ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

М. Тынышбаев атындағы
ҚАЗАҚ КӨЛІК ЖӘНЕ КОММУНИКАЦИЯЛАР АКАДЕМИЯСЫ

КАЗАХСКАЯ АКАДЕМИЯ ТРАНСПОРТА И КОММУНИКАЦИЙ
имени М. Тынышпаева

QazATK
since 1931

МАГИСТРАНТТАРДЫҢ ҒЫЛЫМИ ЕҢБЕКТЕРІНІҢ ЖИНАҒЫ

СБОРНИК НАУЧНЫХ ТРУДОВ МАГИСТРАНТОВ

Алматы - 2018

СЕКЦИЯ №3. АКТУАЛЬНЫЕ ВОПРОСЫ В ЭЛЕКТРОЭНЕРГЕТИКЕ

СЕКЦИЯ №4. ИННОВАЦИИ В IT

Интернет вещей позволяет автоматизировать многие операции, как и в области корпоративных сетей, так и за этой областью, за счет:

- автоматического сбора информации об объектах (механизмах, оборудовании, устройствах, помещениях) для отслеживания статуса или поведения;
- использование этой информации для контроля и управления, что помогает оптимизировать процессы и использование ресурсов, а также улучшить процесс принятия решений.

Для того чтобы данные, генерируемые Интернетом вещей, стали инструментом развития, организации должны решить три основные задачи:

- интегрировать данные из большого количества источников;
- автоматизация сбора данных;
- анализ данных для получения ценной информации.

Выводы. Планирование корпоративной сети заключается в том, чтобы оценить все имеющиеся на сегодняшний день технологические решения, оценить то, что станет доступным и необходимым завтра, и объединить все это в единую, крупномасштабную сеть предприятия с возможностью масштабирования. Для этого требуется большой практический опыт в планировании сетей, а также знание рынка и будущих трендов, только в этом случае можно будет профессионально спланировать и построить, а также модернизировать корпоративную сеть.

ЛИТЕРАТУРА

[1] Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 5-е изд. –СПб.: Питер, 2016.

[2] Сайт Wikipedia.org

[3] Доклад С-Терра на «ИнфоФоруме-2017»

[4] Сайт https://www.cisco.com/c/ru_ru/about/press/press-releases/2017/06-09b.html

[5] Сайт habr.com

[6] Возможности Интернета вещей: как перейти от подключения объектов к сбору и анализу данных Энди Норона, Роберт Мориарти, Кэти О'Коннелл, Никола Вилла. Cisco, 2014.

УДК 004.451.6

А.Н. Нургулжанова[1,a], Е. Омирзакулы[2,a], М.А. Оразханова[1,a]

[1]Казахская академия транспорта и коммуникаций им. М.Тынышпаева, г. Алматы, Казахстан

[2]Алматинский технологический университет

[a]a.nurgulzhanova@kazatk.kz

УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ПРИЛОЖЕНИЯХ ДЛЯ МОБИЛЬНЫХ СИСТЕМ

Аннотация. Мобильные телефоны в современном мире являются не просто средством связи, а устройством, которое содержит уязвимые персональные данные, несанкционированный доступ к которым может привести к непредсказуемым результатам. В настоящий момент современные средства защиты не позволяют в полной мере решить вопросы безопасности мобильных систем и оценить возможные риски потенциальных злоумышленных действий. В связи с этим, возникает задача систематизировать основные угрозы и уязвимости мобильных приложений для последующего формирования методики по оцениванию угроз информационной безопасности в приложениях для мобильных систем.

Ключевые слова: мобильная операционная система, приложение, уязвимость, анализ защищенности, мобильная платформа, мобильное устройство.

Түйінді сөздер: мобильді операциялық жүйе, қосымша, осалдық, қорғауды талдау, мобильді платформа, мобильді құрылғы.

Аңдатпа. Қазіргі әлемдегі ұялы телефондар тек байланыс құралы ғана емес, осал дербес деректерді қамтитын құрылғы болып табылады. Қазіргі уақытта заманауи қорғаныс құралдары мобильді жүйелердің қауіпсіздігі мәселелерін толық көлемде шешуге және ықтимал қаскүнемдік іс-әрекеттердің ықтимал тәуекелдерін бағалауға мүмкіндік бермейді. Осыған байланысты мобильді жүйелерге арналған қосымшаларда ақпараттық қауіпсіздік қатерлерін бағалау жөніндегі әдістемені қалыптастыру үшін мобильді қосымшалардың негізгі қатерлері мен осалдығын жүйелеу міндеті туындайды.

Abstract. Mobile phones in the modern world are not just a means of communication, but a device that contains vulnerable personal data, unauthorized access to which can lead to unpredictable results. At the moment, modern security tools do not allow to fully address the security issues of mobile systems and to assess the possible risks of potential malicious actions. In this regard, the task arises to systematize the main threats and vulnerabilities of mobile applications for the subsequent formation of methods for assessing threats to information security in applications for mobile systems.

Key words: mobile operating system, application, vulnerability, security analysis, mobile platform, mobile device.

В соответствии с последними данными исследовательской компании eMarketer [1], специализирующейся на анализе рынка высоких технологий, смартфонами уже пользуется четверть мирового населения. Это около 2 млрд человек. И тенденция роста пользователей мобильных устройств продолжается. На рисунке 1 представлена динамика роста числа пользователей смартфонов в период с 2013 по 2016 г. с прогнозом на 2017–2018 г.

Мобильные телефоны в современном мире являются не просто средством связи, а устройством, которое содержит уязвимые персональные данные: номера кредитных карт, электронную почту, геолокационные сведения [2], профили в социальных сетях, средства удалённого доступа и управления предприятием, фотографии, видео и т. д. Несанкционированный доступ к таким чувствительным данным может привести к критической ситуации.

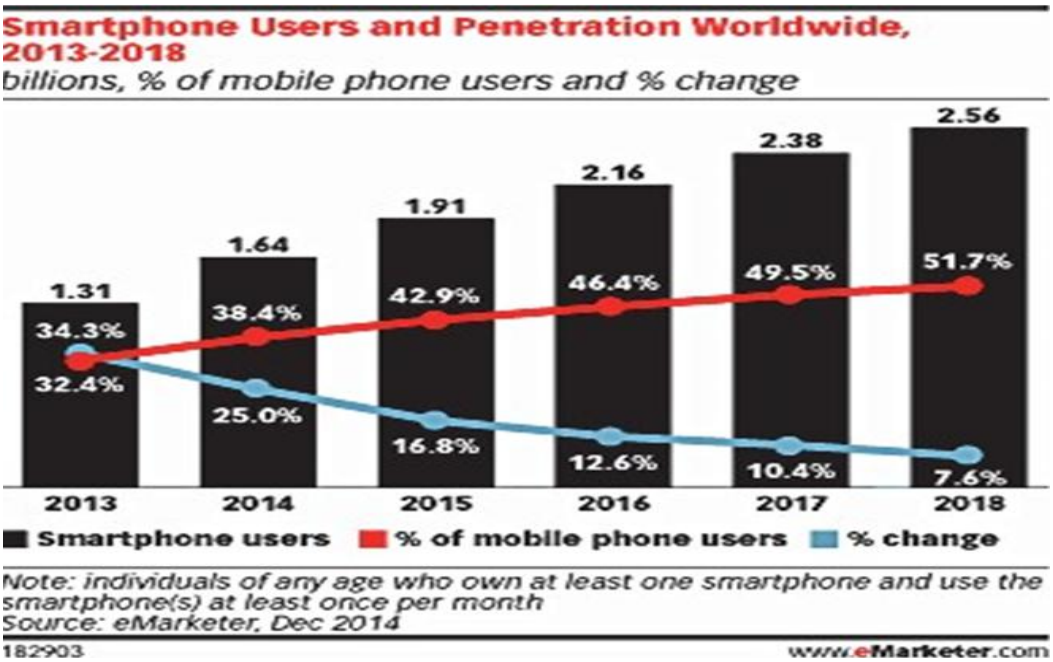

Рисунок 1 – Прогноз роста числа пользователей смартфонов

Между тем, рынок мобильных приложений растёт с большой скоростью, а пользователи особенно не задумываются о том, какие разрешения они предоставляют приложениям, устанавливая их на свой смартфон, а также о последствиях, которые могут наступить.

Проблемы безопасности касаются не только банковского сектора. Игры на мобильных устройствах, множество других популярных приложений могут быть потенциально опасными. Например, популярное приложение «Музыка ВКонтакте», размещённое на площадке Google Play и имеющее довольно высокий рейтинг (4,5 из 5), а также более 500 тысяч скачиваний, вовсе похищало идентификационные данные пользователей, что приводило к потере доступа к профилю в социальной сети.

Всё это говорит о том, что существует реальная необходимость оценить текущее состояние информационной безопасности наиболее распространённых мобильных операционных систем, систематизировать основные угрозы и уязвимости мобильных приложений и составить детальный подход к разработке методики по оцениванию угроз информационной безопасности в приложениях для мобильных систем.

Сегодня наиболее распространёнными мобильными операционными системами являются ОС Android, iOS и ОС Windows Phone. По последним данным, 8 из 10 современных мобильных устройств работают на базе операционной системы с открытым кодом Android. На рисунке 2 приведена статистика с сайта https://www.statista.com. На графиках продемонстрированы доли рынка мобильных операционных систем в соответствии с продажами устройств конечным пользователям в период с 2009 по 2018 г. В третьем квартале 2015 г. 84,7 % от количества всех проданных смартфонов базировались на операционной системе Android.

По последним статистическим сведениям, ОС Android получила статус самой уязвимой. В 2018 г. на ОС Android специалисты по информационной безопасности нашли 523 уязвимости. На рисунке 3 приведена статистика 2016 г., демонстрирующая количество уязвимостей на различных мобильных операционных системах.

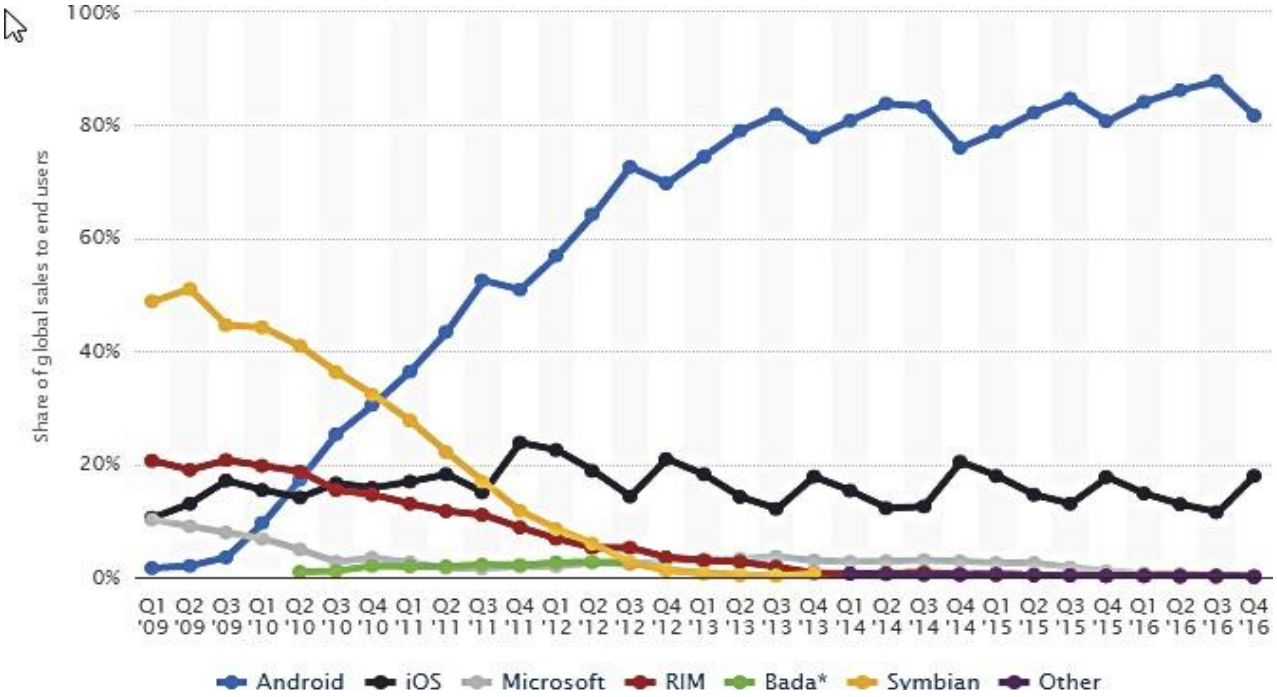

Рисунок 2 – Доли рынка мобильных операционных систем в соответствии с продажами мобильных устройств конечным пользователям в 2009–2018 гг.

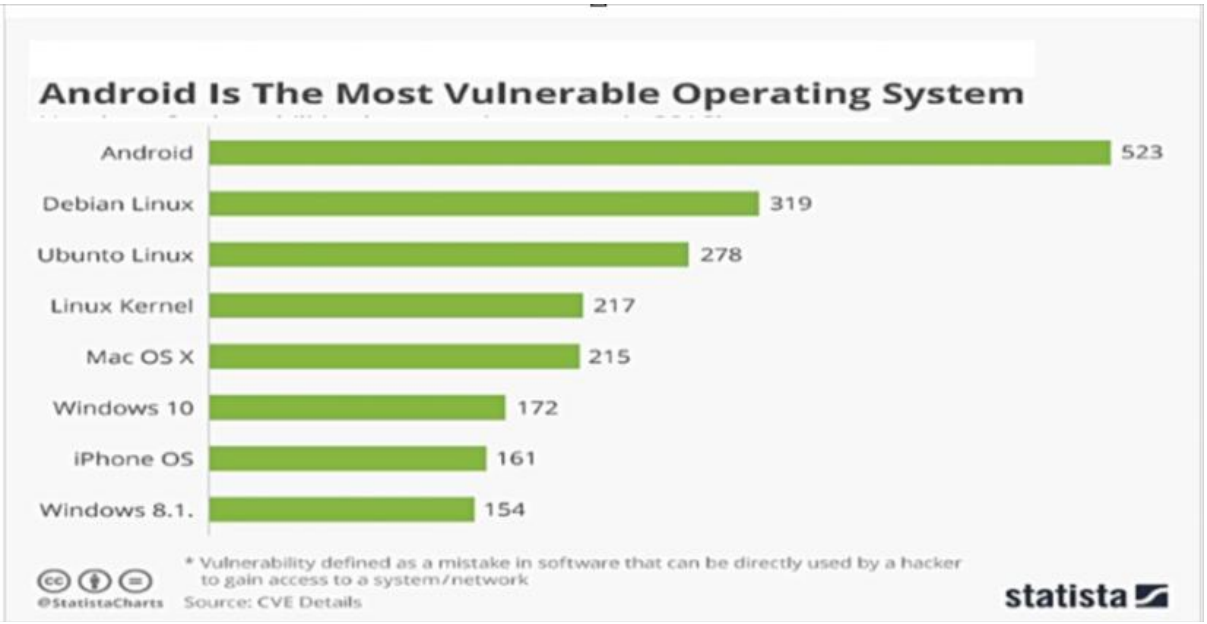

Рисунок 3 – Количество уязвимостей, найденных в мобильных операционных системах, 2018 г.

Методы анализа защищенности в мобильных приложениях. Существуют различные методы оценивания угроз информационной безопасности в приложениях для мобильных систем, которые применяются как в отдельности, так и в совокупности. Разделить их можно на две большие категории: статистические и динамические.

В качестве методов динамического анализа используются:

- стресс-тестирование;
- анализ сетевого трафика мобильного приложения;
- анализ памяти приложения;
- анализ взаимодействия приложения с файловой системой.

К методам статистического анализа относятся [3]:

- аудит безопасности кода приложения;
- Reverse Engineering;
- дизассемблирование;
- декомпиляция.

Для комплексной оценки состояния защищенности мобильной системы необходимо исследовать три составляющих: клиентскую часть, серверную часть и непосредственно канал связи. Для этого применяют такие методы:

- комплексный анализ архитектуры клиентской и серверной части приложения;
- моделирование угроз в соответствии с логикой приложения;
- проектирование модели нарушителя.

Исследование динамики угроз в мобильных платформах. Как было отмечено выше, в качестве исследуемых мобильных платформ были взяты Android и iOS версий, выпущенных за последние 5 лет. Общее количество заявленных уязвимостей для ОС Android – 2956. На рис. 4 представлено их распределение.

Можно заметить, что явно выделяются два пика обнаружения уязвимостей – сентябрь и октябрь 2014 г. В этот период на смартфонах активно работали версии Android 4.1/4.2/4.3 «Jelly Bean» [4]. Именно они обеспечивали подавляющее количество установок на мобильные телефоны, работающие под платформой Android. Именно в этой версии были найдены множественные уязвимости в области работы с данными и протоколами.

Например, в версии 4.3.4 была обнаружена грубая ошибка по работе с протоколом OpenSSL [5].

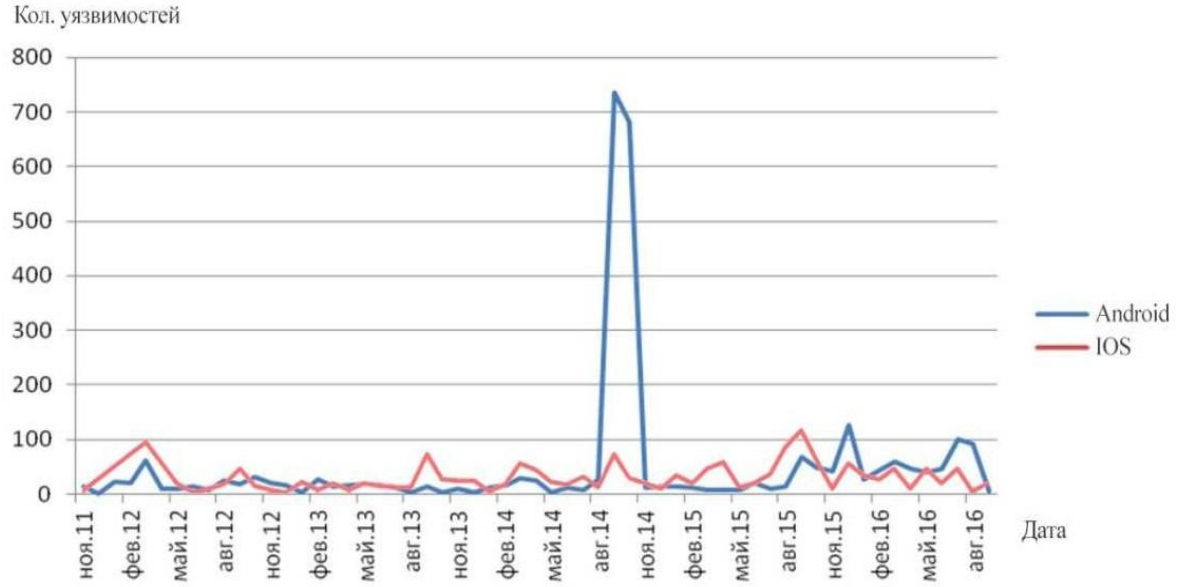

Рисунок 4 – Динамика распределений заявленных угроз для ОС Android и iOS за последние 5 лет

При анализе графика можно обнаружить, что количество уязвимостей после октября 2014 г. снизилось и более не принимало столь критичных значений. До пика среднее количество угроз равнялось 43, после – 65. Иначе обстоят дела у ОС iOS (см. рис. 4). Общее количество заявленных уязвимостей – 2198. Таким образом, это на 26 % меньше, нежели чем у ОС Android.

Среднее количество угроз за рассматриваемые периоды равно 76. Можно заключить, что если бы не пик обнаружения угроз у Android в среднем у ОС iOS среднее количество угроз и уязвимостей выше на 29 %.

Стоит заметить, что в данном случае на графике просматривается периодичность, т.е. приблизительно через равные промежутки времени появляются как максимумы, так и минимумы. Это явная отличительная особенность анализа угроз и уязвимостей платформы iOS над платформой Android.

Это может быть связано с тем, что количество обновлений, выпускаемых компанией Google (разработчик платформы Android), больше, нежели компанией Apple (разработчик платформы iOS), и скорость их применения более оперативна [6]. С другой стороны, разработчики Android с целью повышения качества и безопасности работы софта постоянно его улучшают, что приводит к неминуемому росту пользователей данной ОС по сравнению с другими платформами, тогда как разработчики других платформ более инертно реагируют на появившиеся угрозы, подвергая тем самым угрозе своих пользователей.

Несмотря на большое количество методов обеспечения безопасности информации, хранящейся на мобильных устройствах, уровень распространения вредоносных приложений в мобильном сегменте растёт высокими темпами. Угрозы безопасности создают риски персональным данным пользователя, риски компрометации критичных данных вплоть до хищения денежных средств. К тому же разработчики мобильных приложений не всегда уделяют достаточного внимания проблемам безопасности или просто не следуют руководствам по безопасной разработке.

На настоящий момент ни высокие рейтинги приложения, ни большое количество скачиваний, ни список ресурсов, доступ к которым пользователь предоставляет

приложению перед его установкой, не позволяют оценить возможные риски персональным данным и последствия потенциальных злоумышленных действий. Современные средства защиты (антивирусы, снифферы) могут помочь предотвратить определенный спектр угроз, но их применение не позволит решить проблему безопасности комплексно. В связи с этим, возникает задача разработки комплексной методики по оцениванию угроз информационной безопасности в приложениях для мобильных систем, а также методики анализа приложений на предмет их соответствия требованиям информационной безопасности.

ЛИТЕРАТУРА

[1] Аналитический центр InfoWatch. Глобальное исследование утечек корпоративной информации и конфиденциальных данных, 2018. URL: https://www.infowatch.ru/report2018 (дата обращения 01.12.2018).

[2] Михайлов Д. М. Исследование уязвимости мобильных устройств систем Apple и Google / Д.М. Михайлов, А.В. Зуйков, И. Ю. Жуков и др. // Спецтехника и связь, 2011, № 6. С. 38-40. URL: http://cyberleninka.ru/article/n/issledovanie-uyazvimosti- mobilnyh-ustroystv-sistem-apple-i-google#ixzz4hjVQGz9w.

[3] Цыганенко Н. П. Статический анализ кода мобильных приложений как средства выявления его уязвимостей / Н. П. Цыганенко // Тр. БГТУ. Сер. 6: Физико-математические науки и информатика, 2015, № 6. С. 200-203. URL: http:// cyberleninka.ru/article/n/staticheskiy-analiz-koda-mobilnyh- prilozheniy-kak-sredstvo-vyyavleniya-ego-uyazvimostey.

[4] Android: A visual history [Электронный ресурс]. – URL: http://www.webcitation.org/6DpDvrrwH (дата обращения: 28.12.2018).

[5] Whitwam R. Google Rolling Out Android 4.4.4 Update (KTU84P) With A Security Fix, Factory Images/Binaries Up For Nexus Devices [Электронный ресурс]. – URL: http://www.androidpolice.com/2014/06/19/google-rolling-out-android-4-4-4-update-ktu84p-with-a-security-fix-factory-images- binaries-up-for-nexus-devices/ (дата обращения: 28.12.2018).

[6] When Malware Goes Mobile [Электронный ресурс]. – URL: https://www.sophos.com/en-us/security-news-trends/security-trends/malware- goes-mobile.aspx (дата обращения: 28.12.2018).

УДК 004.451.6

А.Н. Нургулжанова[1,a], Е. Омирзакулы[2,a]

[1]Казахская академия транспорта и коммуникаций им. М.Тынышпаева, г. Алматы, Казахстан

[2]Алматинский технологический университет

[a]a.nurgulzhanova@kazatk.kz

АНАЛИЗ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ ПО КАНАЛАМ СОТОВОЙ СВЯЗИ

Аннотация. В статье приведены анализ защищенности информации по каналам сотовой связи. Предлагаемое в данной статье устройство построено по гибридному принципу с уровнем защиты, обеспечивающее временную стойкость. Для проверки достоверности работы модели схемы защиты речевой информации, имеющий аналоговый вид, разработана модель на пакете программ SystemView. Она позволяет оценить результаты эксперимента и дает визуальную информацию форм сигналов данного устройства.

Ключевые слова: аналоговые сигналы, гибридные сигналы, полосовые фильтры, защита информации, скрэмблеры, биквадратный фильтр.

Андатпа. Мақалада ұялы байланыс арналары бойынша ақпараттың қорғалуына талдау келтірілген. Ұсынылған мақалада құрылғы уақытша төзімділікті қамтамасыз ететін қорғаныс деңгейі бар гибрид принципі бойынша салынған. Аналогты түрі бар, сөйлеу ақпаратын қорғау схемасының моделі жұмысының дұрыстығын тексеру үшін SystemView бағдарлама пакетінде жасалған. Эксперимент нәтижелерін бағалауға және осы құрылғының сигнал формаларының визуалды ақпаратын көрсетуге мүмкіндік береді.