УДК 355.23:004.056.5:004.382:378

Д.М. Ермоленко, преп. кафедры связи
(БГУИР, г. Минск)

ИНТЕГРАЦИЯ ТЕХНОЛОГИЙ КВАНТОВОЙ И ПОСТКВАНТОВОЙ КРИПТОГРАФИИ В СИСТЕМУ ПОДГОТОВКИ СПЕЦИАЛИСТОВ СВЯЗИ

Современный этап развития вооруженных сил характеризуется стремительным ростом роли информационных технологий в управлении войсками и оружием. В условиях гибридных конфликтов и сетецентрических войн защита каналов связи становится не просто обеспечивающей функцией, а критически важным элементом боевой устойчивости. Для Республики Беларусь, развивающей собственную систему военной безопасности, подготовка офицерских кадров, способных эксплуатировать перспективные средства защиты информации, является приоритетной задачей. В рамках данной работы рассматривается необходимость актуализации образовательных программ подготовки специалистов связи с учетом внедрения технологий квантовой и постквантовой криптографии.

Актуальность темы обусловлена глобальным технологическим переходом. Традиционные методы шифрования, используемые в том числе в военных системах связи (основанные на сложности факторизации больших чисел и дискретного логарифмирования), стоят на пороге уязвимости. Развитие квантовых вычислений создает угрозу так называемого «квантового прорыва», когда алгоритм Шора позволит дешифровать перехваченный трафик за приемлемое время. Это ставит под угрозу конфиденциальность стратегической информации, срок актуальности которой исчисляется десятилетиями. Следовательно, система военного образования должна работать на упреждение, готовя специалистов для эксплуатации техники нового поколения уже сегодня.

В настоящее время в Республике Беларусь действуют национальные стандарты в области криптографической защиты информации, такие как СТБ 34.101.31 (алгоритмы электронной цифровой подписи и транспорта ключа) и СТБ 34.101.45 (алгоритмы шифрования и контроля целостности). Данные стандарты обладают высокой стойкостью к атакам с использованием классических вычислительных мощностей. Однако учебные программы профильных дисциплин зачастую ограничиваются изучением принципов работы симметричных блочных шифров и классической асимметричной криптографии. Курсанты и студенты получают навыки настройки аппаратуры, работающей на

текущих принципах, но недостаточно осведомлены о физических и математических основах перспективных средств защиты.

Для устранения разрыва между текущим состоянием технологий и будущими угрозами необходимо обращать повышенное внимание в учебном процессе двум ключевым направлениям: квантовому распределению ключей (QKD) и постквантовой криптографии (PQC).

Первое направление – квантовое распределение ключей – представляет собой аппаратный метод защиты, основанный на законах квантовой физики. Внедрение этой темы в образовательный процесс требует междисциплинарного подхода. Будущий офицер связи должен понимать не только протоколы передачи данных, но и физические ограничения квантового канала (дальность передачи, влияние атмосферных помех для спутниковых каналов, необходимость доверенных узлов). Предлагается включить в курс «Специальные системы связи» лабораторные работы по моделированию квантового канала связи и изучению принципов работы детекторов одиночных фотонов. Это сформирует у обучающихся понимание того, как обеспечивается абсолютная теоретическая секретность ключа шифрования.

Второе направление – постквантовая криптография – подразумевает переход на новые математические алгоритмы (например, на основе решеток или кодов, исправляющих ошибки), устойчивые к атакам квантового компьютера. В отличие от QKD, это программное решение, которое может быть внедрено на существующей элементной базе, включая программируемые радиостанции (SDR) и тактические терминалы.

Особое внимание в образовательном процессе следует уделить специфике применения данных технологий в различных звеньях управления. Если на стратегическом уровне (стационарные узлы связи) возможно применение громоздкого оборудования квантового распределения ключей по оптоволоконным линиям, то в тактическом звене (полевые условия) основным средством защиты останется математическая криптография. Следовательно, методика подготовки курсантов и студентов должна дифференцироваться.

При подготовке специалистов для тактического звена управления необходимо делать упор на изучение ресурсоемкости постквантовых алгоритмов. Новые методы шифрования требуют значительно больше вычислительной мощности и памяти, чем традиционные, что критично для носимых радиостанций и терминалов с батарейным режимом питания. Будущий инженер войск связи должен уметь оценивать баланс между стойкостью шифра и производительностью канала

связи, чтобы применение усиленной защиты не приводило к неприемлемым задержкам в передаче команд в системе боевого управления.

Важным методическим аспектом является внедрение в учебный процесс понятия «криптоагильность» (криптографическая гибкость). В условиях быстро меняющихся угроз офицер войск связи должен быть готов к оперативной смене криптографических примитивов без полной замены аппаратной части. Обучение должно включать практические занятия по удаленному обновлению микропрограммного обеспечения средств криптографической защиты информации (СКЗИ) в условиях радиоэлектронного подавления противника. Это требует от обучающихся глубокого понимания архитектуры современных программируемых логических интегральных схем (ПЛИС), используемых в белорусских военных средствах связи.

Для реализации этих задач предлагается использование виртуальных киберполигонов. Поскольку реальное оборудование квантовой криптографии является дорогостоящим и уникальным, первичные навыки целесообразно отрабатывать в средах имитационного моделирования. Разработка и внедрение на кафедре связи специализированного программного обеспечения, эмулирующего работу гибридных сетей (где часть каналов защищена квантовыми ключами, а часть – постквантовыми алгоритмами), позволит проводить тактико-специальные учения в виртуальной среде. Курсанты и студенты смогут наглядно увидеть последствия компрометации классических ключей и эффективность применения новых методов защиты.

Особое внимание следует уделить изучению отечественных разработок. Научные организации Республики Беларусь ведут активные исследования в области фотоники и защиты информации. Включение в учебный процесс ознакомления с опытными образцами белорусской шифровальной техники нового поколения позволит сократить время адаптации выпускников-связистов в войсках. Также важно рассматривать вопросы стандартизации. Специалист должен уметь не просто нажать кнопку «Загрузить ключ», но и понимать, соответствует ли выбранный режим работы требованиям руководящих документов по защите госсекретов в условиях наличия у противника вычислительных мощностей следующего поколения.

Педагогическая модель внедрения данных технологий должна строиться по принципу «от теории к эксплуатации». На первом этапе (базовая подготовка) курсантам и студентам необходимо давать обзор уязвимостей классических систем перед квантовыми вычислениями. На втором этапе (специальная подготовка) – изучать схемотехнику квантовых генераторов случайных чисел и программную реализацию

постквантовых алгоритмов. На третьем этапе (военно-профессиональная подготовка) – отрабатывать тактику применения гибридных систем связи, где для наиболее важных каналов управления используются квантово-защищенные линии.

Реализация предложенных изменений в учебных планах позволит сформировать у выпускников-связистов компетенции, необходимые для обеспечения информационной безопасности государства в долгосрочной перспективе. Это полностью соответствует требованиям Военной доктрины Республики Беларусь, которая относит информационное противоборство к одной из основных черт современных военных конфликтов. Переход к изучению перспективных технологий шифрования – это инвестиция в интеллектуальный потенциал офицерского корпуса, способного противостоять высокотехнологичному противнику.

Таким образом, развитие системы военного образования в части специальной подготовки связистов должно носить опережающий характер. Интеграция курсов по квантовой коммуникации и постквантовым алгоритмам в учебные программы кафедры связи является необходимым шагом для поддержания высокого уровня боеготовности подразделений связи и защиты национальных интересов Республики Беларусь.

ЛИТЕРАТУРА

1. Концепция национальной безопасности Республики Беларусь : утв. Указом Президента Респ. Беларусь, 9 нояб. 2010 г., № 575 (в ред. Указа Президента Респ. Беларусь от 24.01.2014 г. № 49) // Нац. реестр правовых актов Респ. Беларусь. – 2014. – № 1/14788.

2. Информационные технологии и защита информации. Криптографические алгоритмы шифрования и контроля целостности : СТБ 34.101.45-2013. – Введ. 01.07.2014. – Минск : Госстандарт, 2014. – 42 с.

3. Липницкий, В. А. Современная прикладная криптография : пособие / В. А. Липницкий, Д. В. Конопелько. – Минск : БГУИР, 2020. – 98 с.

4. Иванов, А. В. Перспективы развития систем военной связи в условиях современных угроз / А. В. Иванов // Вестник Военной академии Республики Беларусь. – 2024. – № 2. – С. 45–51.