РЕЦЕНЗИЯ

на выпускную квалификационную работу

Обучающегося Владимира Владимировича Митращука
(фамилия, имя и отчество обучающегося полностью)

группы МКБ16-01

направления(специальности) 10.04.01 (код) Информационная безопасность (наименование)

направленности(профиля, специализации, магистерской программы) Управление (наименование)

информационной безопасностью автоматизированных систем (наименование)

выполнивший ВКР в виде магистерская диссертация
(бакалаврская работа/дипломная работа/дипломный проект/магистерская диссертация)

на тему Протокол передачи информации, реализация и тестирование шифратора с (наименование)

переменной фрагментацией блока и генератора ключей для него (наименование)

Актуальность темы, выбранной для диссертационного исследования магистрантом Митращуком В.В. не вызывает сомнений, поскольку в условиях постоянно развивающихся вычислительных мощностей информационных систем растет потребность в повышении стойкости и производительности шифрования информации.

В выпускной квалификационной работе Владимира Владимировича, четко сформулирована цель, поставлены задачи, определены требования к разрабатываемому протоколу и раскрыты выводы полученные в результате проведения диссертационных исследований. Постановке задачи магистрант уделил особое внимание и посвятил главу работы, что позволило наиболее глубоко раскрыть замысел проводимых исследований. Работа состоит из введения, 3-х глав, заключения и библиографического списка. Тема исследования автором раскрыта полностью, в работе содержится достаточное количество таблиц и рисунков, что способствует улучшению восприятия полученных результатов.

Во второй главе Владимир Владимирович, проводит анализ существующих протоколов и алгоритмов шифрования и сравнивает их параметры, имеющие наибольшее значение для решения задач потребителя. По результатам данного обзора становятся очевидны недостатки существующих протоколов и алгоритмов шифрования, которые делают их применение для передачи телеметрии неэффективным или вовсе невозможным. Для удовлетворения потребностей в обеспечении конфиденциальности, целостности и доступности передаваемой информации с допустимой при этом скоростью передачи данных автор предлагает разработку собственного протокола на базе использования существующего шифратора «Шифратор 125». Также для повышения стойкости шифрования автор предлагает использовать не стандартный алгоритм шифрования, а его модифицированную версию.

К достоинствам рассматриваемой выпускной квалифицированной работы можно отнести:

– системность подхода автора к процессу изучения и решения выбранной проблемы;

– высокий уровень знаний автора в рассматриваемой предметной области, что позволило провести полноценный анализ существующих протоколов и алгоритмов шифрования;

– наличие результатов тестирования разработанного протокола на программно-аппаратной платформе в реальных условиях.

Однако, есть в работе ряд недостатков. В частности, выбор в пользу разработки нового протокола передачи данных вместо доработки существующего OpenVPN недостаточно обоснован. Также, считаю, что сравнение в таблице 2.1. еще не разработанного протокола «Протокол 125» с реальными существующими протоколами некорректно.

Не смотря на указанные замечания, считаю, что работа выполнена на высоком уровне. В целом работа соответствует требованиям, предъявляемым к магистерским диссертациям, и заслуживает оценки отлично.

Рецензент _____ подпись

Мушовец К.В.
к.т.н., ведущий администратор по информационной безопасности группы безопасности Филиала «ЦентрСибаэронавигация» ФГУП «Госкорпорация по ОрВД»

Фамилия Имя Отчество
ученая степень, ученое звание, должность,
место работы

«_____»_____20_____г.

С рецензией ознакомлен
обучающийся _____ подпись _____ инициалы, фамилия

«_____»_____20_____г