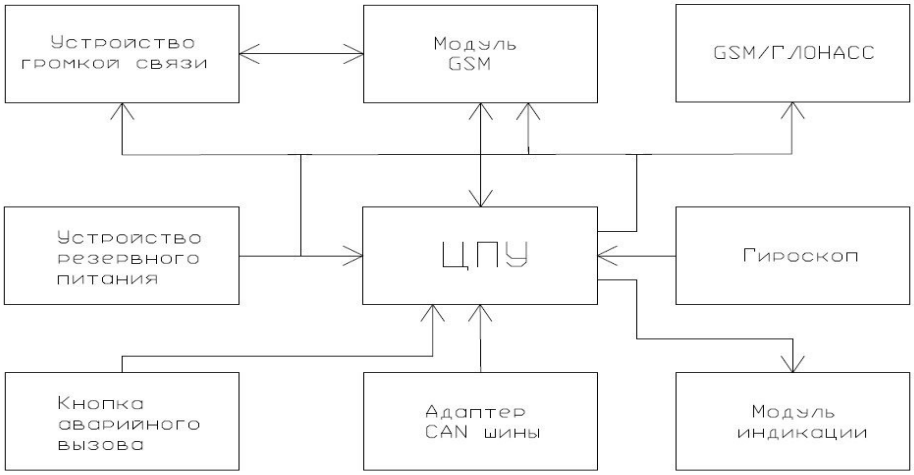

Рисунок 1 – Схема электрическая структурная

Основой в разрабатываемом устройстве является ЦПУ. Микропроцессор отслеживает текущее состояние отдельных модулей системы, их настройки и передачу данных между ними. при дорожно-транспортом происшествии ЦПУ должно автоматически отправить SMS сообщение в службу спасения или звонок может быть инициирован нажатием кнопки SOS. При этом SMS сообщение должно содержать координаты местоположения**.** При неудачной отправке SMS сообщения, как правило, при неисправной или разряженной аккумуляторной батарее, система должна формировать сообщение с указанием ошибки на дисплей. Устройство должно учитывать малую скорость и небольшое изменение координат. При получении SMS сообщения по каналу GSM на модем или GSM модуль, ЦПУ должно иметь возможность дешифровать текст сообщения.

В задачу устройства громкой связи входит обеспечение возможности общения водителя или пассажиров транспортного средства в салоне автомобиля через встроенные микрофон и динамик. Если в машине уже предусмотрена громкая связь, она будет подключаться к устройству.

Инновационной составляющей разрабатываемого устройства является применение повышающего-понижающего преобразователя, что позволяет увеличить срок службы аккумулятора.

Список использованных источников:

1. ГЛОНАСС мониторинг транспорта [Электронный ресурс].– Режим доступа: http://rnsinfo.ru/materials/articles/monitoring/1417/. – Дата доступа 15.03.2018.

2. Слепушкин, Ю. GPS технологии на транспорте/ Ю.Слепушкин // Беспроводные технологии – №4. – 2007. – С.50-52.

О КОМПЛЕКСНОСТИ НАУЧНЫХ ИССЛЕДОВАНИЙ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Прузан А.Н.

Таболич Т.Г. – к.т.н., доцент

Обсуждается проблема комплексности научных исследований в области безопасности облаков учёных СНГ с точки зрения числа рассматриваемых направлений информационной безопасности по сравнению с практическими направлениями аналогичных исследований учёных дальнего зарубежья. Делается вывод.

Информационная безопасность облачных вычислений является, несомненно, одним из приоритетных направлений в современных ИТ-технологиях. Подтверждением этому служат составляемые раз в полугодие компанией Cisco Systems, Inc. отчеты по информационной безопасности, где обязательно присутствует раздел «Интеллектуальные системы кибербезопасности компании Cisco для облачных вычислений» [1]. Этот раздел может служить примером комплексности практических исследований в области информационной безопасности в облаках. Например,, в [1, с. 62] одновременно (в комплексе) исследуются:

1) предотвращение потери данных;
2) защита от DDoS-атак;
3) защита электронной почты;
4) шифрование/конфиденциальность/защита данных;
5) защита оконечных устройств/антивирус/защита от вредоносных программ;
6) веб-безопасность;
7) защищённая беспроводная связь и ряд других направлений защиты информации в облаке.

Возникает закономерный вопрос: настолько ли комплексными с точки зрения числа рассматриваемых

направлений информационной безопасности являются научные исследования учёных СНГ как практические исследования в той же области компании Cisco Systems, Inc.?

Для ответа на вопрос проанализируем результаты работ по защите информации в облаке известного на Украине коллектива исследователей под руководством академика Украины, д т н., профессора В. С. Харченко [3] (Национальный аэрокосмический университет им. Н. Е. Жуковского «Харьковский авиационный институт»). Среди работ коллектива ввиду ограниченного объёма этой публикации рассмотрим только три статьи – работы [4–7]. В [4–6] рассматриваются только DDoS-атаки на облако. В [7] анализируются только стандарты информационной безопасности для облачных технологий и тенденции их развития.

Коллектив из БГУИР (д. т. н., профессор В. А. Вишняков и его аспирант М. М. Гондаг Саз) в своих работах [8–11], опубликованных в реферируемом журнале, рассматривает только проблемы аутентификации пользователей в облаках. Здесь, правда, неясно, используют ли модели аутентификации в облачных вычислениях для мобильных приложений из статьи [10] алгоритмы аутентификации пользователей в мобильной среде из тезисов [11] (в [11] нет упоминаний об облаках, поэтому может показаться, что данные алгоритмы пригодны везде, а не только в облачных вычислениях).

ВЫВОД: по состоянию на сегодня ни о какой комплексности научных исследований в области безопасности облаков учёных СНГ с точки зрения числа рассматриваемых направлений информационной безопасности по сравнению с практическими направлениями аналогичных исследований учёных дальнего зарубежья не может быть и речи.

Список использованных источников:

1. Отчет. Cisco по информационной безопасности за первое полугодие 2017 г. – Сан-Хосе (Калифорния): Cisco Systems, Inc., июль 2017. – 90 с.

2. Журавлёв, М. С. Краткий обзор украинских работ по защите данных в облаках / М. С. Журавлёв // В наст. сборнике.

3. Профессор Вячеслав Сергеевич Харченко: библиографический указатель к 60-летию со дня рождения / И. В. Олейник, В. С. Гресь, К. М. Нестеренко, В. М. Новичкова. – Харьков, Национальный аэрокосмический университет им. Н. Е. Жуковского «Харьковский авиационный институт». 2012. – 258 с.

4. Меленец, А. В. Защита Cloud-архитектур от DDoS-атак / А. В. Меленец // Радіоелектронні і комп'ютерні системи. – 2013. – № 5 (64). – С. 64–69.

5. Меленец, А. В. Многоверсионная модель защиты облака от DDOS-атаки / А. В. Меленец // Радіоэлектронні і комп`ютерні системи. – 2014. – № 6 (70). – С. 140–144.

6. Melenets, A. The State Corporate Cloud Computing- Based Network for Registration of Potentially Dangerous Objects / A. Melenets // Information & Security: An International Journal. – Sofia, Bulgaria, 2012, – Vol. 28, – N 1 & 2. – P. 52–62.6.

7.Поночовный, Ю. Л. Стандарты информационной безопасности для облачных технологий и тенденции их развития / Ю. Л. Поночовный, А. А. Фурманов, В. С. Харченко // Радіоэлектронні і комп`ютерні системи. – 2015. – № 4 (74). – С. 25–33.

8. Вишняков, В. А. Модели и средства аутентификации пользователей в корпоративных системах управления и облачных вычислениях / В. А. Вишняков, М. М. Гондаг Саз // Доклады БГУИР. – 2016. – № 3 (97). – С. 111–114.

9. Вишняков, В. А. Концепция и обеспечение безопасности корпоративных информационных систем с использованием облачных вычислений / В. А. Вишняков, М. М. Гондаг Саз, М. Г. Моздурани Шираз // Доклады БГУИР. - 2016. – № 8 (102). – С. 101–102.

10. Вишняков, В. А. Модели аутентификации в облачных вычислениях для мобильных приложений с интеллектуальной поддержкой выбора / В. А. Вишняков, М. М. Гондаг Саз // Доклады БГУИР. – 2017. – № 1 (103). – С. 82–86.

11. Гондаг, С. М. Алгоритмы аутентификации санкционированных пользователей в мобильной среде / С. М. Гондаг, В. А. Вишняков // Технические средства защиты информации: Тезисы докладов XIV Белорусско-российской научно-технической конференции, 25-26 мая 2016 г., Минск. – Минск: БГУИР, 2016. –С. 28–29.

КОМПЛЕКСНАЯ ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ НА БАЗЕ ПО NET STUDIO

Белорусский государственный университет информатики и радиоэлектроники,
г. Минск, Республика Беларусь

Пуйдак В.А.

Пачинин В. И. – зав. кафедрой ИСиТ, канд. техн. наук, доцент

В работе проведен анализ основные методы комплексной защиты персональных данных на основе современных технологий.

Значительную часть работ по защите информации составляют задачи обеспечения безопасности рабочих станций и серверов. Для их решения применяются продукты класса Endpoint Security, которые компенсируют внутренние и внешние угрозы с помощью различных подсистем безопасности (антивирус, СЗИ от НСД, персональный межсетевой экран и др.) [1].

Модель угроз информационной безопасности традиционно включает целый перечень актуальных для рабочих станций и серверов угроз. Угрозы не получалось нейтрализовать одним-двумя средствами защиты информации (далее — СЗИ), поэтому администраторы устанавливали 3-5 различных продуктов, каждый из которых выполнял определенный набор задач: защиту от несанкционированного доступа, вирусов, фильтрацию сетевого трафика, криптографическую защиту информации и т. д.

Такой подход сводит работу администраторов к непрерывной поддержке СЗИ из различных консолей управления и мониторинга. Кроме того, продукты разных вендоров плохо совместимы, что приводит к нарушению функционирования и замедлению защищаемой системы, а в некоторых случаях — и вовсе ко сбою в работе.