ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРЕДАЧИ ДАННЫХ В СЕТЯХ ВОЕННОГО НАЗНАЧЕНИЯ

Кабаков В.П.

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

Гусаков П.Б.

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 (силами) 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 (сил).

Современные сети связи стали неотъемлемой частью военных операций и обороны. Военные сети обрабатывают огромные объемы информации, включая секретную, конфиденциальную и критически важную информацию, требующую надежной защиты от несанкционированного доступа, взлома или утечки.

Безопасность сети, в свою очередь, имеет несколько аспектов и уровней. Физическая безопасность охватывает защиту линий и узлов сети (например, защиту маршрутизаторов различными средствами управления доступом). В целом же уровень сетевой безопасности решает вопросы защиты связей между двумя узлами. Цель сетевой безопасности в беспроводной сети состоит в том, чтобы обеспечить такую же степень безопасности, как и в проводной сети. Как правило, безопасность сети включает установление подлинности абонента (его идентификацию) и шифрование (кодирование). Кроме того, протоколы безопасности сети должны обеспечить защиту от преднамеренного изменения ее структуры или нарушения управления сетью.

Обеспечение безопасности передачи данных в сетях военного назначения является одним из наиболее актуальных и важных вопросов в области военной техники и обороны. 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].

Данная работа посвящена анализу и разработке эффективных методов обеспечения безопасности передачи данных в сетях военного назначения. В работе рассмотрены основные принципы защиты данных в сетях, включая аутентификацию, шифрование и контроль доступа. Также представлены существующие методы обеспечения безопасности передачи данных в военных сетях, включая системы защиты информации на различных уровнях, средства шифрования, сетевые фильтры и прочие методы.

Кроме того, данная работа содержит анализ современных угроз безопасности в сетях военного назначения и рекомендации по их предотвращению. В целом, цель данной работы - разработать эффективные методы обеспечения безопасности передачи данных в сетях военного назначения для обеспечения защиты национальных интересов и безопасности страны.

Основная часть данной работы посвящена анализу и разработке эффективных методов обеспечения безопасности передачи данных в сетях военного назначения. В этой части рассмотрены основные принципы защиты данных в сетях, включая аутентификацию, шифрование и контроль доступа, а также представлены существующие методы обеспечения безопасности передачи данных в военных сетях, включая системы защиты информации на различных уровнях, средства шифрования, сетевые фильтры и прочие методы. Кроме того, данная работа содержит анализ современных угроз безопасности в сетях военного назначения и рекомендации по их предотвращению.

Принципы защиты данных в сетях военного назначения.

Аутентификация – это процесс проверки подлинности пользователя или устройства, путем проверки учетных данных, таких как имя пользователя и пароль. Аутентификация помогает предотвратить несанкционированный доступ к сети и защитить конфиденциальную информацию.

Шифрование - это процесс преобразования понятной информации в нечитаемую форму, чтобы предотвратить ее прослушивание или вмешательство со стороны злоумышленников. Существует множество алгоритмов шифрования, таких как AES, RSA и другие, которые используются для защиты данных военных сетей.

Контроль доступа – это процесс ограничения доступа к определенным ресурсам или информации только для авторизованных пользователей. Этот процесс включает идентификацию пользователей и устройств, определение прав доступа и мониторинг доступа к ресурсам.

Методы обеспечения безопасности передачи данных в сетях военного назначения.

Системы защиты информации на различных уровнях - это системы, которые обеспечивают защиту информации на различных уровнях сети, включая уровни приложения, сети и транспортного уровня. Каждый уровень имеет свои собственные механизмы защиты, которые помогают защитить информацию от несанкционированного доступа и вмешательства.

Средства шифрования – это программное и аппаратное обеспечение, которое используется для защиты данных военных сетях. Шифрование может происходить на разных уровнях, включая уровень приложения, уровень сети и уровень транспорта. Некоторые из наиболее распространенных алгоритмов шифрования, используемых в военных сетях, включают AES, RSA, Diffie-Hellman и другие.

Сетевые фильтры – это программное обеспечение, которое используется для фильтрации трафика в сети и блокировки нежелательного трафика. Сетевые фильтры могут использоваться для блокировки вредоносного программного обеспечения и других угроз безопасности, а также для предотвращения атак на сеть [2].

Угрозы безопасности в сетях военного назначения.

Существует множество угроз безопасности, которые могут повлиять на военные сети, включая атаки на периметр сети, вредоносное программное обеспечение, атаки на приложения и другие. Атаки на периметр сети могут включать в себя попытки проникновения в сеть через незащищенные узлы, уязвимые точки входа и другие уязвимости в сети. Вредоносное программное обеспечение может использоваться для получения доступа к конфиденциальной информации, блокировки доступа к ресурсам и других угроз.

Рекомендации по предотвращению угроз безопасности в сетях военного назначения.

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 [3].

Таким образом, обеспечение безопасности передачи данных в сетях военного назначения является критически важном вопросе, который требует комплексного подхода и постоянного совершенствования. Использование современных методов шифрования и сетевых фильтров является необходимым условием для защиты конфиденциальной информации в военных сетях. Однако, угрозы безопасности постоянно меняются и развиваются, поэтому необходимо постоянно обновлять системы и программное обеспечение, а также проводить регулярные проверки на предмет обнаружения уязвимостей и атак в сети.

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. Разработка предложений по повышению защищенности информации в локальной вычислительной сети военного назначения от несанкционированного доступа [Электронный ресурс]. – 2020. – Режим доступа : https://knowledge.allbest.ru/programming/3c0b65635a3bd78b5c43a88421306d27_0.html– Дата доступа :28.03.2023.

3. 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-zaschity-informatsii-v-lokalnyh-vychislitelnyh-setyah-voennogo-naznacheniya– Дата доступа :28.03.2023.