СЕТЕВАЯ БЕЗОПАСНОСТЬ И ЕЕ ЗАЩИТА В ВОЕННОЙ СФЕРЕ

Аблакулов Салохиддин Махмуджанович
преподаватель Учебного центра военной подготовки НУУ
Савин Евгений Владимирович
преподаватель Учебного центра военной подготовки НУУ

АННОТАЦИЯ: *с быстрым развитием компьютерных сетевых технологий военная информационная сеть оказала глубокое влияние на стиль современной войны, она стала основной целью нападения на войне и представляет собой проблему, на которой мы должны сосредоточиться в настоящее время. В этой статье в основном представлены основные проблемы и меры противодействия безопасности военной информационной сети.*

КЛЮЧЕВЫЕ СЛОВА: *информация, сетевая безопасность, защита безопасности.*

NETWORK SECURITY AND ITS PROTECTION IN THE MILITARY SPHERE

Ablakulov Salokhiddin Makhmudzhanovich
Lecturer at the NUU Military Training Center
Savin Evgeny Vladimirovich
Lecturer at the NUU Military Training Center

SUMMARY: *With the rapid development of computer networking technology, the military information network has had a profound impact on the style of modern warfare, it has become the main attack target in war, and is a problem that we should focus on at present. This article mainly introduces the main problems and countermeasures of military information network security.*

KEY WORDS: *information, network security, security protection*

Будучи специализированной сетью, объединяющей военный офис, обучение и командование, военная информационная сеть является основой для эффективного военного управления и операций. Принятие практических и эффективных мер защиты для обеспечения безопасности и надежности системы - это проблема, на которую необходимо срочно обратить внимание и решить.

1. Основные проблемы обеспечения безопасности информационных сетей военного назначения.

1.1. Уязвимость к физическому урону.

Большинство используемых в настоящее время военных магистральных сетей строятся и развиваются в соответствии с принципом военно-локальной интеграции и совместного использования войск и вооружения при подготовке к чрезвычайным ситуациям. Магистральные сети в основном распределены по крупным и средним городам. Крупные и средние станции находятся в рабочем состоянии круглый год, большинство из них не защищено электромагнитным экранированием, а характеристики электромагнитного излучения очевидны. Сильный враг в военное время, безусловно, выберет объекты военной информационной сети страны в качестве основной цели жесткого уничтожения, что представляет серьезную угрозу безопасности сети.

1.2. Недостаточное количество независимых программных и аппаратных исследований и технологий разработки.

Информационные технологии появились относительно поздно, а ее научно-исследовательские и производственные возможности в области основного базового оборудования и программного обеспечения относительно слабы. Подавляющее большинство процессоров в военных информационных сетях производятся Intel и AMD, что составляет 90%. Вышеупомянутые операционные системы относятся к серии Windows, и большое количество основного сетевого оборудования (маршрутизирующего и коммутационного оборудования) производится за границей, и существует риск вредоносных бэкдоров, которые будут огромной угрозой безопасности армии в военное время.

1.3. Защитный механизм не идеален и конструкция отстает.

В настоящее время механизм безопасности военной информационной сети несовершенен, метод защиты относительно прост, а способность противостоять атакам могущественных врагов все еще относительно слаба. Построение профессиональной «киберармии» началось с опозданием, а ее построение явно отставало: подразделения на уровне бригад и батальонов не уделяли должного внимания сетевой безопасности, а их сетевые возможности противоборства и реагирования все еще нуждаются в срочном усилении.

2. Эффективные меры по совершенствованию возможностей защиты военной информационной сети.

2.1. Усиление защиты и последовательность жесткого разрушения.

Как нерв боевого управления, военная информационная сеть является первой целью, подлежащей уничтожению противником. Ввиду слабости, легко разрушаемой точными ударами, во-первых, необходимо усилить скрытность и маскировочную защиту ключевых коммуникаций сетевых объектов, чтобы уменьшить вероятность обнаружения противником. Во-вторых, построить транспортные средства полевой связи, которые могут выполнять аварийную мобильную замену в любое время, когда стационарный наземный объект подвергается нападению. В-третьих, усилить исследования, разработки и использование методы беспроводной связи, а также использовать спутники, короткие волны и микроволны в качестве важных резервных методов для оптоволоконных сетей в военное время.

2.2. Внедрение продуктов и технологий собственной разработки.

Использование криптографических технологий в военных информационных сетях, использование самоуправляемых канальных шифровальных машин, машин сетевой безопасности и другого оборудования для шифрования и дешифрования данных во время передачи информации может эффективно изолировать вредоносные бэкдоры и предотвратить незаконные вторжения.

Как основное оборудование сети, маршрутизаторы находятся под угрозой паралича всей сети в любое время после того, как на них нападут злоумышленники. Высокопроизводительный защитный маршрутизатор

использует криптографическую технологию и специальные микросхемы шифрования и дешифрования. Он также может реализовать взаимосвязь, изоляцию и управление потоком внутренней сети и внешней сети каждой воинской части, исследования в области высокопроизводительных маршрутизаторов безопасности с независимыми правами интеллектуальной собственности достигли большого прогресса, и необходимо ускорить развертывание ключевых узлов для замены иностранных продуктов.

3. Использование нескольких средств для создания глубокой системы защиты сетевой безопасности.

Безопасность военной информационной сети — это всесторонняя безопасность. Любое слабое звено в сетевой системе может привести к сетевым атакам. Поэтому необходимо учитывать физическую безопасность, безопасность протоколов, безопасность сетевого уровня, системную безопасность, физическую безопасность и безопасность управления, и комплексное рассмотрение. Можно использовать канальные шифровальные машины для реализации зашифрованной передачи информации для обеспечения безопасности передачи; реализации защиты границ сети с помощью брандмауэров и устройств предотвращения вторжений; обнаружения и устранения угроз безопасности системы в режиме реального времени с помощью систем обнаружения уязвимостей.

Безопасность военной информационной сети связана с передачей в режиме реального времени приказов военной разведки и высокой эффективностью боеспособности военных, что ограничивает стабильное и быстрое развитие военной информатизации. Необходимо усилить рациональное распределение людей, денег и материалов, в частности, в полной мере использовать субъективную и активную роль профессиональных сил безопасности, мыслить позитивно и действовать на опережение, создать безопасную и эффективную военную информационную сеть, чтобы гарантировать, что армия останется непобедимой в информационной войне.

ЗАКЛЮЧЕНИЕ: Военные берут на себя важную задачу по защите страны, а защита безопасности военных информационных сетей требует очень строгого отношения и не допускает ошибок. В последние годы поэтапное и комплексное построение военной информационной сети сыграло очень важную роль в военном боевом управлении и военных учениях. В настоящее время сетевая безопасность по-прежнему является главным приоритетом работы военной информационной безопасности. Необходимо признать ситуацию в процессе развития и активно принимать эффективные меры для укрепления построения безопасности военной информационной сети.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ:

1. Ван Майвэй. Исследование построения системы защиты сетевой безопасности. Безопасность киберпространства, 2017г.
2. Ли Чжиюань. Защита и управление сетевой безопасностью в армейских коммуникациях. Современные информационные технологии, 2019г.
3. Ли Тао, Введение в сетевую безопасность. Пекин: Electronics Industry Press, 2004г.
4. Ван Лэй, Ли Фэнцзюй. Защита сетевой безопасности в армейской коммуникационной работе. Информационная связь, 2015г.
5. https://cyberleninka.ru
6. https://mitc.uz/ru/pages/info_security.