопасности, под которым понимается состояние защиты от внутренних и внешних угроз государству, обществу, объекту информатизации и компьютерных систем общего и специального

назначения, заключающееся в их надежном и полностью корректном функционировании в киберпространство в условиях бурного развития ИКТ.

Список литературы:

1. Багмет А.М. Уголовное право. Словарь терминов. М.: ЮНИТИ-ДАНА, 2018. 99 с.

2. Гельдибаев М.Х. Уголовное право в схемах и определениях. СПб.: Юридический центр Пресс, 2018. 520 с.

3. Гладышев Ю.А. Уголовное право России. Общая часть в определениях и схемах: учебное пособие. М.: Российский государственный университет правосудия, 2017. 216 с.

4. Скурко Е.В. Уголовное право и криминология: актуальные проблемы взаимодействия. СПб.: Юридический центр Пресс, 2018. 128 с.