ПРИМЕНЕНИЕ ETHERNET ТЕХНОЛОГИИ В СИСТЕМЕ ВОЕННОЙ СВЯЗИ. НИЗКАЯ ЗАЩИЩЕННОСТЬ IP СЕТЕЙ

Дашко Н.Ю.

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

Федоренко В.А.

Аннотация. Актуальные вопросы применения сетевых технологий в Вооруженных Силах Республики Беларусь. Проблема нехватки специалистов и наработанных материалов по применению основополагающих мер безопасности при эксплуатации сетевого оборудования военного назначения. Контроль наличия устройств в сети, фильтрация трафика с помощью сетевых экранов. Изучение мирового опыта атак на информационные сети с целью оптимизации защищенности IP сетей военного назначения.

Технология Ethernet семейство выделяемая по пакетному типу передачи информации между устройствами сети. Стандарты интернет определяют на физическом уровне модели проводные соединения и электрические сигналы, на канальном уровне формат кадров и протоколы управления доступом к среде.

Применяемые в войсках системы связи активно оснащаются интерфейсами Ethernet, которые позволяют организовывать IP-сети передачи данных, которые обеспечивают обмен всеми видами информации, построение различных сетевых конфигураций и централизованное управление системой связи на основе данной технологии. За всеми преимуществами скрываются высокие требование к безопасности такой системы. Мировой опыт показал не только эффективность технологии, но и наглядно – ее недостатки – уязвимости, которые позволяют проводить различного рода манипуляции используя несовершенство стека протоколов TCP/IP на основе которого строится все сетевое оборудование, включая АРМ операторов любых станций.

Основной проблемой является недостаточное внимание к назревающей проблеме нехватки специалистов способных анализировать ситуацию применения сетей в вооруженных силах и комплексного применения методов защиты сетей передачи данных. Реализация сети основанной на технологии Ethernet не обеспечена достаточным уровнем защиты. Опыт применения этих сетей показывает острую необходимость в полноценной, комплексной защите. Высококачественному обучению специалистов и проработки вопросов обеспечения целостности, конфиденциальности и отказоустойчивости системы.

Исходя из мировых тенденций ведения войны, применение диверсионно-разведывательных групп и информационных спецопераций современная военная система связи обязана быть готова к применению различных инструментов для незаконного, несанкционированного получения информации, реконфигурирования. В настоящий момент в Вооруженных Силах Республики Беларусь не в полной мере реализуется комплекс современных, эффективных мер защиты. Более того, не учтен факт необходимости контроля адресного пространства, нет единой системы выдачи сетевых адресов, что может привести к конфликту оборудования и упрощает возможность доступа к передаваемой информации и структуре сети, а также использование уязвимостей злоумышленнику.

В результате проработки вопроса сетевой безопасности, настройки оборудования, комплексного применения средств фильтрации трафика, изолирующих сеть специального назначения мы получаем повышенную устойчивость и безопасность системы связи. Но в данный момент системы связи ВС РБ не в полной мере способны противостоять возможному воздействию противника и, соответственно не совершенна

Таким образом система связи обязана соответствовать современным вызовам. Вовремя замеченная попытка подключения неопознанного сетевого устройства или выявление нехарактерных для данного сегмента сети пакетов позволяет предупредить и отработать попытку несанкционированного доступа, выведения из строя узлов сети, а также вскрытия все топологии сети данных.

Список использованных источников:

1. Блинов А.М. Информационная безопасность – М.: Учебное пособие. Часть 1. – СПб.: Изд-во СПбГУЭФ, 2010. – С. 96.

2. Герасименко В. А. Основы защиты информации / В. А. Герасименко, А. А. Малюк – М.: Минобразования России, 1997. – С. 438.

3. Зегжда Д. П. Основы безопасности информационных систем / Д. П. Зегжда; А. М. Ивашко – М.: Горячая линия-Телеком, 2000. – С. 577.

4. Почепцов Г. Г. Информационные войны / Г. Г. Почепцов – М.: Реф-бук, Ваклер, 2000. – С. 390

5. Молдовян А.А., Молдовян Н.А., Советов Б.Я. Криптография. – СПб.: Издательство "Лань", 2001. –С. 224.

6. Козлов С.Н. Защита информации, устройства несанкционированного съёма информации и борьба с ними. – Академический проект, 2019. – 286с.

7. Таненбаум Э. Компьютерные сети. Пятое издание / Уэзеролл Д. – М.: Издание на русском языке, оформление ООО Издательство «Питер», 2012. – С. 384 – 526, 807 – 927.