

ПРОТИВОДЕЙСТВИЕ ИСПОЛЬЗОВАНИЮ ТЕХНОЛОГИЙ ГЕЙМИФИКАЦИИ В ТЕРРОРИСТИЧЕСКИХ И ЭКСТРЕМИСТСКИХ ЦЕЛЯХ

В.В. Меркурьев¹, О.В. Хлопкова², А.С. Клементьев³

¹ Научно-исследовательский институт Университета прокуратуры Российской Федерации, г. Москва, Российская Федерация

² Московский автомобильно-дорожный государственный технический университет (МАДИ), г. Москва, Российская Федерация

³ ПАО «РусГидро», г. Москва, Российская Федерация

Информация о статье

Дата поступления

2 ноября 2019 г.

Дата принятия в печать

10 февраля 2020 г.

Дата онлайн-размещения

28 февраля 2020 г.

Ключевые слова

Терроризм; экстремизм; геймификация; технологии управления; социальные процессы; информационные технологии; террористическая деятельность; игры в альтернативной реальности

Аннотация. Развитие информационных технологий, изменение характера труда, трансформация общественных ценностей обусловили распространение технологии геймификации и ее широкое использование в сфере социального управления государственными и бизнес-структурами. В статье рассматривается исторический аспект развития технологии геймификации и ее практическое применение в различных общественных сферах. Обобщение имеющихся данных о сущности геймификации позволило вывести ее концепт. В статье раскрывается механизм создания игровой модели и уделяется внимание подходам к ее построению. Авторы убеждены, что преимущества геймификации как социальной технологии базируются на особенностях человеческой психики и позволяют использовать ее как механизм скрытого манипулирования. В статье приводятся примеры применения геймификации в сфере бизнеса, государственного регулирования, управления социальными процессами. На основе исследования деятельности международных террористических организаций делается вывод о том, что технологии геймификации активно используются в террористических и экстремистских целях. Анализируются угрозы использования геймификации в экстремистской и террористической деятельности, в частности для привлечения интереса к такой деятельности, вербовки членов террористических организаций, повышения активности сторонников, сбора денежных средств и совершения террористических актов. Отдельное внимание уделяется угрозам использования технологии геймификации на территории Российской Федерации. В контексте противодействия использованию технологии геймификации в террористических и экстремистских целях анализируются нормативные правовые акты Российской Федерации, в том числе Комплексный план противодействия идеологии терроризма в Российской Федерации на 2019–2023 годы. Авторами предлагается комплекс мер по противодействию использованию технологии геймификации в террористических и экстремистских целях.

COUNTERACTING THE USE OF GAMIFICATION TECHNOLOGY FOR TERRORIST AND EXTREMIST PURPOSES

Victor V. Merkuriev¹, Oksana V. Khlopova², Aleksandr S. Klementev³

¹ Research Institute, University of the Prosecutor's Office of the Russian Federation, Moscow, the Russian Federation

² Moscow Automobile and Road Construction State Technical University (MADI), Moscow, the Russian Federation

³ PJSC «RusHydro», Moscow, the Russian Federation

Article info

Received

2019 November 2

Accepted

2020 February 10

Available online

2020 February 28

Abstract. The development of information technologies, changes in the nature of work, transformation of public values lead to a spread of gamification technology and its wide use in the sphere of social management of public and business structures. The authors examine the historical aspect of the development of gamification technology and its practical application in different public sectors. Generalization of the existing data on the essence of gamification made it possible to work out its concept. The authors describe the mechanism of creating a game model and analyze approaches to its design. They are convinced that the advantages of gamification as a social technology are based on specific traits of human psychology and enable its use as a mechanism of covert manipulation. The paper presents examples of using gamification in business, state regulation, management of social processes. The research of the activities of transnational terrorist organizations became a basis for the

Keywords

Terrorism; extremism; gamification; management technology; social processes; information technologies; terrorist activities; alternate reality games

conclusion that gamification technologies are actively used for terrorist and extremist purposes. The authors also analyze the threats of using gamification in terrorist activities, specifically, for increasing interest in such actions, recruiting new members of terrorist organizations, intensifying the activity of supporters, fundraising and committing terrorist acts. Specific attention is paid to threats of using the gamification technology on the territory of the Russian Federation. The counteraction to the use of gamification technology for terrorist and extremist goals becomes a context for analyzing the normative legal acts of the Russian Federation, including the Complex Plan of Counteracting the Ideology of Terrorism in the Russian Federation in 2019–2023. The authors present a complex of measures aimed at counteracting the use of gamification technology for terrorist and extremist purposes.

Роль информации в жизни личности, общества и государства в последние годы значительно возросла. Сегодня сложно представить ту или иную сферу жизнедеятельности, которой бы не коснулся процесс информатизации. Возможности современных информационных технологий все чаще используются для достижения геополитических, противоречащих международному праву военно-политических, криминальных, в том числе террористических, целей. В настоящее время широкое распространение в сфере социального управления государственными и бизнес-структурами получила технология геймификации.

Применение террористическими и экстремистскими организациями технологии геймификации в целях расширения своего присутствия в цифровой среде, используемой для ведения террористической пропаганды, рекрутирования и вербовки новых членов, координации и организации своих действий по насильственному изменению основ конституционного строя, нарушению целостности Российской Федерации и дестабилизации деятельности органов власти, является одной из угроз национальной безопасности Российской Федерации.

История использования геймификации в сфере социального управления

Геймификация — современная социальная технология, применяемая в различных сферах, связанных с управлением людьми¹. Основная цель использования геймификации состоит в повышении вовлеченности людей в процесс достижения цели, заданной разработчиком: рост эффективности труда, увеличение продаж, формирование лояльности, сбор данных, удержание клиентов и др.

¹ Иногда используются термины «игрофикация» или «геймизация».

Начало активного применения игровых методов в социальном управлении связано с периодом индустриализации и формирования общества массового потребления. Одним из первых примеров использования геймификации можно считать продажу «зеленых марок» компанией Sperry & Hutchinson в 1896 г. Магазины, заправочные станции, рестораны приобретали «зеленые марки» у компании и выдавали их покупателям после каждой покупки. Накопив определенное количество марок, покупатели могли обменять их на призы. Данный способ стимулировал потребителей совершать больше покупок [1].

Технология геймификации применялась и на государственном уровне. «Социалистические соревнования», проводившиеся в СССР с середины 1920-х гг., служили одним из средств мобилизации населения на совершение «социалистического рывка». Основной целью использования технологии являлось повышение производительности труда при минимальном материальном стимулировании. Принципы социалистического соревнования, в котором рабочие, группы рабочих и целые предприятия конкурировали друг с другом, были сформулированы В.И. Лениным в декабре 1917 г. в статье «Как организовать соревнование» [2, с. 195–205]. «Социализм не только не угашает соревнования, а, напротив, впервые создает возможность применить его действительно широко действительно в массовом размере, втянуть действительно большинство трудящихся на арену такой работы, где они могут проявить себя, развернуть свои способности, обнаружить таланты, которых в народе — непочатый родник и которые капитализм мямл, давил, душил тысячами и миллионами», — отмечал В.И. Ленин. Социалистическое соревнование предполагало разнообразные формы игрового стимулирования трудовых ресурсов в диапазоне от непосредственно конкурентных игр, связанных

с производительностью, до командных игр, нацеленных на создание инновационного продукта. Примеры использования методов геймификации в целях повышения производительности труда несложно найти и в других странах [3].

Развитие информационных технологий в конце XX — начале XXI в. привело к новому этапу использования технологий геймификации, который характеризуется массовостью применения и вовлеченности. Удобство и распространение информационных технологий упростили процессы создания и внедрения элементов игры в социальное управление, снизили требования к необходимым организационным и материальным ресурсам для использования технологий геймификации, позволили эффективно оформлять игровые элементы.

Рост использования геймификации также связан с трансформацией отношения к труду и материальным благам. Ориентация при выборе работы на такие критерии, как интерес, креативность, возможность самореализации, требует внедрения новых подходов к мотивации персонала. Использование игровых элементов может значительно усилить мотивацию, повысить эффективность работы, увеличить объем продаж. Получение материального вознаграждения не всегда необходимый элемент игры: игра сама по себе становится вознаграждением.

Концепт геймификации

Термин «геймификация» был введен английским программистом Ником Пеллингом в 2002 г. [4]. Концептуально геймификацию можно определить как «использование игрового дизайна в неигровом контексте» [5].

Геймификация базируется на механизме создания игровой модели реальности, включающей следующие элементы:

- четкие, однозначные, измеримые и достижимые цели и задачи, стоящие перед участниками;
- нормы и правила, определяющие пути и способы продвижения к цели;
- сюжет, создающий в игре логику воображаемых событий или изменяющий смысл событий, происходящих в действительности;
- система обратной связи [6, р. 21].

Геймификация не подразумевает под собой создание полноценной игры для развлечения. Основной целью применения технологии геймификации является решение задач, не связанных непосредственно с игрой (рост объема

продаж, получение прибыли, получение данных). Игровые элементы используются лишь как инструмент техники скрытого манипулирования поведением людей [7].

Можно выделить следующие основные подходы к построению стратегии геймифицированных технологий:

1. Геймификация наград для игроков, участвующих в соревновании или выполняющих необходимые задачи. Вознаграждение может осуществляться в добавлении баллов, отличительных знаков, уровней, «жизней», рейтингов и т.д. Основная цель такой стратегии — сделать награды видимыми и обеспечить конкуренцию за поощрение эффективности участия в игре.

2. Геймификация задач. Главная цель данного подхода — представить задачи, стоящие перед участниками, в виде игрового задания, похожими на игру. Это осуществляется, например, посредством добавления повествовательного компонента, усложнения «реальности» или включения элемента значимого выбора, который должен совершить игрок на той или иной стадии игры [8].

Преимуществами технологии геймификации являются:

1. Использование потребности человека в целостных эмоциональных переживаниях. Психологическим источником игры являются биологические механизмы, выраженные в инстинктивных потребностях человека. Применение игры как формы социального управления позволяет обеспечить единство мыслей, чувств и действий, пробудить творческий потенциал, усилить ощущение солидарности и конкуренции.

2. Принцип добровольности. Как правило, деятельность, сконструированная по принципу игры, предполагает добровольное участие или создание подобного ощущения у игроков.

3. Вовлеченность участников в процесс. Геймификация усиливает вовлеченность участников в процесс. Использование психологических особенностей при выстраивании игровой технологии позволяет привлекать новых участников, а также длительное время удерживать их внимание на процессе. В частности, геймифицированная технология может строиться на основе использования таких потребностей, как потребности в достижении успеха и поощрении, познании, общении, влиянии на других.

4. Эксплуатация чувства безопасности. Игровая форма снимает напряжение участников и обеспечивает им ощущение защищенно-

сти, отсутствия угроз из-за вымышленности происходящего в игре.

5. Обеспечение эффекта «размытой ответственности». Участие в игре позволяет человеку не задумываться о последствиях своей деятельности и совершать поступки, которые при других обстоятельствах он не стал бы совершать по моральным, статусным и иным соображениям.

Таким образом, технология геймификации использует потребности человека в общении, обучении, конкуренции, достижении успеха, признании, самовыражении. Представление действий, которые необходимо выполнить, в качестве игры формирует у человека реакцию на возникшую ситуацию как на игровую, устраняя тревоги и сомнения [9]. Основа геймификации — вызов, выражаемый в достижении цели игровыми способами.

Преимущества игровых технологий обуславливают их проникновение в сферы управления, маркетинга, обучения, здравоохранения, массовых коммуникаций и т.д. Так, в 2014 г. китайское правительство объявило, что к 2020 г. будет введена в действие система социального кредита доверия, в основе которой будет лежать принцип геймификации: выстраивание рейтинга гражданина на основе хорошего с точки зрения государства поведения (своевременные платежи, образовательные достижения, уместные покупки и т.д.) [10]. Рейтинг каждого гражданина Китая будет сравниваться с рейтингом сограждан, и на основе его места в общей системе будет определяться, достоин ли он получить ипотеку, устроиться на конкретную должность, отправить детей в школу и т.д. Рекрутинг новобранцев в армию США производится в том числе с использованием игровых технологий, с помощью которых играющих обеспечивают опытом виртуальной службы [4].

Эти и другие примеры демонстрируют широкие перспективы применения геймификации в сфере управления людьми. Вместе с тем данные преимущества делают технологию геймификации привлекательной не только для государства и бизнес-структур, но и для экстремистских и террористических организаций.

Геймификация в экстремистской и террористической деятельности

В 2011 г. американские консультанты по вопросам безопасности и внешней политики Джаррет Брахман и Аликс Левин заявили об использовании принципов геймификации на сай-

тах, связанных с террористическими исламистскими организациями [10]. Данный феномен авторы назвали «миром Святого Варкрафта», подчеркивая сходство методов, применяемых террористическими организациями, например «Аль-Каидой» (организация запрещена законодательством РФ), с принципами создания компьютерных игр. Наиболее популярные исламистские сайты используют принципы геймификации — рейтинги, ранги, поощрения — для стимулирования пропаганды ненависти и поощрения воинственности, например путем размещения пропагандистских постов на внешних интернет-ресурсах, комментариев постов других пользователей и т.д. [11]. Тот человек, который разместил пропагандистские посты наибольшее количество раз, получает наивысший рейтинг, а также различные дополнительные возможности в виде открытого доступа к размещению аватара, выделения тем или иным образом своего ника и т.д. Это, отмечают эксперты, порождает эффект замены внутренних стимулов участия в экстремистской и террористической деятельности на внешние, что вызывает некие идеологические споры об их применимости в террористической среде. Авторы исследования считают, что, с одной стороны, подобные сайты — это безопасное пространство для агрессивных людей, где они могут выплеснуть свою агрессию в ненасильственное поле, с другой — пользователи террористических сайтов со временем стремятся соответствовать своим виртуальным образам, что отражается на их реальном поведении в физическом мире (как подростки, воспроизводящие игру *Grand Theft Auto* в виде грабежей и убийств). Джаррет Брахман и Аликс Левин предсказывают, что время между регистрацией на исламистском сайте и реальным актом насилия будет сокращаться, так как разработчики ресурсов будут активнее использовать методы геймификации, а также добавлять более экстремальные уровни участия в игровом процессе [12].

Alternate Reality Games (игры в альтернативной реальности) является еще одним методом, применяемым современными экстремистскими и террористическими группами. В качестве платформы таких игр используется реальный мир. ARG — это гигантские многопользовательские головоломки, своеобразный микс ролевых и компьютерных игр, флешмонов, мистификаций. Главный принцип ARG получил название TINAG (*This is not a game* — «Это не игра»). Он предполагает сомнение у участников в игровом

характере происходящего. В качестве элементов игры используются реально существующие объекты. Создатели и координаторы игры, как правило, неизвестны, реальность их существования обычно находится под вопросом. Несмотря на то что участники получают задания, выполнение которых предопределяет их дальнейшее положение в игре и возможность выигрыша, они не знают точно, игра это или реальность.

Элементы игры могут использоваться террористическими группами и в виде отдельных заданий [13]. При этом участники могут не предполагать и не осознавать возможные последствия выполнения заданий. Так, гражданка Индонезии, подозреваемая в убийстве брата лидера КНДР, заявила, что ее попросили брызнуть в лицо Ким Чон Наму, как ей сказали, «детским маслом» в качестве розыгрыша в реалити-шоу².

Общественный резонанс вызвали игры в альтернативной реальности суицидальной направленности, организуемые через так называемые группы смерти. Их появлению способствовал рост социальных сетей, возникновение сетевых молодежных субкультур и контркультур, интернет-фольклора и сленга. Одна из таких контркультур — «нетсталкинг». Основная идея «нетсталкинга» заключается в убеждении в том, что в недрах Сети существует «глубинный Интернет», который содержит страшную для человеческого сознания информацию. «Глубокое» погружение в Сеть позволяет соприкоснуться с мистическим миром, где цифры, формы и смыслы теряют свое значение. Самый глубокий слой — «тихий дом», куда уходят души мертвых и уже не возвращаются.

Так, создатели сетевого сообщества f57 попытались совместить популярную среди подростков мифологию «нетсталкинга» с тематикой суицида. Игровые задания для подростков включали разгадывание таинственных шифров, поиск определенного контента в Сети, создание тематических фан-артов и т.д. Итоговым заданием игры являлись фотографии участника с изрезанными венами или прямая трансляция в Periscope, демонстрирующая суицид.

Игра «Большая игра. Сломай систему» в 2009 г. признана в России первым террористическим игровым ресурсом. Сюжет игры основан на ультранационалистических и антигосударственных идеях. Сайт ресурса содер-

жит информацию об изготовлении муляжей взрывных устройств, радиоуправляемых пестард. Участникам игры предлагалось за плату в реальной действительности совершать различные действия. Вначале игроки увлекаются только игровыми действиями, а впоследствии и материалом с экстремистским содержанием. Для игроков, перешедших на седьмой уровень, задания рассылались в индивидуальном порядке на личные почтовые адреса.

При помощи технологий геймификации организаторы террористической деятельности могут ранжировать потенциальных и реальных участников экстремистских ячеек, выявлять наиболее активных и эффективных игроков. Эти люди с большой вероятностью могут быть назначены лидерами ячеек, групп либо исполнителями наиболее важных и сложных поручений [14]. По аналогии с корпорациями, использующими подобные социальные технологии, террористические организации могут формировать свой актив и кадровый резерв на основе полученной в ходе игр и прочей деятельности с игровыми и соревновательными элементами информации [15].

Еще одним следствием геймификации может быть появление специфических терминов, условных знаков, символов, команд, понятных только участникам игр и посвященным. Данное обстоятельство может затруднить противодействие преступным сообществам так же, как затруднена борьба с замкнутыми этническими преступными группировками, использующими редкие языки и диалекты.

Специалисты в области безопасности прогнозируют, что в ближайшем будущем мир столкнется с краудфандинговыми преступлениями и краудфандинговым террором. Террористические организации посредством игр в альтернативной реальности смогут осуществлять разведку местности, перевозку и доставку грузов и иные действия путем использования ничего не подозревающих участников увлекательных квестов [16].

Противодействие использованию технологии геймификации в террористических и экстремистских целях

Для успешного противодействия экстремистской и террористической деятельности необходимо реализовать комплекс мероприятий, учитывающий современные технологии и тенденции социального управления.

² Подозреваемая в убийстве Ким Чон Нама «думала, что это розыгрыш». URL: <http://www.bbc.com/russian/news-39090754>.

В настоящее время к распространяемой с нарушением закона информации относятся призывы к массовым беспорядкам, осуществлению экстремистской деятельности, участию в массовых (публичных) мероприятиях, проводимых с нарушением установленного порядка, недостоверная общественно значимая информация, распространяемая под видом достоверных сообщений и создающая угрозу причинения вреда жизни и (или) здоровью граждан, имуществу, угрозу массового нарушения общественного порядка и (или) общественной безопасности либо угрозу создания помех функционированию или прекращения функционирования объектов жизнеобеспечения, транспортной или социальной инфраструктуры, кредитных организаций, объектов энергетики, промышленности или связи, а также информационные материалы иностранной или международной неправительственной организации, деятельность которой признана нежелательной на территории Российской Федерации [17].

Между тем в перечне запрещенной информации, предусмотренном ст. 15.3 Федерального закона «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ, не указаны материалы и информация, содержащие пропаганду, оправдание и поддержку терроризма, что, на наш взгляд, является явным пробелом. В законодательство необходимо внести соответствующие коррективы. Это особенно важно в связи с тем, что террористическими и экстремистскими организованными преступными формированиями активно используются манипулятивные технологии. После совершения террористического акта резко усиливается роль оправдывающей терроризм информации: появляются соответствующие статьи, посты, иной материал, смещающие ответственность за жертвы террористических актов на власть, нередко пытающиеся выставить спецслужбы инициаторами террористических актов, а самих террористов — борцами за справедливость и права «угнетенных» мусульман.

Вместе с тем само использование террористическими группировками сети Интернет открывает возможности для сбора разведывательной информации и проведения различных оперативно-разыскных мероприятий, направленных на предотвращение и пресечение преступлений, а также на сбор доказательств в це-

лях последующего уголовного преследования за их совершение. Значительный объем знаний о составе, участниках, видах деятельности, о планах совершения преступлений можно извлечь из сообщений на сайтах и в социальных сетях, из переписки участников террористической организации. Кроме того, чем шире Интернет используется в экстремистских и террористических целях, тем, соответственно, более доступными становятся электронные данные, которые можно подвергать обобщению и анализу для борьбы с данным видом преступности.

В этой связи в рамках формирования системы противодействия идеологии терроризма одной из важных мер должна стать организация мониторинга текущего состояния пропаганды идеологии терроризма и ее прогнозирования. В том числе это относится к автоматизации процесса мониторинга ресурсов сети Интернет, направленного на поиск, анализ и сохранение всей информации, касающейся пропаганды террористической идеологии, в форумах, на сайтах, в чатах, социальных сетях, блогах, видеозаписях, а также к созданию межведомственной базы данных для хранения и обработки оперативной и справочной информации, наполняемой с помощью специальной поисковой системы и из оперативных источников.

В настоящее время в Интернете насчитывается более 10 тыс. сайтов практически всех действующих международных террористических структур, а также созданы сотни тысяч аккаунтов в социальных сетях. Материалы террористической и экстремистской направленности публикуются на более чем 40 языках мира, прежде всего на арабском, английском и русском. Террористы стремятся максимально охватить все возможные целевые аудитории. В закрытых группах социальных сетей проводятся тренинги по тактике ведения боевых действий против силовых структур. В докладе на Международной конференции по проблемам борьбы с международным терроризмом в г. Санкт-Петербурге 18 апреля 2019 г. А.В. Бортников отметил: «Расследование преступлений боевиков в России и ряде европейских стран свидетельствует, что их исполнители следовали инструкциям своих интернет-наставников, в том числе в режиме онлайн»³.

³ Бортников призвал к выработке единых международных правил в интернете: Одной из острых проблем глава ФСБ назвал применение криптографии в программах для коммуникации. URL: <https://tass.ru/politika/6350868>.

В этой связи в соответствии с Резолюцией 2354 (2017), принятой Советом Безопасности ООН 24 мая 2017 г., необходимо принять меры к повышению эффективности контрпропагандистских мер. Субъекты антитеррористической деятельности должны поддерживать усилия, направленные на повышение информированности общественности о противодействии распространению террористических идей, привлекаемая органы просвещения и средства массовой информации, взаимодействуя с религиозными организациями [18].

Так, в целях формирования у граждан негативного отношения к идеологии терроризма в средствах массовой информации и на интернет-ресурсах регулярно должны размещаться материалы, направленные на повышение правовой грамотности, разъяснения нормы действующего законодательства в сфере противодействия экстремизму и терроризму. В противодействии радикализации, создающей условия для распространения терроризма, и использованию Интернета в террористических целях не менее важной видится работа с частным сектором, в том числе с поставщиками коммуникационных услуг и администраторами соответствующих приложений [19, с. 19]. На это ориентирует и утвержденный в декабре 2018 г. Президентом Российской Федерации Комплексный план противодействия идеологии терроризма в Российской Федерации на 2019–2023 годы.

Таким образом, для противодействия пропаганде терроризма необходимо организовать широкомасштабную контрпропагандистскую деятельность, эффективность которой должна превосходить действенность методов террористических организаций. Меры контрпропаганды должны иметь не единичный, а системный характер; они должны обеспечить мощнейший идеологический «вброс», раскрывающий суть происходящих процессов (создание и использование деструктивных сил в целях расшатывания духовно-нравственных устоев населения). Контрпропаганда должна строиться на доказательствах, имеющих в священных писаниях, обращении к гуманистическим идеям, показе опасности и античеловеческой сущности террористической идеологии. Построенное таким образом информационное воздействие должно быть направлено на предупреждение распространения террористической угрозы.

Серьезным достижением в деле совершенствования правового регулирования обеспечения информационной безопасности следует признать принятие 23 декабря 2015 г. Генеральной Ассамблеей ООН российской резолюции № 70/237 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», соавторами которой выступили более 80 государств из всех регионов мира. Среди них страны БРИКС, ШОС, СНГ, латиноамериканские и азиатские государства. Впервые соавторами этого документа стали также США, Япония и многие члены ЕС, включая Великобританию, Германию, Испанию, Нидерланды и Францию.

Государствам удалось достичь консенсуса по целому ряду принципиальных вопросов, связанных с использованием информационно-коммуникационных технологий, в частности по поводу того, что технологии должны использоваться исключительно в мирных целях, а международное сотрудничество необходимо нацелить на предотвращение конфликтов в информационном пространстве; государства не должны использовать посредников для осуществления кибератак и допускать, чтобы их территории использовались в этих целях; государства должны бороться с использованием скрытых вредоносных функций — так называемых закладок — в IT-продукции [20].

Выводы и рекомендации

Террористические и экстремистские организации осознают преимущества современных технологий управления, в частности геймификации. Распространение информационных технологий расширяет их возможности для привлечения сторонников и стимулирования их участия в деятельности, направленной на достижение экстремистских целей. Проведенный анализ позволяет выделить следующие направления совершенствования мер по противодействию использованию технологии геймификации в террористических и экстремистских целях:

- укрепление международного сотрудничества, в том числе в сфере унификации необходимых правовых средств, совместного планирования и координации превентивных мер (прежде всего по пресечению криминальной активности международных террористических организаций и сообществ в интернет-пространстве);
- совершенствование профилактической деятельности, связанной с воздействием на общественное сознание, путем информирования

граждан о предпосылках, социальных и юридических последствиях распространения террористической и экстремистской идеологии;

– активизация и расширение такого воздействия посредством использования информационных технологий, включая возможности самих

электронных и информационно-телекоммуникационных сетей;

– формирование системы технических и технологических мер, направленных на противодействие использованию сети Интернет в террористических и экстремистских целях.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Neubert M. This Marketing Technique Has Worked for 100+ Years / M. Neubert // Wizards Play Network. — URL: <https://wpn.wizards.com/en/article/marketing-technique-has-worked-100-years>.
2. Ленин В.И. Как организовать соревнование // Полное собрание сочинений / В.И. Ленин. — Москва : Политиздат, 1967. — Т. 35. — С. 195–205.
3. Nelson M.J. Soviet and American Precursors to the Gamification of Work / M.J. Nelson // Proceedings of the International Academic Mind Trek Conference. — 2012. — P. 23–26. — URL: http://www.kmjn.org/publications/Gamification_MT12.pdf.
4. Хлопкова О. Человек играющий, или Геймификация социальной реальности / О. Хлопкова // The wall magazine. — 2017. — 11 авг. — URL: <http://thewallmagazine.ru/gaming>.
5. Gamification: Toward a Definition / S. Deterding, R. Khaled, L. Nacke, D. Dixon // CHI 2011. Gamification Workshop Proceedings. — Vancouver, 2011. — URL: <http://gamification-research.org/wp-content/uploads/2011/04/02-Deterding-Khaled-Nacke-Dixon.pdf>.
6. McGonigal J. Reality Is Broken: Why Games Make Us Better and How They Can Change the World / J. McGonigal. — New York : Penguin Group, 2011. — 416 p.
7. From Game Design Elements to Gamefulness: Defining «Gamification» / S. Deterding, R. Khaled, L. Nacke, D. Dixon. — DOI: 10.1145/2181037.2181040 // Mind Trek. Envisioning Future Media Environments : Proceedings of the 15th International Academic Conference. — New York, 2011. — P. 9–15. — URL: https://www.researchgate.net/publication/230854710_From_Game_Design_Elements_to_Gamefulness_Defining_Gamification.
8. Deterding S. Just add Points & What UX Can (and Cannot) Learn from Games / S. Deterding // The Next Web. — 2010. — 28 Sept. — URL: <http://smartgrand.icyte.com/saved/www.slideshare.net/302731>.
9. Hidi S. Interest, a Motivational Variable that Combines Affective and Cognitive Functioning / S. Hidi, K.A. Renninger, A. Krapp // Motivation, Emotion and Cognition: Integrative Perspectives on Intellectual Functioning and Development / eds. D.Y. Dai, R.J. Sternberg. — London : Lawrence Erlbaum Associates publisher, 2004. — P. 89–115.
10. Brachman J. The World of Holly Warcraft / J. Brachman, A. Levine // Foreign Policy. — 2011. — 13 Apr. — URL: <https://foreignpolicy.com/2011/04/13/the-world-of-holly-warcraft>.
11. Greenberg K. Counter-radicalization via the Internet / K. Greenberg // The ANNALS of the American Academy of Political and Social Science. — 2016. — Vol. 668, no. 1. — P. 165–179.
12. Ungerleider N. Welcome to Jihad Ville / N. Ungerleider // Fast Company. — URL: <https://www.fastcompany.com/1749266/welcome-jihadville>.
13. Сундиев И.Ю. Бесструктурные и бесконтактные способы вовлечения молодежи в террористическую и экстремистскую деятельность / И.Ю. Сундиев, А.А. Смирнов, Н.Г. Андрихин // Научный портал МВД России. — 2018. — № 2 (42). — С. 52–60.
14. Williams L.M. Cyberhate on Social Media in the Aftermath of Woolwich: a Case Study in Computational Criminology and Big Data / M.L. Williams, P. Burnap // British Journal of Criminology. — 2016. — Vol. 56, iss. 2. — P. 211–238.
15. Bowman-Grieve L. A Psychological Perspective on Virtual Communities Supporting Terrorist & Extremist Ideologies as a Tool for Recruitment / L. Bowman-Grieve // Security Informatics. — 2013. — Vol. 2, no. 9. — P. 1–5.
16. Lafree G. Editor's Introduction: Quantitative Approaches to the Study of Terrorism / G. Lafree, J.D. Freilich // Journal of Quantitative Criminology. — 2011. — Vol. 28, iss. 1. — P. 1–5.
17. Противодействие вербовочной деятельности международных террористических организаций на территории Российской Федерации : пособие / под общ. ред. В.В. Меркурьева ; Акад. Генер. прокуратуры Рос. Федерации. — Москва, 2017. — 124 с.
18. Борьба с терроризмом: новые вызовы и угрозы / под ред. В.В. Меркурьева. — Москва : Проспект, 2019. — 709 с.
19. Бадамшин С.К. Преступления террористической направленности, совершаемые с использованием электронных или информационно-телекоммуникационных сетей: уголовно-правовая и криминологическая характеристика : дис. ... канд. юрид. наук : 12.00.08 / С.К. Бадамшин. — Москва, 2018. — 275 с.
20. Perry S. The Application of the «Law of Crime Concentration» to Terrorism: The Jerusalem Case Study / S. Perry // Journal of Quantitative Criminology. — 2019. — URL: <https://doi.org/10.1007/s10940-019-09411-2>.

REFERENCES

1. Neubert M. This Marketing Technique Has Worked for 100+ Years. *Wizards Play Network*. Available at: <https://wpn.wizards.com/en/article/marketing-technique-has-worked-100-years>.
2. Lenin V.I. How to organize a competition. *Polnoe sobranie sochinenii* [Complete Works]. Moscow, Politizdat Publ., 1967. Vol. 35, pp. 195–205. (In Russian).
3. Nelson M.J. Soviet and American Precursors to the Gamification of Work. *Proceedings of the International Academic Mind Trek Conference*, 2012, pp. 23–26. Available at: http://www.kmjn.org/publications/Gamification_MT12.pdf.
4. Khlopkova O. Homo ludens, or the gamification of social reality. *The Wall Magazine*, 2017, August 11. Available at: <http://thewallmagazine.ru/gaming>. (In Russian).
5. Deterding S., Khaled R., Nacke L., Dixon D. Gamification: Toward a Definition. *CHI 2011. Gamification Workshop Proceedings*. Vancouver, 2011. Available at: <http://gamification-research.org/wp-content/uploads/2011/04/02-Deterding-Khaled-Nacke-Dixon.pdf>.

6. McGonigal J. *Reality Is Broken: Why Games Make Us Better and How They Can Change the World*. New York, Penguin Group, 2011. 416 p.
7. Deterding S., Khaled R., Nacke L., Dixon D. From Game Design Elements to Gamefulness: Defining «Gamification». *Mind Trek. Envisioning Future Media Environments. Proceedings of the 15th International Academic Conference*. New York, 2011, pp. 9–15. DOI: 10.1145/2181037.2181040. Available at: https://www.researchgate.net/publication/230854710_From_Game_Design_Elements_to_Gamefulness_Defining_Gamification.
8. Deterding S. Just Add Points & What UX Can (and Cannot) Learn from Games. *The Next Web*, 2010, September 28. Available at: <http://smartgrand.icyte.com/saved/www.slideshare.net/302731>.
9. Hidi S., Renninger K.A., Krapp A. Interest, a Motivational Variable that Combines Affective and Cognitive Functioning. In Dai D.Y., Sternberg R.J. (eds.). *Motivation, Emotion and Cognition: Integrative Perspectives on Intellectual Functioning and Development*. London, Lawrence Erlbaum Associates publisher, 2004, pp. 89–115.
10. Brachman J., Levine A. The World of Holy Warcraft. *Foreign Policy*, 2011, April 13. Available at: <https://foreignpolicy.com/2011/04/13/the-world-of-holy-warcraft>.
11. Greenberg K. Counter-radicalization via the Internet. *The ANNALS of the American Academy of Political and Social Science*, 2016, vol. 668, no. 1, pp. 165–179.
12. Ungerleider N. Welcome to JihadVille. *Fast Company*. Available at: <https://www.fastcompany.com/1749266/welcome-jihadville>.
13. Sundiev I.Y., Smirnov A.A., Andruhin N.G. Structureless and Non-contact Methods of Youth Involvement in Terrorist and Extremist Activities. *Nauchnyi portal MVD Rossii = Scientific Portal of the Russian Ministry of the Interior*, 2018, no. 2 (42), pp. 52–60. (In Russian).
14. Williams L.M., Burnap P. Cyberhate on Social Media in the Aftermath of Woolwich: a Case Study in Computational Criminology and Big Data. *British Journal of Criminology*, 2016, vol. 56, iss. 2, pp. 211–238.
15. Bowman-Grieve L. A Psychological Perspective on Virtual Communities Supporting Terrorist & Extremist Ideologies as a Tool for Recruitment. *Security Informatics*, 2013, vol. 2, no. 9, pp. 1–5.
16. Lafree G., Freilich J.D. Editor's Introduction: Quantitative Approaches to the Study of Terrorism. *Journal of Quantitative Criminology*, 2011, vol. 28, iss. 1, pp. 1–5.
17. Merkurev V.V. (ed.). *Protivodeistvie verbovochnoi deyatel'nosti mezhdunarodnykh terroristicheskikh organizatsii na territorii Rossiiskoi Federatsii* [Counteracting the recruitment efforts of international terrorist organizations on the territory of the Russian Federation]. Moscow, University of the Prosecutor's Office of the Russian Federation Publ., 2017. 124 p.
18. Merkurev V.V. (ed.). *Bor'ba s terrorizmom: novye vyzovy i ugrozy* [Counteracting Terrorism: New Challenges and Threats]. Moscow, Prospekt Publ., 2019. 709 p.
19. Badamshin S.K. *Prestupleniya terroristicheskoi napravlenosti, sovershaemye s ispol'zovaniem elektronnykh ili informatsionno-telekommunikatsionnykh setei: ugovolno-pravovaya i kriminologicheskaya kharakteristika*. Kand. Diss. [Terrorist crimes committed with the use of electronic or information-telecommunication networks: criminal law and criminological characteristics. Cand. Diss]. Moscow, 2018. 275 p.
20. Perry S. The Application of the «Law of Crime Concentration» to Terrorism: The Jerusalem Case Study. *Journal of Quantitative Criminology*, 2019. Available at: <https://doi.org/10.1007/s10940-019-09411-2>.

ИНФОРМАЦИЯ ОБ АВТОРАХ

Меркурьев Виктор Викторович — заведующий отделом научного обеспечения прокурорского надзора и укрепления законности в сфере федеральной безопасности, межнациональных отношений и противодействия экстремизму Научно-исследовательского института Университета прокуратуры Российской Федерации, доктор юридических наук, профессор, г. Москва, Российская Федерация; e-mail: merkuriev-vui@mail.ru.

Хлопкова Оксана Васильевна — доцент кафедры социологии и управления Московского автомобильно-дорожного государственного технического университета (МАДИ), кандидат философских наук, г. Москва, Российская Федерация; e-mail: oksana-hlopkova@mail.ru.

Клементьев Александр Станиславович — главный эксперт Информационно-аналитического управления Департамента безопасности ПАО «РусГидро», кандидат юридических наук, г. Москва, Российская Федерация; e-mail: alex_klem@list.ru.

ДЛЯ ЦИТИРОВАНИЯ

Меркурьев В.В. Противодействие использованию технологий геймификации в террористических и экстремистских целях / В.В. Меркурьев, О.В. Хлопкова, А.С. Клементьев. — DOI: 10.17150/2500-4255.2020.14(1).87-95 // Всероссийский криминологический журнал. — 2020. — Т. 14, № 1. — С. 87–95.

INFORMATION ABOUT THE AUTHORS

Merkuryev, Victor V. — Head, Department of Research Support for Prosecutor's Supervision and Strengthening Legality in the Sphere of Federal Security, Interethnic Relations and Extremism Counteraction, Research Institute, University of the Prosecutor's Office of the Russian Federation, Doctor of Law, Professor, Moscow, the Russian Federation; e-mail: merkuriev-vui@mail.ru.

Khlopkova, Oksana V. — Ass. Professor, Chair of Sociology and Management, Moscow Automobile and Road Construction State Technical University (MADI), Ph.D. in Philosophy, Moscow, the Russian Federation; e-mail: oksana-hlopkova@mail.ru.

Klementev, Aleksandr S. — Leading Expert, Information and Analytical Directorate of the Department of Security, PJSC «RusHydro», Ph.D. in Law, Moscow, the Russian Federation; e-mail: alex_klem@list.ru.

FOR CITATION

Merkuryev V.V., Khlopkova O.V., Klementev A.S. Counteracting the use of gamification technology for terrorist and extremist purposes. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2020, vol. 14, no. 1, pp. 87–95. DOI: 10.17150/2500-4255.2020.14(1).87-95. (In Russian).