АКЦИОНЕРНОЕ ОБЩЕСТВО
ТЕХНОЛОГИИ РАДИОКОНТРОЛЯ

ОСОБЕННОСТИ ЗАЩИТЫ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ В РОБОТОТЕХНИЧЕСКИХ СИСТЕМАХ

Докладчик: **Шенчелов Федор Петрович**

Начальник отдела

Акционерное общество «Технологии радиоконтроля»

Санкт-Петербург

Защита информации в БЛА

АКЦИОНЕРНОЕ ОБЩЕСТВО
ТЕХНОЛОГИИ РАДИОКОНТРОЛЯ

Цели оценки угроз

- Идентификация уязвимостей в бортовых системах БЛА и комплексах управления БЛА
- Анализ вероятностей возникновения угроз, направленных на использование таких уязвимостей
- Оценку последствий успешной реализации угрозы
- Оценку стоимости вторжений
- Анализ стоимости применимых мер противодействия
- Выбор оптимальных механизмов защиты

Защита информации в БЛА

АКЦИОНЕРНОЕ ОБЩЕСТВО
ТЕХНОЛОГИИ РАДИОКОНТРОЛЯ

Угрозы

- Перехват управления БЛА
- Противоправные перехват и использование информации
- Внедрение устройств негласного получения информации
- Радиоэлектронное подавление
- Навязывание ложной информации навигационной системе БЛА
- Воздействие на парольно-ключевые системы
- Компрометация ключей СКЗИ
- Перехват и дешифрование полученной информации

Защита информации в БЛА

АКЦИОНЕРНОЕ ОБЩЕСТВО
ТЕХНОЛОГИИ РАДИОКОНТРОЛЯ

Объект защиты

- Ключевая информация
- Команды управления БЛА
- Команды управления полезной нагрузкой
- Данные позиционирования БЛА в пространстве
- Специальная информация, полученная с полезной нагрузки
- Телеметрическая информация

Защита информации в БЛА

АКЦИОНЕРНОЕ ОБЩЕСТВО
ТЕХНОЛОГИИ РАДИОКОНТРОЛЯ

Уязвимости

- Применение элементной базы зарубежного производства
- Необходимость постоянного обмена информацией с НПУ
- Использование внешней системы позиционирования БЛА
- Наличие открытых потоков телеметрической информации
- Отсутствие или ограниченное использование СКЗИ
- Вероятность компрометации ключевой информации и СКЗИ
- Необходимость постоянного информационного взаимодействия с пилотируемыми летательными аппаратами

Тип стратегии	Сценарий выбора реализуемой стратегии нарушителем	Критерии оптимальности мер противодействия
Нарушение конфиденциальности	Раскрытие шифров. Нарушение правил шифрования. Компрометация ключей до запуска БЛА или на НПУ. Перехват и статистическая обработка криптограмм. Вскрытие шифра в результате криптоанализа. Дешифрование специальной информации.	Максимизация ожидаемого безопасного времени работы СКЗИ до взлома подсистемы защиты Минимизация вероятности раскрытия ключа шифра Минимизация вероятности дешифрования специальной информации
Нарушение имитостойкости	Перехват и модификация команд управления БЛА. Навязывание ложных команд управления БЛА. Вскрытие алгоритма и ключа обеспечения имитостойкости. Подавление и навязывание ложных навигационных данных.	Минимизация навязывания ложной информации Минимизация вероятности трансформации информации
Нарушение достоверного информационного взаимодействия	Радиоэлектронное подавление команд управления БЛА, телеметрических и навигационных данных. Нарушение правил вхождения в связь.	Минимизация вероятности искажения информационного символа Минимизация вероятности подавления информации Минимизация вероятности необнаружения искажений Минимизация времени доведения информации
Нарушение сохранности (работоспособности) подсистем	Внедрение средств негласного получения информации. Модификация ПО. Подмена, уничтожение, хищение наиболее важных компонентов БЛА. Воздействие на элементы инфраструктуры: электропитание, линии связи и т.п.	Минимизация вероятности необнаружения закладочных устройств и несанкционированной модификации ПО Максимизация вероятности восстановления работоспособности устройств БЛА
Нарушение регистрируемости		Минимизация вероятности незарегистрируемости факта воздействия и ошибок в подсистемах БЛА

История изучения проблемы ПЭМИН

АКЦИОНЕРНОЕ ОБЩЕСТВО
ТЕХНОЛОГИИ РАДИОКОНТРОЛЯ

- 1918 год – докладная записка американского телеграфиста Герберта Ярдли (Herbert Yardley) о проблеме криптоустойчивости американских шифров.
- 1943 год – исследование смесителя 131-B2 компании Bell Telephone, применявшихся американским криптроцентром. Перехват осуществлен инженерами Bell Telephone из соседнего здания рядом с криптоцентром на расстоянии в 25 метров.
- 1951 год – проблему с 131-B2 актуализировали (обнаружили самостоятельно) представители ЦРУ. Перехват осуществлен на расстоянии чуть ли не в полкилометра.
- 1985 год – демонстрация голландским инженером Вим ван Эком (Wim van Eck) возможности перехвата композитного сигнала видеомонитора при помощи технически доработанного монитора. Статья «Электромагнитное излучение видеодисплейных модулей: Риск перехвата информации?»
- 2004 год – немецкий ученый-исследователь Маркус Гюнтер Кун (Markus Guenther Kuhn) в своей статье достаточно подробно описал возможности перехвата цифрового сигнала видеомонитора.

История изучения проблемы ПЭМИН

АКЦИОНЕРНОЕ ОБЩЕСТВО
ТЕХНОЛОГИИ РАДИОКОНТРОЛЯ

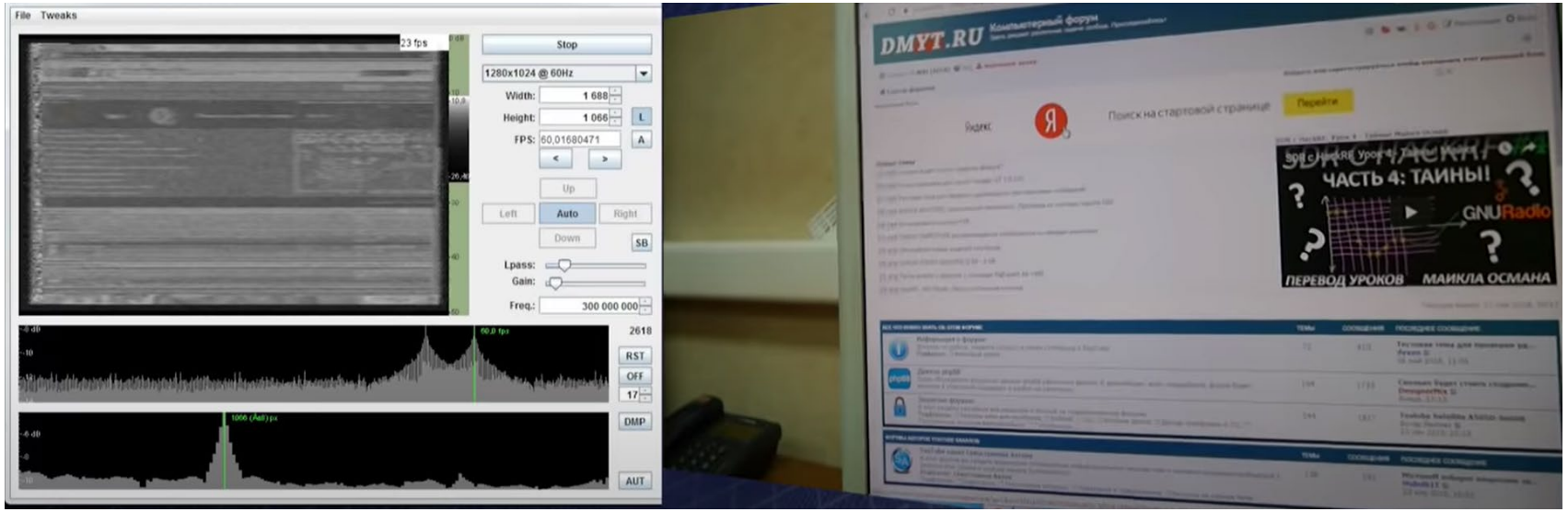
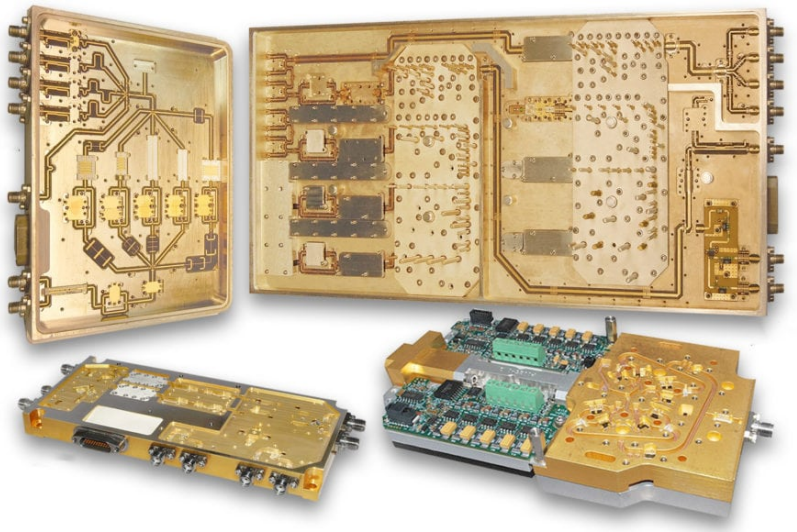


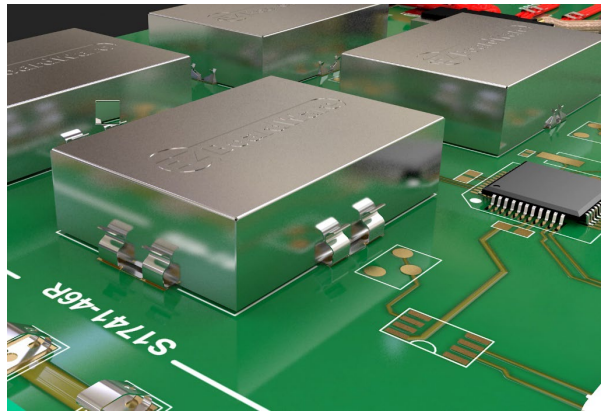
Иллюстрация примера перехвата побочных электромагнитных излучений ЖК-монитора. Из технических средств использовался широкополосный радиоприёмник RTL-SRD (диапазон частот от 1 МГц до 6 ГГц) и антенна телескопическая для портативных радиостанций. Далее применялся анализ полученного сигнала и последующее восстановление информации.

Решение проблемы ПЭМИН

АКЦИОНЕРНОЕ ОБЩЕСТВО
ТЕХНОЛОГИИ РАДИОКОНТРОЛЯ

- Экранирование блоков и узлов, имеющих ПЭМИН
- Проектирование изделий, с учетом требований по экранированию и фильтрации сигналов
- Уменьшение уровней напряжений и токов
- Применение дифференциальных линий передачи данных
- Разработка организационно-распорядительной документации

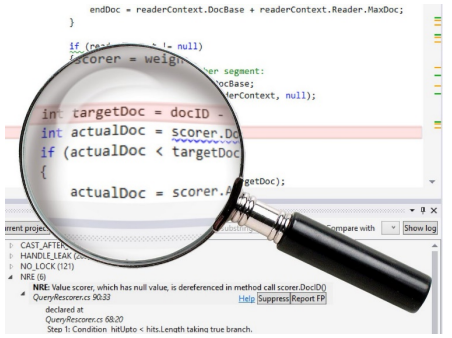




Решение проблемы ТЗИ РТК

АКЦИОНЕРНОЕ ОБЩЕСТВО
ТЕХНОЛОГИИ РАДИОКОНТРОЛЯ

- Использование в ходе производства комплектующих, подвергнутых проверке на наличие устройств негласного получения информации
- Проведение исследований ПЭМИН от изделий и его комплектующих
- Проведение исследований и анализа программных продуктов
- Проведение испытаний на стендах и полигонах
- Использование сертифицированных средств защиты
- Проведение организационных и технических мероприятий



Контакты

АКЦИОНЕРНОЕ ОБЩЕСТВО
ТЕХНОЛОГИИ РАДИОКОНТРОЛЯ

Спасибо за внимание!

Прошу задавать вопросы.