КИБЕРБЕЗОПАСНОСТЬ В ВОЙСКАХ СВЯЗИ ВООРУЖЕННЫХ СИЛ РЕСПУБЛИКИ БЕЛАРУСЬ

Остапчук Ю.М.

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

Масейчик Е.А.

Аннотация. В докладе рассмотрены перспективы и преимущества использования мобильных технологий в военных операциях, а также выделены основные проблемы и уязвимости, связанные с их использованием.

Современные войска связи Республики Беларусь используют компьютерные сети и Интернет для передачи и обработки информации. Это делает их уязвимыми для кибератак и других угроз. Поэтому необходимо создание мощной системы кибербезопасности, которая будет обеспечивать защиту от взлома и хакерских атак [1].

Для обеспечения кибербезопасности в Вооруженных Силах Республики Беларусь необходима система, которая будет включать в себя несколько ключевых элементов. Например, для обеспечения конфиденциальности передаваемых сообщений и данных необходимо использовать криптографические методы и технологии.

Криптография - это наука о методах защиты информации от несанкционированного доступа, использования и изменения. Системы шифрования данных и коммуникаций должны быть построены на основе новейших алгоритмов и стандартов, обеспечивающих надежность и безопасность передачи информации [2].

Для защиты от взлома и хакерских атак необходимо использовать средства защиты информации, такие как брандмауэры, антивирусы, антишпионы и другие.

Брандмауэры используются для блокирования несанкционированных соединений и передачи информации, антивирусы обнаруживают и блокируют вирусы, антишпионы - для защиты от шпионского ПО.

Еще один элемент системы кибербезопасности - это контроль и управление доступом к информации. Для этого необходимо использовать системы аутентификации и авторизации, позволяющие определить, кто имеет доступ к каким данным и какие действия могут выполнять.

Одним из самых важных элементов системы кибербезопасности является обучение и подготовка персонала, который будет работать с системами связи и защиты информации. Специалисты должны иметь не только технические знания и навыки, но и понимание основных принципов кибербезопасности.

Для эффективной работы системы кибербезопасности Вооруженных Сил Республики Беларусь, необходимо также учитывать множество факторов, таких как персональные данные, защита облачных систем хранения данных, а также обеспечение безопасности мобильных устройств и приложений [2].

При работе с облачными системами хранения данных, необходимо использовать меры защиты, такие как многофакторная аутентификация, шифрование данных и аудит действий. Также необходимо строго контролировать доступ к информации в облачных системах, предоставляя его только необходимому количеству пользователей с минимальными правами доступа.

При использовании мобильных устройств, таких как смартфоны и планшеты, необходимо использовать средства защиты информации, такие как антивирусы, антишпионы, брандмауэры и VPN-сервисы. Также необходимо обеспечивать регулярное обновление операционной системы и установленных приложений для минимизации рисков уязвимостей и уязвимых мест [2].

Для обучения и повышения квалификации специалистов в области кибербезопасности, Вооруженные Силы Республики Беларусь могут использовать различные методы, такие как обучение в учебных центрах, симуляторах и компьютерных тренажерах. Также возможно привлечение экспертов в области кибербезопасности для проведения тренингов и мастер-классов.

В целом, система кибербезопасности Вооруженных Сил Республики Беларусь должна обеспечивать надежную защиту от кибератак и других угроз, которые могут возникнуть при использовании информационно-коммуникационных систем и услуг.

Важно понимать, что создание и поддержание такой системы требует постоянного мониторинга и обновления технологий и методов защиты, а также обучения и подготовки специалистов в области кибербезопасности.

Список использованных источников:

1. *Электронный ресурс министерства обороны РБ.*
2. *Электронный ресурс министерства связи и информатизации Республики Беларусь*