ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРЕДАЧИ ДАННЫХ В СЕТЯХ ВОЕННОГО НАЗНАЧЕНИЯ

Матусевич К.Л.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Сасновский А.А.

Аннотация. Рассмотрены основные принципы защиты данных в сетях, включая аутентификацию, шифрование и контроль доступа. Представлены существующие методы обеспечения безопасности передачи данных в военных сетях, включая системы защиты информации на различных уровнях, средства шифрования, сетевые фильтры и прочие методы.

В настоящее время проблема ведения военных действий в едином информационном пространстве приобретает особую актуальность, поскольку при реализации сетецентрического принципа управления войсками информация играет ключевую роль в обеспечении анализа ситуации в реальном масштабе времени и принятия обоснованного решения. С помощью информационных и телекоммуникационных технологий можно мгновенно собрать, обработать и распространить информацию (или дезинформацию) в любой точке зоны ответственности группировки войск.

Современные сети связи стали неотъемлемой частью военных операций. Военные сети обрабатывают огромные объемы информации, включая секретную, конфиденциальную и критически важную информацию, требующую надежной защиты от несанкционированного доступа, взлома или утечки. Несанкционированный доступ к секретной информации может привести к серьезным последствиям для национальной безопасности, а также может нанести значительный ущерб военным операциям и оперативной работе [1, 2].

По мере возрастания информационно-технологического прогресса возможности группировок войск по ведению военных действий в едином информационном пространстве будут возрастать. Поэтому самыми уязвимыми компонентами инфраструктуры являются телекоммуникационные сети, а обеспечение их информационной безопасности должно стать одним из приоритетных направлений военного строительства и строительства Вооруженных Сил Республики Беларусь [3, 4].

При нарастании военной угрозы и в военное время обеспечение безопасности телекоммуникационной сети для органов государственного и военного управления становится сложной и многогранной проблемой. Это обуславливается бескомпромиссностью информационной войны и антагонизмом преследуемых ею целей, динамичностью информационной среды, широким применением ранее считавшихся запрещенными приемов и методов разрушения информации или ее подмены ложной. Динамичность заключается в том, что требования к безопасности информации, военной связи и разведывательной защищенности телекоммуникационной сети будут меняться вследствие существенного увеличения числа мобильных сетевых узлов, их частого перемещения и повышения удельного веса беспроводных линий связи в их общем количестве. Вследствие резкого увеличения размерности сети и ее реконфигурации за счет добавления к стационарным большого числа подвижных (мобильных) пользователей невозможно установить одинаковые требования к безопасности информации и связи для всех узлов. Следовательно, всякий раз при изменении конфигурации сети нужно устанавливать новые требования к ее разведывательной защищенности, безопасности информации и связи. Практика показывает, что традиционные протоколы этого профиля становятся слишком громоздкими для их практического применения в условиях, когда ресурсы сети недостаточны, а узлы слишком быстро или часто перемещаются [5, 6].

Беспроводные сети не только уязвимы для атак, по и содержат явные и вторичные разведпризнаки пользователей, что позволяет противнику добывать важную информацию о сети, принадлежности пунктов управления и намерениях органов управления. Скрытие такой сети, как и полное исключение ее разведывательной доступности, фактически невозможно. Кроме того, антагонистическая окружающая сетевая среда предполагает новые информационные угрозы, которые ранее не были свойственны телекоммуникационным сетям - например, компрометация узлов связи. Скомпрометированный узел - это свой узел, которым управляет противник. Следовательно, против атак, исходящих изнутри сети, все традиционные решения проблемы ее безопасности неприемлемы. Использование криптографической защиты в этих условиях не имеет смысла, поскольку скомпрометированный узел имеет доступ к ключам и шифрам [7].

Таким образом, телекоммуникационные сети, с одной стороны, позволяют должностным лицам обмениваться информацией независимо от их местоположения, что устраняет факторы места и времени, которые ранее вынуждали вести военные действия на ограниченных пространствах. С другой стороны, если безопасность сети нарушена, противник способен вмешаться в процесс выработки и принятия решения. Информация может быть перехвачена, задержана или изменена, следовательно, нарушается ситуационная осведомленность и адекватное восприятие обстановки. В конечном счете, если информация будет противоречить объективно сложившейся обстановке,

принимаемые в соответствии с ее оценкой решения будут либо неправильными, либо необоснованными, либо отсроченными, что может позволить противнику получить определенные преимущества.

Сети военного назначения подвергаются различным угрозам безопасности, которые могут привести к серьезным последствиям. Некоторые из основных угроз безопасности в сетях военного назначения включают:

1. Кибератаки: Враждебные государства, хакеры или киберпреступники могут осуществлять кибератаки на сети военного назначения с целью перехвата секретной информации, нарушения работы систем или даже нанесения ущерба важным военным объектам.

2. Вредоносное программное обеспечение: Вирусы, черви, троянские программы и другие виды вредоносного ПО могут быть использованы для атак на сети военного назначения с целью украдения информации, блокирования работы систем или проведения шпионских операций.

3. Фишинг: Атаки методом фишинга могут быть направлены на военный персонал с целью получения доступа к защищенным системам или кражи учетных данных.

4. Доступ несанкционированных лиц: Несанкционированные лица могут попытаться получить доступ к секретной информации путем взлома паролей или других методов аутентификации.

5. Социальная инженерия: Атаки с использованием социальной инженерии могут быть направлены на обман военного персонала для получения доступа к защищенным данным или системам.

6. Утечки данных: Непреднамеренные утечки данных или утечки из-за ошибок в настройках могут привести к раскрытию секретной информации.

Для борьбы с угрозами безопасности в сетях военного назначения необходимо применять комплексные меры защиты, включая шифрование данных, аутентификацию пользователей, мониторинг сети, обучение персонала и постоянное обновление систем безопасности.

Для предотвращения угроз безопасности в сетях военного назначения необходимо использовать комплексный подход, который включает в себя использование средств аутентификации, шифрования и контроля доступа, а также обновление систем и программного обеспечения для предотвращения уязвимостей. Также рекомендуется использовать многофакторную аутентификацию и применять меры по защите от вредоносного программного обеспечения, такие как установка антивирусных программ и регулярное обновление программного обеспечения. Кроме того, необходимо обучать пользователей безопасности и проводить регулярные проверки на предмет обнаружения уязвимостей и атак в сети. Использование современных методов шифрования и сетевых фильтров является необходимым условием для защиты конфиденциальной информации в военных сетях. [8].

Безопасность сетей военного назначения играет критически важную роль в защите национальных интересов и безопасности страны. Поэтому необходимо уделять особое внимание разработке и реализации мер по обеспечению безопасности передачи данных в военных сетях. Только комплексный и постоянно совершенствующийся подход к обеспечению безопасности может обеспечить эффективную защиту конфиденциальной информации в сетях военного назначения.

В заключении можно сказать, что обеспечение безопасности передачи данных в сетях военного назначения является критически важным вопросом для национальной безопасности и защиты конфиденциальной информации. Необходимо использовать современные методы шифрования и сетевые фильтры для защиты данных военных сетей, а также постоянно обновлять системы и программное обеспечение, а также проводить регулярные проверки на предмет обнаружения уязвимостей и атак в сети.

Поддержание безопасности сетей военного назначения является сложным и постоянным процессом, который требует комплексного подхода и постоянного совершенствования. Только такой подход может обеспечить эффективную защиту конфиденциальной информации и национальной безопасности.

Список использованных источников:

1. Информационная безопасность вооруженных сил РФ [Электронный ресурс]. – 2020. – Режим доступа https://searchinform.ru/resheniya/otraslevye-resheniya/informatsionnaya-bezopasnost-vooruzhennykh-sil-rf/. – Дата доступа :28.03.2023.

2.Теория управления в системах военного назначения / под ред. И. В. Котенко. М., 2001.3.Косачек И.М., Хижняк А.В. // Вестн. Воен, акад. Респ. Беларусь. 2010. Л° 2 (27).

4.Копытко В.К., Шептура В.Н. // Военная Мысль, 2011. N° 10. С. 16-26.

5.Candolin C. Securing military decision making in a Network-centric environment / Doctoral Dissertation, Helsinki University of Technology Department of Computer Science and Engineering Laboratory for Theoretical Computer Science. 2005.

6.Candolin C. Kari H. A security architecture for wireless ad hoe networks // In Proceedings of TEEE Milcom, Anaheim, California, USA. - 2002. - October 2002.

7.Паршин С.А.. Горбачев О.Е., Кожаное Ю.А. Кибервойны - реальная угроза национальной безопасности? М., 2011.

8. Использование хеш-функции для защиты информации в локальных вычислительных сетях военного назначения [Электронный ресурс]. – 2020. – Режим доступа : https://cyberleninka.ru/article/n/ispolzovanie-hesh-funktsii-dlya-zaschityinformatsii-v-lokalnyh-vychislitelnyh-setyah-voennogo-naznacheniya– Дата доступа :28.