Проект «Народный перевод»

СОЦИАЛЬНЫЕ СЕТИ

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

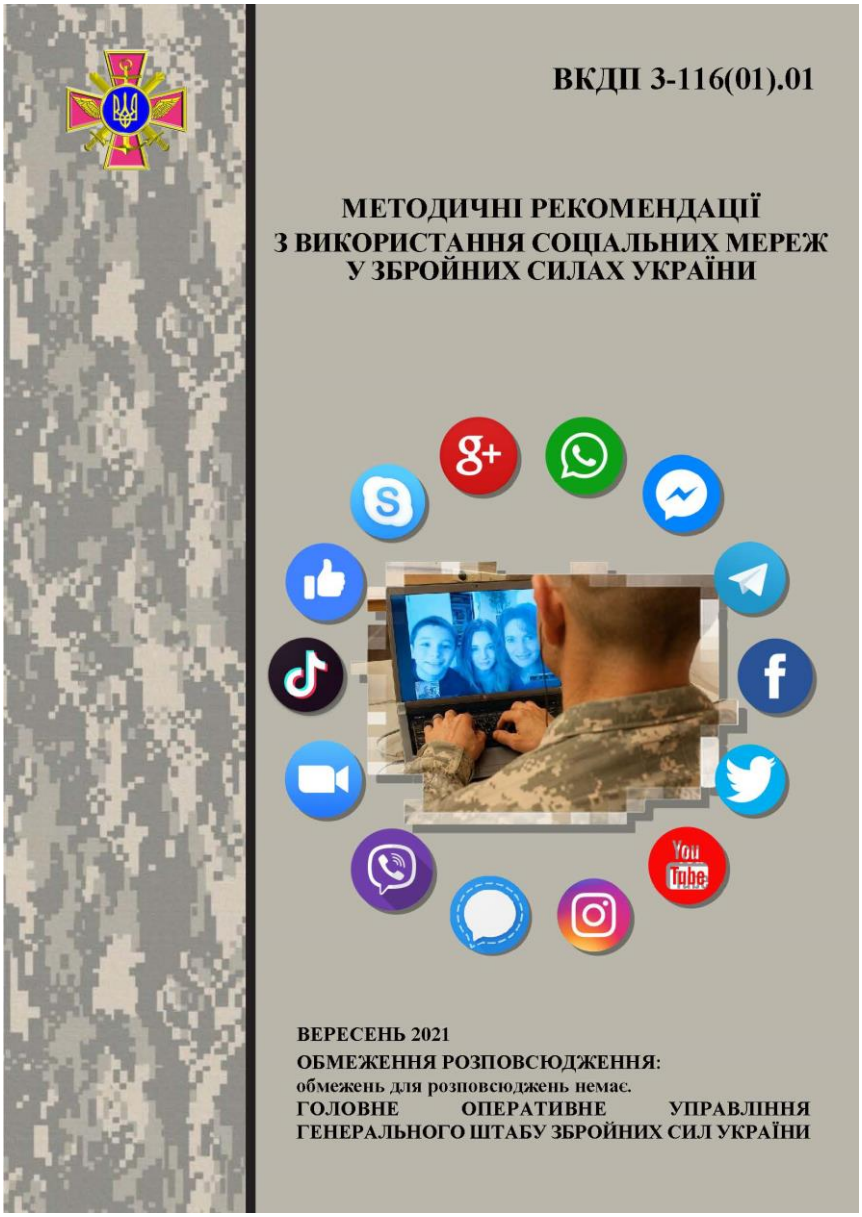
Первоначально издано ВСУ (ВКДП 3-116(01).01) в сентябре 2021 года.

Переведено неофициально на русский язык в январе 2023 года.

Данное пособие издано впервые Главным оперативным управлением Генерального штаба ВСУ в 2021 году на украинском языке, без ограничений на распространение.

Утверждено Главнокомандующим ВСУ генерал-лейтенантом Валерием Залужным.

Оригинальная обложка:



Переведено на русский язык участниками проекта «Народный перевод».

Данный текст является прямым переводом с украинского языка, составлен в научно-познавательных и справочных целях, не редактировался, не должен использоваться для обучения без осмысления и интерпретации с учётом обстоятельств его происхождения, не отражает позицию переводчиков и иных участников проекта «Народный перевод». Относитесь к написанному критически и в случае сомнений по сути и форме написанного обращайтесь к специалистам в соответствующем вопросе.

народный перевод.рф

t.me/svo_institute

Оглавление

ПРЕДИСЛОВИЕ 4
Введение 4
Перечень сокращений и условных значений 5
Ссылки на военные публикации 6
Основные термины и определения 7
1. ОБЗОР СОЦИАЛЬНЫХ СЕТЕЙ И МЕССЕНДЖЕРОВ 10
2. БЕЗОПАСНОСТЬ И РИСКИ В СОЦИАЛЬНЫХ СЕТЯХ 15
2.1. Опасные факторы во время работы в Интернете 16
2.2. Примеры служебной и конфиденциальной информации и возможные последствия ее распространения в социальных сетях (медиа) 18
3. ПОРЯДОК СОЗДАНИЯ ОФИЦИАЛЬНЫХ СТРАНИЦ ОРГАНОВ ВОЕННОГО УПРАВЛЕНИЯ, ВОЕННЫХ ЧАСТЕЙ И ПОДРАЗДЕЛИЙ ВООРУЖЕННЫХ СИЛ УКРАИНЫ В СОЦИАЛЬНЫХ СЕТЯХ И ТРЕБОВАНИЯ К НИМ 21
3.1. Порядок создания официального аккаунта и его верификация 21
3.2. Требования к информации, распространяемой на официальных страницах 23
3.3. Символика Вооруженных сил Украины 26
4. ПРАВИЛА ПОВЕДЕНИЯ В СОЦИАЛЬНЫХ СЕТЯХ 27
5. РЕКОМЕНДАЦИИ ПО ЗАЩИТЕ ИНФОРМАЦИИ В СОЦИАЛЬНЫХ СЕТЯХ И МЕССЕНДЖЕРАХ 31
6. ЗАКЛЮЧИТЕЛЬНАЯ ЧАСТЬ 34

ПРЕДИСЛОВИЕ

Методические рекомендации по использованию социальных сетей в Вооруженных Силах Украины (далее — Рекомендации) разработаны Главным оперативным управлением Генерального штаба Вооруженных Сил Украины и согласованы с заинтересованными органами военного управления и структурными подразделениями Генерального штаба Вооруженных Сил Украины.

Эти Рекомендации разработаны с целью предоставления советов и предложений по освещению информации о деятельности Вооруженных Сил Украины и правил поведения военнослужащих в социальных сетях.

Все вопросы, касающиеся этих Рекомендаций, направлять в ***

Введение

Современные вызовы обусловлены применением Р~~оссийской Федерацией технологий гибридной войны~~ и переносом театра военных действий в плоскость информационного пространства, превратив его в одну из ключевых арен противоборства.

Анализ способов ведения последних вооруженных конфликтов свидетельствует, что в военном деле наступил новый этап развития, когда эффективность современных средств поражения все больше определяется не столько огневой мощью, сколько степенью информационной безопасности. В сущности военных действий все больше возрастает значимость информационного противоборства и преимущество в степени информированности становится непременным условием победы в войне.

На сегодня социальные сети являются удобным и эффективным средством коммуникации. Они дают огромную свободу высказываний в информационном пространстве, которое является открытым и доступным для всех. При эффективном их использовании они становятся мощным инструментом для поднятия имиджа и репутации Вооруженных Сил Украины, поддержания связей с общественностью, общения и обмена опытом и тому подобное.

Кроме того, социальные сети могут эффективно использоваться в ходе реабилитации военнослужащих, для повышения и поддержания на высоком уровне их морально-боевого духа и популяризации военной службы среди населения.

В то же время открытый и глобальный характер социальных сетей и медиа создает предпосылки к сбору и анализу иностранными разведками конфиденциальной информации о деятельности Вооруженных Сил Украины, персональных данных военнослужащих и членов их семей, а также использования противником

социальных сетей для вербовки личного состава и получения необходимой ему информации.

Руководство Вооруженных Сил Украины не запрещает военнослужащим и работникам Вооруженных Сил Украины использование социальных сетей. Однако с целью обеспечения их защиты и безопасности важно, чтобы они были осведомлены о возможных угрозах, которые влияют как на их служебную деятельность, так и на частную жизнь.

Положения этой публикации изложены с целью оказать помощь военнослужащим и работникам Вооруженных Сил Украины, членам их семей и близким в правильном использовании социальных сетей, медиа-порталов и мессенджеров, распространении информации о деятельности Вооруженных Сил Украины и ограничении доступа к их персональным данным.

Перечень сокращений и условных значений

Сокращения и условные обозначения (русский)	Расшифровка сокращения и условного обозначения
СМИ	Средства массовой информации
НАТО **(NATO)**	Организация Североатлантического договора (en: North Atlantic Treaty Organization)
ОИД	Объект информационной деятельности
ПЭВМ	Персональная электронно-вычислительная машина
СНБО	Совет национальной безопасности и обороны

Ссылки на военные публикации

Отметка военной публикации	Полное наименование военной публикации
	Закон Украины «Об основных принципах обеспечения кибербезопасности Украины», с изменениями, Верховная Рада Украины, Киев, 2020
	Закон Украины «О телекоммуникациях», с изменениями, Верховная Рада Украины, Киев, 2020
	Закон Украины «Об информации», с изменениями, Верховная Рада Украины, Киев, 2016
ВКП 18-00 (01) .01	Доктрина публичного общения, Киев, 2020
	Памятка по обеспечению информационной безопасности при работе в сети интернет, Департамент контрразведывательной защиты интересов государства в сфере информационной безопасности Службы безопасности Украины, Киев, 2019
	Рекомендации для персонала Министерства обороны Украины и Генерального штаба Вооруженных Сил Украины по обращению в социальных сетях, Управления информационных технологий, Киев, 2014
ВП 1-185 (49) 03.01	Пособие «Медиаграмотность. Практические советы военнослужащим Вооруженных Сил Украины», Киев, 2021
	U.S. Marine Corps Social Media Handbook, Headquarters Marine Corps Communication Directorate Production and Engagement, 2021
	Using Social Media in the British Army, The British Army's Social Media Policy, Digital Army, Version 5, July 2020
	Family Guidance For the Intenet and Social Media. OPSEC, PII and Identity Management, United States Fleet Forces, February 2019
	U.S. Navy Social Media Handbook for Navy leaders, communicators, Sailors, families, ombudsmen and civilians, March2019
	Identity Awareness, Protection, and Management Guide. A Guide for Online Privacy and Security Comprised of the Complete Collection of Department of Defense Smart Cards Seventh Edition, US Department of Defense, September 2018
	Guide du bon usage des reseaux sociaux, A destination de tous les militaires et civils du ministere de la Defense et de leur entourage, 2016
	U.S. Army Social Media Handbook, Army Office of the Chief of Public Affairs, Online and Social Media Division, 1500 Pentagon, Washington, DC, January 2011
	The U.S.M.C. Social Media Principles marine Corps, Insider Threat Working Group, the Marine Corps Production Directorate, Defense Media Activity, the Marine Corps Division of Public Affairs

Основные термины и определения

IP адрес (Internet Protocol Address) — это идентификатор (уникальный числовой номер) сетевого уровня, который используется для адресации компьютеров или устройств в сетях, построенных с использованием протокола TCP/IP.

Аккаунт (учетная запись) — совокупность информации о пользователе, средствах и его правах относительно многопользовательской системы. Учётная запись, как правило, содержит сведения, необходимые для идентификации пользователя при подключении к системе, информацию для авторизации и учета. Это имя пользователя и пароль.

Вебсайт (или сайт) — совокупность веб страниц и содержимого, доступных в Интернете, которые объединены как по содержанию, так и по навигации под единым доменным именем. Сайтом также называют узел Интернета (компьютер), за которым закреплен уникальный IP—адрес, идентифицирующий его в сети.

Видеоконференция — телекоммуникационная технология, обеспечивающая одновременную двустороннюю передачу, обработку, преобразование и представление интерактивной информации на расстоянии в режиме реального времени (***Skype, Viber, Zoom***).

Угрозы информационной безопасности — совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства в информационной сфере.

Защита информации — совокупность правовых, административных, организационных, технических и других мероприятий, обеспечивающих сохранность, целостность информации и надлежащий порядок доступа к ней.

Информация — это любые сведения и/или данные, которые могут быть сохранены на материальных носителях или отражены в электронном виде.

Информационная безопасность — способность обеспечивать защиту от уничтожения, искажения, блокировки информации, ее несанкционированной утечки или от нарушения установленного порядка ее маршрутизации.

Информационная угроза — намерения, действия или явления, которые путем информационного воздействия на социальные объекты, информационную инфраструктуру и информационные ресурсы могут усложнить (исключить) реализацию национальных интересов государства (функций его структурных органов).

Информационный ресурс — документы или массивы документов, которые хранятся в информационных системах.

Информационная система — это совокупность оборудования, методов и процедур, и, в случае необходимости, персонала, организованного для выполнения функций накопления, обработки, хранения и передачи данных.

Информационное пространство — это информационная среда, в которой происходят информационные процессы и информационные отношения по созданию, сбору, получению, хранению, использованию, распространению, охране и защите информации, информационных продуктов и информационных ресурсов.

Информационная среда — это часть информационного пространства, характеризующаяся минимальной территорией распространения и ограниченным количеством субъектов информационной деятельности, обуславливается своеобразным информационным микроклиматом, включающим совокупность способов, приемов, мероприятий и условий непосредственного осуществления информационной деятельности.

Киберугроза — имеющиеся и потенциально возможные явления и факторы, создающие опасность жизненно важным национальным интересам Украины в киберпространстве, негативно влияют на состояние кибербезопасности государства, кибербезопасность и киберзащиту его объектов.

Кибербезопасность — защищенность жизненно важных интересов человека и гражданина, общества и государства при использовании киберпространства, при котором обеспечиваются устойчивое развитие информационного общества и цифровой коммуникативной среды, своевременное выявление, предотвращение и нейтрализация реальных и потенциальных угроз национальной безопасности Украины в киберпространстве.

Киберзащита — совокупность организационных, правовых, инженерно—технических мероприятий, а также мероприятий криптографической и технической защиты информации, направленных на предотвращение киберинцидентов, выявление и защиту от кибератак, ликвидацию их последствий, восстановление постоянства и надежности функционирования коммуникационных, технологических систем.

Киберпространство — среда (виртуальное пространство), которая предоставляет возможности для осуществления коммуникаций и/или реализации общественных отношений, образованное в результате функционирования совместимых (соединенных) коммуникационных систем и обеспечения электронных

коммуникаций с использованием сети Интернет и/или других глобальных сетей передачи данных.

Кибероборона — совокупность политических, экономических, социальных, военных, научных, научно—технических, информационных, правовых, организационных и других мероприятий, которые осуществляются в киберпространстве и направлены на обеспечение защиты суверенитета и обороноспособности государства, предотвращение возникновения вооруженного конфликта и отпор вооруженной агрессии.

Коммуникация — процесс передачи информации (фактов, идей, взглядов, эмоций и т.д.) вербальным, письменным, печатным, аудиовизуальным, электронным и другим способом между субъектами или от субъекта к объекту информационно—коммуникационной деятельности и в обратном направлении.

Медиа—блог — это вебсайт, главное содержание которого записи, изображения или мультимедиа, которые регулярно публикуются.

Медиахостинг (медиа—портал) — услуга предоставления дискового пространства, подключения к сети и других ресурсов для размещения медиа (фото, видео) информации на сервере, постоянно находящемся в Интернете ***(YouTube, Vimeo)***.

Мессенджеры — это приложения (платформы), позволяющие создавать обмен сообщениями между пользователями в режиме реального времени (онлайн) ***(Viber, Telegram, WhatsApp, Signal, Facebook Messenger)***.

Прокси—сервер — сервер (компьютерная система или программа) в компьютерных сетях, позволяющий клиентам выполнять косвенные (через посредничество прокси—сервера) запросы к сетевым сервисам.

Социальные медиа — онлайн технологии, благодаря которым пользователи контента через свои сообщения становятся его соавторами и могут сотрудничать, общаться, делиться информацией или участвовать в любой другой социальной активности со всеми другими пользователями сервиса ***(TikTok, Likee)***.

Социальная сеть — это сервис (веб приложение), который используется пользователями для поддержания социальных связей в Интернете. Важным элементом сети является контент (содержание, информация), который создается ее пользователями ***(Facebook, Instagram, Twitter, MySpace)***.

Фишинг — вид мошенничества, целью которого является приобретение у доверчивых или невнимательных пользователей социальных сетей собственных (других пользователей) персональных данных или сведений.

1. ОБЗОР СОЦИАЛЬНЫХ СЕТЕЙ И МЕССЕНДЖЕРОВ

Развитие Интернета, мобильных устройств и компьютерных технологий, а также глобальное использование социальных сетей и медиа стали неотъемлемой частью современного общества.

Социальные сети постоянно меняются, они могут включать в себя новые информационные и коммуникационные инструменты, работающие на персональных компьютерах, ноутбуках, мобильных устройствах и смартфонах. Использование социальных сетей позволяет пользователям осуществлять публикацию и распространение фото и видеоматериалов, обмен информацией и общение в режиме реального времени.

На сегодня, учитывая опыт, принципы и стандарты, принятые в государствах-членах НАТО, использование социальных сетей следует разделять на три основные категории:

Персональное онлайн присутствие — это коммуникации в Интернете, которые осуществляются военнослужащими (работниками) в их личной жизни, за пределами их служебных обязанностей.

Указанные коммуникации включают: вебсайты, медиа блоги, аккаунты в социальных сетях, на сайтах знакомств (объявления, форумы и т.д.) и игры.

Официальное онлайн присутствие — коммуникации воинских частей и подразделений Вооруженных Сил Украины в Интернете, которые официально зарегистрированы, одобрены соответствующими заинтересованными органами и курируются определенными лицами или подразделениями. Официальные коммуникации используются для сознательной, координированной публикации и распространения информации о воинских частях и подразделениях Вооруженных Сил Украины, организации взаимодействия с общественностью, но с обязательным официальным согласованием с Управлением стратегических коммуникаций Аппарата Главнокомандующего Вооруженных Сил Украины.

Корпоративное онлайн присутствие — это коммуникации Вооруженных Сил Украины в Интернете, которые централизованно руководствуются специалистами Управления стратегических коммуникаций Аппарата Главнокомандующего Вооруженных Сил Украины.

К ним относятся: официальный сайт Вооруженных Сил Украины (*zsu.gov.ua*) и официальные страницы Генерального штаба Вооруженных Сил Украины, органов военного управления в социальной сети «Facebook» в других социальных сетях и медиахостингах.

Рис.1 *– Логотипы популярных мессенджеров и соцсетей.*

Мессенджеры и другие приложения для обмена сообщениями — это программы или мобильные приложения, с помощью которых пользователи могут осуществлять обмен сообщениями в режиме реального времени.

Изначально мессенджеры были составляющей социальных сетей, но многие из них превратились в отдельные (автономные) платформы, позволяющие осуществлять общение, обмен информацией любого типа, платежи и торговлю и тому подобное. В основном они используются через мобильные приложения на смартфонах, но некоторые приложения также имеют программное обеспечение для операционных систем Windows и Linux.

На сегодняшний день одними из самых популярных приложений для обмена сообщениями и информацией являются *WhatsApp, Viber, Telegram, Signal* и другие. Некоторые социальные сети предлагают услуги обмена сообщениями в качестве компонента их общей платформы (*Facebook Messenger*), а также функции прямого обмена сообщениями (*Instagram и Twitter*).

В то же время все более широкое распространение приобретают онлайн приложения, благодаря которым пользователи могут в режиме реального времени создавать и распространять любой контент, сотрудничать, общаться, делиться информацией со всеми другими пользователями сервиса (*TikTok, Likee, Instagram*).

Также результатом перехода от традиционных платных звонков и SMS-сообщений к бесплатным сервисам предоставления услуг связи стало использование телекоммуникационных видеотехнологий, с помощью которых осуществляется двусторонняя передача, обработка, преобразование и представление интерактивной информации на расстоянии в режиме реального времени (*Skype, Viber, Zoom*).

Следует отметить, что мессенджеры хранят все переписки пользователей на своих серверах, что автоматически ставит их под угрозу в случае взлома аккаунта или необходимости получения их спецслужбами той страны, где находятся серверы.

В современном мире социальные сети и мессенджеры настолько прочно укоренились в обществе, что их проникновение в личную жизнь пользователей и дальнейшее влияние на них незаметно.

Например, анализ социальных сетей может помочь найти важную (критическую) информацию о лицах и военных объектах или оказывать поддержку нужным сообществам в ходе конфликтов. Также он дает возможность направлять информацию к выбранной целевой аудитории и влиять с помощью нее на восприятие реальности, принятие решений или поведение определенных лиц. Геокодированные посты могут дополнить анализ и помочь оценить географию распространения необходимой информации.

Поэтому, благодаря анализу социальных сетей, медиапорталов и мессенджеров возможно осуществлять сбор и оценку информации о деятельности органов военного управления, соединений, воинских частей и подразделений Вооруженных Сил Украины, способствовать или наоборот противодействовать распространению искаженных и ложных сведений, разоблачать или скрывать меры безопасности применения войск (сил).

Ниже приведены результаты собственного исследования, проведенного информационным агентством Министерства обороны Украины **АрмияInform** «Безопасность военных в социальных сетях» в 2020 году.

Учитывая современные тенденции развития социальных сетей и манипуляционных технологий, приведенные цифры указывают, что военные как целевая аудитория являются легкодоступной именно в социальных сетях. Это со своей стороны несет определенные угрозы, но и одновременно может быть эффективным каналом для реализации коммуникации высшим военным руководством Вооруженных Сил Украины с личным составом.

Почти 70% военнослужащих ежедневно посещают социальные сети. По меньшей мере около 44% опрошенных проводят там до 2 часов в сутки.

Военные ВСУ являются легкодоступной аудиторией именно в социальных сетях. Это, в свою очередь, несет ряд угроз, но и одновременно может быть эффективным каналом коммуникации высшего военного руководства ВСУ с подчиненным личным составом

Полученные данные свидетельствуют о вероятном потреблении информации из ненастоящих профилей, продублированных страниц, которые могут иметь вражеские смыслы и символы. Такой значительный процент говорит о низком уровне информационной безопасности в воинских подразделениях

Рис.2 *– Результаты социологического опроса, часть 1.*

Рис.3 *– Результаты социологического опроса, часть 2.*

2. БЕЗОПАСНОСТЬ И РИСКИ В СОЦИАЛЬНЫХ СЕТЯХ

Using public source openly and without resorting to illegal means is possible to gather at least 80% of information about the enemy. The percentage varies depending on the government's policy on freedom of the press and publication.

Document found on a suspected terrorist computer during a police raid in Manchester, England, 10 May 2000

Свободно используя открытые источники и не прибегая к незаконным средствам, можно собрать не менее 80% информации о противнике. Процент колеблется в зависимости от политики правительства в отношении свободы прессы и публикации.

Документ обнаружен на компьютере подозреваемого в терроризме во время полицейского рейда в Манчестере, Англия, 10 мая 2000 года

Личный состав Вооруженных Сил Украины является неотъемлемой составляющей общества, стремительная информатизация которого постепенно охватывает все большую часть населения государства. Но необратимый процесс информатизации также является причиной появления нетрадиционных угроз безопасности государства и создает принципиально новые сложности для системы национальной безопасности. На сегодня особенно в связи с проведением ~~операции Объединенных сил на востоке Украины~~, как никогда остро встает вопрос защиты информации, информационных услуг и систем обеспечения информационной безопасности государства и общества в целом.

Предотвращение возможных угроз информационной безопасности может быть обеспечено различными мерами и средствами от создания глубокой, эшелонированной комплексной системы защиты информации, состоящей из физических, аппаратных, программных и криптографических средств до внедрения философии сознательного отношения населения к проблеме информационной безопасности и защиты информации.

Такой вариант выхода из ситуации как полный запрет пользования социальными сетями для военнослужащих является неэффективным, поскольку чаще всего вызывает обратную реакцию. Поэтому важным в сфере обеспечения информационной безопасности является вопрос предоставления советов военнослужащим Вооруженных Сил Украины относительно использования социальных сетей и медиа с целью уменьшения (недопущения) утечки служебной и конфиденциальной информации о деятельности Вооруженных Сил Украины, а также нейтрализации негативного информационно-психологического воздействия на личный состав.

2.1. Опасные факторы во время работы в Интернете

Опасные факторы во время работы в Интернете условно делятся на информационные и технические.

Следует отметить, что информационные и технические факторы относятся к такой сфере деятельности государства как информационная безопасность, а их отличие заключается только в путях, по которым тот, кто оказывает влияние, будет достигать конечной цели.

Информационные угрозы, как правило, направлены на лицо (группу лиц) с целью принуждения его к необходимым действиям (бездействию) и принятия им неправильных управленческих решений путем введения объекта влияния в заблуждение за счет дезинформации, фейков, подмены фактов и тому подобное.

Техническими угрозами являются получение иностранными спецслужбами несанкционированного, неправомерного доступа к информации и информационным ресурсам или неконтролируемая утечка служебной и персональной информации и тому подобное.

Одним из самых распространенных методов ~~введения общества в заблуждение, которое активно использует Российская Федерация~~, является создание и распространение фейковой (неправдивой, искаженной) информации. Поэтому важно умение распознавать фейки среди потока информации и эффективно противостоять им.

Ниже приведены рекомендации по проверке информации на достоверность:

1. Обратите внимание на источник распространения информации. Обычно для распространения фейковой информации используют малоизвестные или только что созданные ресурсы, прибегают к сокращенным ссылкам, созданным с помощью онлайн- генераторов *(bit.ly)* или сайтов, похожих на официальные *(m1l.gow.ua).*
2. Проверьте автора поста *(не бот ли он?).* Перейдите на его страницу и посмотрите, как давно она создана, сколько там друзей, фото, публикаций, и тому подобное.
3. Наличие эмоционального заголовка (*«Шок!», «Сенсация!», «Это было скрыто!»*) свидетельствует о вероятности манипулирования общественным мнением.
4. Обезличивание действующих лиц *(«жительница области», «военные жалуются», «эксперты советуют»*) и несоблюдение баланса мнений — признаки неполной или недостоверной информации.

5. Большое количество активных комментаторов может свидетельствовать об использовании ботов и попытке повлиять на восприятие аудиторией.
6. Внимательно присмотритесь к визуальному контенту (фото, видео) на наличие эффектов Photoshop или монтажа, а также соответствие текста сообщения изображению или ролику.
7. Воздерживайтесь от комментирования или распространения сообщений, в правдивости которых сомневаетесь.

В условиях ведения так называемой «гибридной войны», в которой п~~ропаганда Российской Федерации с полностью подчиненными СМИ ведет информационную войну против Украины~~, одним из ключевых вопросов остается **обеспечение собственной безопасности и безопасности своей семьи**.

Это должно побудить личный состав Вооруженных Сил Украины и членов их семей к правильному поведению в информационном пространстве и возможным нарушениям вопросов безопасности применения войск (сил) в нем, а также последствий, к которым может привести, например, размещение в социальной сети сведений о себе, сослуживцах, подразделениях и местах прохождения военной службы, служебных документов и т.п.

Кроме того, в современных условиях существует высокая вероятность вербовки противником военнослужащих Вооруженных Сил Украины с использованием социальных сетей и мессенджеров для получения необходимой ему информации.

На сегодня практически каждый военнослужащий (сотрудник) Вооруженных Сил Украины имеет личный аккаунт в социальных сетях, где публикует и распространяет информацию о личной жизни, мировых и государственных событиях, комментирует их и высказывает собственное или поддерживает чье-то мнение, загружая фото или видеоматериалы и тому подобное.

Но вместе с этим, каждый из них должен осознать, что социальные сети и медиа являются не только средством общения и главным каналом доведения информации до нашего общества, но и эффективным источником получения необходимых сведений иностранными разведками и разведкой противника.

2.2. Примеры служебной и конфиденциальной информации и возможные последствия ее распространения в социальных сетях (медиа)

Большинство информации, представленной в социальных сетях, доступно без регистрации — достаточно лишь отыскать страницу пользователя в социальной сети, а для поучения другой информации о нем необходимо добавить его в круг своих друзей. Личная информация и личная переписка также доступны для просмотра администрации сети и любые настройки приватности ее не скроют.

Чем больше человек общается в социальных сетях, тем больше информации о нем возможно собрать.

Более того, IP адрес, независимо от его защищенности и уникальности, позволяет определить принадлежность пользователя к определенному провайдеру и городу, в котором он находится.

Распространение персональной информации эффективно используется противником для обновления базы данных ~~«карателей»~~ на сайте «Трибунал», где ~~сепаратисты~~ выкладывают информацию с личными данными военнослужащих Вооруженных Сил Украины, добытой из открытых источников, с целью создания давления на них и их родных.

Поэтому важно быть осторожным при распространении любой информации в Интернете, ведь невнимательность может привести к размещению сведений, которые не должны быть обнародованы и доступны.

Ниже приведены примеры информации, распространение которой в социальных сетях (медиа) может привести к негативным последствиям и повлиять на выполнение боевых (специальных) задач воинскими частями (подразделениями) Вооруженных Сил Украины.

1. Фото и видео военнослужащих или их коллег в военной форме (особенно с геопривязкой), расположение войск, с помощью которых можно идентифицировать руководящий и личный состав, воинские части (подразделения) и их местонахождение.
2. Фото и видеоматериалы, на которых освещены вооружение и военная техника Вооруженных Сил Украины с военными (бортовыми) номерами, позволяет определить принадлежность ее к соответствующим подразделениям Вооруженных Сил Украины.
3. Фото и видео военнослужащих или их коллег в районе выполнения боевых (специальных) задач, с помощью которых возможно определить тактические

знаки различия подразделений (цветные ленты, снаряжение и оружие, графические фигуры и т.д.).

4. Фото служебных документов (выдержек из приказов, рапортов, заявок, отпускных билетов и т.д.), с помощью которых есть возможность определить формы и порядок оформления документов разного вида, стилистику их написания с целью создания и распространения недостоверной информации.
5. Сведения, раскрывающие подлинные наименования воинских частей (подразделений), других военных объектов, а также уровень их укомплектованности личным составом, вооружением и военной техникой, материально-техническими средствами, их состояние и места хранения или районов их сосредоточения.
6. Информация относительно оперативного развертывания войск (сил), порядка их перемещения в районы выполнения задач.
7. Фото и видеоматериалы, с помощью которых есть возможность выявить элементы системы охраны и обороны военных объектов и средств защиты личного состава, вооружения и военной техники, которые выполняют боевые (специальные) задачи.

Рис.4 *– Плакаты-напоминания о соцсетях.*

Обнародование в Интернете информации такого содержания и неосторожное использование военнослужащими (сотрудниками) и членами их семей социальных сетей (медиа) создает предпосылки к сбору и анализу данных о военнослужащих Вооруженных Сил Украины и установлению характера их деятельности. Также это позволяет разведке противника получать необходимую информацию относительно расположения и перемещения подразделений, выявить оборонительные позиции и места сосредоточения войск в районе выполнения боевых (специальных) задач, что может привести к их срыву, потерям среди личного состава и уничтожению военной техники.

Поэтому социальные сети (медиа) предоставляют возможность сбора информации о персональных данных военнослужащих Вооруженных Сил Украины другими лицами без их ведома, поскольку отследить процесс ее получения в таких системах практически невозможно.

При таких условиях необходимо проводить предупредительную разъяснительную работу по ограничению распространения публикаций, фото и видеоматериалов, которые раскрывают деятельность Вооруженных Сил Украины, с разработкой наглядных агитационных материалов с последующим их распространением среди военнослужащих и членов их семей.

3. ПОРЯДОК СОЗДАНИЯ ОФИЦИАЛЬНЫХ СТРАНИЦ ОРГАНОВ ВОЕННОГО УПРАВЛЕНИЯ, ВОЕННЫХ ЧАСТЕЙ И ПОДРАЗДЕЛЕНИЙ ВООРУЖЕННЫХ СИЛ УКРАИНЫ В СОЦИАЛЬНЫХ СЕТЯХ И ТРЕБОВАНИЯ К НИМ

Официальные страницы (сайты) органов военного управления, воинских частей и отдельных подразделений в социальных сетях создаются для повышения имиджа Вооруженных Сил Украины, сознательной (координированной) публикации и распространения информации о деятельности Вооруженных Сил Украины. Они должны быть официально зарегистрированы, верифицированы и согласованы с соответствующими заинтересованными органами, вестись и контролироваться определенными лицами или подразделениями.

3.1. Порядок создания официального аккаунта и его верификация

Политика Вооруженных Сил Украины, как правило, предполагает ведение только одной официальной страницы в каждой социальной сети для органов военного управления, воинской части или отдельного подразделения. Поэтому руководителям (командирам) следует тщательно следить за созданием в Интернете клонов официальных страниц их подразделений, своевременно реагировать на распространяющийся на них контент и принимать меры по их закрытию.

Наличие в одной социальной сети нескольких аккаунтов органов военного управления и воинских частей (подразделений) значительно усложняет их ведение, мониторинг и контроль.

Создание аккаунтов подразделений по уровню ниже отдельной воинской части считается нецелесообразным и бесполезным, поскольку официальные страницы таких подразделений имеют небольшую целевую аудиторию и низкий уровень контроля распространенного контента. Но в случае необходимости и по решению командиров (начальников) создание страниц отдельных подразделений не запрещается.

На сегодняшний день в Вооруженных Силах Украины существует определенный порядок создания официальной страницы (сайта) органа военного управления, воинской части или отдельного подразделения. Согласно приказу Министерства обороны Украины от 28.12.2016 №727 «Об утверждении Порядка использования сети Интернет в системе Министерства обороны Украины» создание новой официальной страницы в социальной сети осуществляется по решению руководства Министерства обороны Украины и Вооруженных Сил Украины.

В целях подготовки указанного решения предлагается придерживаться следующей процедуры:

1. Предоставление командованием воинской части (подразделения) обоснованных предложений по созданию новой официальной страницы в социальной сети (сайта) с указанием его будущих преимуществ для Вооруженных Сил Украины, возможных рисков и угроз информационной и кибернетической безопасности, учитывая информацию, которую планируется публиковать.
2. Согласование создания новой страницы в социальной сети (сайте) воинской части (подразделения) с Управлением стратегических коммуникаций Аппарата Главнокомандующего Вооруженных сил Украины, Главным оперативным управлением Генерального штаба Вооруженных сил Украины.
3. Принятие решения (или отказ) руководством Вооруженных сил Украины о создании страницы в социальной сети или на сайте.
4. В случае согласования и получения разрешения на создание страницы (сайта) командиром воинской части издается приказ о создании официальной страницы (сайта) с указанием ответственных лиц за ее ведение и сопровождение, а также порядка наполнения информацией (сообщениями, фото и видео материалами). Копия приказа направляется в установленном порядке в Управление стратегических коммуникаций Аппарата Главнокомандующего Вооруженных сил Украины и Главного оперативного управления Генерального штаба Вооруженных сил Украины.
5. Создание официальной страницы в социальной сети (сайте), ее регистрация, верификация установленным порядком, последующий запуск и ведение.

Ответственность за контент, который публикуется и распространяется на официальной странице (сайте) в соответствии с Доктриной публичного общения, несет лично руководитель (начальник) органа военного управления, командир воинской части (подразделения) и уполномоченные им лица (представители, пресс-офицеры и т.п.).

3.2. Требования к информации, распространяемой на официальных страницах

В ходе публикации любых материалов о деятельности Вооруженных Сил Украины следует соблюдать правильную стилистику ее изложения с целью недопущения раскрытия критической (важной) информации для иностранных разведок и спецслужб противника.

Ниже приведены примеры корректного изложения информации о событиях в войсках (силах) Вооруженных Сил Украины и их деятельности:

❌ в 65 омбр оперативного командования «Запад»;	✔ в одной из воинских частей (бригад) Вооруженных сил Украины;
❌стрелок-зенитчик срв 1 мб 65 омбр солдат Андрей ПРИДАТКО «СТРЕЛА»;	✔ военнослужащий Вооруженных сил Украины (без позывных, должностей и фамилий);
❌ КШН привлекается 2875 военнослужащих, танков – 15, БМП – 20, средств ПВО – 32, РСЗО – 22…;	✔ к учениям привлекается около 3000 личного состава и 100 единиц техники;
❌ Сегодня, 23 апреля, во время обстрела противником ВОП «Квадрат» вблизи н.п. Алексеевка (Волновского р- на) погибли пять в/с и получили ранения одиннадцать бойцов 65 омбр…;	✔ Сегодня противник еще раз ~~нарушил Минские договоренности~~ и осуществил обстрел позиций Вооруженных Сил Украины (не следует предоставлять противнику результаты его огневого поражения)
❌ в Белую Церковь вернулись бойцы 65 омбр, которые в течение 6 месяцев защищали Украину на Мариупольском направлении…;	✔ В ППД из района выполнения боевых задач (или ООС) вернулся личный состав одной из бригад Вооруженных сил Украины (или воинской части А3232) (без детализации сроков и мест выполнения боевых заданий);
❌21-22 марта на 242 общевоинском полигоне (пгт. Гончаровское) пройдут бригадные тактические учения с 65 омбр, после проведения которых она убывает в район выполнения боевых задач…	✔ В марте на Гончаровском полигоне пройдут обучение с подразделениями одной из бригад Вооруженных Сил Украины для повышения их обученности и слаженности (не указываются сроки готовности и выхода подразделений в район проведения ООС и из него).

Согласно требованиям приказа Службы безопасности Украины от 23.12.2020 № 383 «Об утверждении Свода сведений, составляющих государственную тайну» и приказа Генерального штаба Вооруженных Сил Украины от 22.11.2017 № 408 «Об утверждении Перечня сведений Вооруженных Сил Украины, составляющих служебную информацию» решениями государственных экспертов по вопросам секретности определены сведения, составляющие государственную тайну или служебную информацию.

Поэтому на официальных страницах органов военного управления, воинских частей и отдельных подразделений в социальных сетях ни при каких условиях

НЕ ПОДЛЕЖИТ ПУБЛИКАЦИИ И РАСПРОСТРАНЕНИЮ следующая информация:

- сведения, раскрывающие меры и сроки приведения войск (сил) в готовность к выполнению задач по назначению;
- сведения о мероприятиях, раскрывающих перспективу реформирования и развития Вооруженных сил Украины с указанием боевого состава и штатной численности подразделений, кроме общей информации;
- сведения об обеспеченности материально-техническими средствами, вооружением, ракетами, боеприпасами воинских частей (подразделений) Вооруженных сил Украины;
- информация о текущих операциях (боевых) действиях, составе сил и средств, которые к ним привлечены, ходе их ведения (до предоставления официального разрешения на их обнародование);
- сведения о результатах применения воинских частей (подразделений) радиоэлектронной борьбы;
- сведения о результатах проведения информационных (психологических) операций (акций), мер безопасности применения войск (дезинформации, демонстративных действий, имитации и т.п.);
- информация о перемещении (маршруты, места погрузки (выгрузки), порядке, времени) и развертывании воинских частей и подразделений в районах выполнения боевых (специальных) задач;
- информация о возвращении воинской части (подразделений) из районов выполнения боевых (специальных) задач в пункт постоянной дислокации (не ранее определенного срока);
- подробная информация о применении (испытании) нового вооружения: противотанковых комплексов и ракет к ним, беспилотных аппаратов, артиллерийских систем, средств разведки и наблюдения, зенитных ракетных комплексов, радиолокационных станций, средств связи, их тактико-технические характеристики и боевые возможности;
- сведения о перемещении руководящего (командного) состава, работе рабочих (инспекционных) групп (в том числе иностранных) в районах ведения боевых действий до окончания их работы (указанную информацию рекомендовано публиковать через 2-3 дня после завершения их работы).

Кроме того, НЕ ПОДЛЕЖАЮТ ПУБЛИКАЦИИ в социальных сетях следующие типы фото и видеоматериалов:

- видеоматериалы и фотографии вооружения и военной техники, на которых нанесены знаки взаимного распознавания (условные отметки, бортовые и военные номера), по которым можно идентифицировать воинские части (подразделения), в которых они находятся на вооружении, районы (места) их сосредоточения (хранения);
- фотографии и видеоматериалы, снятые на пунктах управления, боевых позициях и тыловых районах, на фоне четко выраженных объектов (здания, местные ориентиры), по которым можно провести географическую привязку и установить место (район) сосредоточения войск (сил);
- фотографии опытных образцов вооружения, на которых четко изображены конструктивные особенности, тип применяемых ракет и боеприпасов, средства связи, наблюдения и разведки;
- групповые и одиночные фотографии военнослужащих подразделений специального назначения и военной разведки;
- фото и видеоматериалы, на которых изображены боевые (стартовые) позиции подразделений противовоздушной обороны с техникой на них, ориентиры, по которым можно определить места их развертывания и сосредоточения;
- фото и видеоматериалы, на которых изображены рабочие карты, макеты местности и служебные документы.

Также, **СТРОГО ЗАПРЕЩАЕТСЯ ПУБЛИКОВАТЬ И РАСПРОСТРАНЯТЬ**:

- личные данные (фамилия, имя, должность, воинское звание, адрес проживания, место прохождения службы и т.п.) военнослужащих, которые проходят службу в Вооруженных Силах Украины, особенно в подразделениях специального назначения, военной разведки, ракетных войск и артиллерии;
- сведения об эффективности мер маскировки, введения в заблуждение, способах их проведения, средствах имитации, которые используются при ведении боевых действий;
- порядок подготовки снайперов и операторов беспилотных аппаратов, противотанковых комплексов, фото и видеоматериалы из районов их подготовки, выполнение боевых (специальных) задач, специфики (особенностей) их боевой работы;
- недостоверные (непроверенные) и искаженные сведения о деятельности Вооруженных сил Украины (если на это не было отдельных указаний).

3.3. Символика Вооруженных сил Украины

Символика – это не просто знаки, шевроны или эмблемы.

Рис.5 *– Примеры символики ВСУ.*

Это комбинация ценностей, которые отражают историю украинской армии, а также ее новые боевые традиции и создают образ Вооруженных сил Украины, их авторитет. Поэтому при использовании символики Вооруженных Сил Украины в социальных сетях и СМИ очень важно использовать официальные утвержденные эмблемы видов, отдельных родов войск (сил) и воинских частей (подразделений) Вооруженных Сил Украины.

Следует избегать использования на официальных страницах органов военного управления, воинских частей и отдельных подразделений неофициальных (любительских) эмблем и логотипов, которые могут поставить под сомнение общественности их принадлежность к Вооруженным Силам Украины и привести к путанице.

4. ПРАВИЛА ПОВЕДЕНИЯ В СОЦИАЛЬНЫХ СЕТЯХ

Ключевым моментом распространения каких-либо сведений в информационном пространстве является то, что опубликованная информация не является личной. Это касается как частных сообщений в мессенджерах, так и публично размещенного контента на страницах социальных сетей и медиа.

С целью недопущения получения заинтересованными лицами личной информации о военнослужащих (сотрудниках) Вооруженных сил Украины, членов их семей, коллег, а также, информации о местах дислокации и расположении воинских частей и подразделений Вооруженных сил Украины, их состава и укомплектованности, особенно привлеченных к выполнению боевых (специальных) задач, следует соблюдать **основные правила**.

1. Никому не предоставляйте и не распространяйте в Интернете информацию о себе, своих близких и коллегах

Распространение таких сведений может не только идентифицировать личность как военнослужащего или указывать его причастность к определенному подразделению, но и подвергать опасности близких ему людей. Полученные данные могут передаваться заинтересованным лицам (террористам, агентам) с целью создания давления на военнослужащих, используя членов их семей.

Не следует надеяться и полагаться на безопасность Интернет-коммуникаций. Необходимо подумать о последствиях для безопасности и защиты информации, которая планируется к публикации или распространению.

2. Ограничьте круг знакомств в сети, скройте свою причастность к службе в ВСУ

Не следует принимать в «друзья» незнакомых людей (пользователей сети). Это могут быть фейковые (ложные) аккаунты спецслужб противника для сбора необходимой им информации о военнослужащих, их служебной деятельности или Вооруженных силах Украины в целом.

3. Не размещайте на своей странице фото, видео о деятельности ВСУ

Такой контент не только идентифицирует личность как военнослужащего, но и дает информацию о составе, состоянии, местонахождении и перемещении его подразделения (фото на фоне военной техники, позиций, с сослуживцами, видео, где можно услышать команды, сигналы и звуки техники, что двигается и т.д.).

4. Не начинайте и не присоединяйтесь к спорным (провоцирующим) дискуссиям, связанным с деятельностью Вооруженных сил Украины

Как правило, «искусственно созданные» спецслужбами агрессивные переписки направлены на вывод собеседника из психического равновесия, потерю им бдительности и с помощью провоцирующих вопросов (постов) заставляют выдать необходимую им служебную или конфиденциальную информацию или подтвердить (опровергнуть) факты. В случае возникновения таких случаев следует переводить дискуссию в более знакомую сферу знаний.

5. Правильно излагайте информацию о своей деятельности или деятельности своих близких (друзей, коллег)

Во время общения в Интернете или социальных сетях не следует акцентировать внимание на принадлежности к Вооруженным Силам Украины, если в этом нет необходимости.

При предоставлении какой-либо информации или распространении сведений о событиях необходимо избегать их детализации и использовать более общие описания. Например:

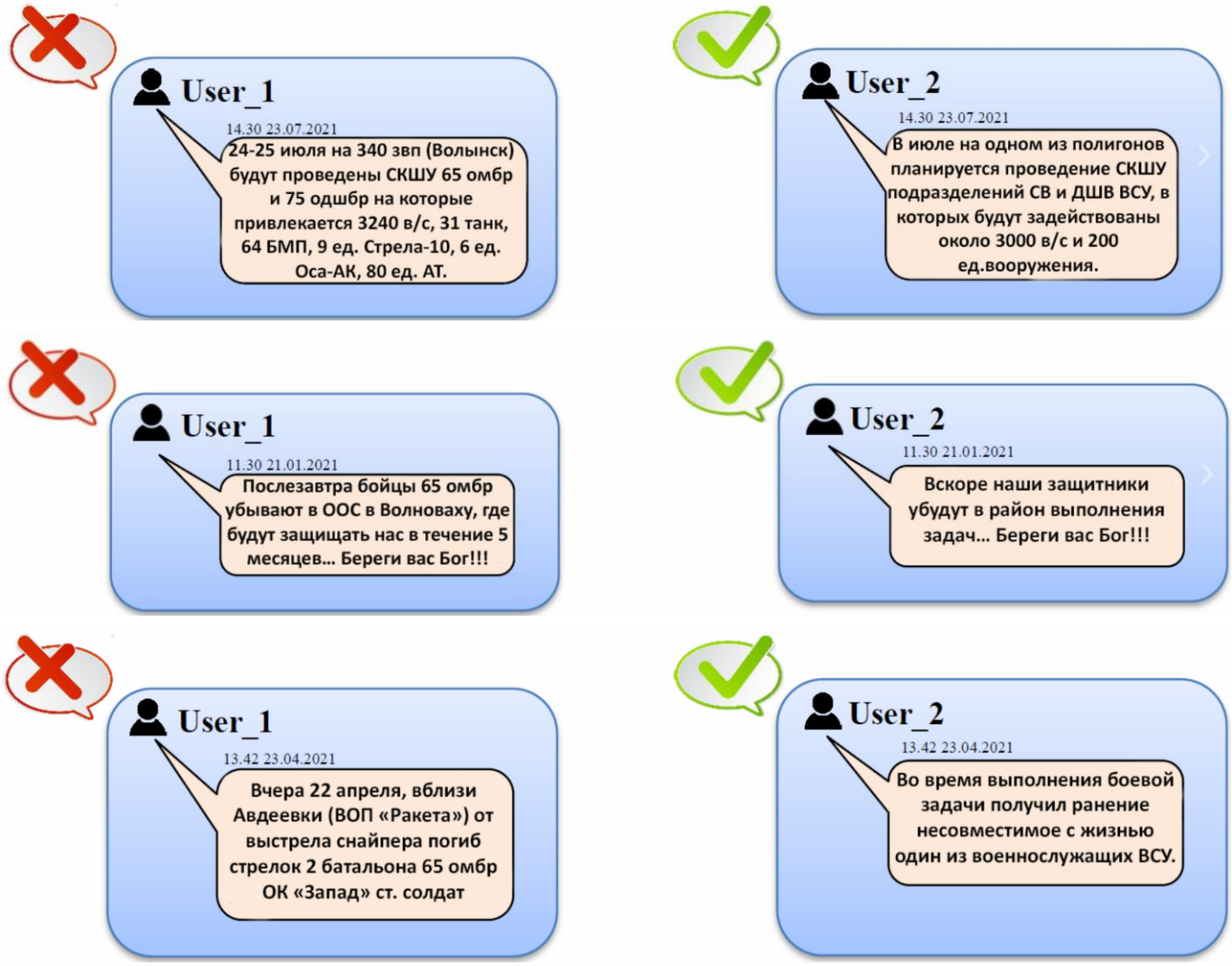


Рис.6 *– Примеры некорректного (слева) и корректного (справа) сообщения.*

6. Не распространяйте и не обсуждайте информацию, о которой не осведомлены, особенно в отношении деятельности Вооруженных сил Украины

Во время общения в социальных сетях следует быть сдержанным и ответственным, оперировать информацией только в пределах своей компетенции, особенно в случаях, когда собеседники выходят за круг доверенной аудитории.

Внимательно читайте и анализируйте публикации других пользователей, прежде чем их оценивать, комментировать или распространять. Будьте осторожны в отношении фейков и фишинга.

7. Поддерживайте «чистую» репутацию аккаунтов в социальных сетях

При распространении на страницах в социальных сетях официальной информации о деятельности Вооруженных сил Украины или о других важных государственных событиях следите за ее оценкой и комментариями. Не допускайте распространения фейков и унижение репутации украинской армии. Прекращайте распространение информации, если на нее введен статус «ограниченное распространение» и при необходимости удалите ее.

8. Откажитесь от использования социальных сетей (ВКонтакте, Одноклассники), мессенджеров (Telegram), почтовых ящиков (Mail.ru, Yandex.ru) российского производства

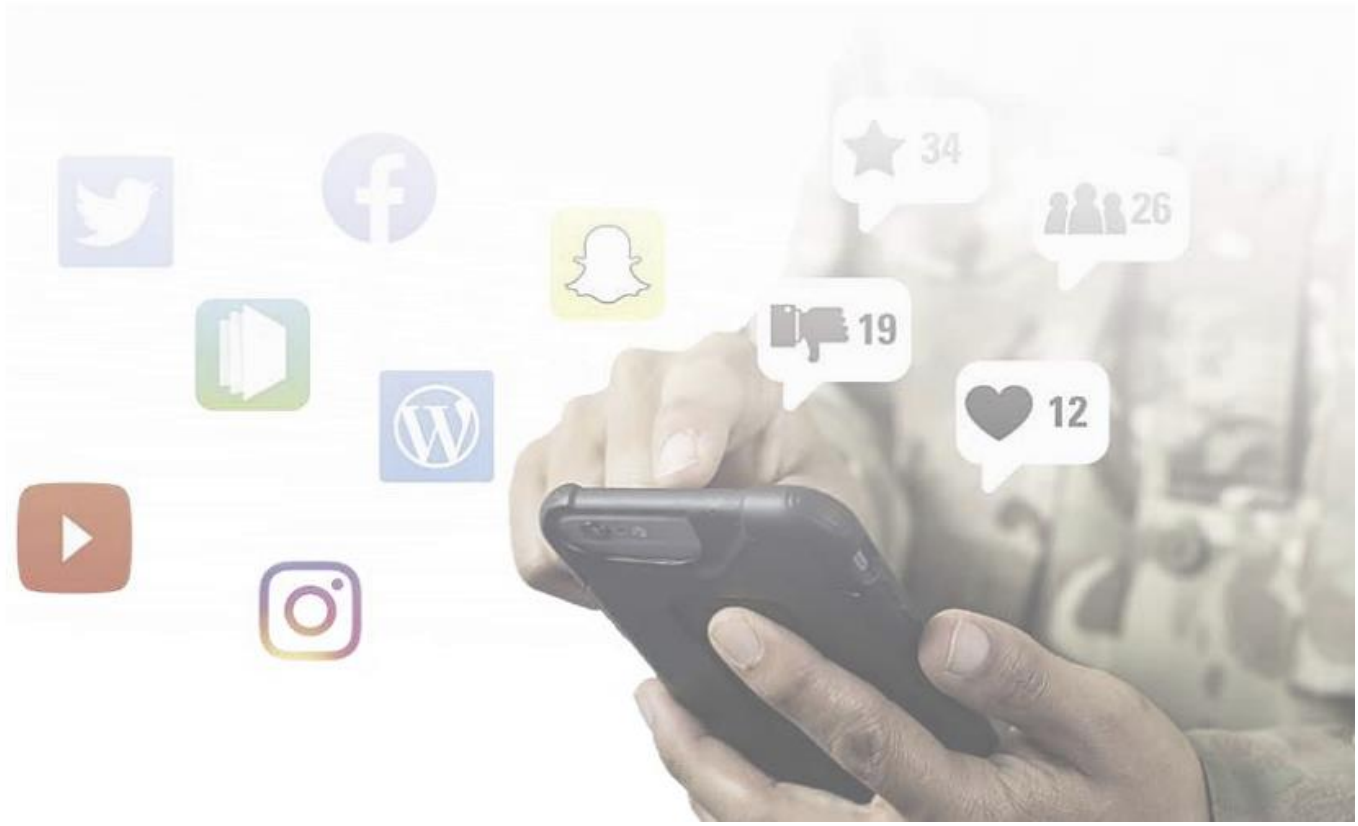
Прямой доступ к базе данных социальных сервисов с необычайной легкостью позволяет российским спецслужбам выявить самый широкий спектр информации, которую обычные граждане и военнослужащие загружают в социальные сети.

Более того, Указом Президента Украины от 14.05.2020 № 184/2020 введено в действие решение СНБО Украины от 14.05.2020 «О применении, отмене и внесении изменений в персональные специальные экономические и другие ограничительные меры (санкции)», которым запрещено интернет-провайдерам предоставлять услуги по доступу пользователям Интернета в ряд российских информационных ресурсов и порталов, в том числе и социальных сетей «ВКонтакте» и «Одноклассники».

Важно уяснить, что страница в любой социальной сети открыта для всех и соответственно требует дополнительной защиты. Не следует создавать дополнительные каналы утечки информации с ограниченным доступом и источники для разведки противника по получению сведений о деятельности Вооруженных Сил Украины. Кроме того, любая информация (фото, видео, другой контент) о Вооруженных силах Украины или связанные с ними сведения, которые размещаются военнослужащими на любом Интернет-ресурсе, рассматриваются как «неофициальные».

Военнослужащие имеют право выражать свои политические и общественные взгляды, давать оценку деятельности любой организации или лицу, но они не должны это делать от имени своего подразделения или Вооруженных сил Украины в целом.

Возможно, соблюдение этих правил иногда создает дискомфорт в общении военнослужащих с родными, друзьями и коллегами, но самое важное, что определенные положения способствуют выполнению боевых (специальных) задач, защите персональных данных и служебной информации.



5. РЕКОМЕНДАЦИИ ПО ЗАЩИТЕ ИНФОРМАЦИИ В СОЦИАЛЬНЫХ СЕТЯХ И МЕССЕНДЖЕРАХ

Ниже приведены основные рекомендации, соблюдение которых минимизирует риски утечки служебной и конфиденциальной информации и, соответственно, последствий, которые она может повлечь за собой.

Выполнять их несложно, но крайне **важно!**

1. Выключите геолокацию или определение местоположения на всех устройствах, которые используете

Желание поделиться своими фотографиями с друзьями может привести к идентификации местоположения с помощью функции геолокации телефона, планшета или компьютера.

Некоторые программы самостоятельно включают геопозиционирование устройства и отправляют эти данные в сеть. Большинство современных телефонов во время съемки фотографий самостоятельно добавляют данные не только о времени, дате снимка, но и о расположении ближайшей базовой станции. Это позволяет узнать, где именно он был сделан.

То, что интересно в гражданской жизни – для военного может быть крайне опасно.

2. Постоянно обновляйте антивирус!

Компьютер, телефон или планшет являются потенциальным источником утечки информации. Современные шпионские программы позволяют не только копировать информацию с устройства и передавать ее для дальнейшего анализа, но и включать камеру, записывать звук или даже скрыто передавать данные о местонахождении.

Одним из инструментов защиты устройств от вредоносных программ является антивирусное обеспечение. Желательно использовать только антивирусы, которые прошли экспертизу соответствующего органа и имеют возможность планового обновления. И ни в коем случае не следует использовать антивирусы российского производства. (Касперский, Dr.Web).

3. Используйте надежные пароли

Вскрытый (сломанный, скомпрометированный) пароль, например, к электронному ящику, дает иностранным разведкам и спецслужбам доступ к профилям в социальных сетях, медиа порталах и возможность выполнять их настройки безопасности (передачу данных, включение геолокации и т.п.).

Чтобы этого не случилось, необходимо использовать надежную защиту паролем, состоящую не менее чем из 10 символов с цифрами, прописными и строчными буквами и не менее одного неалфавитного символа (!, №, %, ?, & и другие).

Не следует использовать личную информацию (даты рождения, девичью фамилию матери и другую информацию, которую можно узнать из открытых источников), названия логинов или один и тот же пароль для нескольких сайтов и устройств.

Это существенно упрощает процесс взлома защиты учетных записей и устройств иностранными спецслужбами. Также не следует делиться ни с кем паролями – доверенный друг сегодня может им не быть в будущем.

4. Не используйте WiFi-роутеры и Интернет-модемы

При выполнении задач или в служебной деятельности самостоятельное использование дополнительного сетевого оборудования (Wi-Fi-роутеров, Интернет-модемов) **строго запрещается** (*за исключением подразделений Сил специальных операций ВС Украины при выполнении специальных задач*).

Прежде всего такие устройства могут быть взломаны иностранными спецслужбами и взяты под их контроль. Поэтому их настройкой должны заниматься квалифицированные специалисты, которые могут установить надежную защиту. В противном случае просмотр информации, которая циркулирует в сети Wi-Fi-роутера или Интернет-модема, станет вопросом времени.

Кроме того, не стоит забывать, что роутеры и модемы по своей сути являются радиоизлучающими средствами, которые противник может запеленговать с точностью до 10-15 метров и соответственно определить место их нахождения или район расположения использующего их подразделения.

5. Не используйте служебные объекты информационной деятельности (компьютеры) для входа в Интернет

Вход в личные (неофициальные) аккаунты социальных сетей со служебного автоматизированного рабочего места **строго запрещен**. Социальная сеть является средой, в которой распространены вредоносные и шпионские программы, которые способны не только заразить объект информационной деятельности или всю корпоративную сеть, но и привести к утечке и потере секретной, служебной или конфиденциальной информации.

6. Не загружайте приложения и программное обеспечение неизвестного происхождения

На сегодняшний день спецслужбы имеют возможность создания (написания) приложений, игр и любого программного обеспечения для осуществления наблюдения за пользователем и сбора необходимой информации о нем. Следует быть внимательным при их установке и тщательно проставлять отметки («галочки»), которые предоставляют разрешения неизвестному программному обеспечению на передачу данных, самостоятельное включение GPS или Wi-Fi.

Важно помнить! Игры, в которых Вы отстреливаете «~~сепаратистов» или уничтожаете Кремль~~, не обязательно написаны патриотами. Как правило, они рассчитаны на свою целевую аудиторию, которая впоследствии становится источником информации.

7. Не переходите по ссылкам на неизвестные сайты и не открывайте сообщения от незнакомых пользователей

Следует соблюдать осторожность при переходе по ссылкам, публикуемым другими пользователями сети или друзьями. Необходимо убедиться, что отправленная ссылка является безопасной и надежной.

При приеме и открытии сообщений, поступивших в сети, желательно убедиться (по телефону или другим способом), что оно было отправлено знакомым. Не следует открывать подозрительные сообщения, их нужно игнорировать или немедленно удалять. Существует много случаев несанкционированной установки на устройствах пользователей деструктивного программного обеспечения и взлома аккаунтов с помощью рассылки сообщений.

Также полезно просматривать список друзей в социальных сетях и в случае обнаружения среди них незнакомых или подозрительных лиц (аккаунтов, ботов) следует немедленно их удалять.

8. Регулярно проверяйте и обновляйте настройки социальных сетей и медиа

При использовании социальных сетей необходимо ограничить доступ к частной информации в настройках конфиденциальности учетной записи (аккаунта). В частности, не указывать геолокацию (место расположения), доступность просмотра для посторонних номера мобильного телефона и адреса почтового ящика, персональных данных пользователя и т.п.

Следует отметить, что в случае автоматического обновления программного обеспечения, его настройки безопасности и конфиденциальности сбрасываются по умолчанию на базовые настройки.

9. Периодически очищайте историю своих сообщений в мессенджерах и требуйте этого от ваших собеседников

6. ЗАКЛЮЧИТЕЛЬНАЯ ЧАСТЬ

Сегодня поразительная популярность социальных медиа и мессенджеров приводит к появлению в открытом доступе огромного количества информации о деятельности военных, что является потенциальным источником получения информации иностранными разведками и спецслужбами противника. Поэтому армии разных стран миру уделяют большое внимание поведению военнослужащих и членов их семей в социальных сетях (медиа) и мессенджерах для создания благоприятных условий выполнения ими задач, а также обеспечения их личной безопасности. Вооруженные Силы Украины также не исключение.

Положения этих Рекомендаций не преследуют цель ограничить свободу общения военнослужащих и работников Вооруженных Сил Украины в социальных сетях, а наоборот направлены на осознание ими необходимости выполнения правил и рекомендаций с целью обеспечения личной безопасности и безопасности членов их семей, соблюдения режима секретности, а также обеспечения выполнение мер безопасности применения войск (сил).

Кроме того, с целью предотвращения утечки информации с ограниченным доступом руководителям (начальникам) органов военного управления, командирам всех уровней целесообразно организовывать постоянный мониторинг официальных страниц своих частей и подразделений на предмет публикации и распространения военнослужащими и членами их семей контента запрещенного содержания, т.е. нарушающего законодательство Украины.

Объясните эти требования коллегам, родным и друзьям!!!

ПОМНИТЕ, БЕЗОПАСНОСТЬ ВОЕННЫХ – ЭТО БЕЗОПАСНОСТЬ ИХ И ВАШИХ СЕМЕЙ!!!