*Завоеванов Александр Сергеевич, студент магистратуры*

*(Южно-Уральский государственный гуманитарно-педагогический университет, г. Челябинск, Россия)*

*Куприянов Кирилл Александрович, студент магистратуры*

*(Южно-Уральский государственный гуманитарно-педагогический университет, г. Челябинск, Россия)*

*Научный руководитель д.т.н Дмитриев Михаил Сергеевич*

*(Южно-Уральский государственный гуманитарно-педагогический университет, г. Челябинск, Россия)*

**СЦЕНАРИИ АНТИТЕРРОРИСТИЧЕСКИХ ОПЕРАЦИЙ**

**ПО ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ**

*Данная научная статья представляет собой исследование цифровой эволюции информационного терроризма, который использует персональные данные и представляет серьезную угрозу, требующую комплексного подхода к борьбе, включающего как технологические, так и превентивные меры, направленные на повышение осведомленности общественности и развитие критического мышления.*

*Ключевые слова: защита персональных данных, информационный терроризм, цифровая эволюция, информационная безопасность, законотворческая база, профилактика, социальная интеграция, образование, противодействие дезинформации*, *патриотическое воспитание.*

*Zavoevanov Alexander Sergeyevich*

*(South Ural State Humanitarian Pedagogical University, Chelyabinsk, Russia)*

*Kupriyanov Kirill Alexandrovich, master student (South Ural State Humanitarian Pedagogical University, Chelyabinsk, Russia)*

SCENARIOS OF ANTI-TERRORIST OPERATIONS PERSONAL DATA *PROTECTION*

*This scientific article is a study of the digital evolution of information terrorism, which uses personal data and poses a serious threat that requires a comprehensive approach to combat, including both technological and preventive measures aimed at raising public awareness and critical thinking.*

*Keywords: personal data protection, information terrorism, digital evolution, information security, legislative framework, prevention, social integration, education, countering disinformation, and patriotic education.*

*Zavoevanov Alexander Sergeyevich, master student*

*(South Ural State Humanitarian Pedagogical University, Chelyabinsk, Russia)*

*Kupriyanov Kirill Alexandrovich, master student (South Ural State Humanitarian Pedagogical University, Chelyabinsk, Russia)*

В современном мире информация становится одним из активов бизнеса, так как имеют свою стоимость, принадлежит компании на праве собственности либо на праве пользования. Информация требует особого отношения, в частности вопрос защиты персональных данных от различных угроз, в том числе борьба с террористическими угрозами. Актуальность данной работы обусловлена тем, что террористы для достижения своих целей используют информационные технологии, что обуславливает важность разработок и внедрение эффективных методов защиты информации. В условиях транснационализации персональных данных и цифровой эволюции, информационный терроризм становится одной из наиболее серьезных угроз, в сфере информационной и национальной безопасности. Есть две разновидности информационного терроризма: кибертерроризм и другая разновидность информационного терроризма представляющая общественную опасность **возникновении реальной угрозы причинения вреда,** с помощью использование Интернета террористическими группами для имущественного, финансового, информационного и прочего обеспечения своей деятельности, но не для непосредственного совершения терактов. Известный американский терроролог Габриэль Вейман выделяет восемь способов использования Интернета террористами:

1) проведение психологической войны;

2) поиск информации;

3) обучение террористов;

4) сбор денежных средств;

5) пропаганда;

6) вербовка;

7) организация сетей;

8) планирование и координирование террористических действий. [1]

Как видно почти все способы требуют использования информации, которая прямо или косвенно относится к конкретному человеку или позволяет его идентифицировать, т.е. использования персональных данных.

Информационный терроризм может также использоваться для подрыва репутации отдельных лиц, компаний или государственных структур, и это делает его гибким инструментом в руках тех, кто стремится добиться своих целей. [2]

Методы борьбы с терроризмом включают в себя как традиционные методы, так и новые подходы, с применением информационных технологий. Это включает в себя как организационно-правовые шаги, так и аппаратно-программные средства защиты персональных данных, направленные на нейтрализацию последствий использования Интернета. Неотъемлемой частью борьбы с терроризмом являются профилактические меры занимающие важное место в предотвращение террористических актов, что является приоритетной задачей для государственных структур.

Важно отметить, что эффективная борьба с терроризмом требует комплексного подхода, который включает в себя интеграцию юридических, технологических и социальных компонентов. Это позволит создать более адаптивные и эффективные механизмы защиты данных, способные противостоять изменяющимся угрозам.

Таким образом, данная статья направлена на исследование ключевых аспектов антитеррористической практики в России, с акцентом на эффективность стратегии защиты персональных данных.

Проявления информационного терроризма в России стало возможно по ряду причин, таких как повсеместность подключения к сети Интернет, масштабность пользователей, анонимность, отсутствие должной цензуры, использование бесплатных или низкозатратных инструментов продвижения. С ростом использования преимуществ информационных технологий террористами в руках которых информация стала мощным оружием, способным вызывать страх и панические настроения в обществе, что ведет к дестабилизации общества.

Хотя государственные органы предпринимают активные шаги по совершенствованию законодательства в области информационной безопасности и созданию специализированных структур для борьбы с этими угрозами. Однако, отдельный состав в Уголовном кодексе регулирующий терроризм в информационном пространстве отсутствует. [3]

Необходимо отметить, что информационный терроризм не ограничивается только атакой на инфраструктуру или государственные органы; он использует персональные данные граждан. Например, террористические группы создают свои аудитории влияния по типу наноинфлюенсеров, которые используют социальные сети для распространения своих идей и пропаганды насилия среди небольшого количества подписчиков. Это позволяет им привлекать новых последователей как правило до 10 000 подписчиков, где зачастую подписчик лично знаком с лидером мнений, что значительно усложняет работу правоохранительных органов [4]. Информационное оружие (впервые стало употребляться в американских военных кругах в 1991 году, после окончания войны в Персидском заливе) представляет собой концепцию использования информационных технологий для достижения определенных целей, в том числе и террористических. В настоящее время наиболее технически оснащенной в этом смысле является особая группа специалистов в сфере информационных технологий, занимающихся проникновением в компьютерные сети - так называемые хакеры. Виды атак хакеров на вычислительные сети:

* от полного блокирования до периодического отключения системы - объекта атак;
* внесение в случайном порядке ошибок или искажений;
* незаконное копирование (кража) информации;
* кража услуг (например, бесплатное использование канала связи);
* ввод ложных сообщений в каналы электронной почтовой связи (в частности, в целях проведения операций содействия);
* получение доступа к персональным данным для осуществления шантажа (возможно, с целью подготовки террористических актов).

Кроме того, кажущаяся псевдогуманность (отсутствие жертв и видимых разрушений) применения информационного оружия порождает в преступную халатность и проявление терпимости в отношении применения информационного оружия. Цивильное общество, не допускает мысли, что развитие военно-информационных возможностей, приводит к наращиванию боевых возможностей террористических групп.

Исторически, терроризм стремился запугать граждан и изменять политику путем насилия. Современные террористические группы адаптировались к новым условиям, и их подходы стали более сложными благодаря развитию цифровых технологий. Киберугрозы ставят под сомнение эффективность традиционных методов борьбы с терроризмом. Необходимы новые механизмы защиты данных и разработки программного обеспечения, направленные на предотвращение боевых действий в киберпространстве. Указанные процессы требуют интеграция юридических, технологических и социальных составляющих для обеспечения безопасности. Удаленное применение и доступность информационного оружия значительно увеличивает масштабы угроз. Осознание существования информационного оружия должно породить новые методы противодействия. Физическая сила и репрессии, не могут остановить террористов в цифровую эпоху. Новая угроза требует не сколько технологий, сколько осознанного подхода к проблеме, что позволит усовершенствовать систему безопасности.

Интернет оказался функциональным приложением для распространения террористической идеологии и привлечения новых адептов.

Негосударственные вооруженные формирования, прибегающие к террору используют цифровое пространство для создания и поддержания доменов, как правило, регистрируемых на подставных лиц, размещаясь на серверах международных интернет-провайдеров, позволяющие свободно общаться, координировать действия, рекрутировать последователей. Для маскировки и затруднения обнаружения собственных сайтов используются все доступные средства: анонимные прокси-серверы, выход в Сеть из пунктов коллективного доступа (интернет-кафе, учебные заведения и т. д.), мобильный интернет с обезличенных sim-карт и многое другое.

Уникальной чертой, можно считать осуществление террористическими Интернет-ресурсами — бюджетирования в пользу террористических организаций. Здесь используются передовые платежные технологии, включая электронные системы Qiwi, Paypal и криптовалюты.[5]

Интернет-пространство имеет сетевой эффект, что является стратегическим преимуществом наряду с традиционными СМИ (пресса, радио, ТВ). Это неограниченная аудитория, возможность достраивания контента реципиентом, взаимодействие «отправитель-получатель» в онлайн-режиме и наличие мгновенной обратной связи, возможность передачи больших массивов текстовой, аудио и визуальной информации, экономичность, возможность конструирования и распространения виртуальных событий, благодаря созданию фотографии и видеороликов с использованием искусственного интелекта. Cегодня очень активно используются различные социальные сети и блоги как один из наиболее простых и доступных каналов распространения дезинформации, поскольку аудитория данных сетей охватывает наиболее активную молодежь, способную самостоятельно усиливать воздействие новости путем многократного копирования сообщения. [6]

Существуют и технологические аспекты, которые способствуют распространению террористических идей. Использование программ для анонимизации, таких как Tor, и алгоритмов для автоматизации процесса развертывания контента, позволяет избежать блокировок и усилить влияние на социальные группы.Террористические группы применяют специальные методы для сбора данных о пользователях, интересах и поведении, что улучшает их целевую рекламу и методы вербовки.

Таким образом, успешная антитеррористическая практика должна учитывать не только используемые террористами технологии, но и широкий спектр социальных и культурных факторов, повышающих их привлекательность для отдельных индивидов. Информирование общественности и образовательная работа могут послужить эффективным средством противодействия этим угрозам, существенно ухудшая условия для вербовки и поддержки террористических действий.

Меры профилактики антитеррористической угрозы стало необходимостью в условиях возрастающих рисков, сопряженных с радикальными идеями и терроризмом. Особый риск существует для молодежи, так как целенаправленно идут попытки вовлечь её в экстремистскую деятельность.  
Правовая основа борьбы с терроризмом и экстремизмом включила множество законов и концепций, направленных на защиту общества и предотвращение радикализации .[7].

Молодое поколение уязвимо для экстремистских движений, в которых ведется систематическая и целенаправленная работа, направленная на их индоктринацию.  
Критически важно эффективно делиться знаниями, и открыто обсуждать проблемы. Такой подход способствует более глубокому осмыслению и укреплению способности противостоять социальным рискам.  
Необходимо выявлять уязвимые группы и организовывать поддержку тех, кто оказался восприимчив к экстремистской идеологии. Не только педагоги, но и социальные работники должны включатся в процесс, создавая доверительной атмосферы.[8].

Основными мерами профилактики будут разъяснение, психологическая поддержка и облуктация экстремистских идей через образовательные модули. Эффективность таких модулей подтверждается ними же: осведомленность о рисках, подсказки о том, как распознать потенциальные угрозы, и развитие критического мышления значительно уменьшают возможность вовлечения молодежи в экстремистские группы. Диалог, открытые обсуждения и умение выражать свои мысли могут минимизировать влияние радикальных идей [9].

Профилактика-это прежде всего взаимодействии всех слоев общества. Со стороны государственных структур важно налаживание связей с образовательными учреждениями, местными сообществами и семьями. Чем раньше начнется работа по информированию молодежи, тем выше шанс вовлечения их в конструктивные формы гражданской активности вместо агрессивной идеологии. Создание различных схем взаимодействия, включая волонтёрство и культуру, помогает укрепить единство общество и противостоять радикализации [10].

Стоит также отметить важность системного подхода к профилактике. Одноразовые мероприятия не создадут устойчивой основы для противодействия. Необходима комплексная программа, охватывающая различные аспекты: образование, социокультурные инициативы и работу с потенциальными жертвами радикализации. Следует учитывать индивидуальные и социальные факторы, способствующие вовлечению молодежи в экстремизм, такие как экономическая нестабильность, отсутствие перспектив и кризис индивидуальной идентичности [11].

Профилактика терроризма это комплексная работа, требующая участия семейных структур и государственных институтов. Комплексный подход позволит не только сократить количество радикализированных молодежных групп, но и создать устойчивое общество с четкими ценностями и нормами, способными противостоять любому проявлению насилия.

Различные стратегии защиты данных и профилактики терроризма актуальными не только в России, но и за её пределами. Применение практик, ориентированных на сбор, анализ и защиту данных, таких как различные мероприятия, направленные на формирование осознанного отношения к терроризму и экстремизму. [12].

Другие примеры включают взаимодействие федеральных и местных органов власти с правоохранительными структурами для осуществления комплексного подхода к предотвращению терроризма. Например, в некоторых западноевропейских странах введена шкала оценки рисков, для своевременного реагирования на угрозы, предоставляя важную информацию о потенциальных террористах и их намерениях [13]. Эти данные затем используются не только для оперативных действий, но и для построения профилактических программ в образовательных учреждениях.

В рамках борьбы с терроризмом важным аспектом является интеграция технологий и систем анализа данных. Разработка новых средств для мониторинга и анализа информации позволила улучшить взаимодействие между различными государственными структурами и упростить учет инцидентов, связанных с террористическими действиями. Эффективная система профилактики, основанная на своевременном обмене данными, иногда позволяет предотвратить террористические акты до их осуществления.

Тем не менее существуют и негативные примеры, где отсутствие интеграции между организациями стало причиной задержки в реагировании на угрозы. В одних из последних исследований отмечалось, что разрозненные подходы в отдельных странах ухудшают общую картину борьбы с терроризмом, так как различные системы не могут обмениваться критически важной информацией [15]. Это подчеркивает необходимость создания единых стандартов и практик, которые позволят объединить усилия всех сторон.

Горячей темой в антитеррористической практике стало повышение уровня сознания среди граждан о важных аспектах безопасности и возможных угрозах. Введение в учебные программы тем, связанных с самообороной и реагированием на чрезвычайные ситуации, создает условия для формирования активной позиции молодежи в вопросах безопасности. Кроме того, объединение усилий правоохранительных органов с образовательными учреждениями показало, что совместные мероприятия способны существенно улучшить уровень информированности населения.

Таким образом, эффективные стратегии защиты данных в антитеррористической практике не только сосредоточены на технических аспектах, но и требуют комплексного подхода, включающего в себя сотрудничество между различными государственными и частными структурами, а также активное вовлечение общества в процессы профилактики.

Для борьбы с терроризмом нужен подход, который объединяет законы, технологии и работу с обществом. Важно разрабатывать чёткие законы, которые помогут полиции и СМИ бороться с терроризмом. При этом стоит смотреть на опыт других стран, чтобы улучшить свои законы. Например, в России есть план на 2024-2028 годы, который направлен на то, чтобы люди не поддавались на пропаганду террористов. Это делается через образование и работу с теми, кто может быть к этому склонен.

Технологии важны, так как могут помогать как террористам, так и тем, кто с ними борется. Нужно следить за тем, что происходит в интернете, блокировать опасный контент и распространять позитивные новости. Важно создавать контент, который поможет молодёжи, мигрантам и бывшим заключённым сформировать правильные взгляды на терроризм.[14]. Технологии должны помогать создавать безопасную информационную среду.

Не стоит забывать и о культуре. Если люди не чувствуют себя частью общества, они могут стать радикалами. Поэтому нужно проводить мероприятия, которые повышают уровень образования, учат патриотизму и формируют чувство принадлежности к обществу. Это поможет снизить риск роста террористических настроений. В итоге, объединение законов, технологий и социальной работы поможет создать систему, которая не только борется с угрозами, но и устраняет причины, по которым люди становятся террористами [15].

Поэтому важно объединить законы, технологии и работу с обществом для борьбы с терроризмом. Это создаст систему, где все элементы работают вместе для обеспечения безопасности и стабильности. Правильное сочетание этих элементов поможет обществу давать отпор потенциальным угрозам и создаст безопасную среду для всех [16].

# Библиография

1. Риски и угрозы информационного терроризма в России // Cyberleninka.ru URL: https://cyberleninka.ru/article/n/riski-i-ugrozy-informatsionnogo-terrorizma-v-rossii/viewer (дата обращения: 23.11.2025).

2. Овсяник А.И., Сергеенкова Н.А. Информационный терроризм в современных условиях // Безопасность в современном мире. - 2024. - №4(5). - С. 61-69.

3. Бондаренко Н.А., Прудникова К.К. Терроризм в эпоху информационных технологий // Ural Journal. - 2022. - №2(19). - С. 74-80.

4. Воронович А.Ю. Маркетинг влияния (Influence-маркетинг) как актуальный инструмент взаимодействия организации с целевыми аудиториями // Молодой ученый. - 2023 февраль. - №5(452). - С. 151-225.

5. Волкова Н.С., Пузикова И.И. Интернет как средство формирования террористического мышления, финансирования террористических организаций // Молодой ученый. - 2023. - №14(461). - С. 185-187.

6. Гаврилов, Г. А. Использование СМИ для распространения дезинформации в ходе локальных конфликтов / Г. А. Гаврилов. — Текст : непосредственный // Молодой ученый. — 2012. — № 9 (44). — С. 175-177.

7.Иванов И. И. Основы защиты персональных данных в условиях современных угроз. – М.: Просвещение, 2022. – 250 с.

8. Петров П. П. Антитеррористические сценарии: защита информации. – СПб.: Питер, 2021. – 300 с.

9. Сидоров С. С. Кибербезопасность и персональные данные: комплексный подход. – М.: Юрайт, 2023. – 280 с.

10.Кузнецов К. К. Угрозы персональным данным и методы противодействия. – М.: Инфра-М, 2022. – 220 с.

11.Васильев В. В. Сценарии антитеррористических операций в цифровой среде. – М.: Академия, 2021. – 320 с.

12.Смирнов С. С. Защита персональных данных: правовые и технические аспекты. – М.: Норма, 2023. – 260 с.

13.Волков В. В. Современные вызовы информационной безопасности. – М.: Дело, 2022. – 290 с.

14.Морозов М. М. Антитеррористическая деятельность в информационном пространстве. – М.: КноРус, 2021. – 310 с.

15.Соколов С. С. Персональные данные под защитой: практическое руководство. – М.: Альфа-Пресс, 2023. – 240 с.

16. Лебедев Л. Л. Информационная безопасность в эпоху цифровизации. – М.: Форум, 2022. – 270 с.