Киселев Сергей Владимирович, Магистрант 3 курса
направления подготовки 40.04.01 «Юриспруденция»
Ростовского института (филиала) ВГУЮ (РПА Минюста России)

Научный руководитель: **Семенцова Ирина Анатольевна,**
к.ю.н., доцент кафедры Уголовного права и криминологии
Ростовского института (филиал) ВГУЮ (РПА Минюста России)

ОБЩАЯ ХАРАКТЕРИСТИКА МЕХАНИЗМА ПРОТИВОДЕЙСТВИЯ ПРЕСТУПНОСТИ В ИНФОРМАЦИОННОЙ СФЕРЕ

Аннотация: В статье рассмотрены актуальные вопросы противодействия преступности в информационной сфере. Установлено, что механизм противодействия включает в себя международный и внутригосударственный уровни; комплекс мероприятий, направленных на предотвращение киберпреступности состоит из общесоциальных и специальных мер. Выявлены недостатки профилактического воздействия на информационную преступность.

Ключевые слова: преступность в информационной сфере, противодействие преступности, киберпреступность, кибербезопасность.

Ускоренное развитие ИТ сферы и цифровизация общества сопровождается с одной стороны, ростом количества киберпреступлений, распространением разнообразных методов и технологий кибератак, с другой стороны, предоставляет возможность эффективнее от них защищаться. Поиск механизмов и инструментов обеспечения информационной безопасности в частности, разработка соответствующих технологий, является актуальным и важным направлением деятельности государства.

Вопросы информационной безопасности не новы. Например, во время холодной войны Советское правительство разработало сложную систему систематизации информации, в соответствии с которой печатные документы были четко определены по уровню их секретности. В начале развития эры компьютерной техники, компьютерной безопасностью в организациях в большинстве случаев занималась команда профессионалов по организации информационных систем и технологий ИТ, которая часто имела опыт и средства для обеспечения физического и электронного доступа к компьютерному оборудованию и услугам. Поскольку компьютеры перешли к системам совместного использования ресурсов, требуют значительных ресурсов, разработки соответствующей стратегии, механизмов противодействия киберпреступлениям и координации действий между различными субъектами рынка, ответственность за безопасность вышла далеко за рамки ИТ-команды любой отдельной организации. Поскольку Интернет стал более распространенным в обычной жизни, есть все большее осознание того, что кибербезопасность не может быть просто реакцией на возникающие проблемы, она должна предупреждать угрозы киберпреступлений. Более того, подходы к обеспечению кибербезопасности больше не являются в основном техническими.

Преодоление киберпреступности в обществе является основополагающим для мирового сообщества. Генеральным секретарем ООН в 1999 г. было признано существование проблемы в сфере международной информационной безопасности и была принята Резолюция Генеральной Ассамблеи ООН 53/70 от 4 января 1999 г. «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» [2, с. 36-40]. В дальнейшем было одобрено несколько резолюций [2, 3] и документов ООН, представлены доклады Группы правительственных экспертов, что и сформировало на сегодняшний день ядро регулирования вопросов международной информационной безопасности в рамках ООН [4, с. 103].

Эффективность кибербезопасности зависит не только от действий ООН, она должна достигаться превентивными мерами и иметь поддержку во всем обществе. Ее нельзя обеспечить с помощью одной только технологии, планированием и управлением кибербезопасностью, ее обеспечение во всем обществе должно быть приоритетной задачей.

Международная политика безопасности в информационной сфере включает в себя: взаимодействие субъектов государств, компаний для борьбы с киберпреступностью, участие в международных организациях, которое способствует этому взаимодействию.

Следует отметить, что для достижения кибербезопасности не только весь мир должен противодействовать киберпреступлениям, но и каждое государство, компания и отдельный человека должны внедрять собственную стратегию противодействия преступности в информационной сфере.

Противодействие преступности в информационной сфере в Российской Федерации представляет собой комплекс мероприятий, направленных на предотвращение правонарушений и устранение причин, способствующих их совершению. Эти меры можно классифицировать на общесоциальные и специальные, каждая из которых имеет свои характеристики и цели.

Общесоциальные меры направлены на создание атмосферы стабильности и доверия в обществе. Они включают: поддержку образования и культуры, правовую пропаганду и создание условий для социальной активности. Уровень образования и культурного развития населения напрямую влияет на уровень преступности. Исследования показывают, что более образованные граждане менее склонны к совершению правонарушений. Осуществление правового воспитания и формирование законопослушного поведения среди граждан. Стимулирование граждан к участию в общественной жизни способствует снижению уровня преступности.

Специальные меры направлены на устранение конкретных причин преступности и могут быть разделены на несколько категорий:

– профилактика включает общие и индивидуальные меры, направленные на предупреждение преступлений на ранних стадиях формирования антисоциальных установок у граждан.

– Предотвращение направлено на недопущение совершения уже запланированных преступлений, оно включает работу с потенциальными правонарушителями.

– пресечение осуществляется через контроль за поведением лиц, находящихся под подозрением, а также через оперативные мероприятия правоохранительных органов.

Индивидуальная профилактика включает в себя: профилактические беседы (разъяснение ответственности за возможные правонарушения и убеждение в необходимости законопослушного поведения), наблюдение за поведением (контроль за лицами, склонными к совершению преступлений, с целью предотвращения их действий), работу с окружением (привлечение родственников и общественности для создания поддержки и контроля за поведением потенциальных правонарушителей).

Эффективная профилактика преступности в информационной сфере требует комплексного подхода, который сочетает как общесоциальные, так и специальные меры. Это включает в себя как работу с обществом в целом, так и индивидуальное воздействие на конкретных лиц, что позволяет значительно снизить уровень правонарушений и создать безопасную среду для граждан.

Несмотря на усилия в противодействии преступности в информационной сфере, существует ряд недостатков. Недостатки профилактического воздействия на информационную преступность можно сгруппировать в нескольких ключевых аспектах:

1. Ограниченная осведомленность населения. Одним из основных недостатков является недостаточная осведомленность граждан о киберугрозах и методах защиты. Несмотря на усилия правоохранительных органов и образовательных учреждений, многие пользователи остаются уязвимыми из-за отсутствия знаний о безопасном поведении в интернете. Например, распространение информации о фишинге и других киберугрозах не всегда достигает целевой аудитории, что приводит к тому, что многие люди становятся жертвами мошенников.

2. Быстрое развитие технологий. Технологический прогресс создает новые возможности для киберпреступников, что делает существующие меры профилактики устаревшими. Киберпреступники используют современные технологии и методы, такие как искусственный интеллект для создания фишинговых атак, что затрудняет их выявление и предотвращение. Профилактические меры часто не успевают за эволюцией угроз, что требует постоянного обновления знаний и навыков специалистов в области информационной безопасности.

3. Недостаток ресурсов и координации. Правоохранительные органы сталкиваются с ограниченными ресурсами для борьбы с киберпреступностью. Часто отсутствует координация между различными государственными и частными организациями, что затрудняет обмен информацией о новых угрозах и методах их предотвращения. Это также включает недостаточную материально-техническую базу для расследования киберпреступлений, что делает их раскрытие более сложным.

4. Проблемы с законодательством. Законодательство в области киберпреступности часто оказывается неэффективным из-за своей разрозненности и устаревания. В большинстве случаев оно не охватывает все аспекты современных киберугроз, что создает пробелы в правоприменении. Необходимость постоянного обновления законодательства и ужесточения наказаний за киберпреступления также подчеркивает важность адаптации правовых норм к новым реалиям.

5. Социальные факторы. Социальные факторы, такие как рост онлайн-взаимодействий и изменение поведения молодежи в интернете, также влияют на эффективность профилактических мер. Увеличение случаев кибербуллинга и манипуляций в сети требует более глубокого анализа и разработки специфических программ профилактики для уязвимых групп населения.

Отмеченные недостатки требуют комплексного подхода для их устранения. Это включает улучшение образовательных программ, обновление законодательства, а также усиление координации между различными заинтересованными сторонами.

В целом, реализация предложенных мер должна проводиться комплексно и систематически. Необходимо учитывать специфику каждой отрасли и разрабатывать отдельные стратегии для ее защиты. В работе по противодействию киберпреступлениям необходимо учитывать интересы граждан и обеспечить баланс между безопасностью и свободой информации.

Список литературы:

1. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности: Резолюция Генеральной Ассамблеи ООН 53/70 от 4 января 1999 г. / Официальный сайт ООН. URL: https://www.un.org/ga/search/view_doc.asp?symbol=A/RES/53/70&referer=/english/&Lang=R

2. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности: Резолюция A/K.E8/73/27 от 5 декабря 2018 г. / Официальный сайт ООН. URL: https://www.un.org/en/ga/search/view_doc.asp?symbol=A/ RES/73/27&Lang=R

3. Advancing responsible State behaviour in cyberspace in the context of international security: Резолюция Генеральной Ассамблеи ООН 73/264 от 22 декабря 2018 года/ Официальный сайт ООН. URL: https:// www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/73/266

4. Сидорова Т. Ю. Международная информационная безопасность: правовые аспекты и деятельность ООН // Сибирский юридический вестник. – 2020. – №3 (90). – С. 103-108.