

УДК 343.140.02

Чимаров Сергей Юрьевич

доктор исторических наук, профессор,
профессор кафедры управления персоналом
и воспитательной работы,
Санкт-Петербургский университет МВД России
serg120756@gmail.com

Sergey Yu. Chimarov

Doctor of Historical Sciences, Professor,
Professor of the Department of Personnel
Management and Educational Work,
St. Petersburg university of the Ministry
of Internal Affairs of Russia
serg120756@gmail.com

**Об учете вопросов контент-хакинга и аспирации его итогов
в ряде телеграмм-каналов при решении воспитательных задач
с личным составом органов внутренних дел Российской Федерации**

**On accounting for content hacking and aspiration of its results
in a number of telegram channels when solving educational problems with
the personnel of the internal affairs bodies of the Russian Federation**

***Аннотация.** Современная тенденция цивилизационных изменений в сторону передела устоявшегося миропорядка и активное вовлечение в этот процесс Российской Федерации предопределяют целесообразность научного осмысления феномена дигитальных способов воздействия на личность сотрудника органов внутренних дел Российской Федерации, должность которого, по определению, предназначена на поддержание в обществе внутреннего спокойствия. В этой связи автор апеллирует к важности правильной ориентации личного состава системы МВД России в массиве цифровой формы доведения до современного человека большого объема разносторонней информации. Акцентируя внимание на целесообразности аналитической работы организаторов воспитательных подразделений в органах внутренних дел по выявлению наиболее значимой информации и ее дальнейшей трансформации в приемлемом виде до каждого сотрудника, автор обращает внимание на остроту проблемы формирования у сотрудников таких качеств как бдительность и патриотизм.*

***Ключевые слова:** воспитательная работа, бдительность, хакинг, контент, мессенджер, телеграмм-канал, органы внутренних дел.*

***Annotation.** The current trend of civilizational changes towards the redistribution of the established world order and the active involvement of the*

Russian Federation in this process predetermine the expediency of scientific understanding of the phenomenon of digital methods of influencing the personality of an employee of the internal affairs bodies of the Russian Federation, whose position, by definition, is intended to maintain internal peace in society. In this regard, the author appeals to the importance of the correct orientation of the personnel of the system of the Ministry of Internal Affairs of Russia in the digital form of bringing a large amount of versatile information to a modern person. Focusing on the expediency of the analytical work of the organizers of educational departments in the internal affairs bodies to identify the most significant information and its further transformation in an acceptable form to each employee, the author draws attention to the severity of the problem of forming such qualities in employees as vigilance and patriotism.

Key words: *educational work, vigilance, hacking, content, messenger, telegram channel, internal affairs bodies.*

Динамика современных изменений геополитического характера и ситуация ужесточения противостояния между Россией и коллективным Западом, выступающим наравне с Украиной в роли американского сателлита, предопределяет целесообразность осмысления современных технологических решений в области воздействия на сознание человека. Отмеченный тезис корреспондирует необходимости более эффективного решения воспитательных задач с личным составом российских органов внутренних дел. Указанное обстоятельство соответствует нормативному установлению пункта 11.12 Приказа МВД России от 29 июня 2022 г. № 480, предписывающего обязательность воспитательной работы по организации контрпропаганды и информационно-психологической защиты личности сотрудника данной государственной институции [1].

Применительно к системе МВД России, практическое воплощение данной идеи во многом базируется на новых подходах к конструированию объема необходимой информации и задействованию контента цифровой формы текста, с целью формирования у сотрудников профессионально значимых качеств, обусловленных их правоохранительной миссией. В данном случае, речь идет о феномене хакинга и соответственно о контент-хакинге.

Термин «хакинг» тождественен понятию «взлом», а содержание данного термина заключается в преднамеренной попытке неавторизованного пользователя каким-либо образом повлиять на нормальное функционирование определенной информационной (компьютерной) системы, в целях последующего полного или частичного контроля над ней и использования полученной хакерским способом информации в личных целях. Применительно к области современного Интернет-пространства, технология хакинга реализуется компьютерными специалистами-практиками (хакерами), обладающими уникальными знаниями для получения доступа к «закрытому» массиву информации с использованием набора хакерских атак: от взлома

пароля защищенного паролем веб-сайта до установки аппаратных или программных методов кейлоггинга для записи нажатий клавиш, включая любые пароли, используемые на этом компьютере и/или устройстве.

Существующая практика современного контент-хакинга свидетельствует об актуальности учета палитры информационных потоков, формируемых различного рода микроинфлюенсерами (блогерами с минимальной по числу аудиторией, но чрезвычайно активной по своему вовлечению в существо конкретной проблемы) и, собственно, хакерами, в последующем, использующих для продвижения полученной информации технологии хакинга новостей («news hacking») и формирования вирусного контента. При этом в большинстве случаев, задействуется феномен «обратной связи», на языке «пиара» именуемый как «фидбэк» [2].

В некоторых случаях, хакинг не всегда сопряжен с электронным вандализмом, а его деятельность не имеет отношения к преступному деянию. При этом суть компьютерного взлома заключается в том, чтобы «установить некоторые свойства конкретной ситуации и применить их для решения определенной проблемы» [7, р. 15].

Отмеченный феномен контент-хакинга ряда информационных источников и их последующая публичная презентация в цифровой форме, предоставляет организаторам воспитательной работы с личным составом органов внутренних дел обширный материал для целенаправленного воздействия на сознание личного состава, с целью формирования у него качеств бдительного сотрудника, патриота своей Родина и стойкого ее защитника. В данном случае следует акцентировать внимание на некотором опыте легализации информации (в формате создания отдельных сайтов в сети Интернет) с помощью различных информационных ресурсов, контент которых представляет очевидный интерес для органов правоохранения, а именно:

- 1) сайт «Немезида»;
- 2) российское общественное движение «Антимайдан»;
- 3) хакерская группировка RaHDit («Злые русские хакеры»);
- 4) украинская женская хакерская группа «Берегини», взаимодействующая с учредителями сайта «Немезида», и ряд других [3, с. 154].

Из числа отмеченных и некоторых иных Интернет-источников, особый интерес представляют электронные страницы инициативных группировок, хакерским образом получающих доступ к украинским государственным учреждениям, с целью размещения соответствующей информации посредством различных мессенджеров, включая телеграмм-каналы. В этой связи, нам представляется целесообразным обратить внимание на важность аспирации (лат. «aspiratio»-«втягивание», «вдыхание») наиболее значимых для воспитания сотрудников элементов информационной мозаики, полученной с помощью контент-хакинга и доводимой до общественности с помощью российских и пророссийских телеграмм-каналов:

1) «НемеZида», презентующего информацию волонтерского проекта «Злые русские хакеры» («RaHDit») [4];

2) украинской хакерской группы «Берегини» (англ. «Beregini»), действующей под девизом «Мы знаем все!» [5];

3) украинской хакерской группы «Заря», девиз которой «Великая истина и она восторжествует!» [8].

К примеру, телеграмм-канал «НемеZида» представляет информацию:

1) справочного характера о деятельности националистических организациях Украины и их активистах, иностранных пособниках нацизма, военных преступниках, а также, о сетевых террористах и личном составе украинских нацистских подразделений, 16 и 72 Центров информационно-психологических операций;

2) материалы специальных расследований, включая оценку степени участия иностранных государств в оказании военной помощи Украине.

Данные направления контент-хакинга и анализ полученной информации представляют несомненное значение для понимания личным составом органов внутренних дел действительного положения дел по превращению населения Украины в ожесточенного врага нашей страны и необходимости проявления бдительности в процессе несения сотрудниками своей службы, в первую очередь, в особых условиях на входящей в зону специальной военной операции территории.

Содержание контент-хакинга украинской нормативной базы и иных руководящих документов зафиксировано в телеграмм-канале, указанной выше хакерской группы «Берегини», предоставляющем своему читателю эксклюзивную информацию об особенностях морально-психологической работы с личным составом ВСУ (Вооруженные Силы Украины), закрепленных в их «Боевых уставах» и имеющих прикладное значение для их обобщения и применения в целях воспитания личного состава органов внутренних дел Российской Федерации, с целью формирования у него правильного понимания идеологических установок противника. Кроме того, важность анализа, размещенной в телеграмм-канале «Берегини» информации, обусловлена телеграмм-сообщением о содержании украинских учебных пособий для личного состава ВСУ, в которых обстоятельно проанализированы, в том числе, современные тактические способы функционирования Национальной полиции Украины в составе «объединенных сил» и в формате (по украинской терминологии) «Операции объединенных сил на востоке Украины». Как следует из текста одного пособия такого рода, миссия Украины в данной операции заключается в том, чтобы «уничтожить носителей неприемлемых типов сознания, сочетая при этом военные и полицейские методы» [6, с. 30].

Подводя итог изложенному, нам представляется необходимым сформулировать следующие выводы:

во-первых, новые обстоятельства ведения современного типа концентрированной войны (войны за сознание человека) определяют

актуальность перестройки всей системы воспитательной работы с личным составом органов внутренних дел Российской Федерации и ее переводу из повседневного состояния мирного времени в состояние повышенного уровня мобилизации сотрудников, выполняющих профессионально-значимые служебные задачи и осознающих степень реальной угрозы мирной жизни наших граждан в условиях открытого противостояния между Россией и коллективным Западом и Украиной, действующих под руководством США;

во-вторых, современная модель воспитательной работы личного состава системы МВД России, безусловно, требует учета и практической реализации новых способов ее ведения и новых технологических решений, основанных в том числе, на потенциале активно применяемых мессенджеров.

Литература:

1. Приказ МВД России от 29 июня 2022 г. № 480 «Об утверждении Положения о Главном управлении по работе с личным составом Министерства Внутренних Дел Российской Федерации» // СПС КонсультантПлюс

2. Контент-хакинг: 15 лайфхаков, которые помогут вывести контент на новый уровень // <https://vc.ru/marketing/230273-kontent-haking-15-layfhakov-kotorye-pomogut-vyvesti-kontent-na-novyy-uroven> (дата обращения: 12.12.2022).

3. Косолапов А.Д., Чимаров С.Ю., Бородавко Л.Т. Правоохранительный аспект легализации информации в сети Интернет об украинских преступных организациях и военных преступниках // Гуманитарные, социально-экономические и общественные науки. - 2022. - № 9. - С. 153-155.

4. NemeZida // https://t.me/nemeZ1da_ru (дата обращения: 11.12.2022).

5. Bereginі // <https://t.me/hackberegini> (дата обращения: 11.12.2022).

6. Дикий С.О. Гібридна війна РФ в Україні: досвід для Балтії. Вільнюс: Литовська військова академія імені генерала Йонаса Жямайтіса, 2016. - 125 с.

7. Erickson J. Hacking: The Art of Exploitation. - San Francisco: No Starch Press, 2008. - 492 p.

8. Zаря // <https://t.me/informZarya> (дата обращения: 11.12.2022).

Literature:

1. Order of the Ministry of Internal Affairs of Russia No. 480 dated June 29, 2022 "On Approval of the Regulations on the Main Directorate for Work with Personnel of the Ministry of Internal Affairs of the Russian Federation" // SPS ConsultantPlus

2. Content hacking: 15 life hacks that will help bring content to a new level // <https://vc.ru/marketing/230273-kontent-haking-15-layfhakov-kotorye-pomogut-vyvesti-kontent-na-novyy-uroven> (date of application: 12.12.2022).

3. Kosolapov A.D., Chimarov S.Yu., Borodavko L.T. Law enforcement aspect of legalization of information on the Internet about Ukrainian criminal organizations and war criminals // Humanities, socio-economic and social sciences. - 2022. - No. 9. - pp. 153-155.

4. Khemezuga // https://t.me/nemeZ1da_ru (date of application: 11.12.2022).

5. *Beregini* // <https://t.me/hackberegini> (date of application: 11.12.2022).
6. *Wild.O. Gibridna viina RF in Ukraine: dosvid for Baltic. Vilnyus: Litovska viiskova akademiya imeni generala Jonas Zhamaitis, 2016. - 125 p.*
7. *Erickson J. Hacking: the Art of exploitation. - San Francisco: No Starch Press, 2008. - 492 p.*
8. *zarya* // <https://t.me/informZarya> (date of application: 11.12.2022).