ВКР.22.КТсо5-5.100503.07

МИНОБРНАУКИ РОССИИ
Федеральное государственное автономное образовательное
учреждение высшего образования
«ЮЖНЫЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Институт компьютерных технологий и информационной безопасности
Кафедра безопасности информационных технологий

Выпускная квалификационная работа

Анализ безопасности протоколов управления БПЛА

Руководитель: к.т.н., доц., доцент каф. БИТ Басан Елена Сергеевна

Исполнитель: студент группы КТсо5-5 Ованесян Даниил Арменович

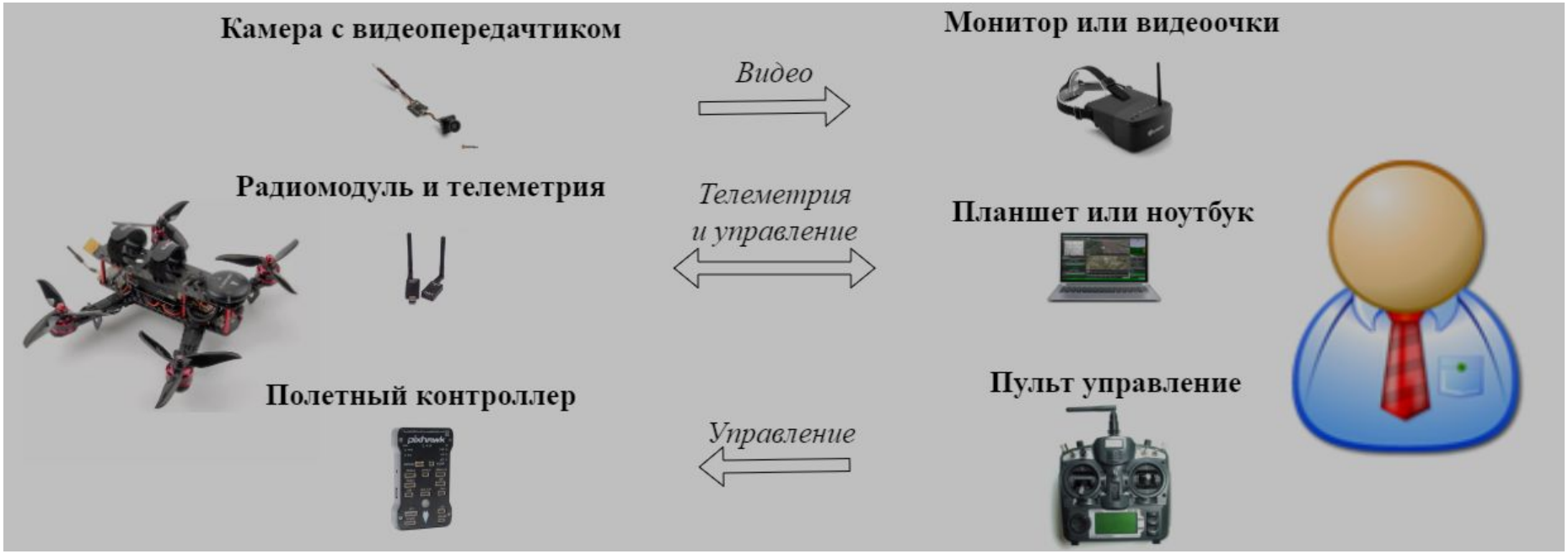
Перечень решаемых задач

Цель работы: проанализировать протоколы управления БПЛА и разработать методики атак

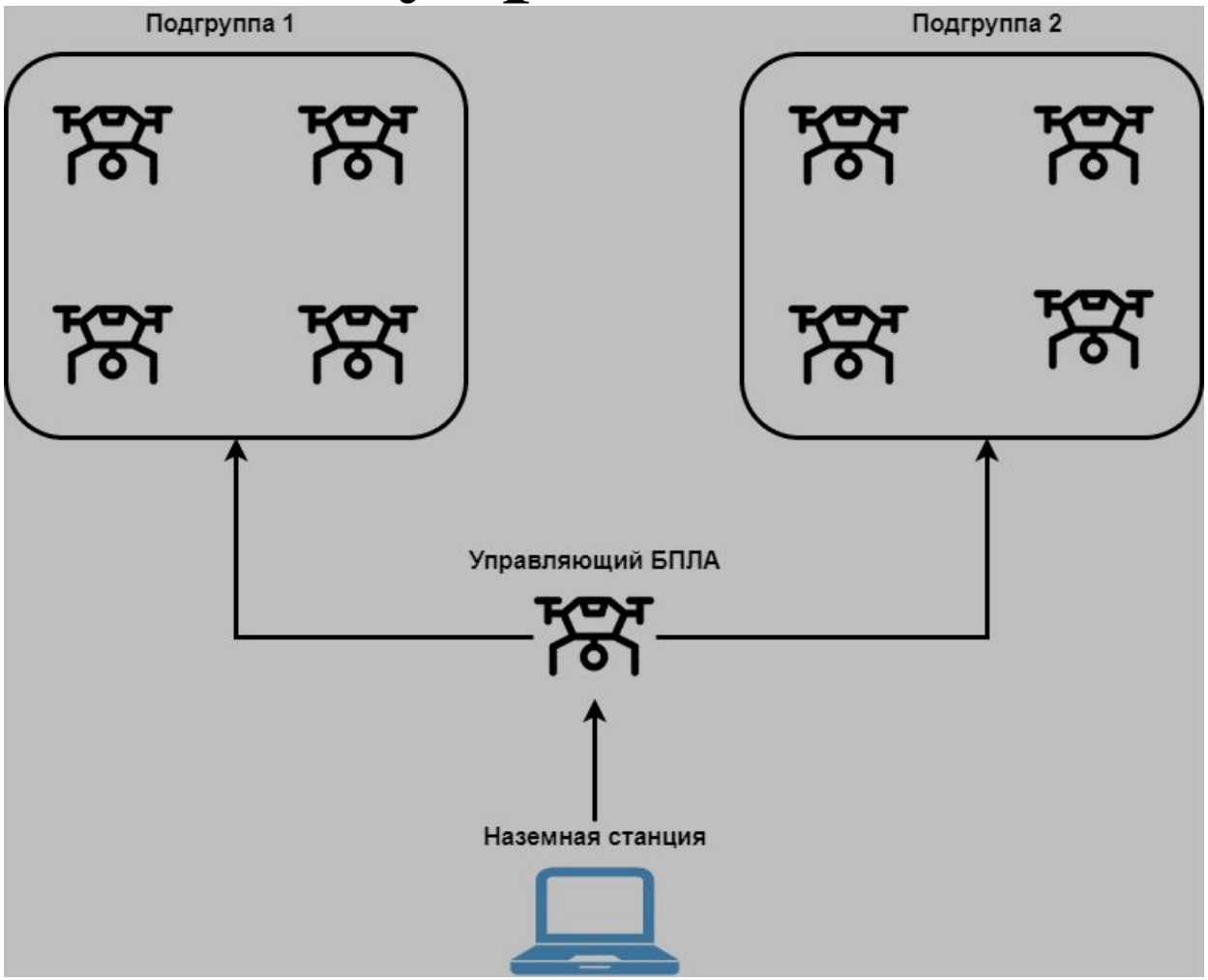
Задачи:

1. Теоретический анализ безопасности протоколов управления БПЛА.
2. Исследование угроз и уязвимостей протоколов управления БПЛА.
3. Разработка методики атак типа «отказ в обслуживании».
4. Разработка методики атак типа «человек посередине».
5. Разработка методики атак типа «подслушивание».
6. Рассмотрение вопросов безопасности человеко-машинного взаимодействия при ее эксплуатации.
7. Рассмотрение вопросов технико-экономического обоснования.

Способы управления БПЛА



Способы управления БПЛА



Методы атак на БПЛА

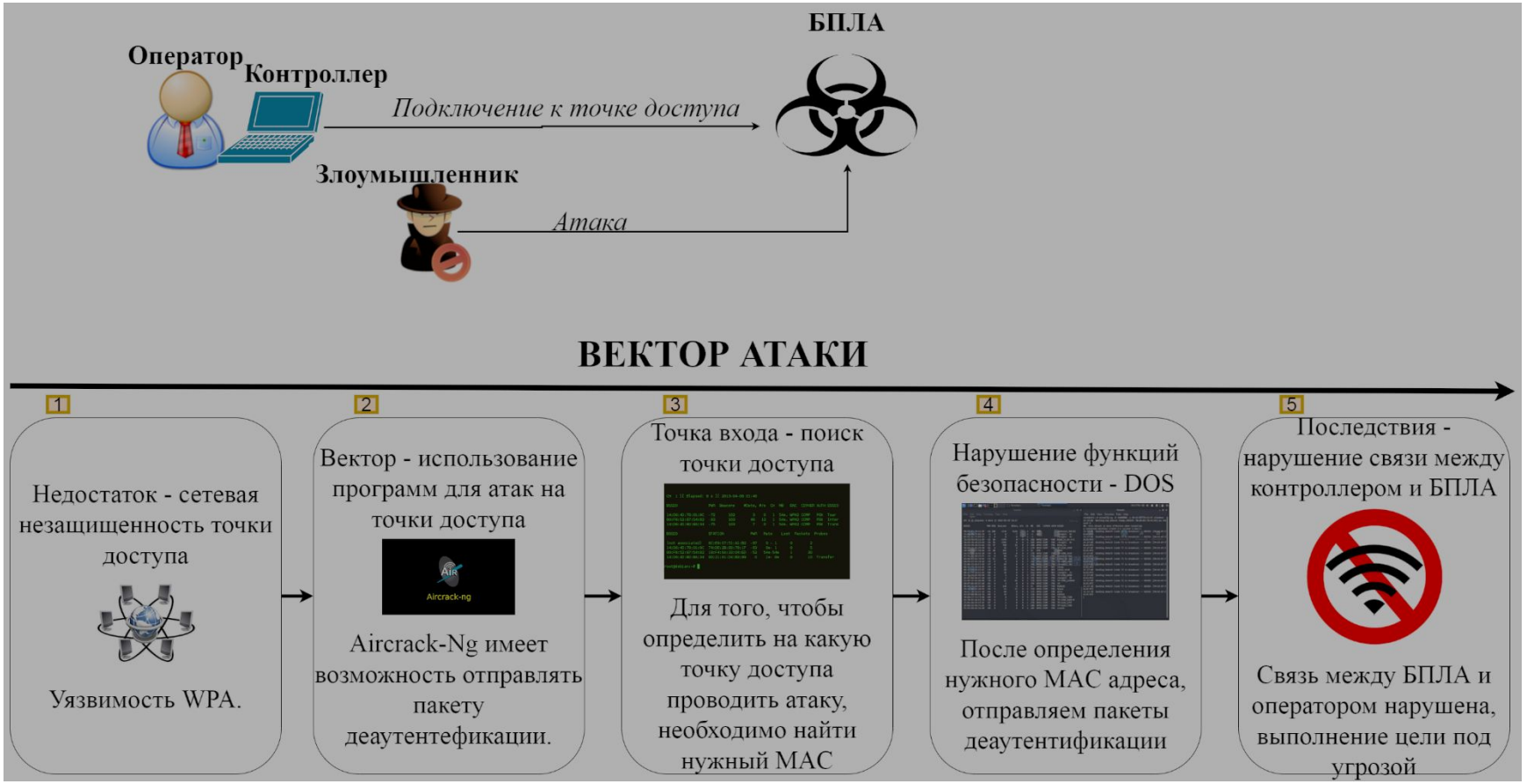
Цель	Метод атаки
Конфиденциальность	Подслушивание
	Hijacking(угон)
	Man-In-The-Middle
Целостность	Внедрение пакетов
	Replay атака
	Man-In-The-Middle
	Удаление сообщений
Доступность	DOS
	Fuzzing
	Глушение
	Флуд
	DOS

Разработанные сценарии атак

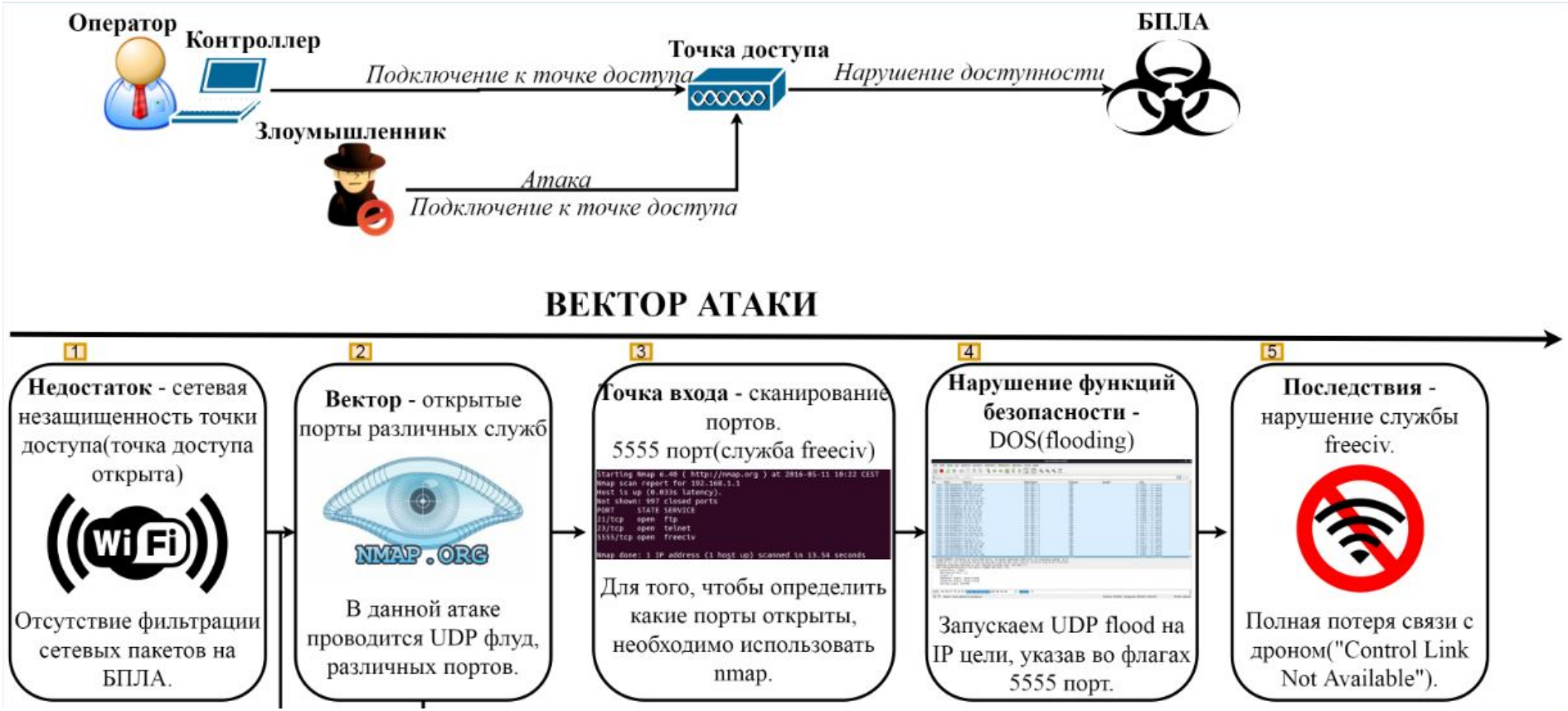
В данной работе были реализованы следующие сценарии атак:

- Отказ в обслуживании – DOS
- Подмена пакетов
- Человек посередине – поддельная точка доступа
- Подмена GPS
- Угон – hijack

Атака деаутентификации

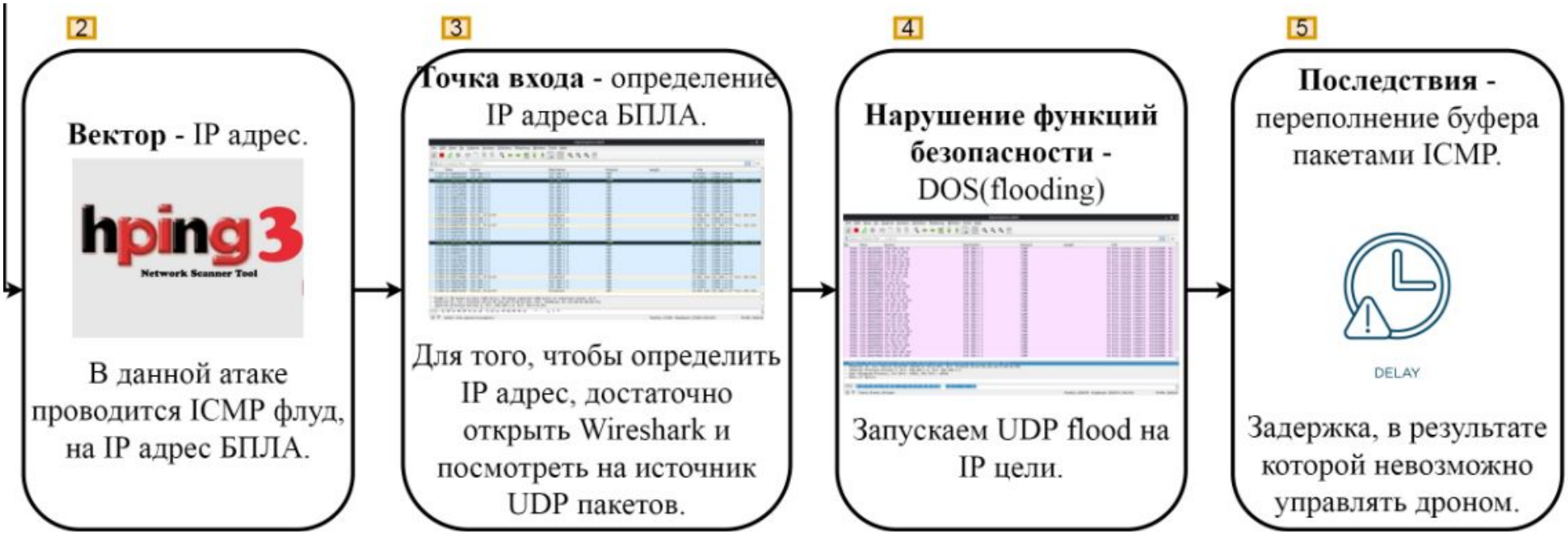


UDP flood


Оператор
Контроллер
Точка доступа
БПЛА
Подключение к точке доступа
Нарушение доступности
Злоумышленник
Атака
Подключение к точке доступа
ВЕКТОР АТАКИ
1
Недостаток - сетевая незащищенность точки доступа(точка доступа открыта)
Wi Fi
Отсутствие фильтрации сетевых пакетов на БПЛА.
2
Вектор - открытые порты различных служб
NMAP .ORG
В данной атаке проводится UDP флуд, различных портов.
3
Точка входа - сканирование портов.
5555 порт(служба freeciv)
Для того, чтобы определить какие порты открыты, необходимо использовать nmap.
4
Нарушение функций безопасности - DOS(flooding)
Запускаем UDP flood на IP цели, указав во флагах 5555 порт.
5
Последствия - нарушение службы freeciv.
Полная потеря связи с дроном("Control Link Not Available").

ICMP flood

Недостаток данной методики наследуется из диаграммы, где рассмотрен UDP flood.

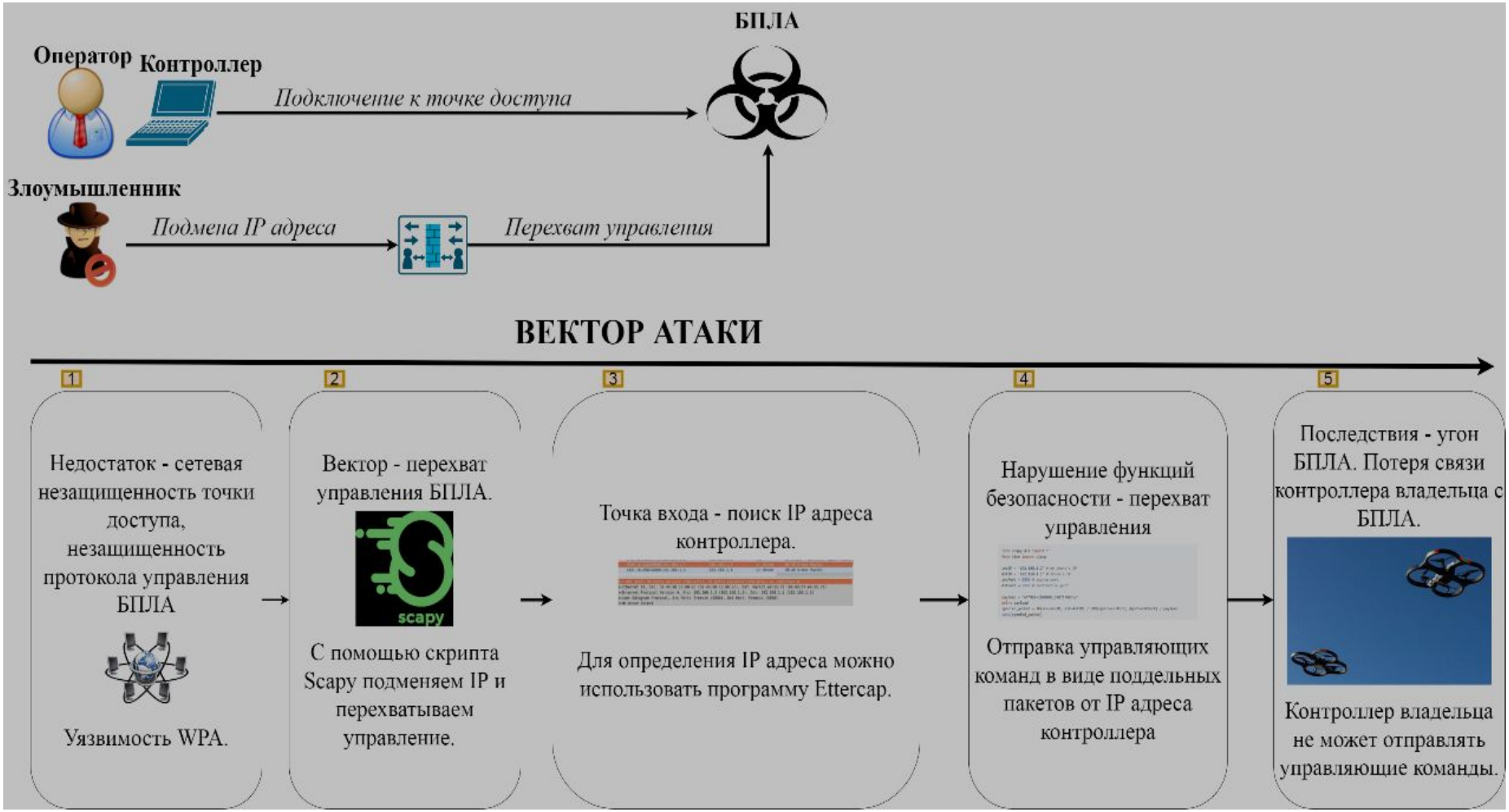


Экспериментальное исследование

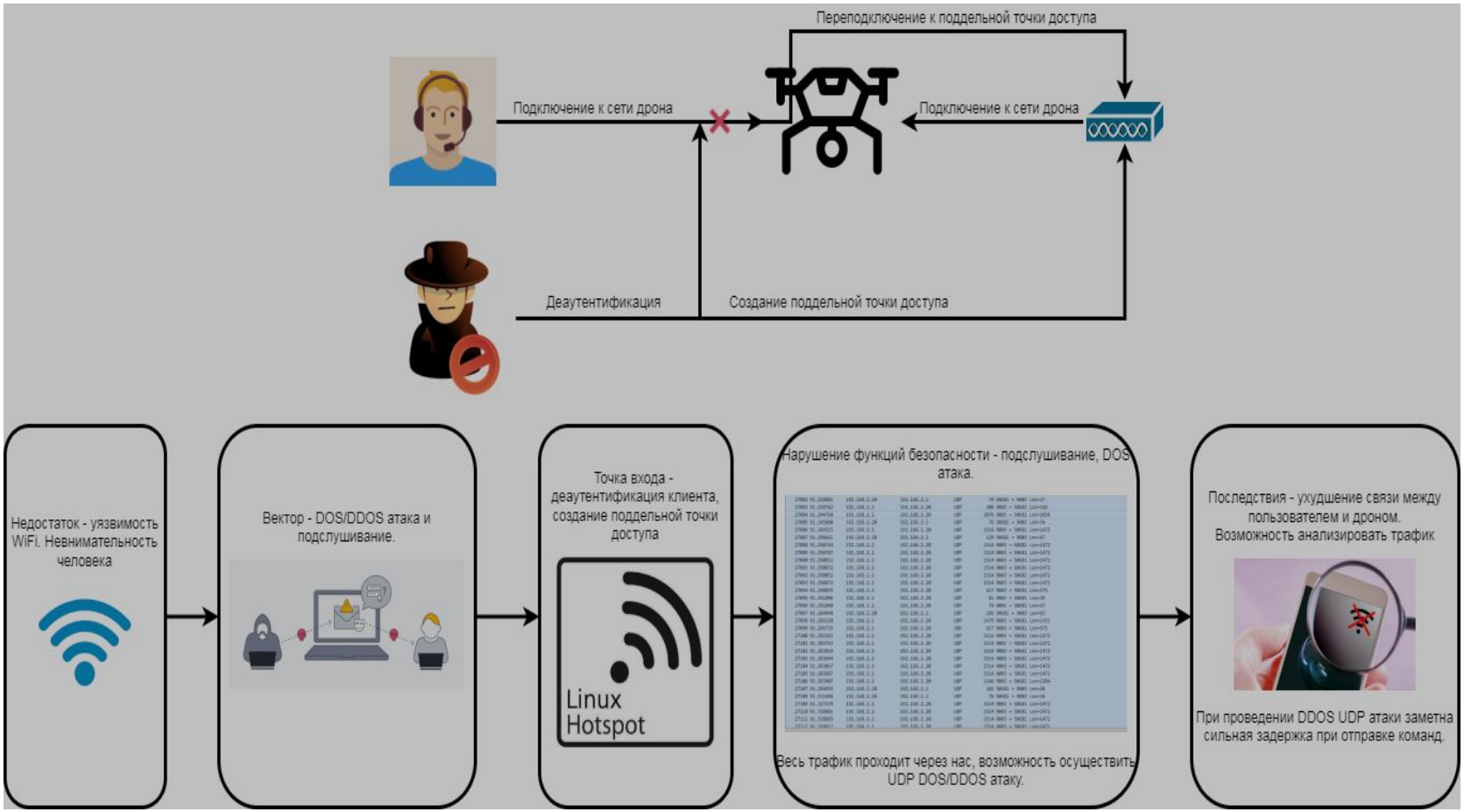
DJI MAVIC AIR

AR.DRONE

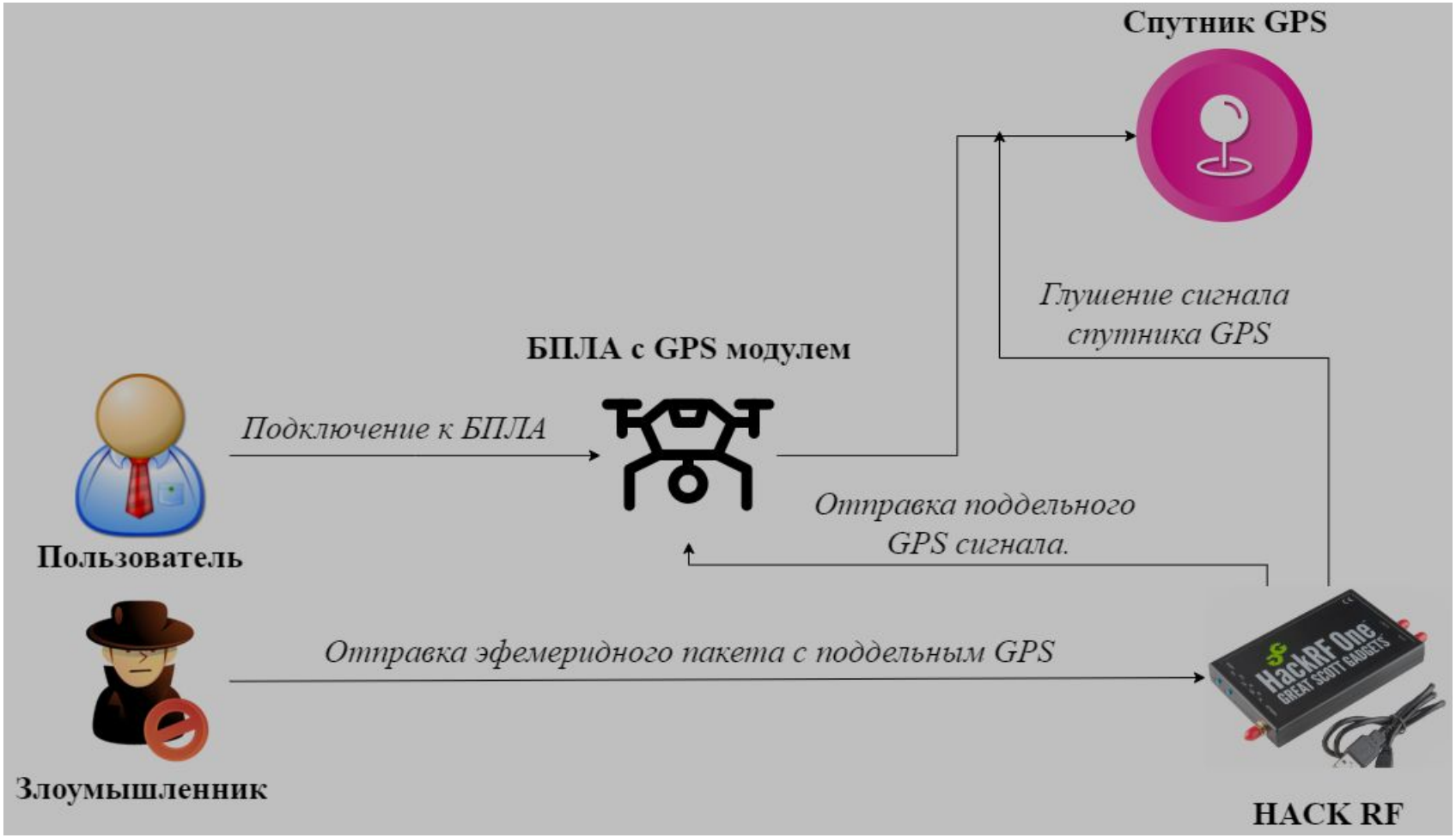
Подмена пакетов



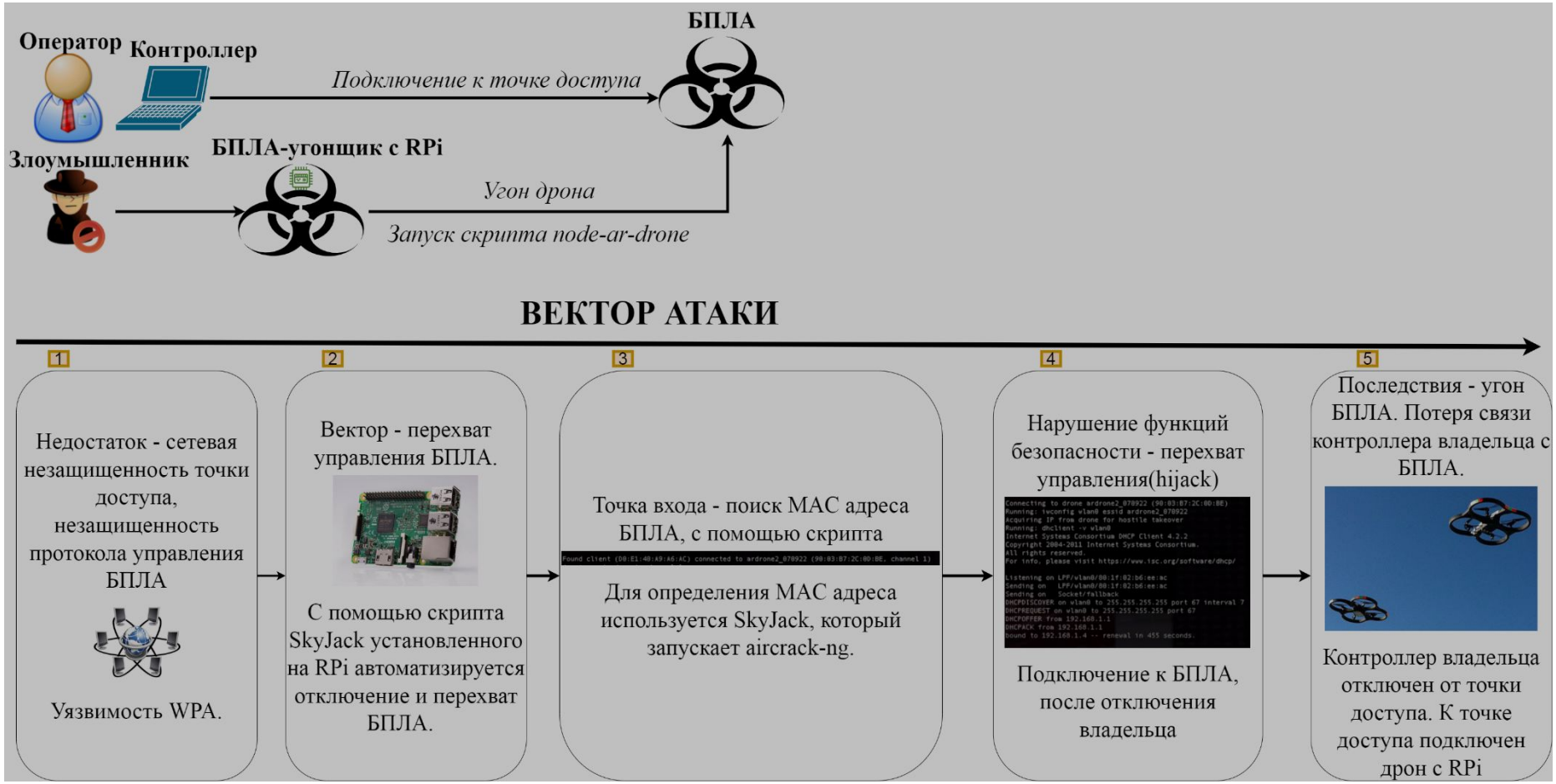
MITM с поддельной точкой доступа



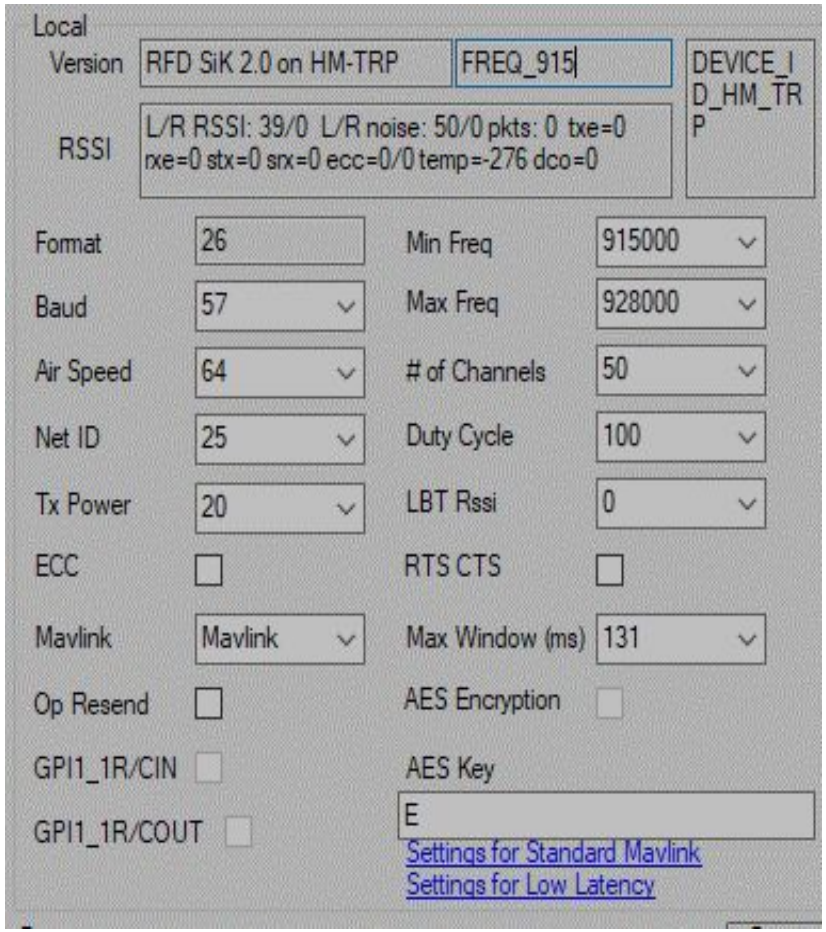
Подмена GPS


Спутник GPS
Глушение сигнала спутника GPS
БПЛА с GPS модулем
Подключение к БПЛА
Пользователь
Отправка поддельного GPS сигнала.
Отправка эфемеридного пакета с поддельным GPS
Злоумышленник
HACK RF

Hijack с БПЛА-угонщиком



Подмена пакетов(радиотелеметрия)



Для перехвата управления с помощью телеметрии требуется подобрать NetID

Экспериментальное исследование

AR.Drone

БПЛА с Pixhawk

DJI Mavic Air

Анализ протоколов

БПЛА	Протокол	DOS атака	MITM атака	Подмена GPS	Подмена пакетов
AR.Parrot	UDP	+	+	-	+
БПЛА с Pixhawk	MAVlink	-	-	+	+
DJI MAVIC	UDP	+	+	+	-

Безопасность человеко-машинного взаимодействия

Можно отметить, что и до внедрения программного продукта, и после, условия труда являются «Допустимыми», так как выполняется следующее условие: от 1 до 5 показателей отнесены к 3.1 и/или 3.2 степеням вредности, а остальные показатели имеют оценку 1-го и/или 2-го классов.

После проделанного анализа внедрение используемого продукта напряженность трудового процесса у пользователей уменьшилась.

Технико-экономическое обоснование

Стоимость эксплуатации рассмотренных систем сопоставима. Значение сравнительной технико-экономической эффективности разработки (1,3) выше единицы, что свидетельствует о положительной оценке целесообразности внедрения разработки.

Разработанный продукт может быть коммерциализирован следующими путями:

– предоставление услуг по тестированию БПЛА,

– анализ подходящих для БПЛА протоколов,

Заключение

В рамках выполнения выпускной квалификационной работы были решены и проведены следующие задачи:

1. проанализированы протоколы управления БПЛА,
2. исследованы угрозы и уязвимости в системах БПЛА,
3. разработаны методики атак «отказ доступа»,
4. разработаны методики атак «человек посередине»,
5. разработаны методики атак «подслушивание».

Результаты ВКР были представлены на следующей конференции:
Всероссийская научно-техническая конференция «Фундаментальные и прикладные аспекты компьютерных технологий и информационной безопасности».