

УДК 343.98:004:366.54

НЕКОТОРЫЕ АСПЕКТЫ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ КАК НАПРАВЛЕНИЯ ГОСУДАРСТВЕННОЙ ПОЛИТИКИ СОВРЕМЕННОЙ РОССИИ

Бертовский Лев Владимирович,

доктор юридических наук, профессор
Московская академия Следственного Комитета России (г. Москва)

Курбатова Светлана Михайловна,

доктор юридических наук, доцент, профессор кафедры уголовного процесса, криминалистики и основ судебной экспертизы,
профессор кафедры общественного здоровья
Красноярский государственный аграрный университет (г. Красноярск)
Красноярский государственный медицинский университет (г. Красноярск)

В статье рассмотрен ряд вопросов, касающихся особенностей современной киберпреступности и, как следствие, – формирования ответных мер противодействия со стороны российского государства. Отмечена значимость системного подхода к разработке и реализации данных мер. Сформулировано направление политики современного российского государства по вопросам противодействия киберпреступности.

Ключевые слова: киберпреступность, противодействие преступности, государственная политика, национальные интересы.

SOME ASPECTS OF COUNTERING CYBERCRIME AS A DIRECTION OF STATE POLICY IN MODERN RUSSIA

Bertovsky Lev Vladimirovich,

D.in Law, Professor
Moscow Academy of the Investigative Committee of Russia (Moscow)

Kurbatova Svetlana Mikhailovna,

D. in Law, Associate Professor, Professor of the Criminal Procedure, Criminalistics and Fundamentals of Forensic Examination Department,
Professor of the Public Health Department
Krasnoyarsk State Agrarian University (Krasnoyarsk)
Krasnoyarsk State Medical University (Krasnoyarsk)

This article examines a number of issues related to the characteristics of modern cybercrime and, consequently, the development of countermeasures by the Russian state. The importance of a systematic approach to the development and implementation of these measures is emphasized. The direction of modern Russian state policy on countering cybercrime is formulated.

Key words: cybercrime, crime prevention, government policy, national interests.

Глобальный переход к цифровой экономике означает, что деятельность правительств, критически важных инфраструктурных объектов, предприятий и частных лиц теперь представляет собой единую интегрированную систему взаимосвязанных ресурсов. Всё: от торговли и банковского дела до предоставления критически важных услуг и управления международ-

ными транспортными и энергетическими сетями – теперь происходит онлайн, многие лежащие в основе этих процессов ресурсы (такие, как цепочки поставок) являются взаимозависимыми. Помимо прямого ущерба, киберпреступность создаёт огромные препятствия для цифрового доверия, подрывает преимущества киберпространства, усиливает гло-

бальное неравенство и препятствует международным усилиям по обеспечению киберстабильности. Несмотря на серьёзность проблем, связанных с киберпреступностью, система мер борьбы с ней до настоящего времени не сформирована [1].

Как результат, в последние годы наблюдается рост киберпреступности, поскольку новые технологические решения и инструменты, равно как и IT-технологии, становятся всё более доступными. Фреймворки и платформы, продаваемые на подпольных форумах, позволяют злоумышленникам даже с низкой квалификацией обходить защитные барьеры. Например, несложные с точки зрения технологичности программы-вымогатели (как услуга) стали одним из векторов атак, позволяющих обычным пользователям, даже практически не разбирающимся в кибербезопасности, атаковать как частных лиц, так и компании, используя данные этих программ. Кроме того, из-за сложности новых технологий, используемых хакерами (таких, как искусственный интеллект), обнаружить вредоносные действия становится всё труднее.

Традиционно правоохранительные органы вмешивались в ситуацию с киберпреступностью только после того, как был нанесён значительный ущерб, например, когда системы оказывались в заложниках у программ-вымогателей или происходила кража важных корпоративных или личных данных.

Однако по мере того, как атаки становятся всё более частыми, а их последствия всё более разрушительными, правоохранительные органы, даже на местном уровне, обязаны создать эффективную систему борьбы с цифровой преступностью.

Например, в числе ответных мер со стороны правоохранительных органов могут быть:

- *расширение используемых инструментов и привлечение различных гражданско мотивированных сообществ.* Существует множество доступных ресурсов, в том числе отраслевые

инициативы: центры обмена информацией и анализа; каналы с открытым исходным кодом, которые предоставляют актуальные данные о киберугрозах и аналитическую информацию. Это могут широко использовать сотрудники правоохранительных органов;

- *более активное привлечение экспертных знаний.* Развитие необходимых экспертных знаний у сотрудников – изменение должностных обязанностей существующего сотрудника или найм штатного аналитика по угрозам, может обеспечить более тесную связь с разведывательным сообществом и помочь правоохранительным органам максимально эффективно использовать имеющуюся у них информацию;

- *поиск подходящих союзников и партнёров.* Союзниками выступают иные органы власти. Поэтому вопросы координации разных органов власти в вопросах противодействия киберпреступности должны приобретать первостепенное значение, так как это позволяет производить обмен опытом, координировать усилия по конкретным вопросам, разрабатывать алгоритмы проведения совместных мероприятий партнёров и т. д. Партнёрами по анализу угроз могут быть как поставщики систем безопасности, так и различные фирмы, мотивированные на взаимодействие и сотрудничество с органами власти. Например, партнёры могут предоставить общие индикаторы и данные, которые помогут предотвратить атаки, а также рекомендации по реагированию на инциденты в случае взлома;

- *анализ криминалистически значимых данных.* Использование внутренних или внешних ресурсов цифровой криминалистики и реагирования на инциденты в качестве источников ключевых данных во время или после кибератак может дать ценную информацию для борьбы с киберпреступниками;

- *обмен информацией,* собранной с помощью других правоохранительных органов и организаций, специализирующихся на расследовании утечек данных и реагировании на ин-

циденты, связанные с кибератаками, может способствовать накоплению полезных знаний, которые станут мощным противодействием киберпреступной деятельности [2].

Следует отметить, что в последние годы на уровне российского законодательства принимаются вполне конкретные меры, направленные на противодействие киберпреступности.

Например, 14 августа 2025 года Правительство РФ утвердило комплексный план мероприятий по реализации Концепции государственной системы противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий. План направлен на системное укрепление борьбы с киберпреступностью и формирование безопасной цифровой среды для граждан и организаций. Однако в настоящее время в России отсутствует правовая база, которая бы в полной мере регулировала все цифровые отношения, выступающие объектом одного из самых опасных видов международной преступности – киберпреступности, на что справедливо обращают внимание исследователи [3, с. 84].

Поэтому представляется первоочередным и необходимым разработка отдельного направ-

ления государственной политики по противодействию киберпреступности. Причём это должно включать в себе как деятельность конкретных органов государственной власти в рамках своих компетенции и полномочий, так и их координации и взаимодействия между собой и с разными институтами гражданского общества.

И, конечно же, следует уделять внимание вопросу кадрового обеспечения. Причём данный элемент можно назвать одним из решающих элементов в противодействии киберпреступности. В связи с этим необходимо организовывать и развивать подготовку специалистов с бинарными компетенциями – как в сфере правоохранительной деятельности, так и в области IT-технологий. Одна из таких программ реализована в НИИ МИЭТ (г. Москва), где обучающиеся уже с первого курса получают знания как по юридическим дисциплинам, так и по высокотехнологичным предметам [4].

Только подобного рода системный комплексный подход позволит сформировать единство государственной политики по противодействию киберпреступности, а также обеспечит её реализацию на практике.

Библиографический список

1. Франк Э. Новый атлас киберпреступности: совместный подход к борьбе с цифровой преступностью. 20.01. 2024. URL: <https://securityreviewmag.com/?p=26363> (дата обращения: 29.09.2025).
2. Борьба с цифровой преступностью: новые методы работы полиции. 17.08.2017. URL: <https://www.cybersecurityintelligence.com/blog/fighting-digital-crime-evolving-police-methods-2697.html> (дата обращения: 29.09.2025).
3. Чабукиани О. А., Зорина Е. А., Солодовник В. В. Способы противодействия киберпреступности // Социология и право. 2020. № 3 (49). С. 84–93.
4. Бертовский Л. В. Высокотехнологичное право: современные вызовы // Высокотехнологичное право: современные вызовы: Материалы IV Международной межвузовской научно-практической конференции, Москва-Красноярск, 17–20 февраля 2023 года. Том Часть 1. Красноярск: Красноярский государственный аграрный университет, 2023. С. 26–30.