УДК 004 **Информационные технологии**

Глушков Никита Александрович, *студент филиала ВУНЦ ВВС ВВА, г. Челябинск*

Цыганко Александр Валерьевич, *ст. преподаватель филиала ВУНЦ ВВС ВВА, г. Челябинск*

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВООРУЖЕННЫХ СИЛ РОССИЙСКОЙ ФЕДЕРАЦИИ В СОЦИАЛЬНЫХ МЕДИА-РЕСУРСАХ

Аннотация: в данной статье рассматривается проблема информационной безопасности в социальных медиа-ресурсах в Вооружённых Сил Российской Федерации, которая может: повлечь за собой утечку информации; навредить имиджу Вооружённых Сил Российской Федерации.

Ключевые слова: медиа – ресурсы, информационная безопасность, угрозы, защита информации.

Abstract: this article discusses the problem of information security in social media resources in the Armed Forces of the Russian Federation, which can: lead to information leakage; harm the image of the Armed Forces of the Russian Federation.

Keywords: media resources, information security, threats, information protection.

На сегодняшний день контроль над информационной безопасностью Вооружённых сил в сфере медиаресурсов является одним из наиболее актуальных вопросов. Утечка информации через медиаресурсы, составляющих служебную тайну, это подавляющий фактор. И это чаще всего вина человека. Не вычислительная техники или же операционная система, а именно человек несёт главную ответственность за утечку информации через медиа ресурсы.

Распространение иных данных, как правило, влечёт за собой нанесение ущерба государству, как в политическом плане, так и в экономическом, а также наносит ущерб имиджу Вооруженных Сил Российской Федерации.

В связи с фактом того, что происходит утечка данных через социальные медиа-ресурсы, правительством был издан Федеральный закон «О статусе военнослужащих», а именно: Федеральный закон от 06.03.2019 года №19-ФЗ «О внесении изменений в статьи 7 и 28.5 Федерального закона О статусе военнослужащих».

В Федеральном законе говорится о том, что военнослужащим и гражданам, призванным на военные сборы, запрещено в средствах массовой информации либо с использованием социальных медиа-ресурсов распространять или предоставлять информацию:

- позволяющую определить принадлежность или предназначение военнослужащих и граждан, призванных на военные сборы, к Вооруженным Силам РФ, другим войскам, воинским формированиям и органам;

- о других военнослужащих и гражданах, призванных на военные сборы, гражданах, уволенных с военной службы, членах их семей или их родителях, в том числе информацию, позволяющую определить место нахождения указанных лиц в определенный период другим лицам;

- о своей деятельности или деятельности других военнослужащих, граждан, призванных на военные сборы, и граждан, уволенных с военной службы, связанной с исполнением обязанностей военной службы;

- о деятельности органов военного управления или органов управления другими войсками, воинскими формированиями и органами, о деятельности объединений, соединений, воинских частей и иных организаций, входящих в состав Вооруженных Сил РФ или других войск, воинских формирований и органов, о деятельности подразделений указанных органов военного управления или органов управления, воинских частей и организаций, в том числе информацию о дислокации или передислокации органов военного управления или органов управления, объединений, соединений, воинских

частей, организаций и подразделений, не отнесенную к перечню сведений, составляющих государственную тайну.

Нарушение указанных запретов будет расцениваться как грубый дисциплинарный проступок [1].

Таким образом органы государственной власти решили предотвратить опасность, которая может повлечь за собой последствия в сфере защиты служебной тайны и утечку информации через медиа-ресурсы.

Вооруженные Силы Российской Федерации становятся объектом информационных атак со стороны вероятного противника. В этих условиях страна должна обеспечить на высоком уровне информационную безопасность, так как это успешное решение задачи по уменьшению опасностей в настоящее время. Но стоит отметить, что информационная безопасность Вооружённых Сил Российской Федерации в медиа-ресурсах - это личная ответственность каждого военнослужащего и лиц гражданского персонала, каждый пользователь ответственен за то, что он выкладывает в различные соцсети и мессенджеры, а также за то, что военнослужащий может сказать в интервью во время репортажа или во время проведения каких-либо агитационных работ.

Современные способы ведения войны обуславливают важность гарантий информационной безопасности Вооруженных Сил Российской Федерации в медиа-ресурсах. Один из видов современных войн – это гибридная война. Цель гибридной войны - это формирование противоречий между населением страны и создание управляемой неразберихи. Поэтому используются: хакерские атаки на важнейшие системы жизнеобеспечения страны, управление работой СМИ, деградация общества путём навязывания ценностей, мониторинг соцсетей военнослужащих и лиц гражданского персонала, которые работают в Министерстве обороны Российской Федерации. И если говорить о социальных сетях, то пользователи чаще всего сами выкладывают информацию, которая содержит сведения составляющие служебные данные. Это может быть фотография на фоне нового образца вооружения, места постоянной или временной дислокации войск. Но также военнослужащий может подвергнуть

как самого себя, так и своих товарищей опасности при выкладывании информации в медиа-ресурсы, ведь после того как военнослужащий раскроет свою принадлежность к Вооруженным силам, он станет объектом наблюдения со стороны разведки противника, а отталкиваясь от того, что в социальных медиа-ресурсах можно найти ближайших родственников пользователя, то есть возможность использования его в своих целях, под предлогом угрозы родственникам и ближайшего окружения военного.

После того, как интернет вошёл в гражданскую сферу, усилилась опасность применения вероятным противником и мировым терроризмом мер информационного характера. При изучении, мониторинге и выявлении военнослужащих, а также лиц гражданского персонала, работающие в Министерстве Обороны Российской Федерации, в медиа-ресурсах, что позволяет противнику узнать какие-либо сведения составляющих служебную тайну, начиная от места дислокации войск, видов вооружения заканчивая тем, что в руки недоброжелателей попадает информация о численности войск.

С каждым днём ценность данных приобретает всё большую весомость, также повышается и степень её защиты, но и растут способы по получению этих данных. Умение правильно пользоваться медиа-ресурсами, предполагает личную дисциплинированность и ответственность за каждое действие в интернете, что повысит защиту сведений составляющих служебную тайну от утечки. Вероятно, сейчас - это становится важнейшей задачей во внеслужебное время.

Меры по обеспечению защиты информации

Меры, которые могут быть применены в целях защиты данных и гаранта безопасности в социальных медиа-ресурсах, делятся на две группы:

- защита информационных систем от повреждения и информации от утечки и перехвата;

- защита психики личного состава от намеренного информационно-психологического воздействия.

Эти меры должны приниматься вместе, опираясь на все новейшие

разработки в сфере информационной безопасности и программные продукты.

Для реализации комплекса этих мер необходимо создание новых структурных подразделений, которые будут действовать в сфере информационной безопасности [2].

Меры упреждающего воздействия

Учитывая возможные действия противника, которые могут быть использованы, нужно предпринимать какие-либо меры для нападения, чтобы блокировать его возможности. Можно производить такие меры, как:

- намеренное введение противника в заблуждение касательно предполагаемых мер и способов борьбы с угрозами информационной безопасности;

- уничтожение или повреждение средств связи и информационных систем;

- изменение работы информационных систем противника;

- обнаружение и уничтожение возможных пунктов поддержки противника, действующих на территории России;

- добывание и использование конфиденциальной информации о возможных действиях противника по снижению степени безопасности войск и использование этих данных для создания стратегий защиты;

- использование средств морально-психологической атаки информационных войск противника [3].

Также стоит отметить, что гибридная война предполагает под собой и создание информационного оружия. Оно должно не только отражать угрозы, но и упреждать, а также выявлять их. Противник может использовать информационное оружие достаточно эффективно, примером являются страны, охваченные гражданскими войнами. Оружие может применяться как в зонах боевых действий, так и там, где только намечается дестабилизация обстановки. Отечественное оружие должно иметь такой же уровень поражаемого действия, возможно оно будет использовано в обозримом будущем.

Нужно создать такой комплекс мер, при котором будет обуславливаться

гарантированная защита безопасности объектов Вооруженных Сил Российской Федерации в социальных медиа-ресурсах. Иначе это может повлечь за собой необратимые последствия [3].

Следует учесть, что меры по улучшению защищенности данных не всегда и не везде применяются при формировании документации, на базе которой создаются массивы данных военного ведомства. Утери данных могут происходить на уровне военных академий и институтов, транспортных компаний, а также сервисных служб. Нереализация основных принципов контроля или же его отсутсвие над военнослужащими и лицами гражданского персонала, которые допускают удаленный доступ, мониторинг и пользование полученной информации в своих интересах со стороны потенциального противника может привести к плачевным итогам.

Угрозы возникают и при распространении частными лицами случайно полученных ими сведений в социальных сетях. Такие риски блокируются только разъяснительной работой с населением, так как ситуации с возбуждением уголовных дел по статье «Государственная измена» за пост в Сети не являются достойной превентивной мерой. Но угроза исходит и со стороны самих военнослужащих, так как они из-за незнания Федерального Закона допускают утечку информации в социальные медиа-ресурсы.

Комплексный подход к обеспечению информационной безопасности Вооруженных Сил Российской Федерации и личного состава должен обеспечить укрепление обороноспособности. Опираясь на доктрину информационной безопасности, можно разрабатывать новые комплексные способы борьбы с нарастающими угрозами.

Таким образом можно сделать вывод, что информационная безопасность Вооружённых Сил Российской Федерации в социальных медиа - ресурсах сети интернет зависит напрямую от военнослужащих и гражданского персонала, ведь именно отсутствие знаний нормативно-правовой базы и недисциплинированность в сети интернет могут привести к утечке сведений составляющих служебную тайну. Органы государственной власти в свою

очередь борются с нарушителями, которые могут повлечь за собой опасность для служебной тайны и имиджа Вооруженных Сил Российской Федерации.

Библиографический список:

1. Федеральный закон №19-ФЗ.
2. Поздняков А. Информационная безопасность страны и вооруженные силы: сущность, структура, актуальные проблемы обеспечения. Вестник МГУ, серия12- 2004. - №2.
3. Цифровой спецназ Шойгу. Чему противостоят войска информационных операций? Еженедельник «Аргументы и факты» №9 01/03/2017.
4. Федеральный закон «О статусе военнослужащего».