**ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО
ОБРАЗОВАНИЯ
МОСКОВСКОЙ ОБЛАСТИ
«ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»,
ИМЕНИ ДВАЖДЫ ГЕРОЯ СОВЕТСКОГО СОЮЗА,
ЛЕТЧИКА-КОСМОНАВТА А.А. ЛЕОНОВА**

**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ
ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ
БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СЕРВИСА»
(ФГБОУ ВО «ПВГУС»)**

ЭВОЛЮЦИОННЫЕ ПРОЦЕССЫ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

**Москва
2022**

УДК 681.3
ББК 32.81
Э15

Рецензенты:

Ставровский М.Е. – д.т.н., профессор, главный научный сотрудник, Федеральное государственное автономное учреждение «Научно-исследовательский институт «Центр экономической промышленной политики» (ФГАУ «НИИ «ЦЭПП»), г. Мытищи, Московская область

Семенов А.Б. – д.т.н., профессор, Федеральное государственное бюджетное образовательное учреждение высшего образования «Национальный исследовательский Московский государственный строительный университет» (НИУ МГСУ), г. Москва

Научный редактор:

Артюшенко В.М. – д.т.н., профессор, заведующий кафедрой «Информационные технологии и управляющие системы», Государственное бюджетное образовательное учреждение высшего образования Московской области «Технологический университет имени дважды Героя Советского Союза, летчика-космонавта А.А. Леонова», г. Королев, Московская область.

Воловач В.И. – д.т.н., доцент, заведующий кафедрой «Информационный и электронный сервис», Государственное бюджетное образовательное учреждение высшего образования, Поволжский государственный университет сервиса, г. Тольятти.

Эволюционные процессы информационных технологий: сборник трудов по материалам 7-й всесоюзной научно-технической конференции 4 апреля 2022 г. / колл. авторов; под общ. науч. ред. док. техн. наук, профессора Артюшенко В.М., и док. техн. наук Воловача В.И. – М.: Издательство «Научный консультант», 2020. – 162 с

Э15

ISBN 978-5-907477-53-7

Предлагаемый сборник научных статей основан на материалах 7-й всесоюзной научно-технической конференции «Эволюционные процессы информационных технологий», прошедшей 4 апреля 2022 г. на базе кафедр «Информационные технологии и управляющие системы» («МГОТУ») и «Информационный и электронный сервис» (ФГБОУ ВО «ПВГУС»). Он стал результатом творчества ученых, профессорско-преподавательского состава, сотрудников, студентов, связанных с информационными технологиями в различных областях деятельности.

Сборник рассчитан на преподавателей, аспирантов, магистров и бакалавров, а также для широкого круга специалистов в области информационных систем.

УДК 681.3
ББК 32.81

Сборник научных статей подготовлен по материалам, представленным в электронном виде. Ответственность за содержание материалов несут авторы.

ISBN 978-5-907477-53-7

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В предлагаемом сборнике научных трудов рассматривается широкий круг вопросов, связанных с применение методов разграничения доступа в информационных системах, оценкой эффективности принятия решений в компьютерных системах, математическим моделированием протяженных целей, проектированием беспроводной локальной вычислительной сети для комплекса зданий и т.д.

Проанализированы вопросы, связанные со сбором и анализом технических данных при реагировании на компьютерные атаки, этапами создания моделей для 3Д визуализаций и компьютерных игр, развитием технологии беспроводной передачи данных - стандарт IEEE 802.11ax.

Рассмотрены технические и организационные рекомендации по проблематике применения цифровых технологий при управлении медицинскими учреждениями, современные технологии для создания WEB-продуктов, динамическая и функциональная модели системы электронного документооборота.

Проведен анализ обеспечения синхронизации многоканального сбора данных с различной степенью дискретизации в момент регистрации в информационно-измерительной системы нового поколения, автоматизации пропускного режима предприятия за счет применения информационно-аналитической системы, особенностей ВОЛС на примере интерактивной системы кабельного телевидения. Рассмотрены вопросы, связанные с современным подход к разработке SPA приложений на фреймворке Angular, использованием хранилища столбцов в ORACLE для анализа данных в OLAP системах.

Материалы данного сборника будут интересны не только бакалаврам и магистрам таких специальностей как: «Информационные системы и технологии», «Прикладная информатика», «Управление в технических системах», но и аспирантам специальностей «Системный анализ, управление и обработка информации», «Теоретические основы информатики», а также для широкого круга специалистов в области информационных технологий.

ОЦЕНКА ЭФФЕКТИВНОСТИ ПРИНЯТИЯ РЕШЕНИЙ В КОМПЬЮТЕРНЫХ СИСТЕМАХ

Аббасова Т. С., доцент, к.т.н.,
Технологический университет («МГОТУ»),
Россия, г. Королев

Рассмотрены задачи анализа сложных технических систем и комплексов. Показано, что запрограммированные решения, типичные для повторяющихся ситуаций, принимаются с соблюдением конкретной последовательности этапов. Новые или сложные ситуации требуют самостоятельного выбора процедуры принятия решения. Предложен метод рационального разрешения проблем с использованием обратной связи.

Ключевые слова: система поддержки принятия решений, запрограммированные решения, обратная связь.

При использовании систем поддержки принятия решений (ССПР) в сложных технических комплексах, таких как стартовые ракетные и космические комплексы, испытательные полигоны, наземные измерительные комплексы, электростанции, системы оптико-лазерных измерений, телекоммуникационные системы и т.п., актуальна разработка методов, учитывающих особенности этих систем и повышающих эффективность принятия решений [1…10].

Аналитическая система, являющаяся составной частью ССПР, осуществляет оперативный и интеллектуальный анализ данных.

К задачам анализа технических систем относятся: накопление знаний и предоставления данных для принятия решений, обеспечивающих надежную и безопасную эксплуатацию сложных технических комплексов; прогнозирование состояния технического оборудования; поиск причин отказа и устранение неисправностей оборудования; анализ возможных последствий аварийных ситуаций и их предотвращение. Как показывает практика [11…20], при анализе состояния технической системы с помощью компьютерной ССПР возникает противоречие между математиком-программистом, который несет ответственность за качество решения математически поставленной задачи, и руководителем, опирающимся на свой собственный опыт и отвечающим за конечный результат. На рис. 1 приведен пример построения зависимости эффективности принятого решения от понимания ситуации и времени принятия решения.

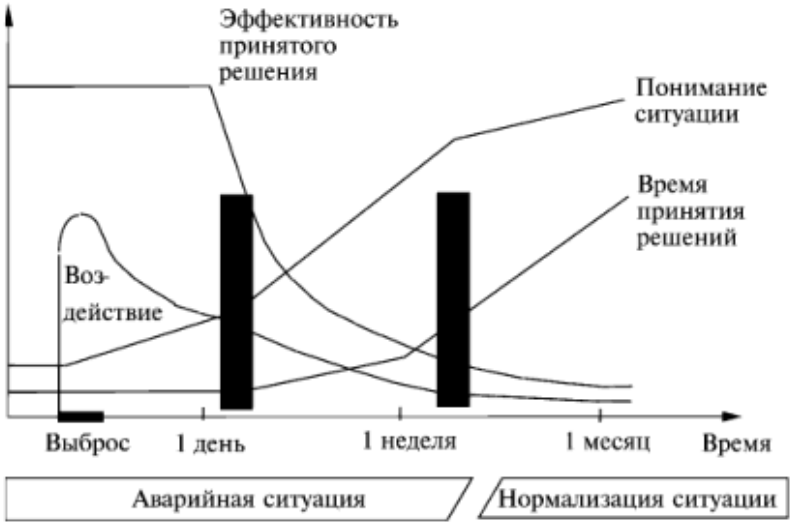


Рис. 1. Эффективность принятого решения в зависимости от понимания ситуации и времени принятия решения

Актуален вопрос об оценке понимания ситуации и проблем, возникающих в технических системах. Этапы рационального решения проблем – диагноз, формулировка ограничений и критериев принятия решений, выявление альтернатив, их оценка, окончательный выбор.

Запрограммированные решения, типичные для повторяющихся ситуаций, принимаются с соблюдением конкретной последовательности этапов. Новые или сложные ситуации требуют, чтобы руководитель (или математик-программист) сам выбирал процедуру принятия решения. Процесс принятия решений является завершенным, когда через систему обратной связи будет засвидетельствован факт реального решения проблемы благодаря сделанному выбору. Или, если такого подтверждения не придет, с помощью обратной связи (отрицательной или положительной, в зависимости от решаемых задач) можно будет скорректировать принятые решения для достижения заданных эксплуатационных показателей технической системы.

Выводы. Решения, принимаемые методом рационального разрешения проблем с использованием обратной связи, способствуют повышению вероятности принятия эффективного решения в сложных технических системах.

Список используемых источников

1. Артюшенко, В. М. Синтез алгоритмов адаптивных блоков нелинейной обработки следящих измерителей при воздействии широ-

кополосных негауссовских помех / В. М. Артюшенко, В. И. Воловач, Т. С. Аббасова // Двойные технологии. 2018. – № 1 (82). – С. 43-46.

2. Привалов В. И., Аббасова Т.С. Анализ проектных решений для перспективных систем высокоскоростного доступа // Современные информационные технологии: сборник трудов по материалам 3-ей межвузовской научно-технической конференции с международным участием 29 сентября 2017 г. / колл. авторов; под общ. науч. ред. док. техн. наук, проф. В. М. Артюшенко. – М. Издательство «Научный консультант», 2017. – С. 115–121 (190 с.).

3. Акимкина, Э. Э. Инструментальный подход к организации сбора данных в хранилище систем поддержки принятия решений / Э. Э. Акимкина // Информационные технологии. – 2017. – №6. – С.424–430.

4. Акимкина, Э. Э. Оптимизация обработки данных в системах поддержки принятия решений с элементами обслуживания // Вестник ВГУ, серия: Системный анализ и информационные технологии. – 2017. – № 2. – С. 79 – 85.

5. Теодорович, Н. Н. Системы безопасности в комплексном интеллектуальном здании / Н. Н. Теодорович // Промышленные АСУ и контроллеры. –2010. – № 6. – С. 54-55.

6. Сидорова, Н. П. Информационные технологии оперативного анализа данных / Н. П. Сидорова, Н. В. Логачева, В. Ю. Добродеев // Информационно-технологический вестник. – 2014. – Т. 01. – № 1. – С. 64-74.

7. Аббасов, А. Э. Оценка качества программного обеспечения для современных систем обработки информации / А. Э. Аббасов, Т. Э. Аббасов // Информационно-технологический Вестник. – №3(05). – 2015. – С. 15 – 27.

8. Акимкина, Э. Э. Проблемы внедрения технологий бесконтактной идентификации на производстве и в банковских структурах / Э.Э. Акимкина, Т.Э. Аббасов, Ю. А. Шмелева // Информационно-технологический Вестник. – № 4(10). – 2016. – С. 18 – 32.

9. Abbasova, T. S., Sidorova, N. P., Teodorovich, N. N.&Abbasov, E. M. Evaluation of Telecommunications Electromagnetic Compatibility with the Use of Three-Dimensional Modeling Technology // Modern Applied Science. – 2016. – Vol. 10, – No. 10, – pp.224-230. ISSN 1913-1844; E-ISSN 1913-1852. Published by Canadian Center of Science and Education doi:10.5539/mas.v10n10p224 URL: http://dx.doi.org/10.5539/mas.v10n10p224.

10. Аббасова, Т. С. Оптимизация конструкции беспроводных устройств связи из композитных материалов /Т. С. Аббасова, А. П. Мороз, Н. А. Васильев, Ю. В. Стреналюк // Двойные технологии. – №2 (75). – 2016. – С. 49 – 51.

11. Аббасова, Т. С. Совмещение управляющих и измерительных функций при интерактивном управлении телекоммуникационными системами / Т. С. Аббасова // Информационно-технологический Вестник. – №2(04). – 2015. – С. 14 – 38.

12. Аббасова, Т. С. Подходы к моделированию и проектированию телекоммуникационных сетей на основе N-мерных технологий / Т. С. Аббасова // Информационно-технологический Вестник. – №2(04). – 2015. – С. 39 – 54.

13. Аббасова, Т. С. Восстановление и проверка корректности телеметрических данных / Т. С. Аббасова, А. А Комраков // Информационно-технологический Вестник. – №2(04). – 2015. – С. 55 – 64.

14. Семенов, А. Б. Улучшение массогабаритных характеристик типовых горизонтальных кабелей СКС / А. Б. Семенов // Информационно-технологический Вестник. – №6(08). – 2015. – С. 46 – 59.

15. Аббасова, Т. С. Обеспечение помехозащищенности беспроводных устройств телекоммуникационных систем / Т. С. Аббасова // Инфокоммуникационные технологии – 2015. – №1. – С. 88 – 92.

16. Артюшенко, В. М. Расчет вероятности блокировки CDMA-ячейки системы подвижной связи при учете структуры трафика / В. М. Артюшенко, Т. С. Аббасова // Радиотехника. – 2015. – № 2. – С. 69-75.

17. Артюшенко, В. М. Повышение эффективности систем спутниковой связи путем оптимизации параметров земных станций / В. М. Артюшенко, Т. С. Аббасова, Б. А. Кучеров // Радиотехника. – 2015. – № 2. – С. 76-82.

18. Artyushenko V.M., Abbasova T. S. Increasing the efficiency of satellite coomunication systems by optimizing the parameters of the ground stations // Radioengineering. – 2015. – № 2. – P. 69-75.

19. Artyushenko V.M., Abbasova T. S., Kucherov B.A. Creating cellular networks in rural areas with the lagest coverage area // Radioengineering. – 2015. – № 2. – P. 76-82.

20. Кучеров Б. А. Адаптация мощности земных станций узловой сети узловой сети спутниковой связи при работе в стволе с прямой ретрансляцией // Двойные технологии. – №1. – 2015. – С. 53–58.

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ПРОТЯЖЕННЫХ ЦЕЛЕЙ

Корнеева Е.В., старший преподаватель,
Артюшенко В.М., д.т.н., профессор,
Автономная некоммерческая организация высшего образования
«Открытый университет экономики, управления и права»
(АНО ВО «ОУЭП»), Россия, г. Москва

В статье рассмотрены и проанализированы вопросы, связанные с описанием математического моделирования протяженных целей.

Ключевые слова: протяженные цели, отражающие элементы, светящаяся точка, многоточечная и двухточечная модель.

Введение. В современных приложениях радиолокации, широко распространенные реальные радиолокационные цели, самолеты, корабли, автомашины и т.д., не могут считаться точечными, так как у них должна учитываться пространственная протяженность по различным координатам. Вследствие сложности формы таких целей и наличия у них большого числа пространственно-разнесенных отражающих элементов возникают значительные ошибки радиолокационного измерения координат, скоростей и ускорений движения целей, которые определяют предельную точность радиолокационных измерительных устройств. Это может быть в условиях, когда размеры цели намного превышают длину рабочей волны и соизмеримы с требуемой точностью радиолокационного измерения ее координат. Примером таких условий является радиолокационное измерение координат, скоростей и ускорений движения целей при сравнительно малых дальностях.

Следует заметить, что одна и та же радиолокационная цель указанного типа в зависимости от дальности может считаться и точечной, и протяженной. Цель будет протяженной, когда ошибки радиолокационного измерения ее координат, скорости и ускорения движения, вызванные протяженностью, превосходят аппаратурные ошибки. При этом продольные и поперечные размеры цели остаются меньшими соответствующих элементов разрешения, что обусловливает на входе радиолокационного измерительного устройства интерференцию сигналов от всех отражающих элементов цели.

При радиолокационном наблюдении за протяженной целью каждая относительно небольшая часть ее облученной поверхности, содержащая совокупность отражающих элементов, вносит свой вклад в общий отраженный сигнал. Эти части цели, отражая падающую на них электромагнитную волну, являются вторичными излучателями, то есть «светятся». Поэтому их называют светящимися точками цели [1]. Обычно число их велико, а распределение в пространстве и величина вклада в общий отраженный сигнал являются случайными и во многом зависят от структуры протяженной цели и угла ее наблюдения, который непрерывно изменяется при движении цели и наблюдателя.

Следовательно, светящаяся точка – это не какая то геометрическая точка протяженной цели, а некоторая совокупность ее отражающих элементов, обусловливающая в связи с этим существование сигнала с гауссовским законом распределения. Любая другая светящаяся точка протяженной цели – это также некоторая совокупность, но других, пространственно-отнесенных отражающих элементов. Можно полагать, что сигналы светящихся точек являются статистически независимыми [3, 4].

С учетом сказанного математическое моделирование протяженных целей осуществляется исходя из двух требований: с одной стороны, модель должна обеспечивать отражение физической сущности происходящих при радиолокации протяженных целей явлений, а с другой – эквивалентность получаемых при ее анализе характеристик практическим результатам. В связи с этим протяженная цель может быть представлена совокупностью большого числа случайных статистически независимых светящихся точек, заполняющих некоторую область пространства, характеризуемую размерами цели. Такая модель получила название многоточечной [5].

Совокупность большого числа светящихся точек в отдельно рассматриваемой координатной плоскости радиолокационного наблюдения может быть сведена к минимуму и в ряде случаев заменена на двухточечную модель [2, 6]. Многоточечная модель позволяет подробнее отобразить сложную структуру и многомерный характер движения различных протяженных целей, а двухточечная модель проще и с большей наглядностью позволяет показать физику происходящих явлений.

Двухточечную модель протяженной цели целесообразно использовать при решении ряда задач, где определяются первые стати-

стические распределения, а многоточечную – при определении всей совокупности статистических свойств сигналов протяженных целей. Кроме того, использование двухточечной модели иногда целесообразно при анализе радиолокационного наблюдения групповой цели и одиночной цели, находящейся над поверхностью раздела двух сред.

Многоточечная и двухточечная модель протяженной цели. Рассмотрим примеры геометрической интерпретации многоточечной и двухточечной моделей протяженной цели. Рис. 1 поясняет многоточечную модель протяженной цели: случайные статистически независимые светящиеся точки, первичные или вторичные излучатели, заполняют некоторую область пространства, форма которой в общем случае произвольна, а в частных случаях определяется структурой и свойствами отображаемой реальной радиолокационной цели.

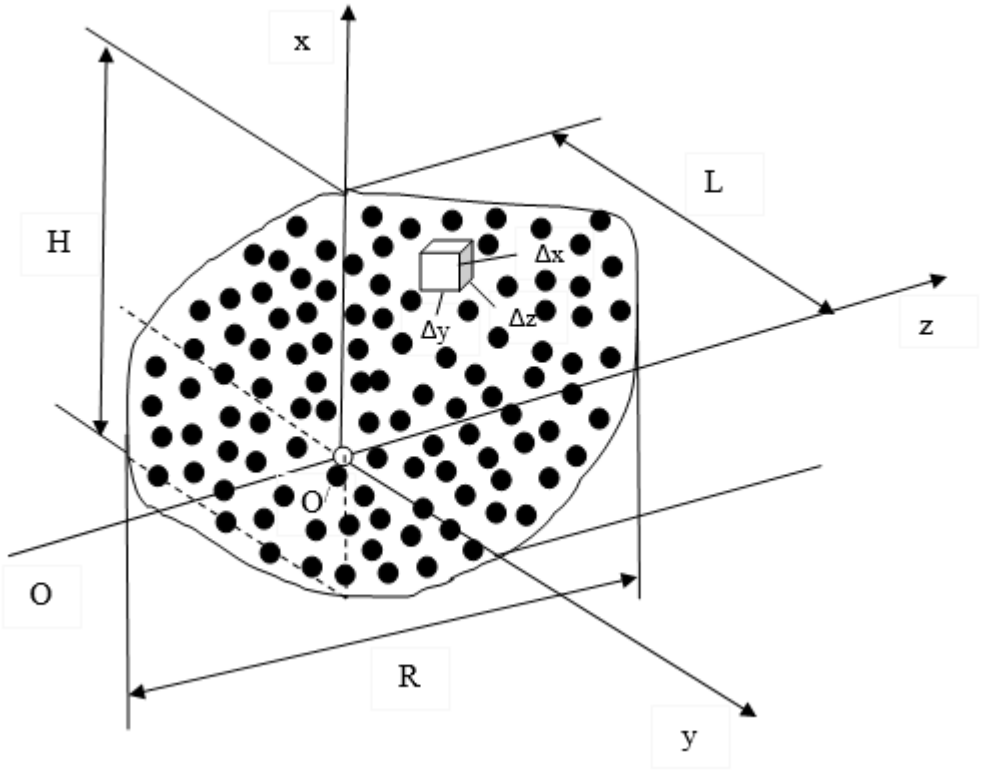


Рис. 1. Многоточечная модель протяженной цели

Цель имеет линейные максимальные продольный размер R (в направлении оси z) и поперечные размеры L и H (в направлении осей y и x); соответствующие угловые размеры цели обозначим α_0 и ε_0.

Произвольная светящаяся точка цели с координатами (x, y, z) создает на входе приемной антенны (точка O) сигнал с напряженностью поля

$$e_{i,j,k}(t) = E_{i,j,k}(t)\cos[\omega t - \psi_{i,j,k}(t)], \quad (1)$$

где ω – частота произвольной гармонической составляющей сигнала; *i, j, k* – индексы отсчета светящихся точек в направлении осей *x*, *y*, *z*.

Сигнал (1) представляет собой гауссовский стационарный узкополосный процесс, характеризуемый нулевым значением математического ожидания ($\langle e_{i,j,k}\rangle = 0$), интенсивностью $\sigma^2_{i,j,k}$ и коэффициентом корреляции $r_{i,j,k}(\tau)$.

Двухточечная модель протяженной цели (рис. 2) содержит две не разрешаемые и не влияющие друг на друга светящиеся точки, разнесенные на расстояние *l* и лежащие в рассматриваемой координатной плоскости радиолокационного наблюдения на дальностях r_1 и r_2 от точки наблюдения *O*.

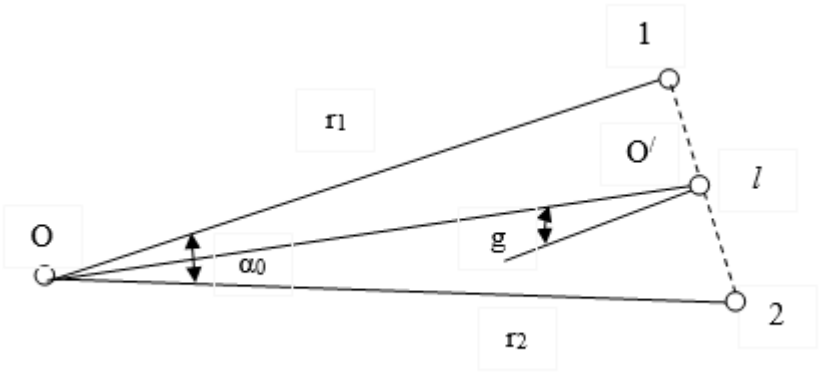


Рис. 2. Двухточечная модель протяженной цели

Двухточечная цель наблюдается под углом *q*; ее продольный размер (проекция на линию визирования OO^*, проходящую через геометрический центр цели O^*) $R = l\sin q$, а поперечный размер (проекция на нормаль к линии визирования) $L = l\cos q$.

Различия структуры протяженных целей с помощью двухточечной модели в некоторых пределах может быть отражено с помощью различных амплитуд сигналов светящихся точек 1 и 2. Многоточечная модель имеет больше возможностей для отображения сложной структуры протяженной цели. Можно использовать функцию $F_r(x, y, z)$, характеризующую распределение по объему цели плотности интенсивности сигналов светящихся точек. Эту функцию введем следующим образом:

$$F_r(x_j, y_i, z_k)\Delta x_j \Delta y_i \Delta z_k = \langle u^2_{i,j,k}\rangle = \langle \vartheta^2_{i,j,k}\rangle, \quad (2)$$

где угловые скобки обозначают усреднение по множеству, u и ϑ – квадратурные компоненты сигнала светящейся точки (1), то есть

$$u_{i,j,k} = E_{i,j,k}\sin\psi_{i,j,k}. \quad (3)$$

Для пояснения вводимой функции на рис. 1 выделен элементарный объем, равный $\Delta x\Delta y\Delta z$ и имеющий координаты центра (x, y, z). Он обощает понятие светящейся точки цели с интенсивностью сигнала $\langle u_{i,j,k}^2\rangle$. Эта интенсивность может быть выражена через плотность $F_r(x_j, y_i, z_k)$, что и записано с помощью выражения (2).

Выводы. Таким образом, рассмотрены вопросы, связанные с математическим моделированием протяженных целей. Показано, что многоточечную модель протяженной цели целесообразно использовать при определении всей совокупности статистических свойств сигналов протяженных целей, а двухточечную - при решении ряда задач, где определяются первые статистические распределения.

Список используемых источников

1. Вайнштейн Л.А., Зубаков В.Д. Выделение сигналов на фоне случайных помех. – М.: Сов. радио, 1970. – 447.

2. Данн Д., Ховард Д., Кинг А. Влияние флюктуаций эхосигнала на работу радиолокационных станций сопровождения цели. – Радиотехника и электроника за рубежом, 1979, №6, С.96 – 113.

3. Зубкович С.Г. Статистические характеристики сигналов, отраженных от земной поверхности. – М.: Сов. радио, 1968. – 224 с.

4. Артюшенко В.М., Воловач В.И. Особенности отражения зондирующих сигналов радиотехнических устройств обнаружения от протяженных объектов сложной формы // Школа университетской науки: парадигма развития. 2012. №2-1 (6). С. 42-46.

5. Артюшенко В.М., Воловач В.И. Измерение параметров движения протяженных объектов в условиях мешающих воздействий и изменяющейся дальности // Двойные технологии. 2015. №1 (70). С. 69-74.

6. Артюшенко В.М., Кучеров Б.А. Оценка экономической эффективности использования автоматизированной системы распределения средств управления космическими аппаратами в условиях ресурсных ограничений // Вестник Поволжского государственного университета сервиса. Серия: Экономика. 2013. № 5 (31). С. 131-136.

ПРИМЕНЕНИЕ МЕТОДОВ РАЗГРАНИЧЕНИЯ ДОСТУПА В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Пушкарев П.В., магистр группы ИМО-ПИ-21,
Солодухин И. В., магистр группы ИМО-ПИ 21,
Технологический университет («МГОТУ»),
Россия, г. Королев

В статье рассматриваются и сравниваются различные методы разграничения доступа в информационных системах. Приводится описание каждого метода и обсуждаются их преимущества и недостатки.

Ключевые слова: разграничение доступа, обмен сообщениями, информационная безопасность.

Введение. В наши дни люди очень часто ведут общение друг с другом через интернет. Сейчас люди все чаще выбирают дистанционный формат общения место того, чтобы встречаться лично. Поэтому существует множество различных способов общения в интернете, самым популярным из которых является мессенджер. В нем люди могут вести диалог с каким-нибудь другим пользователем, либо с несколькими одновременно.

Выбранная для исследования система обмена сообщениями имеет функциональность разделения полномочий пользователей, однако данная система, хоть и имеет гибкую систему разделения прав использования, недостаточно удобна для пользователя из-за того, что пользователям будет сложно адаптироваться к правилам поведения в групповых чатах.

Разграничение доступа — это система определения полномочий субъекта в информационной системе и обеспечения их действий строго в рамках установленных для них полномочий. Система, которая, с одной стороны, определяет, кому из субъектов разрешён допуск к тем или иным объектам, и с другой стороны, не позволяет им превышать собственные полномочия. Разграничение доступа реализуется для решения следующих задач:

- обеспечение конфиденциальности информации;
- обеспечения целостности и информации;
- обеспечения доступности информации.

Обеспечение конфиденциальности достигается за счет того, что субъекту, не входящему в круг легальных пользователей той или иной

конфиденциальной информации, не будет предоставлен доступ к этой информации. Пользователям, которые могут нанести вред целостности или доступности информации, доступ к ней не предоставляется.
Разграничение доступа позволяет обеспечивать контроль действий пользователя. Это происходит за счёт того, что каждый пользователь действует строго в рамках своих полномочий в системе и не может их превысить. Разграничение доступа служит реализацией принципов минимизации полномочий и разделения обязанностей, то есть каждый из субъектов в системе обладает только тем набором прав, который соответствует его должностным обязанностям. Необходимо, чтобы ни к каким дополнительным ресурсам системы пользователь не имел бы доступа, так как это является уязвимостью, которой может воспользоваться злоумышленник, обойдя систему аутентификации и представившись легальным пользователем.
Системы разграничения доступа могут оцениваться по следующим параметрам:

- трудоёмкость первоначальной настройки;
- возможность настройки полномочий в нетипичных случаях;
- удобство добавления нового субъекта или объекта.

Трудоёмкость первоначальной настройки заключается в оформлении прав всех пользователей для того, чтобы система могла начать функционировать и корректно предоставлять пользователям права в информационной системе.
Возможность настройки полномочий в нетипичных ситуациях также характеризует качество системы разграничения доступа. Например, должны ли руководители разных отделов иметь доступ к информации, относящейся к ведению другого отдела? Должен ли бухгалтер иметь доступ к файлу паролей, который, относится к ведению службы безопасности? И наоборот, должен ли администратор безопасности информационной системы иметь доступ к файлу с ведомостью на получение заработной платы сотрудников? Должен ли пользователь быть допущен к информации или нет, зависит от решения того, кто имеет полномочия на разделение прав доступа. Возможность реализации на практике прав доступа зависит от того, какая система разграничения доступа была выбрана. Некоторые модели позволяют более тонкие настройки прав пользователей, а некоторые - нет.

Ещё одно важное качество, которое влияет на удобство системы разграничения доступа - это удобство добавления нового субъекта или объекта. Под субъектом здесь подразумевается пользователь ин-

формационной системы, а под объектом - файл или иной информационный ресурс.

После того, как субъект благополучно пройдёт процедуру авторизации, то есть получит доступ к тем полномочиям, которые предоставлены ему в системе, контроль его подлинности не осуществляется. Как правило, такая процедура проходится единожды. Но, иногда, может потребоваться дополнительное подтверждение подлинности субъекта, и это является хорошим решением.

Система разграничения доступа без использования других средств защиты информации, не ограничивает действия привилегированных пользователей, например, администраторов безопасности и тех сотрудников, службы безопасности, которые производят настройку системы разграничения доступа и имеют полномочия предоставлять права другим пользователям.

Разграничение доступа, как правило, строится на одном из трёх следующих принципиальных подходов: дискреционное разграничение доступа, мандатное разграничение доступа и ролевое разграничение доступа.

Дискреционная модель

Дискреционная модель основывается на разграничении доступа с использованием поименованных субъектов и объектов на основе установленных прав доступа для каждой пары. В основе работы модели лежит формирование так называемой матрицы прав доступа. Строки и столбцы данной матрицы соответствуют субъектам и объектам, а на их пересечении находятся права, которые субъекты имеют по отношению к объектам. Например, субъект может обладать только правом чтения или правами на чтение и запись, либо может иметь какие-то другие наборы прав. В большинстве случаев субъекту выдается признак наличия или отсутствия права доступа, например, ноль или единица.

Каждый из пользователей обращается к системе разграничения доступа через сервер авторизации для того, чтобы осуществить попытку доступа к какому-либо объекту в информационной системе. Сервис авторизации, который, принимает решение о том, обладает ли пользователь правами на получение запрашиваемого объекта, обращается к базе данных, в которой хранится матрица доступа. Матрица содержит строку, в которой записан идентификатор пользователя, и в одном из столбцов — название того объекта, к которому пользователь желает обратиться. Если на пересечении строки и столбца нахо-

дится информация о том, что данный пользователь действительно имеет право для реализации такого доступа, то доступ предоставляется, в противном случае в доступе будет отказано.

Данная модель имеет следующие достоинства:

- Индивидуальная настройка прав для каждого пользователя;
- Для каждого объекта можно настроить права доступа, то есть ту группу субъектов, которая будет иметь к ним доступ.

Индивидуальная настройка прав для каждого пользователя доступна за счет того, что заполняется полная матрица соответствия субъектов и объектов. Например, в модели с двумя начальниками двух отделов можно настроить для каждого из них нужный уровень доступа к тем или иным файлам, относящимся к ведению их отделов, и не предоставлять им прав на доступ к файлам других отделов. При настройке для каждого объекта прав доступа не будет образовываться зависимость между сходством в уровне секретности объектов или в должностном уровне субъектов. Например, два системных администратора, могут иметь совершенно разный набор прав доступа к объектам, например, на основе их опыта, или на основе их должностных обязанностей.

Недостатком модели является то, что для реализации модели требуется полностью заполнить матрицу субъектов и объектов в каждой ее ячейке - на пересечении каждого столбца и каждой строки установить конкретные права доступа данного субъекта к данному объекту. Из этого следует, что для добавления нового субъекта или объекта требуется заполнить все элементы соответствующей строки или столбца матрицы доступа. При добавлении нового субъекта, появляется строка, в которой нужно прописать права его доступа ко всем существующим объектам. А, при добавлении нового объекта, для всех субъектов, которые описаны в системе, требуется установить их права доступа к новому объекту.

Мандатная модель разделения доступа

Мандатная модель основана на использовании так называемых меток конфиденциальности объектов и уровней допуска субъектов. Метка конфиденциальности - это присваиваемый объекту информационной системы уровень конфиденциальности, устанавливающий его место в иерархии уровней доступности объектов. Например, в организации могут быть установлены четыре типа меток конфиденциальности - несекретная информация, информация только для служебного пользования, секретная и совершенно секретная информация.

Это подразумевает, что вся информация в системе иерархически структурируется на четыре уровня доступности. Это и есть метка конфиденциальности - принадлежность того или иного объекта к одному из уровней доступа. Соответственно, для субъектов вводится понятие уровня допуска. Это такой уровень конфиденциальности, к объектам с метками конфиденциальности не выше которого субъект имеет доступ. Например, если субъект имеет уровень доступа «для служебного пользования», то он получает доступ ко всем объектам с метками секретности «не секретно» и «для служебного пользования», но при этом не имеет доступа ни к каким объектам с иными метками. Например, в компании есть работники, которые имеют одинаковую должность. Следовательно, каждый из них получит одинаковый уровень доступа ко всем объектам системы, так как они получат одинаковый уровень допуска. Это означает, множество тех объектов, к которым они фактически будут иметь доступ, будет абсолютно одинаковым.

Для того, чтобы определить, может ли тот или иной пользователь получить доступ к объекту, сравнивается уровень допуска пользователя и метка конфиденциальности объекта. Если уровень допуска не уступает метке конфиденциальности, то доступ предоставляется. Например, если пользователь с уровнем допуска «секретно» пытается обратиться к объекту с меткой конфиденциальности «для служебного пользования», то доступ будет предоставлен. А пользователь, обладающий более низким, чем «для служебного пользования», уровнем допуска, получает отказ в доступе к данном объекту.

Достоинством данного метода является то, что для его реализации достаточно установить каждому объекту метку конфиденциальности, а каждому субъекту - уровень допуска. Это будет происходить намного проще и быстрее, чем полное заполнение матрицы для каждой пары субъект-объект. Из этого следует, что добавление нового объекта или нового субъекта не требует дополнительного редактирования прав других субъектов или объектов. Если в системе появляется новый субъект, ему устанавливается уровень допуска. Если появляется новый объект, ему приписывается метка конфиденциальности - и никаких других действий в системе не требуется.

Недостатком данного метода является то, что доступ к объектам одного уровня секретности предоставляется или ограничивается совместно. Нет возможности разделить всё множество объектов с уровнем секретности, например, «для служебного пользователя» на под-

множество, доступное одному начальнику отдела, и подмножество, ему недоступное.

Ролевая модель разделения доступа

Ролевая модель, как следует из ее названия, основывается на так называемых ролях субъектов информационной системы. Под ролью в данной модели подразумевается совокупность прав доступа субъекта к объектам информационной системы. То есть существует определенное фиксированное значение этих прав доступа субъекта, которое единожды сохраняется и именуется каким-то названием. Например, может быть роль «системный администратор». В этом случае существует некий набор прав, который является стандартным для системного администратора. Так же в системе может присутствовать роль начальника отдела, роль оператора, роль бухгалтера. Каждой роли, по аналогии с дискреционной системой разграничения доступа, присваивается набор прав доступа к различным объектам системы.

Такой подход имеет ряд достоинств:

- Добавление нового субъекта не требует заполнения строки матрицы при наличии подходящей роли;
- Количество ролей ничем не ограничено;
- Роль не предполагает полного нисходящего предоставления доступа к объектам информационной системы.

Для того, чтобы добавить нового пользователя в информационную систему, по сравнению с дискреционной моделью разграничения доступа уже не требуется полностью заполнять всю строчку его прав доступа ко всем объектам в информационной системе, которых может быть очень большое количество. Неограниченное количество ролей дает возможность создавать специальные роли, например, начальника конкретного отдела или помощника начальника конкретного отдела. В отличие от мандатной модели разделения доступа, ролевая модель не предполагает полного нисходящего предоставления доступа к объектам информационной системы. Например, администратору можно предоставить доступ к файлу с уровнем секретности, который в мандатной модели имел бы метку конфиденциальности «секретно», но при этом относится, допустим, к вопросам администрирования информационной системы. И при этом не предоставить ему права доступа к тем объектам, которые в мандатной модели имели бы более низкие метки конфиденциальности. Роль вполне это допускает. Полное нисходящее предоставление доступа к объектам не предполагается.

Недостатком является то, что если для каждого субъекта требуется отдельная роль, то разграничение доступа станет аналогичным дискреционной модели, и необходимость в ролях может отпасть. Если доступ предоставляется к отдельным объектам, а не группам объектов, то добавление нового объекта аналогично дискреционной модели. В классической ролевой модели о группировании объектов речи не идет. Создаются роли для субъектов, а объекты, описываются независимо отдельными строками в этой матрице. По сути, речь идет о формировании такой матрицы, где каждой строкой является не субъект, а роль. Ролевая модель имеет смысл, если под одну роль подходит более одного субъекта.

Заключение

В данной работе была произведен обзор методов разделения доступа в информационных системах. Были рассмотрены основные модели разделения доступа: дискреционная, мандатная и ролевая. Были выявлены их достоинства и недостатки.

Данные подходы будут реализованы в виде программного кода и станет частью информационной системы, развёрнутой в ГБОУ ВО МО «Технологический университет».

Список используемых источников

1. Васильков А.В. Безопасность и управление доступом в информационных системах / А.В. Васильков, И.А. Васильков. - Москва : ФОРУМ: ИНФРА-М, 2013.- 368 с.

2. Мельников В.В. Безопасность информации в автоматизированных системах / В.В. Мельников.- Москва : Финансы и статистика, 2003.- 368 с.

3. Зегжда Д. П. Основы безопасности информационных систем / Д.П. Зегжда, А.М. Ивашко.- Москва : Горячая линяя - Телеком, 2000.- 452 с.

4. Малюк А.А. Введение в защиту информации в автоматизированных системах / А.А. Малюк, С.В. Пазизин, Н.С. Погожин.- Москва : Горячая линия - Телеком, 2001.- 148 с.

ПРОЕКТИРОВАНИЕ БЕСПРОВОДНОЙ ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ ДЛЯ КОМПЛЕКСА ЗДАНИЙ. АНАЛИЗ И СРАВНЕНИЕ МЕТОДОВ И СРЕДСТВ

Солодухин И. В., магистр группы ИМО-ПИ-21
Пушкарев П.В., магистр группы ИМО-ПИ 21,
Технологический университет («МГОТУ»),
Россия, г. Королев

Рассмотрены и проанализированы вопросы, связанные с анализом и сравнением методов и средств проектирования беспроводной локальной вычислительной сети для комплекса зданий. Раскрыты основные требования к сети и предложены решения, позволяющие построить беспроводную локальную вычислительную сеть (ЛВС), соответствующую этим требованиям.

Ключевые слова: Локальная вычислительная сеть, беспроводная сеть, проектирование, сравнение.

Введение. Особенности анализа и применения методов и средств проектирования беспроводной локальной вычислительной сети для комплекса гипотетических зданий заключается в совмещении нескольких методов проектирования [1 – 3]. Пусть в разрабатываемой ЛВС имеется большое количество клиентских компьютеров и периферийных устройств, которые требуется соединить в одну беспроводную сеть, а также требуется установить систему видеонаблюдения, которая будет замкнутой. В связи с наличием указанной системы требуется соответствующее серверное оборудование. Требуется спроектировать сеть с централизованной структурой, повышенной отказоустойчивостью (количество различных сбоев требуется свести к минимуму) и отсутствием перегрузок даже при условии, что большинство устройств будут обмениваться данными в конкретный промежуток времени. Нужно спроектировать сеть, которая будет соответствовать требованиям. В данной работе мы рассмотрим основные средства для проектирования такой сети и сравним их.

Обзор и сравнение существующих технологий для построения беспроводной сети.

Сеть внутри зданий. Рассмотрим основные требования к сети:

1) Масштабируемость. В некоторых кабинетах есть пространство для установки еще одного рабочего места. Нужно учесть возможность такого расширения.

2) Централизованная структура. Обеспечить наличие центрального устройства для управления обменом данных.

3) Наличие выхода в Интернет, однако также требуется надежная фильтрация трафика.

Первый шаг в проектировании – выбор технологий, на которых будет основана беспроводная сеть. Основная технология для построения сети внутри зданий (в эту сеть будут включены компьютеры) – *Wi-Fi*. Имеется два основных частотных диапазона, с помощью которых можно реализовать сеть – 2, 4 ГГц и 5 ГГц.

Диапазон 2, 4 ГГц более популярен, но в этом и его минус. На сегодняшний день этот диапазон очень загружен и имеет не так много каналов (их всего 14, но 14 канал разрешен к применению только в Японии), и если точек много, то построение Wi – Fi сети, не имеющей пересекающихся каналов, будет проблемой. Диапазон частот каждого канала с указанием его центральной частоты показан на рис. 1.

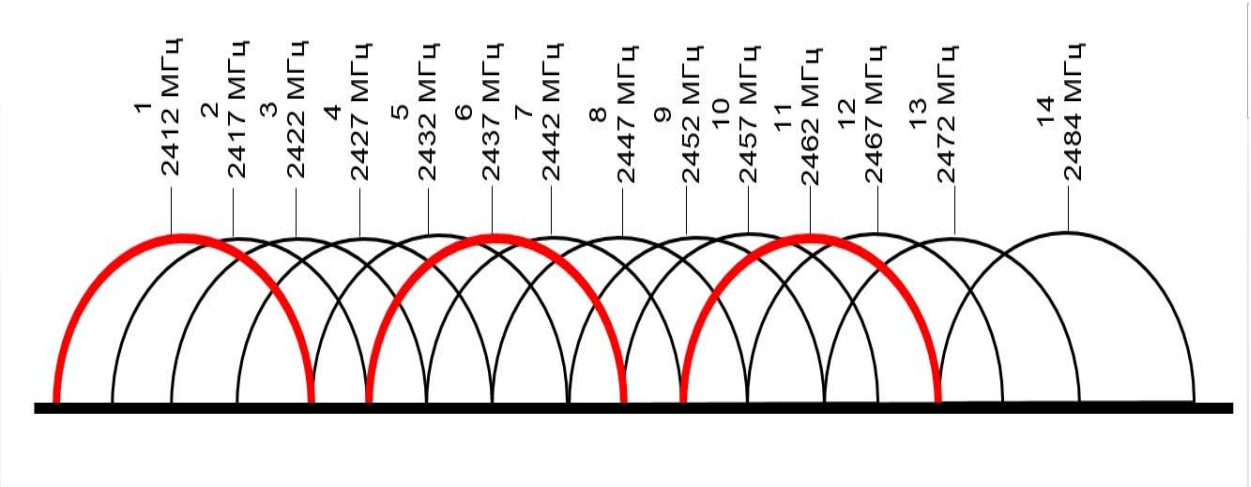


Рис. 1. Распределение частот по каналам

Устройства в этом диапазоне с большей вероятностью будут мешать друг другу. А также, есть много устройств, которые работают в том же диапазоне (например, Bluetooth – устройства). Из этого вытекает еще один недостаток – низкая помехоустойчивость.

Диапазон 5 ГГц не так распространен, и устройства, которые могут его поддерживать, сложнее найти. Стоить они будут дороже. Но взамен мы получаем большее количество каналов и повышенную скорость передачи данных, а это критично для нашей сети. Имеется 23 неперекрывающихся канала по 20 МГц, но большинство из них можно использовать только, если на Wi-Fi роутер поддерживает динамический выбор частот. Однако, даже среди доступных по умолча-

нию каналов есть 4 непересекающихся. Итак, сравнив два вышеуказанных диапазона, можно утверждать, что диапазону 5 ГГц стоит отдать предпочтение при проектировании текущей ЛВС. Расположение всех каналов и частотное распределение показано на рис. 2.

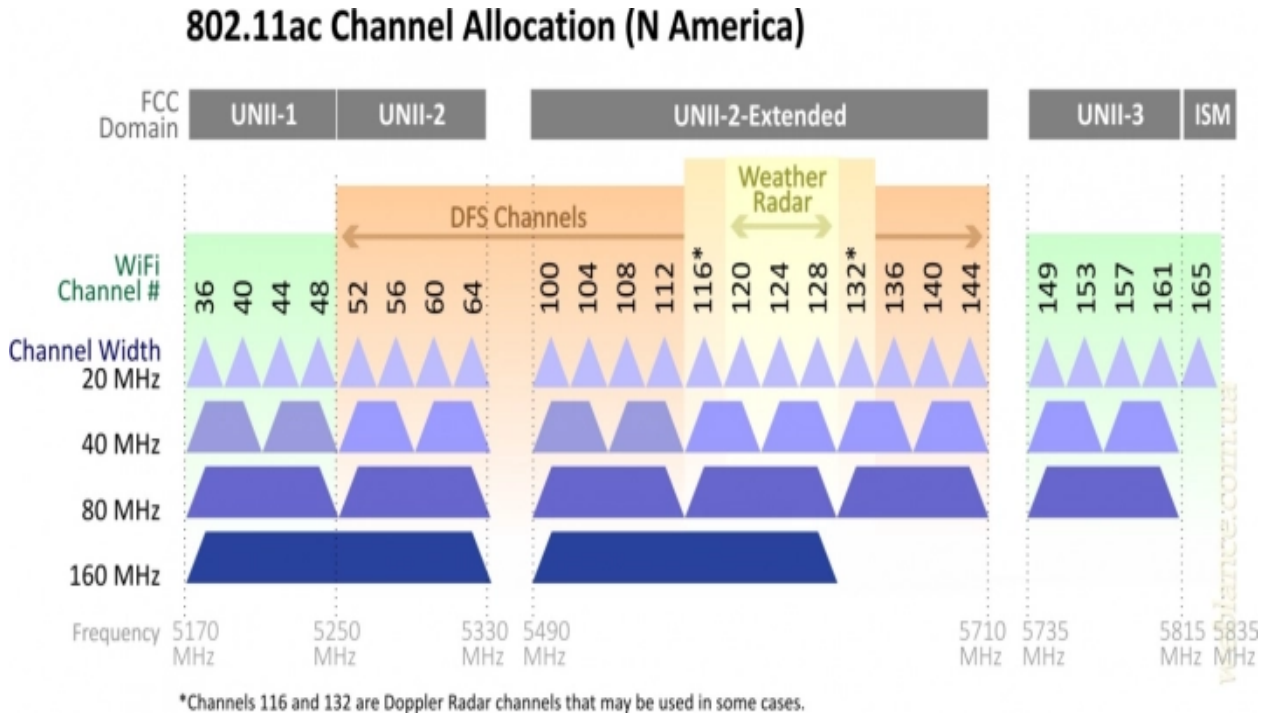


Рис. 2. Частотное распределение в диапазоне 5 ГГц

Соединение беспроводных точек доступа. В нашей сети для лучшего покрытия, а также из – за наличия множества бетонных перекрытий в здании (они сильно гасят сигнал), требуется установить несколько точек доступа. Этими точками лучше всего управлять (и настраивать их) из единого центра. Для этого существуют три решения:

- Кластеризация точек доступа. В данном случае от нас требуется настройка лишь одной точки доступа. Она будет играть роль главной (сервера). Остальные точки, подключенные к ней, скопируют с нее конфигурацию и будут подчиненными. То же самое происходит при обновлении конфигурации. Примерный вариант кластерного соединения представлен на рис. 3.

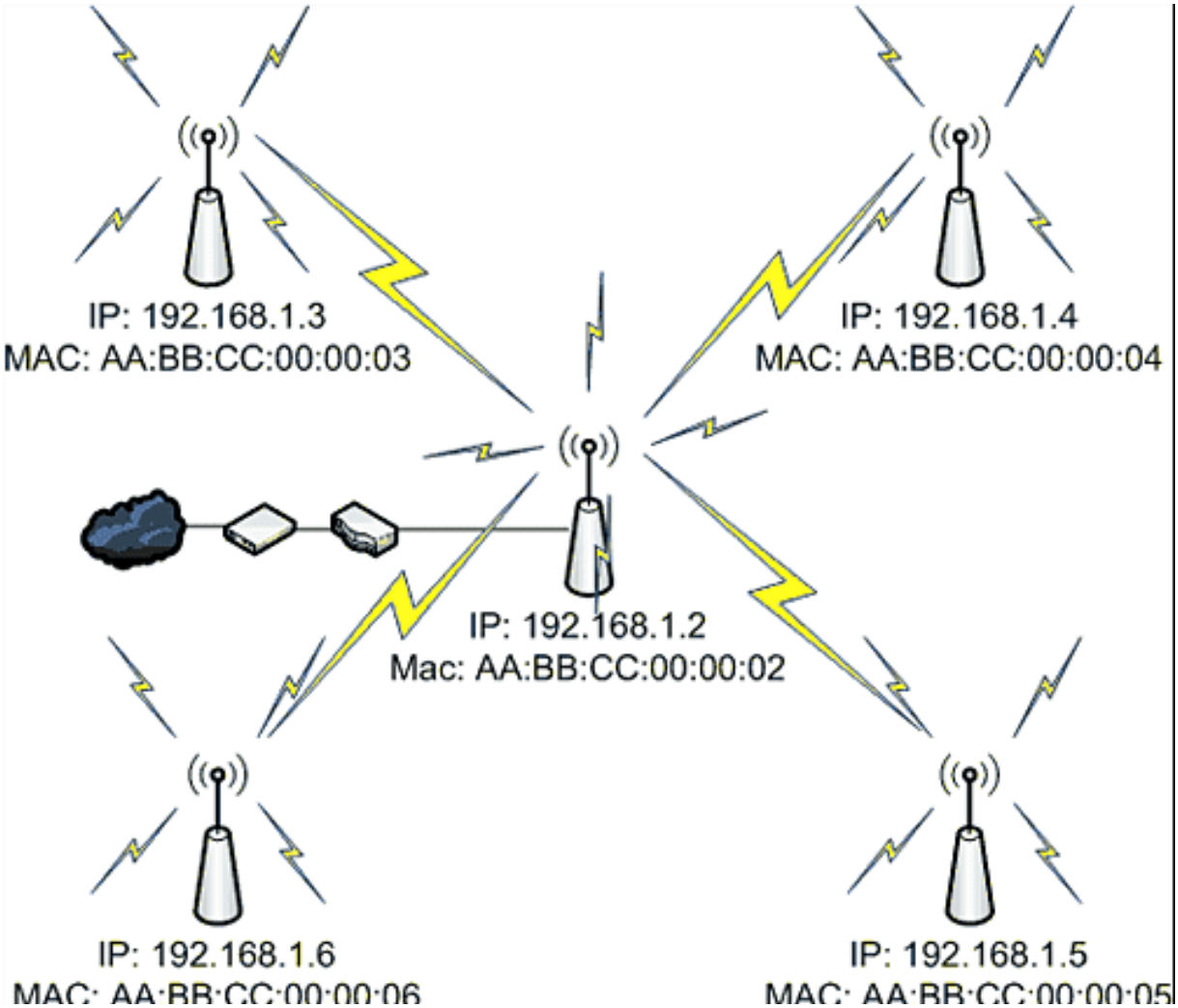


Рис. 3. Примерный вариант кластеризации точек доступа

Однако кластер можно собрать только из идентичных моделей. Если нужная модель исчезнет с рынка, мы не сможем расширить сеть. Также, если нам нужно изменить отдельно параметры главной точки, то нам нужно вывести ее из кластера.

- Программа для управления точками доступа. Отдельное приложение на персональном компьютере (ПК) (сервере). Здесь не существует приоритетов, как в предыдущем случае, и точки можно настраивать по отдельности. Однако, нужно помнить, что с компьютером также могут возникнуть проблемы. Нужен источник бесперебойного питания, чтобы компьютер мог работать в режиме 24/7. Есть риски несовместимости программного обеспечения (ПО), а также возможность появления «синего экрана» после неудачного обновления.

- Аппаратный контроллер точек доступа. Чаще всего – отдельное устройство, включаемое в общую кабельную сеть и являющееся главным для беспроводной сети. Примерный вид такого устройства (выглядит как обычный коммутатор) показан на рис. 4.

Рис. 4. Аппаратный контроллер точек доступа

Конфигурация всех точек доступа будет храниться в одном устройстве. Это устройство будет несложно заменить, если есть резервная копия данных. На некоторых моделях (например, модели от Zyxel) предусмотрена возможность отправки резервной копии конфигурации на электронную почту. Можно выбрать несколько адресов получателей и отправлять туда файлы резервных копий с заранее выбранной периодичностью (ежедневно, еженедельно или ежемесячно). Примерный интерфейс управления контроллером показан на рис. 5.

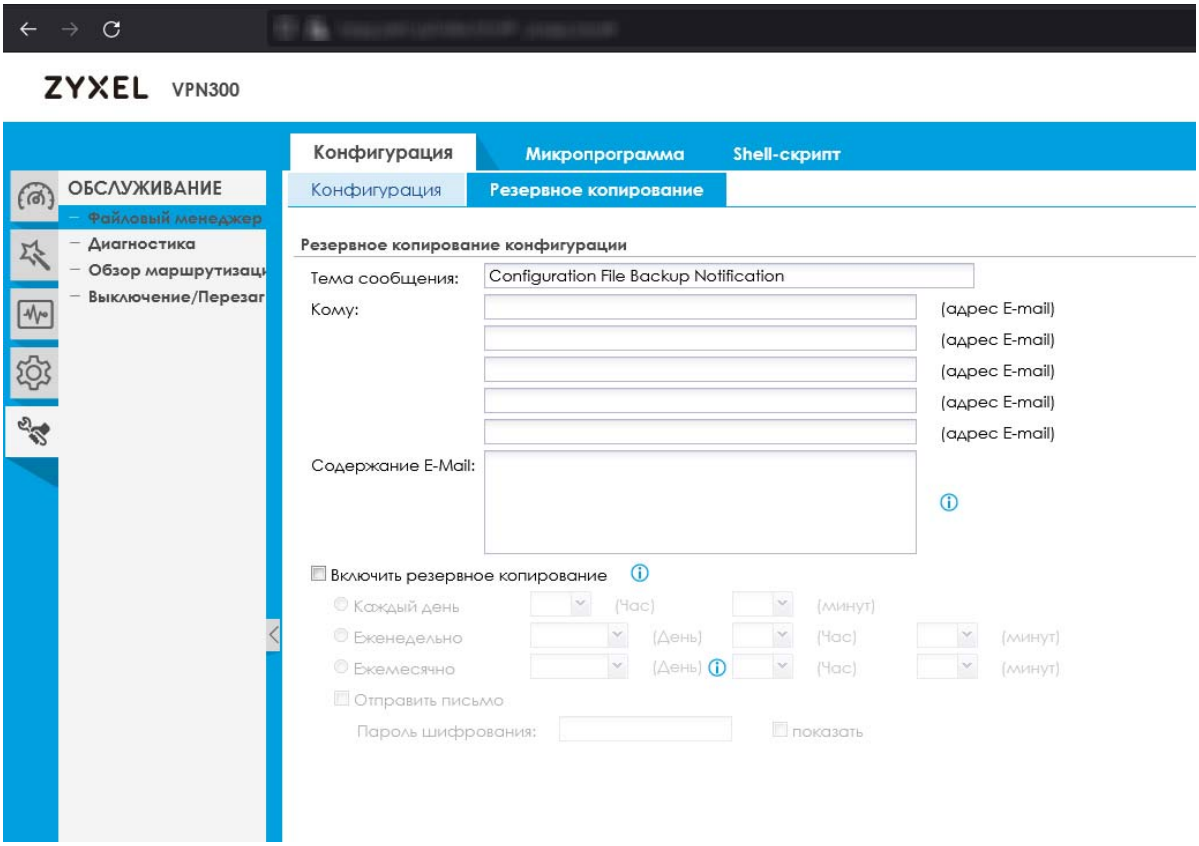


Рис. 5. Интерфейс аппаратного контроллера

Аппаратный контроллер не привязан к моделям точек доступа. Единственная проблема – возможность прекращения поддержки того или иного устройства. Выбрав этот вариант, мы сможем беспрепятственно расширять сеть в течение 7 лет. Это наилучшее решение из всех вышеуказанных.

Связь между корпусами. Ввиду невозможности прокладки оптоволоконного кабеля, нам требуется связать два корпуса предприятия с помощью одной из беспроводных технологий. Расстояние между зданиями - 250 метров. Технология Wi – Fi не действует на расстоянии свыше 100 метров. Именно поэтому данный вариант отметается.

Второй вариант – радиомост. Создается за счет отдельных устройств с узконаправленными антеннами. С помощью них можно передать данные на большое расстояние (до 20 км в зависимости от устройства). На рисунке 6 показан пример соединения двух зданий при помощи радиомоста. В данном случае имеется прямая видимость между зданиями, что и позволяет организовать соединение. Однако в городе таких условий может не быть ввиду большого количества зданий и их плотности (рис. 6).

Рис. 6. Соединение зданий при помощи радиомоста

Данные устройства обеспечивают нужный частотный диапазон, но скорость передачи достаточно низкая для наших условий – 150 Мбит/с. Такой скорости не хватит для большого количества устройств. При одновременном их подключении может случиться перегрузка.

Вариант №3 - FSO (Free Space optics) или атмосферная оптическая линия связи. Представляет собой два устройства (приемник и передатчик), между которыми передается сигнал в виде узконаправленного луча в инфракрасном диапазоне. Расстояние не такое боль-

шое, как у радиомоста (1, 25 км с усиленной мощностью), однако скорость гораздо выше – вплоть до 10 Гбит/с. Примерная схема соединения FSO показана на рис. 7.

Рис. 7. Соединение FSO

На нашем расстоянии вполне способна работать на скорости 1 Гбит/с, имея высокий коэффициент доступности – 0,999, в соответствии с табл. 1.

Таблица 1. Зависимость дальности связи от коэффициента доступности

Коэффициент доступности	Дальность связи, м
0,99	До 1500
0,997	До 700
0,999	До 300
0,9999 (имеется резервный канал)	До 1900

Работа этих устройств зависит от погодных условий (при сильном тумане или задымленности есть риск проблем с соединением) и, кроме того, они требовательны к монтажу. Нужна не просто прямая видимость, а возможность направить устройства точно друг на друга. Ввиду того, что лазерный луч очень узкий, даже небольшое отклонение недопустимо. Также недостатком может стать высокая стоимость оборудования. Однако, как было сказано выше, при правильном монтаже и точной подстройке оборудования, мы получим высокую скорость передачи и хорошие показатели доступности. А это значит, что, сравнив все вышеуказанные варианты, можно отдать предпочтение технологии FSO.

Заключение. В данной работе мы проанализировали некоторые существующие технологии, которые могут применяться для построения беспроводных ЛВС. Были раскрыты требования к проектируемой сети, на основе этих требований было проведено сравнение, и выбраны технологии, позволяющие нам реализовать сеть, которая будет работать стабильно на протяжении долгих лет.

Список использованных источников

1. Введение в структурированные кабельные системы / А.Б. Семенов, В.М. Артюшенко, Т.С. Аббасова: учебное пособие/ под ред. д. т. н., профессора Семенова А.Б. –М.: Издательство «Научный консультант», 2018. – 204с.

2. Информационные технологии и вычислительные системы / Под ред. С.В. Емельянова. - М.:Ленанд, 2019. – 104 с. – ISBN 978-5-9710-0207-9.

3. Шилкин, В. В. Организация зон беспроводного доступа по технологии Wi-fi к информационным ресурсам ЛВС и сети интернет / В. В. Шилкин, Б. П. Борисов // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. – 2012. – № 1. – С. 159-162.

СБОР И АНАЛИЗ ТЕХНИЧЕСКИХ ДАННЫХ ПРИ РЕАГИРОВАНИИ НА КОМПЬЮТЕРНЫЕ АТАКИ

Дуров Д.К., магистр, гр, ИМО-ПИ-21,
Азовцев А.А., магистр группы ИМО-ПИ 21,
Технологический университет («МГОТУ»),
Россия, г. Королев

В статье были проанализированы нормативные источники, регулирующие деятельность и порядок реализации защиты от действия компьютерных атак и при реагировании на них.

Ключевые слова: компьютерная атака, государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак, автоматизированная система, программное обеспечение, операционная система.

Понятие компьютерных атак, классификации, правовое регулирование. Активное развитие компьютерных технологий началось во второй половине 20 века, наравне с этим распространилась и хакерская деятельность. Число киберпреступлений, а также попыток их совершения, растет с каждым годом в геометрической прогрессии. Этому свидетельствуют финансовые потери, утечки информации крупных организаций. Однако специалистов в этой области достаточно мало, а количество открытых ресурсов и пособий по взломам растет. Стоит заметить и тот факт, что на данный момент не существует абсолютно защищенной системы, учитывая, что человек всегда является ее звеном. Исходя из этого, представляется, что тема, связанная с исследованием компьютерных атак всегда будет актуальной.

Стоит отметить, что противоправная деятельность хакеров наказуема в связи со статьями главы 28 Уголовного кодекса. Хакеры реализуют преступную деятельность путем поиска уязвимостей, то есть свойств информационной системы, обусловливающих возможность реализации угроз безопасности, обрабатываемой в ней информации. Угроза безопасности информации реализуема, если есть недостаток или слабое место в информационной системе. Поиск рассматриваемых уязвимостей и использование в корыстных целях реализуется посредством КА. Понятие «компьютерной атаки» содержится в ГОСТе Р 51275-2006 и определяется как целенаправленное несанкционированное воздействие на информацию, на ресурс автоматизи-

рованной информационной системы или получение несанкционированного доступа к ним с применением программных или программно-аппаратных средств . Исходя из определения, КА является таковой при соответствии основным критериям: целенаправленное и несанкционированное воздействие на информацию или ресурс; или несанкционированный доступ к информации и ресурсам; использование при этом программных или программно-аппаратных средств.

При этом понятие «целенаправленный» обозначает активную направленность на совершение КА, отсюда следует умышленность действий правонарушителя. Несанкционированный доступ осуществляется тогда, когда лицо нарушает установленные правила и права, в результате чего может увидеть или прочитать какую-либо информацию. Если же рассматривать воздействие на информацию или ресурс, то это нарушение установленных прав или правил доступа, приводящее к утечке, искажению, подделке, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации. При этом воздействие всегда целенаправленное и умышленное. Третий критерий предполагает использование при доступе или воздействии на информацию или ресурс специальных средств, настольных компьютеров, ноутбуков, других устройств с возможностью их программирования.

На данный момент, существует достаточно большое количество классификаций КА, рассмотрим самые распространенные, выделяют следующие основания классификаций: по направленности и последствия; по объекту воздействия; по средствам воздействия.

По направленности и последствиям КА подразделяются на 3 типа. Нарушающие конфиденциальности информации, реализуемое через получение доступа, хищение или разглашение. Второй тип - нарушающие целостность информации, то есть любая несанкционированная модификация, включая изменение части или всей информации, так же ее уничтожения. И третий тип заключается в нарушении доступности информации для законных пользователей, то есть блокирование информации, нарушение нормального функционирования, вывод из строя компонентов компьютерной системы – технических средств и программного обеспечения.

Следующая классификация разделяет КА в зависимости от объекта воздействия: информация, процессы обработки, программное обеспечение, технические средства и коммуникации. Чаще всего, конечным объектом воздействия является информация, доступ к кото-

рой может осуществляться с помощью специальных средств и методов посредством использования программных, аппаратных уязвимостей. Понятие «информации содержится в законодательстве и определяется как сведения (сообщения, данные) независимо от формы их представления. Информация не всегда находится в статичном состоянии, информация может действовать в рамках каких-либо процессов: в процессе обработки и в процессе передачи по сетям. Тогда источником действия атаки становятся вышеназванные процессы, чаще такие атаки связаны с перехватом данных.

Еще одним объектом воздействия КА может быть программное обеспечение. Компьютерная программа - представленная в объективной форме совокупность данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств в целях получения определенного результата, включая подготовительные материалы, полученные в ходе разработки программы для компьютера, и порождаемые ею аудиовизуальные отображения. Воздействие на программу реализуется также с целью доступа к информации или же для блокирования ее действия, что приводит деятельность к простою.

КА могут реализовывать вредоносное воздействие на технические средства. Это могут быть устройства обработки и хранения информации дисководы, терминалы, оперативная память, процессоры или вспомогательные (обеспечивающие) технические средства, такие как источники электропитания, технические средства контроля доступа, кондиционеры. Особенно актуальным стала реализация воздействия на SMART-устройства, которые подключены к сети и управляются удаленно, тогда становится возможным подключиться к каналам связи для дальнейшей модификации сигнала под нужен нарушителя. Последним элементом КА являются устройства и средства коммуникации: телекоммуникационные каналы и устройства, телефонные линии, модемы, коммутаторы, маршрутизаторы.

Актуальной представляется и классификация по средствам воздействия, то есть, если в предыдущей классификации были объекты воздействия, то в данном случае опора будет именно на средства реализации. Таким образом, выделяют воздействие с помощью технических средств, программных средств, с помощью специализированных или штатных инструментов. Под техническими средствами понимаются совокупность систем, машин, приборов, механизмов, устройств и прочих видов оборудования, предназначенных для автоматизации различных технологических процессов информатики [9], это могут

быть различные считыватели информации, блокираторы и т.д. Также существуют программные средства реализации КА, то есть совокупность кода и процедур, направленных на реализацию вредоносного действия, например, вирусы.

При этом для совершения КА могут быть использованы как штатные средства, то есть создаваемые без цели конечного вредоносного действия, как и специализированные под взломы. Стандартными средствами может явиться программное обеспечение, используемое в компьютерных системах: редакторы, утилиты, отладчики, почтовые системы, анализаторы протоколов и т.д. А специализированными, например, вирусы, «троянские кони», программы подбора паролей и т.д.

Компьютерным атакам может быть подвержена любая компьютерная система: частная или государственная. Статистика, представленная на сайте Positive Technologies, свидетельствует о том, что количество уникальных киберинцидентов в 2020 году выросло на 51% по сравнению с 2019 годом. Семь из десяти атак носили целенаправленный характер. Наиболее интересные отрасли, по мнению злоумышленников, — это государственные и медицинские учреждения, промышленные предприятия [10]. Помимо этого, можно предположить, что на данный момент между некоторыми государствами идет кибервойна. Уменьшить негативные последствия от этого может грамотная систематизация и регламентация действий в области защиты информации. В России, на данный момент, действует ряд документов, затрагивающий вопрос информационной безопасности, также действуют и международные документы. Среди документов в России можно выделить:

– Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ;

– Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 N 187-ФЗ;

– Указ Президента РФ от 22.12.2017 N 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»;

– Приказ ФСБ России от 06.05.2019 N 196 «Об утверждении Требований к средствам, предназначенным для обнаружения, преду-

преждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты» и другие законодательные акты.

На данный момент существуют также ГОСТы с терминологией по исследуемой теме, такие как ГОСТ Р 51275-2006, ГОСТ Р 50922-2006. Однако в связи с давностью их введения, они требуют дополнения, и в августе 2020 года был выложен проект нового ГОСТа «Защита информации. Обнаружение, предупреждение и ликвидация последствий компьютерных атак и реагирование на компьютерные инциденты. Термины и определения», который еще не вступил в силу.

Большее значения для регулирования инцидентов компьютерных атак играют национальные стандарты и методические рекомендации. В этом году произошло обновление документов по оценке сетей на уязвимость, так как прежняя методика не обновлялась с 2008 года. Поэтому на сегодняшний день, вступила в действие другая методика, утвержденная Федеральной службой по техническому и экспертному контролю 5 февраля 2021 – «Методика оценки угроз безопасности информации», которая является важным методическим документом для реализации компьютерной безопасности.

Методика определяет порядок и содержание работ по выявлению угроз безопасности информации, реализация (возникновение) которых возможна в информационных системах, автоматизированных системах управления, информационно-телекоммуникационных сетях, инфраструктурах центров обработки данных и облачных инфраструктурах, а также по разработке моделей угроз безопасности информации систем и сетей.

Важным толчком в развитии государственной компьютерной безопасности явился выход в октябре 2019 года Постановление Правительства о создании отраслевого центра ГосСОПКА и включение его в систему автоматизированного обмена информацией об актуальных киберугрозах. ГосСОПКА выполняет четыре основные задачи:

– прогнозирование ситуации в области информационной безопасности России;

– взаимодействие организаций-владельцев информационных ресурсов (в том числе субъектов критической информационной инфраструктуры);

– контроль защищённости информационных ресурсов от кибератак;

– расследование компьютерных инцидентов [11].

Таким образом, ГосСОПКА на данный момент является стратегически важным федеральным органом исполнительной власти по реализации кибербезопасности страны.

В результате вышеизложенного, можно сделать вывод о том, что исследование КА является актуальной темой, так как угрозе совершения киберпреступления подвержены частные лица, организации и государство, что приносит огромные убытки, простои и утечки информации. Об этом свидетельствует статистика, постоянно развивающиеся технологии, а также активное формирование законодательного регулирование, которого за последние года в рассматриваемой области стало в несколько раз больше. Необходимым для темы исследования является изучение не только теоретических сведений и законодательного регулирования, а также и практические способы по предотвращению и исследованию КА.

Механизм и модели компьютерных атак на теоретическом уровне. Для исследования того, как защищать компьютерные системы от атак, необходимо понимать механизм их реализации. Это поможет в большинстве случаев их избежать, а также вовремя и правильно среагировать на критические обстоятельства. Стоит заметить, что каждый отдельно взятый вид атаки имеет собственный механизм реализации, однако, основные этапы действий киберпреступников можно обобщить. Таким образом, можно выделить 3 тапа реализации компьютерной атаки:

1. Подготовительный этап;
2. Практический этап;
3. Завершающий этап.

На первом этапе осуществляется изучение компьютерной системы. В рамках этого действия реализуется анализ системы защиты и поиск уязвимостей компьютерной системы. К наличию уязвимостей в системе может приводить большое количество факторов, например, ошибки при проектировании, реализации и эксплуатации программно-аппаратного комплекса, несанкционированные действия пользователей в рамках системы, сбои в работе оборудования и другие.

При этом можно определить три вида уязвимостей: субъективные, объективные и случайные. Появление субъективных уязвимостей связано с действиями человека, например, разработчиков или системных администраторов. Сюда входят такие действия сотрудников как нарушение эксплуатации оборудования, что вызывает его перебои, ошибки при разработке программного обеспечения т.д. Объек-

тивные причины основываются на особенностях построения и технических характеристиках оборудования и программных средств, например, использование каналов связи потенциально доступных снаружи охраняемых объектов или побочные излучения, нарушающие работу других устройств. И последний вид уязвимостей – случайные, обуславливающиеся непредвиденными обстоятельствами, такие как неисправность оборудования или размагничивание носителей информации [12].

От определения уязвимостей зависят дальнейшие действия взломщиков, а точнее то, каким образом будет проходить планирование атаки. На данной стадии определяется способ и каналы воздействия на компьютерную систему, а также выбор и подготовка средств воздействия.

Следующий этап практический. В данном случае злоумышленник посредством специальных средств получает несанкционированных доступ к компьютерной системе. Это действие может осуществляться посредством преодоления системы защиты или же использования легальных полномочий. Достаточно часто бывают ситуации, что взломщиком оказывает сотрудник организации. Например, в 2019 году работник ПАО «Вымпелком», используя свое служебное положение, ознакомившаяся с нормативными документами и требованиями по информационной безопасности, умышленно из корыстной заинтересованности, не имея соответствующего заявления клиента, выбрала абонентский номер, зарегистрированный на Фур Ю.В., подделав заявление клиента на замену СИМ-карты, произвела перевыпуск СИМ-карты и произвела модификацию компьютерной информации, получив возможность пользоваться счетом с находящимися на нем деньгами и совершила ряд покупок [17].

Этот пример характеризует и следующий шаг после получения доступа к системе – осуществление задач взлома. Хакеры могут преследовать абсолютно разные цели и мотивы. Чаще всего, КА осуществляется для хищения какой-либо защищаемой законом информации. Данная цель особо актуальна в разрезе доступа к государственной критической информации, все чаще в сети Интернет появляются громкие заявления о получении хакерами стратегических данных правительств разных стран. Другой целью хакеров может явиться модификация информации. Хакеры могут взламывать системы с целью нарушения ее работоспособности, данные действия приводят к простоям организаций.

На завершающем этапе проходит маскировка следов совершения преступления. Хакер может совершать действия по скрытию своей личности путем модифицирования или уничтожения данных. Часто, если преступление совершается сотрудниками организации, они пытаются подделать целенаправленный взлом под неумышленное воздействие. Стоит заметить, все приведенные этапы далеко не всегда присутствуют в реальных ситуациях, их количество убывает со снижением сложности компьютерной системы и степени «разумности» угрозы.

Для более детального изучения механизма реализации компьютерных атак используются методы моделирования. Наиболее популярные типы моделей атак табличные и матричные модели, логические модели, модели, основанные на графах, а также модели, использующие объектно-ориентированный подход. Наиболее распространенными являются модели атак, основанные на графах. Под графом атак понимается граф, содержащий все известные траектории реализации нарушителем угроз с вероятностями их наступления. На основе модели ведется анализ инцидентов, обнаружение возможных атак, которые могут не выявляться стандартными механизмами защиты, оценка мер защиты и минимизация рисков [13].

Существует большое количество программного обеспечения для моделирования компьютерных атак, например, COMNET III, NeuSecure, Eventia, Система анализа защищенности АС и другие. Последнее из названных является разработкой русской компании и предназначена для анализа защищенности АС путем имитации действий нарушителя, построения и анализа дерева атак. Входными данными для моделирования являются спецификации анализируемой АС, модель нарушителя и исходные показатели защищенности, включая интегральный показатель «уровень защищенности АС», на основе которых система строит дерево атак и обеспечивает его графическую визуализацию с целью дальнейшего анализа. Выходными данными являются показатели защищенности, рассчитанные с использованием деревьев атак, а также другая информация об анализируемой сети в виде журналов регистрации событий, отчетов и т.д. Такие программы помогают понимать, где могут оставаться следы от компьютерной атаки, что в дальнейшем может упростить деятельность компьютерного эксперта.

Обнаружение следов компьютерной атаки. Задачей государственной судебно-экспертной деятельности является оказание содей-

ствия судам, судьям, органам дознания, лицам, производящим дознание, следователям в установлении обстоятельств, подлежащих доказыванию по конкретному делу, посредством разрешения вопросов, требующих специальных знаний [4]. При содействии компьютерных экспертов в области защиты от компьютерных атак, они реализуют такие задачи как обнаружение следов, сбор и анализ данных, необходимых для предотвращения и расследования атаки.

Функциями по обнаружению КА являются сбор и первичная обработка событий безопасности, поступающих от ОС, средств обнаружения вторжений, межсетевых экранов, средств предотвращения утечек данных, антивирусного ПО, телекоммуникационного оборудования, прикладных сервисов, средств контроля (анализа) защищенности, средств управления телекоммуникационным оборудованием и сетями связи, систем мониторинга состояния, а также иных средств и систем защиты информации [5].

Целью обнаружения компьютерных атак является своевременное реагирование на связанные с ними инциденты для дальнейшего принятия мер по ликвидации последствий таких инцидентов. За последние 30 лет способы обнаружить действия злоумышленника существенно усовершенствовались. Если раньше хакеров ловили через завербованных информаторов, то сейчас поиск следов компрометации осуществляется средствами интеллектуального обнаружения и автоматизированного анализа. Основной задачей описываемого процесса является обнаружение атаки на ранней стадии, что позволяет минимизировать ущерб. Существует достаточно много классов технологий, рассмотрим некоторые из них.

Основополагающим элементом в защите является межсетевой экран — программный или программно-аппаратный элемент компьютерной сети, осуществляющий контроль и фильтрацию проходящего через него сетевого трафика в соответствии с заданными правилами. Современные межсетевые экраны, помимо самой фильтрации данных реализуют и другие дополнительные функции, например, поведенческий анализ файлов в изолированной среде, регулярные обогащения данными об актуальных угрозах, сигнатурный анализ трафика.

Решения класса Security Information and Event Management предназначены для мониторинга событий, поступающих от различных информационных систем и приложений. Такие системы собирают в себе всю информацию о происходящих в системе процессах, монито-

рит состояние элементов, отвечающих за безопасность, обладает функционалом реагирования на сбои в системе и построение карты сети для прогнозирования цепочек атак. Важным для эксперта является – получение данных для анализа процессов, происходящих в реальном времени, которые могут содержать следовую картину.

Существуют также системы обнаружения атак на конечных устройствах, при этом, на пользовательские системы устанавливается агент, который при фишинговой атаке анализирует изменения в системе, как только вредоносная программа откроет порт и начнет передавать данные, агент это зафиксирует и передаст события в систему защиты, оператор службы безопасности примет необходимые меры по блокировке угрозы – закроет порты, изолирует атакованный сегмент и т.п.

Интерес представляет использование инструмента приманки для хакеров («Honeypot»), его действие заключается в создании изолированных от промышленных систем сред со специально открытыми портами, уязвимостями и другими явными недостатками, маскирующими под важными документами «пустую» информацию. Интерес данных технологий не только в том, что они помогают изучать действия злоумышленников, а также и в том, что можно получить больше информации о самих атакующих и проследить к каким еще системам они подключаются для их дальнейшей идентификации [14].

Существует большое количество программного обеспечения, позволяющего обнаруживать атаки, например, ViPNet IDS, Континент, Рубикон и другие. Такие программы обычно собирают различные статистические данные, которые в дальнейшем можно использовать для расследования атаки.

Часто организации пренебрегают мерами компьютерной защиты, отказываясь оплачивать дорогостоящую защиту, или же системы безопасности не обнаруживают самостоятельно некоторые виды атак (например, руткит-атаки), тогда исследование компьютерной системы проходит вручную. Действие атак оказывает различное влияние в зависимости от вида. Об атаке может свидетельствовать высокий исходящий сетевой трафик, например, когда компьютер работает и подключен к интернету, но не используется, это может свидетельствовать о том, что компьютер используется для скрытой рассылки спама или для размножения сетевых червей. Повышенная активность жестких дисков или подозрительные файлы в корневых директориях также могут свидетельствовать о компьютерной атаке. Многие хаке-

ры после взлома компьютера производят сканирование хранящейся на нем информации в поисках интересующих документов, что и повышает активность процессов. Большое количество пакетов с одного и того же адреса, останавливаемые персональным межсетевым экраном могут свидетельствовать о том, что хакер пытается найти уязвимости в системе, обычно для этого они запускают автоматические сканеры.

Отследить процессы, происходящие в системе без использования специального ПО можно с помощью диспетчера задач. Для этого необходимо перейти во вкладку «Процессы» и в разделе «Сеть» обнаружить, какая программа потребляет трафик. Все версии Microsoft Windows, начиная с Microsoft Windows NT 3.1, имеют возможность ведения файла журнала. Для выявления атаки на самой ранней стадии в ОС Windows есть три полезных событийных источника: журнал событий безопасности, журнал системного мониторинга и журналы Power Shell. В данные журналы входят событие, анализ которых позволит определить компьютерную атаку. Появившиеся новые файлы в системных папках также могут свидетельствовать о КА, так же, как и скрытие файлов, записей в реестре, приложений, когда система не может определить их источник. Следы вредоносных программ можно определить с помощью реестра, например, поскольку вирусы научились прописываться на запуск в безопасном режиме, то следы вредоносной программы можно найти в ветке реестра, которая отвечает за драйверы, загружаемые в таком режиме. Одним из способов внедрения вируса систему, является подмена dll-файла для службы CSRSS, информацию о том, какой службой запускается файл можно также найти в реестре [15].

Сбор и анализ данных при компьютерной атаке. Целью анализа данных при КА является выявление инцидентов, в том числе связанных с ранее неизвестными компьютерными атаками, а также инцидентов, связанных с недостаточной эффективностью принимаемых мер защиты информации для определения типа атаки и нейтрализации ее действия. В организациях для анализа данных используется информация, собранная с систем защиты, которая сопоставляется со сведениями об уязвимостях компонентов для прогнозирования возможных действий злоумышленника при проведении КА.

В соответствии с Методическими рекомендациями ГосСОПКА, для реализации анализа данных центры ГосСОПКА осуществляют сбор результатов работы всех средств защиты информации, напри-

мер, средства обнаружения атак и межсетевые экраны, средства анализа сетевого трафика и поведенческого анализа программного обеспечения, также другие средства защиты, используемые в компьютерной системе. Все процессы рекомендуется проводить в автоматизированном режиме [16].

Часто атаки проходят именно на компьютерные сети, тогда следует исследовать в большей мере следы в сетевом трафике (например, следы перемещение вируса по сети), однако, конечный анализ сводится к поиску следов на локальном компьютере(-ах), через который началась атака или проходила с его использованием. В данной работе был проведен анализ следов, оставляемых КА на конкретном компьютере пользователе. Как уже было выяснено, компьютерная система записывает в определенных структурах все действия, происходящие в рамках нее, тогда становится возможным исследовать данные структуры на нахождение следов.

Если атака плохо реализована, то часто обнаруживается антивирусом, тогда весь дальнейший анализ сводится к исследованию систематизированных данных антивируса и ее нейтрализация может также проходить инструментами программы. В остальных случаях анализ проходит с помощью подручных программ и средств.

Исследовать компьютерную атаку можно начать с диспетчера задач. Данная структура в Windows включает в себя довольно много фоновых процессов, некоторые из них добавлены производителем ПК, а некоторые устанавливаемыми приложениями. Вредоносное ПО часто использует большой объем ресурсов ЦП, памяти или диска, имеет незнакомое название и может быть заметен. При незнакомом процессе, его наименование исследуется с помощью сети Интернет, так как практически все процессы являются определенными, то можно найти информацию о том, каким приложением он запускается и за что отвечает. Вредоносный процесс может также маскироваться под законный, то есть имитировать другую программу (например, Google Chrome), но запускаться будет из другой папки системы. Таким же методом стоит проверять автозагрузку системы.

Вручную также можно проверить системные папки на наличие неизвестных элементов. Например, перейдя по пути C:\WINDOWS\system32 можно обнаружить троянский вирус ворующий пароль, он может иметь любые названия, такие как 15h18d с расширением EXE и другие. Вирус может скачиваться и в такие папки как Documents и Application Data. Папка AppData(Application Data)

скрыта и посмотреть её можно настроив доступ к скрытым файлам и папкам или через специализированную программу, например «Total Commander». Самыми подозрительными являются каталоги временных файлов, такие как Temporary Internet Files и Temp. Большое число вирусов используют именно эти папки как площадки для запуска. Если примерное время заражения определяется, удобным ПО будет FAR Manager с включенной сортировкой по дате, где отображается содержимое интересующего каталога. Особое внимание стоит обратить на скрытые исполняемые файлы.

Также можно исследовать сетевой трафик, как правило, после внедрения, вирус должен связаться с хозяином или с заданным сервером в интернете, признаком чего будут DNS-запросы. В данном случае, удобнее всего воспользоваться программой анализатором протоколов, например, Wireshark. Большое количество пакетов с одного и того же адреса, останавливаемые персональным межсетевым экраном возможно является свидетельством о нахождении вируса. Хотя обычно определить принадлежность трафика именно вредоносному ПО довольно затруднительно, косвенным признаком ненормальности сетевой активности системы могут быть значительные значения счетчиков трафика провайдера, в условиях простоя системы, счетчики из свойств VPN-соединения и т.п. Но умный вирус может их замаскировать, кроме того, он может обойти брандмауэр.

Для анализа можно также использовать реестр. Это совокупность данных, которая содержит массив атрибутов и значений, отвечающих за операционную систему. Автозагрузки системы можно посмотреть и в реестре, по путям HCU HLM \Software\Microsoft\Windows\CurrentVersion\Run при обнаружении подозрительных элементов, их следует удалить. Иногда вирус грузится вместо проводника Windows, заменив запись в реестре HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon. Параметр Shell вместо значения "explorer.exe " заменяется вирусным. Поскольку вирусы научились прописываться на запуск в безопасном режиме загрузки, можно проверить ветку реестра: HLM\SYSTEM\CurrentControlSet\ Control\SafeBoot разделы Minimal и Network. Одним из способов внедрения в систему, является подмена dll-файла для CSRSS. Если посмотреть содержимое записи HLM\SYSTEM\CurrentControlSet\Control\SessionManager\SubSystems, то можно найти значения ServerDll=basesrv, ServerDll=winsrv, кото-

рые являются правильными, если значения отличаются, загрузка системы обеспечивается вредоносной программой.

Обнаружение, сбор и анализ следов, оставляемых программой-шпионом. Реализуем компьютерную атаку, связанную со шпионскими программами. Это вредоносное ПО, которое проникает на компьютер и собирает информацию о пользователе, об истории посещений веб-сайтов, о нажатиях на клавиши, а также другие сведение, таким образом, нарушая законодательство по конфиденциальности данных. Шпионские программы работают в фоновом режиме и не предусматривают стандартную процедуру удаления, даже если она будет обнаружена. Они проникают в систему теми же путями, что и любое другое вредоносное ПО – с помощью троянских программ, червей, других программ для проникновения. Исследуем следы, оставляемые шпионом Spyrix.

После установки шпиона на компьютер, стандартными способами действие программы не обнаруживается. Несмотря на то, что шпион запускается автоматически с запуском операционной системы, через диспетчера задач, в автозагрузках и через реестр в ветке HCU \Software\Microsoft\Windows\CurrentVersion\Run действие программы не обнаруживается в соответствии с рис. 1.

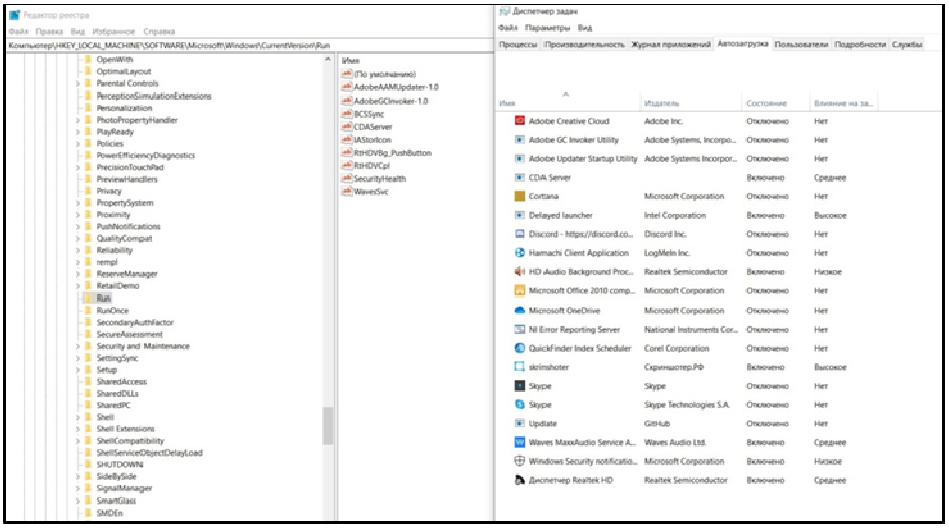


Рис. 1. Окно диспетчера задач и реестра, отображающее автозапускаемые процессы

Чтобы отледить процессы, происходящие в системе, воспользуемся программой Process Monitor. После ее запуска была замечена активность неизвестных процессов spkl.exe, которые постоянно создают

файлы в соответствии с рис. 2. Поиск данных в сети по этому процессу говорит о том, что он является опасным.

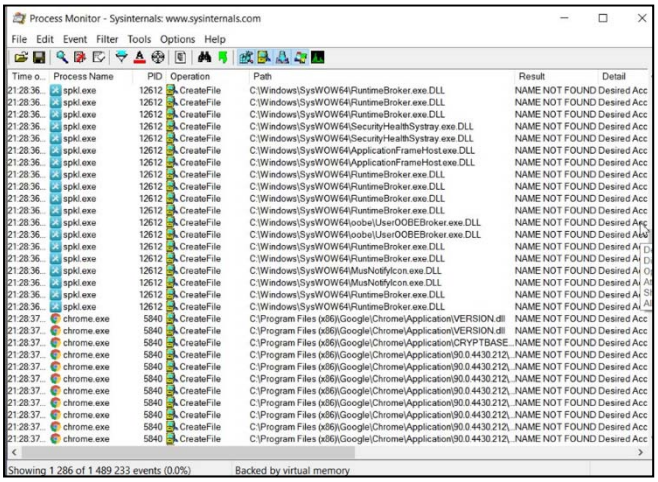


Рис. 2. Окно программы Process Monitor, отображающее действие процесса spkl.exe

Для дальнейшего поиска шпиона, воспользуемся специализированным ПО – Covert. Так как процесс не отображается в диспетчере задач, скорее всего, он является скрытым, поэтому после установки программы, перейдем в раздел процессы, далее, скрытые процессы в соответствии с рис. 3. Программа выделила красным процесс, который потенциально может являться угрозой.

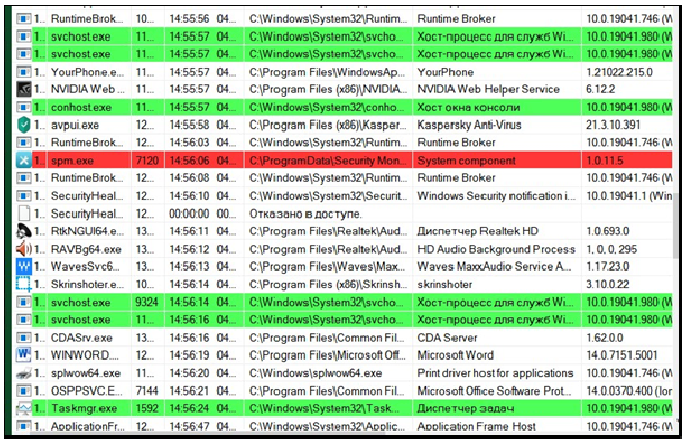


Рис. 3. Окно программы Covert, отображающее скрытые процессы

Программой также обозначен путь до вредоносной программы, она была установлена в папку ProgramData, после отображения всех скрытых папок в нее можно перейти и обнаружить два компонента вредоносной программы: Spyrix monitor, Security monitor в соответствии с рис. 4.

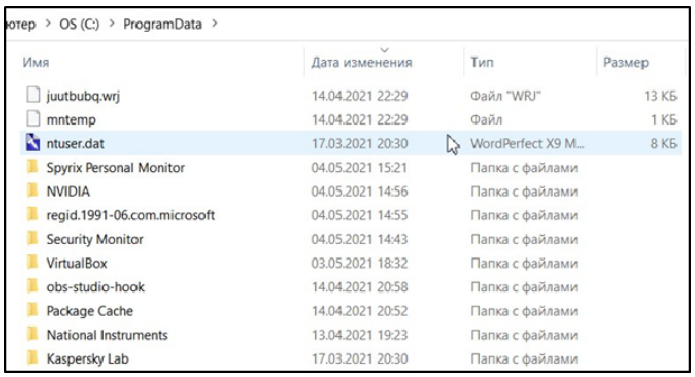


Рис. 4. Окно проводника, отображающее появление новых вирусных компонентов

Первый компонент включает в себя элементы, необходимые для функционирования шпиона, второй компонент состоит из записей и изображений активности, которая передается злоумышленнику: записи всех действий, переходов, использованных программ, время их использования, скриншотов экрана. Чаще всего программы-шпионы прикрываются другими папками системы и без специализированного программного обеспечения не обнаруживаются. С помощью программы Covert осуществим удаление шпиона.

Таким образом, в результате проведенного эксперимента, можно сделать вывод, что следы компьютерной атаки могут содержаться в системных папках, в диспетчере задач, в автозагрузках, в реестре, в журнале Windows. Однако компьютерные атаки часто действуют скрытно и не оставляют следов стандартных программных структурах, тогда могут помочь специальные программные средства.

Заключение. В ходе статьи были проанализированы нормативные источники, регулирующие деятельность и порядок реализации защиты от действия компьютерных атак и при реагировании на них.

Было выяснено, что каждый вид атаки в частности реализуется по-разному и существуют механизмы моделирования атак для их дальнейшего изучения, такие как: табличные и матричные модели, логические модели, модели, основанные на графах и др. Существует также специально ПО, позволяющие упростить процессы моделирования, например, COMNET III, NeuSecure, Eventia.

Для целей обнаружения следов компьютерных атак были определены программные составляющие Windows, которые могут содержать значимую информацию, в этот список вошли диспетчер задач, автозагрузки, журнал действий Windows, реестр, системные папки. Также выделено некоторое ПО позволяющее упростить процессы по-

иска следов, например, Process Monitor, FAR Manager, Wireshark и другие.

В результате работы было определено, что анализ следов компьютерных атак может осуществляться как с помощью специализированного ПО, так и ручным методом, если программы не определяют атаки, а также для поиска дополнительной информации. Целью анализа данных при КА является выявление инцидентов, связанных с ранее неизвестными компьютерными атаками и с недостаточной эффективностью принимаемых мер защиты информации для определения типа атаки и нейтрализации ее действия.

Для подтверждения теоретической информации, в работе была изучена деятельность программы шпиона в рамках компьютерной системы, был осуществлен поиск и анализ следов по выделенным элементам Windows, значимая информация была найдена в системных папках, так как программа действует скрытно, то процесс в диспетчере задач и автозагрузках не обнаружен, в реестре также не было найдено информации. Для исследования было использовано специализированное ПО: Process Monitor, с помощью которого была замечена активность вредоносного ПО, а также программой Covert, которая показала скрытые процессы. Таким образом, был определен и на практике проверен процесс обнаружения анализа данных при реагировании на компьютерные атаки.

Список используемых источников

1. Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 12.11.2018)// Собрание законодательства РФ, 17.06.1996, N 25, ст. 2954.

2. Гражданский Кодекс Российской Федерации (часть третья) от 26.11.2001 N 146-ФЗ (ред. от 03.08.2018)//Собрание законодательства РФ, 03.11.2001. N 49. Ст. 4552.

3. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»//Собрание законодательства РФ, 2006 г., № 31, ст. 3448.

4. Федеральный закон от 31 мая 2001 г. N 73-ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации»//Собрание законодательства РФ от 4 июня 2001 г. N 23 ст. 2291.

5. Приказ ФСБ России от 06.05 2019 г. N 196 «Об утверждении Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагиро-

вания на компьютерные инциденты»//Официальный интернет-портал правовой информации (www.pravo.gov.ru) 31 мая 2019 г.

6. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения//Приказ Федерального агентства по техническому регулированию и метрологии от 27.12.06 г. N 373-ст. – URL: https://docs.cntd.ru/1200058320 (дата обращения 10.04.21) . – Текст: электронный.

7. ГОСТ Р 51275-2006. Защита информации. Факторы, воздействующие на информацию//Приказ Федерального агентства по техническому регулированию и метрологии от 27.12.06 г. N 373-ст. URL: https://docs.cntd.r/1200058320 (дата обращения 10.04.21) . – Текст: электронный.

8. Белоножкин В. И. Системы обнаружения компьютерных атак: учеб. пособие. Воронеж: ФГБОУ ВПО «Воронежский государственный технический университет», 2015. – 370 С.

9. Технические средства информатизации [Электронный ресурс] // Технологии. URL: https://sites.google/informatika (дата обращения 02.04.2021).

10. Актуальные киберугрозы: итоги 2020 года [Электронный ресурс] // Positive Technologies. URL: https://www.ptsecurity.com/ru-ru/cybersecurity-threatscape-2020/ (дата обращения 02.04.2021).

11. Подключение к ГосСОПКА [Электронный ресурс] // Infotrust. URL: https://www.infotrust.ru/services/gossopka (дата обращения 10.04.2021).

12. А. Муханова, А.В. Ревнивых, А.М. Федотов. Классификация угроз и уязвимостей информационной безопасности в корпоративных системах // Вестник НГУ. Серия: Информационные технологии. 2013. №2. URL: https://cyberleninka.ru/article/n/klassifikatsiya-ugroz-i-uyazvimostey-informatsionnoy (дата обращения: 18.04.2021).

13. Д.И. Котенка, И.В. Котенка, И.Б. Саенко. Методы и средства моделирования атак в больших компьютерных сетях: состояние проблемы//Труды СПИИРАН. 2012. Вып. 3(22). С. 5-30.

ЭТАПЫ СОЗДАНИЯ МОДЕЛЕЙ ДЛЯ 3Д ВИЗУАЛИЗАЦИЙ И КОМПЬЮТЕРНЫХ ИГР

Азовцев А.А., магистр, гр. ИМО-ПИ-21,
Дуров Д.К., магистр, гр. ИМО-ПИ-21,
Технологический университет («МГОТУ»),
Россия, Королев.

В данной работе проводится анализ материалов на тему создания 3д моделей, процесса разработки и других технических особенностей моделирования.

Ключевые слова: 3д модель, этапы создания, текстуры, запечка, развертка.

Введение. Одним из основных направлений компьютерных технологий является компьютерная графика, особенно ее раздел — трехмерная графика или 3д-моделирование. Основная задача 3д-моделирования — представить визуальное, трехмерное представление объекта: существующего объекта или только задуманного. Трудно представить нашу жизнь без моделирования. Архитектурная визуализация стала своеобразным направлением в жизни архитекторов, инженеры могут быстрее и эффективнее справляться с системами автоматизированного проектирования. В медицине тоже выделяют отдельные направления: точечная томография, проектирование и изготовление протезов. Трудно не согласиться с тем, что процесс моделирования, охватывающий все новые и новые области промышленности и науки, служит только развитию общества. В этой статье мы рассмотрим процесс создания 3д модели и пошагово разберем все технические нюансы.

Обзор и подробное описание технологического процесса по созданию и оптимизации модели. ААА-конвейер — это довольно большой технологический процесс, направленный на создание и оптимизацию модели, чтобы затем поместить ее в 3д пространство. Процесс начинается с наброска и заканчивается готовой моделью внутри проекта [2].

Технологический процесс состоит из 5 этапов, каждый из которых будет разобран в этой статье: Драфт (формы и силуэт); Сетка (лоуполи, хайполи); Развертка; Запечка; Текстурирование.

Первый этап: драфт. Любая модель начинается с драфта, т.е. наброска модели. А любой драфт начинается с референсов, т.е. с поиска картинок.

Частой ошибкой является создание модели со всеми деталями на начальном этапе. AAA-пайплайн говорит о том, что сначала нужно создать модель всего объекта из самых простых элементов, создать очертания объекта, а затем задавать размеры, стиль и переходить к деталям [4].

Каждый эскиз начинается с этапа блокинга — эскиза примитивной модели, передающей суть объекта. На этом этапе нет мелких деталей, только крупные и средние формы. Все создается с использованием простых форм, квадратов, сфер и цилиндров как на рис. 1:

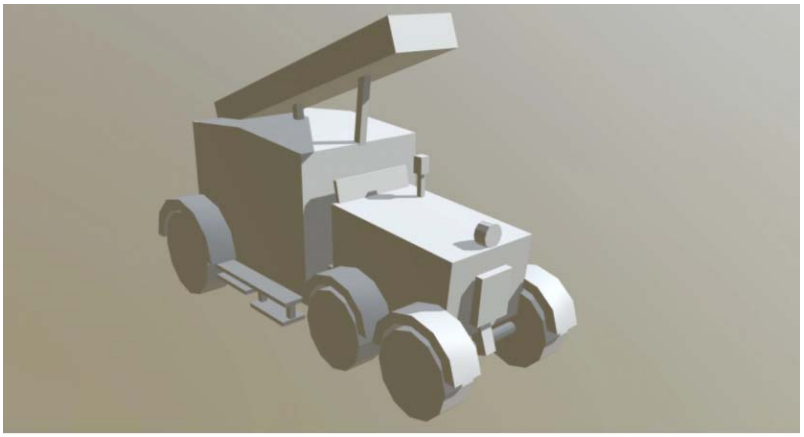


Рис. 1. Набросок автомобиля

Блокинг - это работа над читаемостью силуэта, работа над пропорциями и формами [3]. В среднем на этот этап уходит до 40 минут.

Следующий пункт наброска — это проработка детализации. На этом этапе крайне важно понять механику модели, чтобы любой человек смог поверить в ее работоспособность. Стоит доработать переходы между элементами и продумать важные детали объекта. Этот этап помогает геометрии и силуэту стать более привлекательным (рис. 2).

На этапе драфта решается, как будет читаться модель. Если детализированный драфт вышел невыразительным, то следует его изменить, т.к. на следующем этапе не получится что-либо исправить.

Второй этап: сетка (лоуполи и хайполи).

Когда драфт готов и мы уверены в формах объекта и силуэте, можно приступить к работе с полигональной сеткой. Существует три вида топологии: лёгкая low poly, очень детализированная high poly и

mid poly средняя. Обычно для игр и визуализаций создают 2 модели: хайполи и лоуполи.

Рис. 2. Детализированный драфт

LowPoly — это самая простая 3д модель, в которой элемент, будь то плоскость, грань или вершина имеют особую задачу: воздействуют на силуэт, создают блик, решают задачи правильной топологии и так далее [2].

При этом полигоны, которых не видно из-за геометрии, удаляются, а вся геометрия максимально оптимизируется, цилиндры создаются с сохранением длины сторон. Лоуполи модель имеет множество нюансов, которые влияют на развертку и запекание.

Это пример модели, которую мы будем использовать в качестве примера**.** Именно ее мы попробуем развернуть, запечь и текстурировать. Задача low poly - найти наилучший баланс между четкостью и простотой понимания модели.

Третий этап: развертка. На этом этапе происходит развертка лоуполи моделии на плоскость. Это нужно для того, чтобы редактор понял, как применить текстуру на 3д объект (рис. 3).

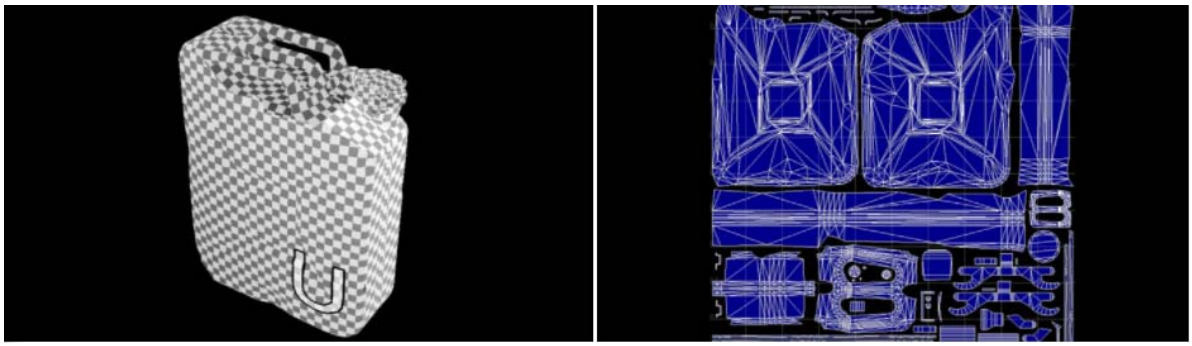


Рис. 3. Развертка канистры для бензина

Главная задача развёртки — это нарезать модель на плоскости с наименьшим числом швов и понять, что текстуры не создают артефакты [1].

Четвертый этап: запечка. Все мельчайшие неровности, помятости и царапины могут быть созданы специальной картой нормалей, что позволяет объединить хайполи с лоуполи, но при всем этом, лоуполи объект будет содержать в себе все детали высокополигонального «брата». Например, если создать куб, то у него будет 6 полигонов, а если начать создавать дополнительные элементы на этом объекте, то полигонов станет значительно больше. Но можно сохранить начальное число полигонов, при этом сохранив и дополнительные элементы на объекте, нужно лишь использовать карту нормалей, как на рис.4.

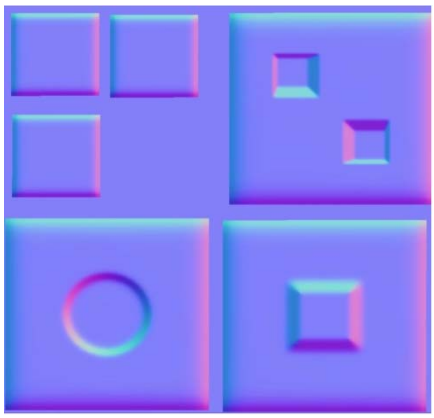


Рис. 4. Карта нормалей для куба

Таким образом, карта нормалей отображает на себе дополнительные элементы с хайполи модели куба, а затем переносит выпуклости на лоуполи, но без добавления какой-либо топологии как на рис. 5.

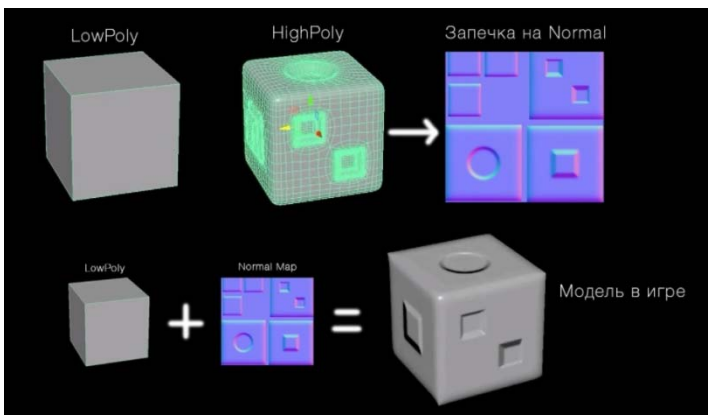


Рис. 5. Применение карты нормалей на лоуполи куб

Пятый этап: текстурирование. На этом этапе происходит покраска созданной лоуполи модели. Существует несколько способов преображения изображения с некоторыми требованиями к текстурам. Например, в мультиках используется только чистые цвета, а в современных моделях, которые будут использовать в визуализациях, фильмах и играх используется рендер PBR. Работает эта технология следующим образом: существует отдельная карта цвета модели без каких-либо бликов и затемнений, так же существует отдельная карта силы отражений, шершавости, гладкости, как на рис. 6.

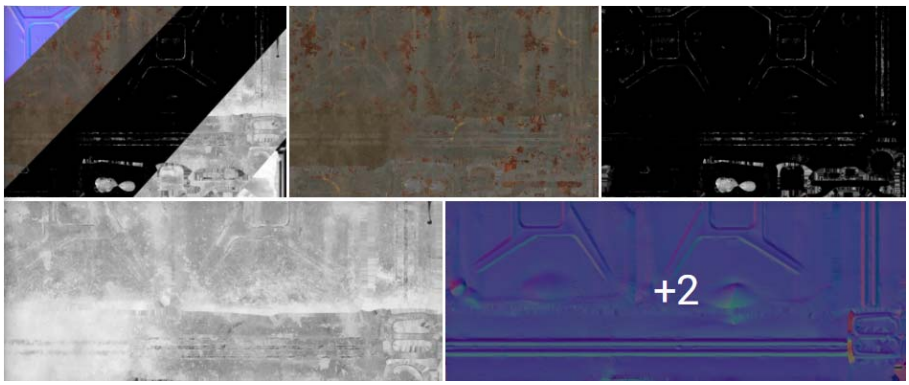


Рис. 6. Карты PBR

Вывод. В данной работе мы рассмотрели полный процесс создания высококачественных моделей для дальнейшего использования в визуализациях, кино и играх. Были раскрыты особенности при создании 3д объекта, выявлены технологии отображения элемента в пространстве, что позволит реализовать точную модель телевизора и внедрить его в визуализацию.

Список используемых источников

1. А.Г. Горелик. Самоучитель 3ds Max М.: Издательство «БХВ-Петербург», 2020. – 49с.
2. В.И. Котов. Развертка и топология для начинающих М.: Форум, 2019. – 3с.
3. М.В. Серова. Учебник - самоучитель по трехмерной графике в blender 3d. Моделирование, дизайн, анимация, спецэффекты М.: Издательство «Солон-пресс». - 2021. – 98с.
4. Сообщество 3д художников [Электронный ресурс] // Технологии. URL: https://dtf.ru/gamedev.

РАЗВИТИЕ ТЕХНОЛОГИИ БЕСПРОВОДНОЙ ПЕРЕДАЧИ ДАННЫХ - СТАНДАРТ IEEE 802.11AX

Родительский И.Ю., магистр группы ИМО-ПИ 21,
Федоров Д.Ю., магистр группы ИМО-ПИ 21,
Технологический университет («МГОТУ»),
Россия, Королев.

В работе рассмотрены и проанализированы вопросы, связанные с технологиями беспроводной передачи данных и их стандарта IEEE 802.11ax.

Ключевые слова: Wi-Fi, стандарт, беспроводные сети.

Введение. В данной работе произведен обзор технологии Wi-Fi 6, исходя из стандарта IEEE 802.11ax. Произведен сравнительный анализ с более старыми стандартами беспроводной связи. В работе будут рассматриваться и анализироваться методы и средства создания максимально надежной и производительной беспроводной связи исходя из актуальных данных, полученных в открытых источниках [1-3]. Приведены характеристики оборудования, применимого для поддержки стандарта IEEE 802.11ax. Их стоимость, доступность и обоснована необходимость применения стандарта IEEE 802.11ax.

Обоснование необходимости применения беспроводных технологий. При проектировании СКС важное значение имеет выбор технологии, по которой будет построена СКС.

- Проводной;
- Беспроводной;
- Комбинированной;

Основными требованиями к СКС

- Удовлетворять требованиям организации к сети;
- Иметь определенный запас по пропускной способности;
- Иметь возможность увеличить количество пользователей;

Исходя из принципов построения сети стоит сделать вывод о том, что сеть должна быть проводной для стационарных рабочих мест, но для возможности масштабирования можно применять технологии Wi-Fi. Хотя для каждой СКС выявляются свои требования к безопасности, скорости и надежности сети и выбор технологии применяется исходя из этих данных.

Обзор и сравнительный анализ существующих стандартов беспроводной связи. IEEE 802 – это семейство стандартов, которые дают требования к характеристикам локальных сетей и сетей мегаполисов. Создание международных стандартов является решением проблем с подключением устройств от разных производителей.

IEEE 802.11 характеризует требования к стандартам относящимся к технологии Wi-Fi.

IEEE 802.11a первая реализованная и запущенная версия Wi-Fi в 1999 году работала на частоте 2,4 ГГц и могла развивать скорость до 11мбит/с.

IEEE 802.11b создан в 2001 году, работал на частоте 5 ГГц и мог развивать скорость до 54мбит/с, была увеличена пропускная способность.

IEEE 802.11g создан в 2003 году, работал на частоте 2,4 ГГц и мог развивать скорость до 54мбит/с, обратно совместим с IEEE 802.11b.

IEEE 802.11n назван Wi-Fi 4, создан в 2009 году, работал на частоте 2,4 или 5 ГГц и мог развивать скорость до 600 Мбит/с, обратно совместим с IEEE 802.11a, IEEE 802.11b и IEEE 802.11g.

IEEE 802.11ac назван Wi-Fi 5 и создан в 2014году, может развивать скорость до 6,8 Гбит/с.

IEEE 802.11ax назван Wi-Fi 6, создан в 2019 году и может развивать скорость до 11Гбит/с и работать на частотах 2,4 и 5 ГГц.

IEEE 802.11be будущая новая версия Wi-Fi 7 на данный момент только разрабатывается.

Особенности стандарта беспроводной связи IEEE 802.11ax. В настоящие время частоты 2.4 ГГц испытывают перегрузку. От высокой нагрузки возникают шумы и помехи, следовательно, скорость работы сети падает. Wi-Fi 6 позволяет выполнять поддержку ранее выпущенных устройств благодаря поддержки частот 2, 4 и 5 ГГц. Но это не является ключевой особенностью данного протокола. Основной особенностью является увеличение средне статической пропускной способности канала из-за более продуктивного использования спектра. В основе всех улучшений использования спектра лежит технология OFDM применявшаяся ранее, но в Wi-Fi 6 она была улучшена и получила название OFDMA.

На рис. 1 предоставлена схема разделения частот между пользователями при использовании технологии OFDM.

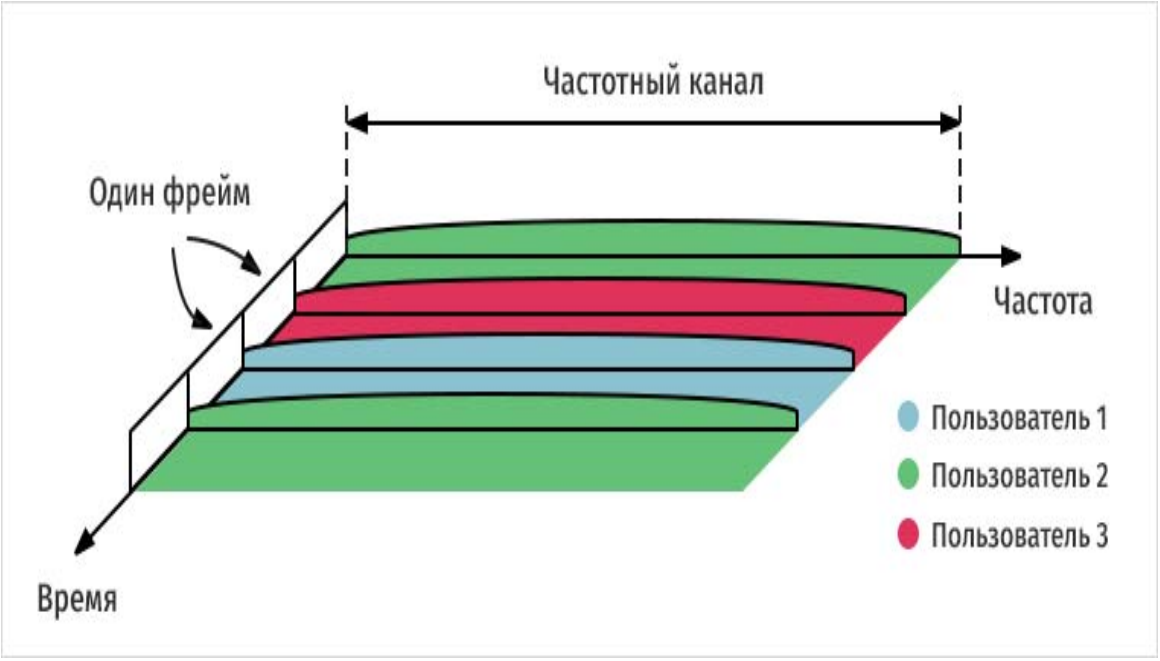


Рис.1. OFDM

На рис. 2 приведена схема технологии OFDMA.

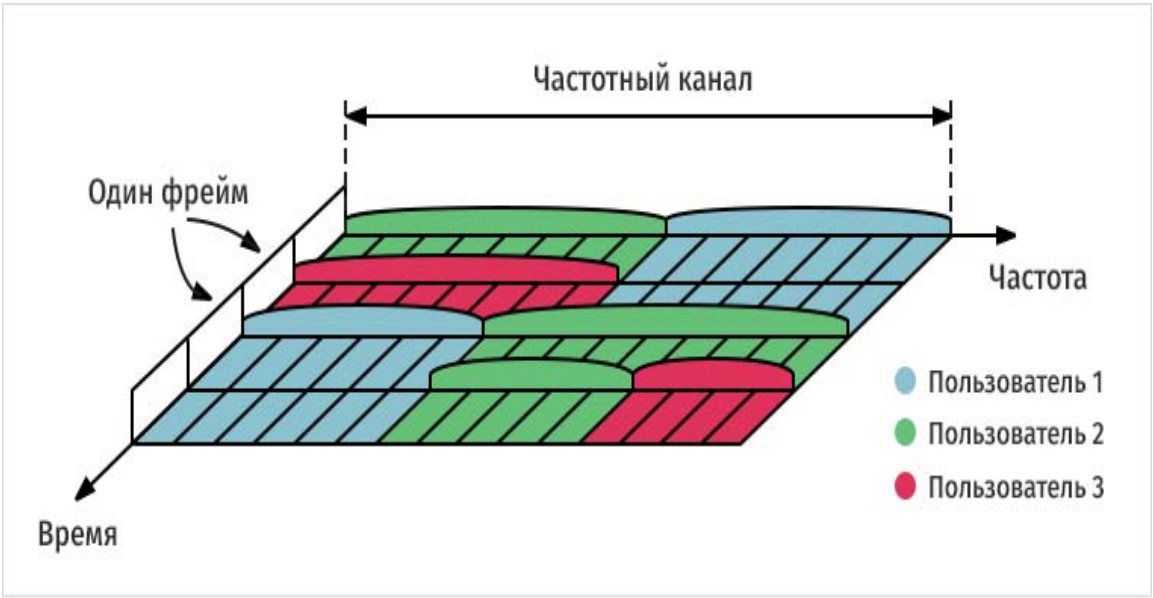


Рис. 2. OFDMA

Эта технология улучшает работу Wi-Fi при высокой плотности беспроводных устройств. Следовательно, уменьшает время ожидания ответа для каждого устройства.

Кроме уплотнения пакетами каналов совершенствуется и сам метод уплотнения информации в пакеты. В Wi-Fi 6 применена технология 1024 –QAM, по сравнению с Wi-Fi 5 где была примерна технология 256–QAM. Теоретически это должно дать прибавку к скорости

до 25 процентов. Графическое сравнение этих технологий приведено на рис. 3.

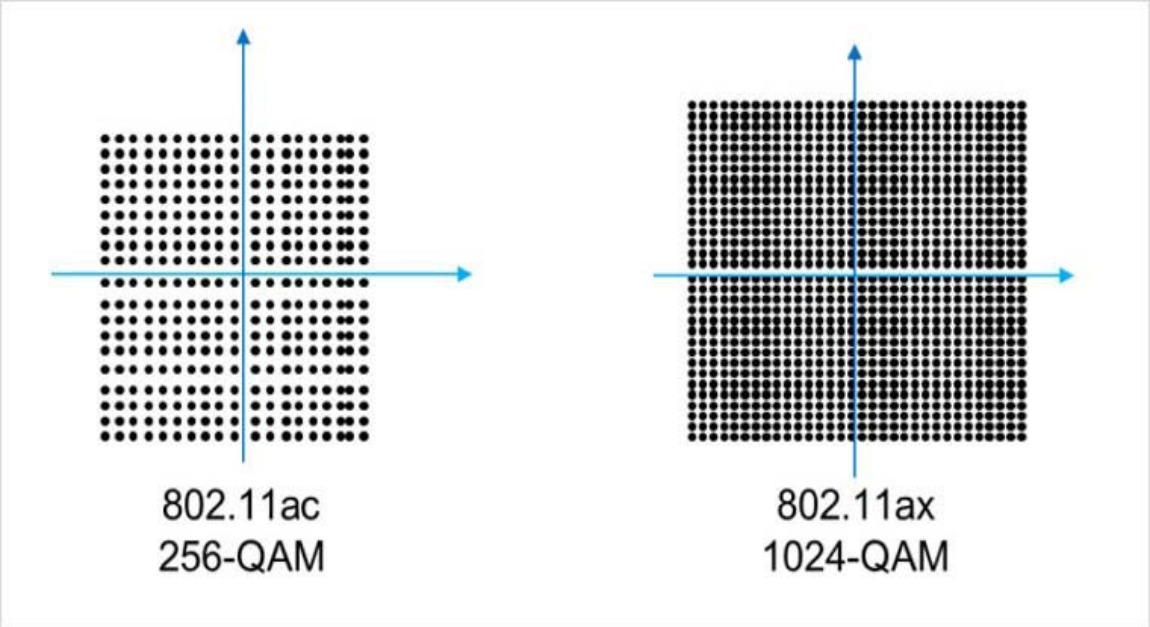


Рис. 3. Уплотнение информации

Актуальность технологии Wi-Fi 6. Wi-Fi 6 является самой актуальной на сегодняшний день технологией беспроводной связи доступной для применения как в крупных компаниях, так и в частных руках.

Также актуальность использования устройств с поддержкой технологии Wi-Fi 6 подтверждает график предоставленный на рис. 4.

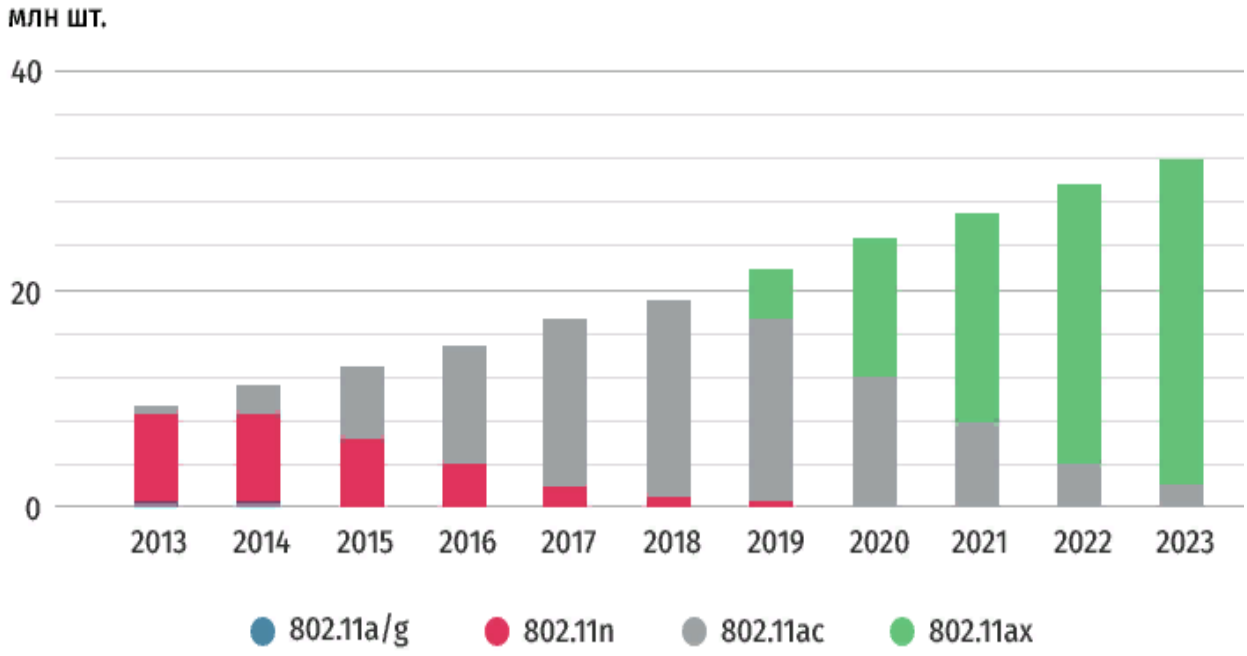


Рис. 4. План производства устройств

Согласно нему устройства Wi-Fi 4 больше не производятся, а устройств Wi-Fi 5 идут на убывание. К 2023 году планируется максимально увеличить производство устройств Wi-Fi 6. Анализируя цены на устройства, соответствующие стандарту IEEE 802.11ax, можно назвать их вполне доступными как для компаний, так и для частных лиц.

Вывод. В следствии проведенного изучения теоретического и практического материала, анализа существующих стандартов и принципов работы устройств, изготавливаемых по этим стандартам, необходимо подтвердить, что стандарт IEEE 802.11ax является наиболее актуальным в настоящее время для применения при создании локальной вычислительной сети. Технология Wi-Fi 6 согласно приведенным данным только набирает свои производственные мощности. В дальнейшем устройства будут становится более доступными и, благодаря поддержки пред ведущих стандартов и примененной технологии работы с 2,4 и 5 ГГц, становится широко распространёнными.

Список используемых источников

1. Артюшенко В.М., Корчагин В.А. Оценка влияния электромагнитных помех радиоэлектронных средств на беспроводные устройства малого радиуса действия // Электротехнические и информационные комплексы и системы. 2010. Т. 6. № 2. С. 10-17.

2. Артюшенко В.М., Гуреев А.К., Абраменков В.В. Енютин К.А. Мультимедийные гибридные сети. Москва, 2007.

3. Артюшенко В.М., Корчагин В.А. Расчет и моделирование вероятности появления внутриканальных и интермодуляционных помех беспроводных устройств с малым радиусом действия // Электротехнические и информационные комплексы и системы. 2014. Т. 10. № 1. С. 57-65.

СКС 8 КАТЕГОРИИ ХАРАКТЕРИСТИКИ И ОБЛАСТЬ ПРИМЕНЕНИЯ

Федоров Д.Ю., магистр группы ИМО-ПИ 21,
Родительский И.Ю., магистр группы ИМО-ПИ 21
Технологический университет («МГОТУ»),
Россия, Королев.

.

В данной статье рассматривается, витая пара 8 категории. Производится сравнение 8 категории с другими на основании их электротехнических характеристик. Рассматривается применение 8 категории в технологии (PoE). Проводится описание недостатков и преимуществ 8 категории витой пары, а также обсуждается область применения.

Ключевые слова: кабель, 8 категория, витая пара, анализ.

Еще столетия назад совершенно обыденные возможности, предоставляемые нам компьютерными технологиями, были лишь несбыточной мечтой, встречаемой лишь в фантастических произведениях наравне с драконами, феями и прочими мифическими существами различных фольклоров. Но прогресс вещь не обратимая и человечество научилось манипулировать с колоссальными объемами информации, а именно собирать, обрабатывать, вычленять нужную информацию и преобразовывать ее в удобный вид для понимания и принятия последующих решений. Все это происходит благодаря вычислительным машинам. Но с каждым годом объемы информации неостановимо растет и, следовательно, вырастают потребности в большей скорости обработки информации. Отсюда же растут требования к более мощным вычислительным машинам, коммутационному оборудованию и кабелям соответственно [1-5].

В данной статье будет рассмотрен проводной рассмотрены кабеля, а если точнее 8 категории. Главной же задачей структурированной кабельной системы безусловно является повышение пропускной способности и быстродействия. Исходя из технических характеристик согласно международным стандартам кабеля делятся на категории. На момент написания существует всего 8 категорий. Чем выше категория, тем соответственно лучше электротехнические характеристики и предельные рабочие частоты [6-10].

На рис. 1 представлены различные категории кабелей и их предельные частоты.

Категория витой пары	Предельная частота, МГц
Категория 1	0,1
Категория 2	1
Категория 3	16
Категория 4	20
Категория 5	100
Категория 5e	100
Категория 6	250
Категория 6A	500
Категория 7	600
Категория 7A	1000
Категория 8	2000
Категория 8.1	2000
Категория 8.2	2000

Рис. 1. Предельные частоты для различных категорий

На момент написания статьи. Витая пара до 5 категории считается устаревшей и мало где активно используется в виду своих довольно посредственных электротехнических характеристик.

Кабеля 8 категории. Рассмотрим и проведем анализ кабелей 8 категории поподробнее. Внешний вид кабеля представлен на рис. 2.

Рис. 2. Внешний вид кабеля 8 категории

Область применения кабелей данной категории довольно ограниченна из-за максимальной длины канала 30 метров, что является довольно посредственным результатом по сравнению с витой парой других категорий, что уже говорить о оптоволокне. Так максимальная протяженность кабелей с 5 по 7 категории составляет 100 метров. Но несмотря на недостаток в длине, у 8 категории имеется огромное преимущество, а именно- предельная частота 2000 МГц. В это же максимальная частота предшественника кабелей 7 категории в два

раза меньше-1000 МГц, а самой распространённой категории на момент написания -5 в целых 20 раз меньше-100 МГц. Также 8 категория поддерживает максимальную скорость до 40 Гбит/с, в это же самое время категория 7А обеспечивает максимальную скорость всего лишь до 10 Гбит/с. Отсюда же выходит, что наиболее вероятной областью применения является сети с огромным трафиком и малым расстоянием между устройствами. Под это описание идеально подходят центры обработки данных.

Все кабеля 8 категории экранированы, неэкранированных не существует вообще. На рис. 3 представлена витая пара 8 категории.

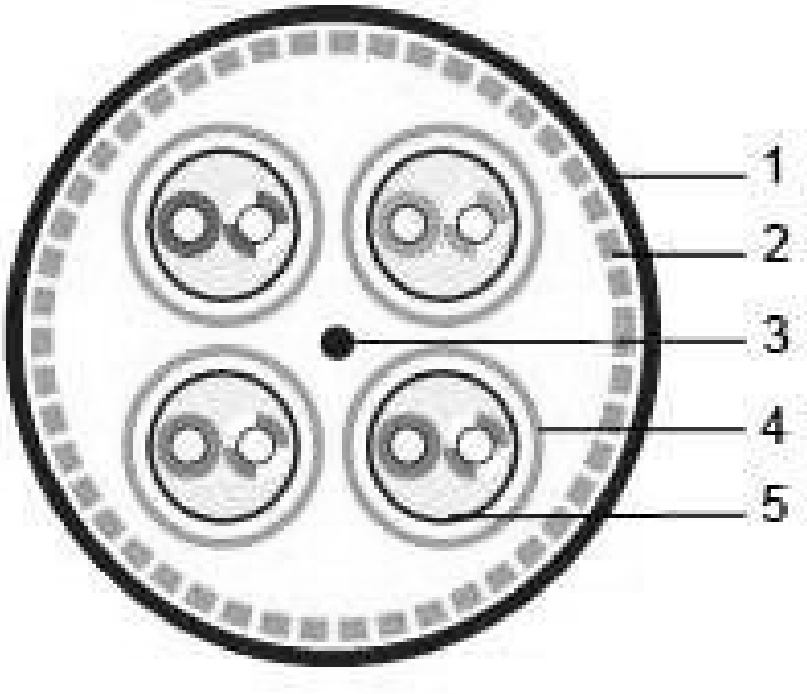


Рис. 3. Вид в разрезе кабеля 8 категории

Сам кабель состоит из:

1. Внешней оболочки;
2. Экрана-сетки;
3. Дренажного провода;
4. Экран из полиэфирной алюминиевой фольги;
5. Витой пары solid.

Конфигурация канала категории 8. Как было написано ранее максимальная длина канала категории 8 составляет 30 метров. Из них протяженность самого горизонтального кабеля составляет всего лишь 24 метров. Остальные 6 метров приходятся на аппаратные шнуры.

Суммарная длина аппаратных шнуров может быть может быть распространена неравномерно.

Также в отличии от категорий 6 и 7 количество разъёмов в канале категории 8 уменьшено в 2 раза и составляет 2 точки соединения. Минимальная толщина по сравнению с 7 категорией также выросла, так как из-за возросшей частоты выросло количество необходимого экранирования, что сказалось на размеры.

Стандартизация 8 категории. По международному стандарту существует всего лишь 2 варианта 8 категории - это категории 8.1 и 8.2. Также существуют просто категория 8, но она принята лишь стандартом ANSI / TIA, который действует только в США. В таблице будут приведены разновидности 8 категории.

Таблица 1 - Разновидности 8 категории.

Категория	Стандарт	Регион	Частота	25 GBASE-T	40 GBASE-T	RJ 45
Кат 8	ANSI / TIA	США	2000 МГц	Да	Да	Да
Кат 8.1	ISO / IEC	Весь мир	2000 МГц	Да	Да	Да
Кат 8.2	ISO / IEC	Весь мир	2000 МГц	Да	Да	Нет

Кат 8.1 поддерживает RJ 45, что делает его совместимым с более ранними категориями такими как: кат 5, кат 5. е, кат 6, кат 6А.Кат 8.2 полностью совместима с 7А и поддерживает коннекторы GG45/ARJ45 и TERA.

Поддержка Poe. Технология Power over Ethernet (PoE) позволяет подавать питание на сетевые устройства по витой паре, позволяя сокращать количество кабелей и розеток, что в свою очередь упрощает и удешевляет создание новой или расширение старой структурированной кабельной системы. В основном используется в ip-камерах и voip-телефонах, различные датчики.

Выводы. Подводя итоги, можно сказать что 8 категория поддерживает невероятную максимальную скорость, а именно 40 Гбит/с, предшественник всего лишь 10 Гбит/с, но небольшая максимальная длина и дороговизна делает данную категорию довольно узконаправленной и мало где применимой.

Список используемых источников

1. Артюшенко В. М. Информационные технологии и управляющие системы: монография / В. М. Артюшенко, Т. С. Аббасова, Ю.

В. Стреналюк, В. И. Привалов, В. И. Воловач, Е. П. Шевченко, В.М. Зимин, Е.С. Харламова, А.Э. Аббасов, Б.А. Кучеров /под науч. ред. док. техн. наук, проф. В. М. Артюшенко // М.: Издательство «Научный консультант». – 2015. – 185 с.

2. Титаев, А. А. Промышленные сети: учебное пособие- М.: Издательство Уральского университета. -2020. – 105 с;

3. Федотова Е.Л. Информационные технологии и системы М.: Форум. - 2018. -149с;

4. Артюшенко В.М. Структурированные кабельные системы. Учебное пособие / Москва, 2005.

5. Артюшенко В.М. Сервис информационных систем в электротехнических комплексах. Монография / Москва, 2010.

6. Артюшенко В.М. Защита структурированных кабельных систем от внешних электромагнитных воздействий // Теоретические и прикладные проблемы сервиса. 2005. № 3 (16). С. 20-27.

7. Артюшенко В.М., Енютин К.А., Буткевич М.Н. Анализ эффективности уменьшения межкабельных переходных помех в экранированных кабельных системах // Электротехнические и информационные комплексы и системы. 2009. Т. 5. № 1. С. 19–23.

8. Советов В.М., Артюшенко В.М. Основы функционирования систем сервиса. Учебное пособие для студентов высших учебных заведений, обучающихся по специальности 100101 «Сервис» / Москва, 2010.

9. Артюшенко В.М., Корчагин В.А. Схемы подключения управляющего и измерительного оборудования в системах автоматизации и жизнеобеспечения зданий // Электротехнические и информационные комплексы и системы. 2009. Т. 5. № 3. С. 3-11.

10. Артюшенко В.М., Аббасова Т.С. Эффективность защиты от внешних помех электропроводных каналов структурированных кабельных систем для передачи высокоскоростных информационных приложений // Информационные технологии. 2014. № 5. С. 52-56.

ПРОБЛЕМАТИКА ПРИМЕНЕНИЯ ЦИФРОВЫХ ТЕХНОЛОГИЙ ПРИ УПРАВЛЕНИИ МЕДИЦИНСКИМИ УЧРЕЖДЕНИЯМИ

Сюсин К.А., магистр группа ИМО-МП-20
Исаева Г.Н., к.т.н.,
Логачева Н.В., к. т. н., доцент
Технологический университет имени («МГОТУ»),
Россия, г. Королев

Рассматриваются проблемы управления медицинскими учреждениями в соответствии с основными целями цифровой экономики в медицинской сфере и технологий при управлении медицинскими учреждениями. Поставлен вопрос о необходимости применения Data-driven подхода в управлении медицинскими учреждениями.

Ключевые слова: Data-driven, цифровые технологии управления, управление, CRISP-DM.

Развитие информационных технологий затрагивает практически все сферы привычной жизни человека. Помимо прочего, технологический прогресс вносит новое, в том числе, в определяющую компоненту существования человека – в управление. От управления отдельным элементом до управления организациями разных масштабов – всё это может развиваться с использованием новых достижений прогресса.

В настоящее время важным является создание экосистемы цифровой экономики, в которой данные в цифровой форме являются ключевым фактором производства во всех сферах социально-экономической деятельности и в которой обеспечено эффективное взаимодействие. Здравоохранение является важной сферой деятельности государства, которая является важным показателем уровня социального и экономического развития общества. Развитие системы здравоохранения в России является одним из приоритетных задач деятельности государства. Здравоохранение, как сфера деятельности, ориентирована на обеспечение качественного и доступного медицинского обслуживания. Оно развивается в современных рыночных условиях, что предполагает разработку механизмов эффективного использования ограниченных ресурсов.

Здравоохранение в России является одним из направлений, включенных в национальную программу «Цифровая экономика Рос-

сийской Федерации» [4]. В развитие этой программы реализуется федеральный проект «Создание единого цифрового контура в здравоохранении на основе единой государственной информационной системы в сфере здравоохранения (ЕГИСЗ)».

Эффективность использования имеющихся ресурсов не является достаточно высокой, по сравнению с развитыми странами [2]. Среди проблем развития здравоохранения в России следует отметить следующие:

– недостаточно сбалансированная программа государственных гарантий бесплатного оказания медицинской помощи;

– структурная диспропорция источников финансирования на здравоохранение;

– слабая мотивация работников сферы здравоохранения.

Выделенные проблемы затрагивают, в том числе, и управление медицинским учреждением. Сегодня можно выделить довольно широкий спектр проблем, связанных с управлением медицинским учреждением и его (управления) эффективностью:

– Кадровый вопрос (проблемы укомплектования кадрами в динамически изменяющихся условиях окружающей общественно-экономической среды, проблемы рационального использования кадров, обучение)

– Вопрос использования ограниченных бюджетных ресурсов в динамических изменяющихся условиях окружающей общественно-экономической среды

– Вопрос распределения рабочих задач во времени (необходимость грамотного распоряжения всеми имеющимися ресурсами для достижения заданных целей в ограниченные сроки)

– Вопрос доступности получения медицинских услуг

– Вопрос качества услуг, оказываемых учреждением.

Одним из направлений решения указанных проблем является применение подходов, связанных с цифровой медициной.

Цифровая медицина является одним из направления совершенствования предоставления медицинской помощи. Она предполагает существенное повышение качества и эффективности медицинского обслуживания за счет использования результатов обработки и анализа больших объемов медицинских данных в цифровом виде. В настоящее время по данным аналитического агентства cnews [1] информационные технологии обработки медицинской информации применяются в основном для проведения статистического анализа.

Поэтому одним из основных направлений развития цифровой медицины можно назвать применение математических методов (включая методы искусственного интеллекта, глубокого изучения и обработки больших данных) при обработке медицинских данных.

Цели цифровой экономики в медицинской сфере:

1. Повышение конкурентоспособности на глобальном рынке как отдельных отраслей экономики Российской Федерации, так и экономики в целом

2. Создание необходимых и достаточных условий институционального и инфраструктурного характера для создания и развития высокотехнологичных медицинских отраслей

3. Повышение эффективности управления медицинскими организациями

Для достижения этих целей необходимо применение подходов, опирающихся на глубокое изучение данных, позволяющий принимать соответствующие решения на основе конкретных метрик-показателей, являющимися основой для проверки достижения целей, поставленных конкретными бизнес-задачами. Такой подход, основанный на глубоком изучении данных, получил название Data driven (управляемый данными). В настоящее время он активно применяется в различных сферах деятельности.

Основная идея использования data-driven подхода [3] заключается в том, чтобы принимать решения, основываясь на анализе данных статистики, а не на интуиции и личном опыте.

Важно отметить, что, основанный на анализе данных data-driven, требует предварительной подготовки собираемых данных для последующего анализа. Подготовка данных требует тщательной подготовки, так как именно результаты их анализа должны служить основной принятия управленческих решений.

Можно выделить основные принципы data-driven подхода:

- Данные необходимо извлекать, хранить, анализировать, интерпретировать и визуализировать
- важная часть работы с данными - их анализ и построение гипотез. Для этого требуются специальные знания и опыт
- данные должны быть точными и чистыми - тогда им можно будет доверять и правильно интерпретировать
- прежде чем предпринять что-то важное, нужно собрать и проанализировать данные.

Представление данных, в свою очередь, сводится к:

- формированию необходимой структуры данных
- сбору данных
- применению структурированных данных в анализе.

Одним из описаний возможного подхода является методология CRISP-DM - Cross-Industry Standard Process for Data Mining.

Согласно CRISP-DM, аналитический проект состоит из шести основных этапов, выполняемых последовательно:

1. Бизнес-анализ (Business understanding).
2. Анализ данных (Data understanding).
3. Подготовка данных (Data preparation).
4. Моделирование (Modeling).
5. Оценка результата (Evaluation).
6. Внедрение (Deployment).

Оригинальные этапы создания аналитического проекта в рамках методологии CRISP-DM представлены на рис. 1. Перевод на русский язык представлен под английским оригиналом.

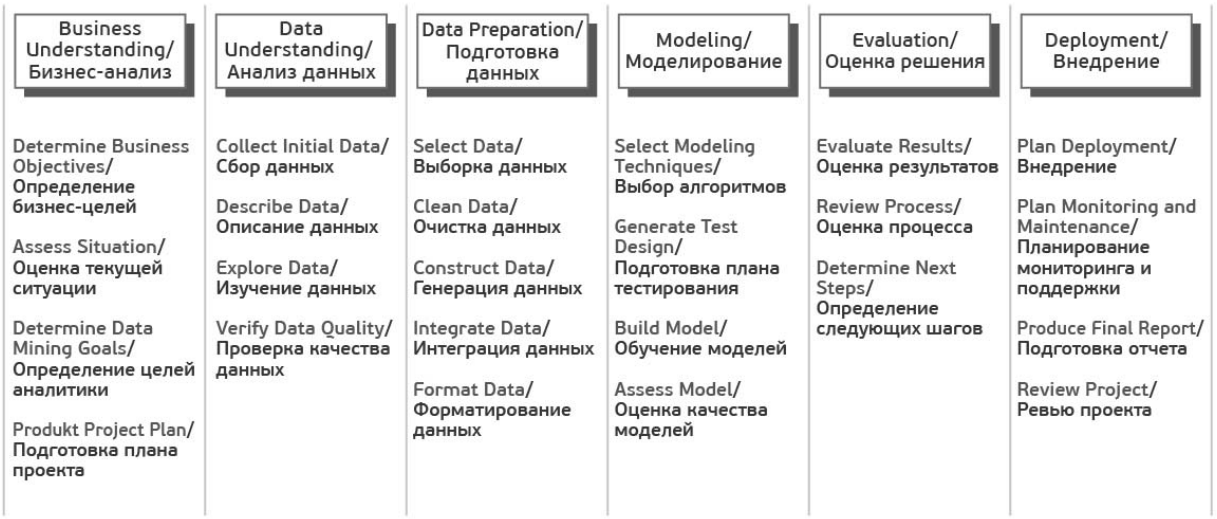


Рис. 1. Этапы создания аналитического проекта в методологии CRISP-DM

В случае применения принципов data-driven подхода для управления медицинским учреждением, нужно внимание на:

1. Бизнес-анализ и постановку целей.
2. Процесс анализа данных – выбор нужного источника данных, изучение данных и их проверка.
3. Процесс подготовки данных – их выборки, формирования, представления, интеграции и интерпретации.
4. Оценку решения.
5. Принятие решения.

Важно, чтобы текущие бизнес-цели были достижимы и были подобраны соответствующе метрики, которые показывают степень достижения поставленной цели. Такие метрики должны обладать следующими свойствами:

1. Метрик не должно быть чрезмерно много.
2. Метрика должна быть сравнимой (для получения возможности сравнения с предыдущим периодом, так как интерес может представлять и динамика изменения).
3. Метрика должна выражаться в относительных показателях.

Также принятию решения может способствовать визуализация – графики и тепловые карты можно использовать для наглядной демонстрации тех, или иных аспектов управления медицинским учреждением, когда, например, решается вопрос о распределении сил на разные направления.

Таким образом, представляется возможным применение принципов data-driven и для управления медицинскими учреждениями.

В ходе данной работы были рассмотрены цели цифровой экономики в области медицины, а также рассмотрена возможность использования управленческого подхода на основе глубокого анализа данных в сфере управления медицинскими учреждениями.

Были сделаны выводы о наличии возможности использования такого управленческого подхода в сфере управления медицинскими учреждениями.

Список использованных источников

1. ИТ в здравоохранении 2020/ [Электронный ресурс] URL: https://www.cnews.ru/reviews/it_v_zdravoohranenii_2020 (дата обращения: 5.05.2021)

2. Назаров В.С., Аквисентьев Н.А. Российское здравоохранение: проблемы и перспективы // Финансовый журнал. 2017. №4. [Электронный ресурс] . URL: https://www.nifi.ru/images/FILES/Journal/Archive/2017/4/articles_2017_4/fm_2017_4_01.pdf (дата обращения: 7.05.2021)

3. Описание подхода data-driven, Методология CRISP-DM 1.0 [Электронный ресурс]. URL: https://www.the-modeling-agency.com/crisp-dm.pdf (дата обращения: 5.05.2021)

4. Цифровая экономика Российской Федерации. [Электронный ресурс] URL: http://static.government.ru/media/files/ 9gFM4FHj 4PsB79I5v7yLVuPgu4bvR7M0.pdf (дата обращения: 7.05.2021)

СОВРЕМЕННЫЕ ТЕХНОЛОГИИ ДЛЯ СОЗДАНИЯ WEB-ПРОДУКТОВ

Исаева Г. Н., к.т.н.,
Логачёва Н.В, к.т.н., доцент,
Авраменко И.А., бакалавр группы ИО-18 ,
Технологический университет имени («МГОТУ»),
Россия, г. Королев

В данной статье рассмотрены современные технологии для создания web-продуктов в малых и средних проектах. Наиболее популярными считаются технологии, позволяющие создавать простые мобильные приложения, основанные на каком-либо web-продукте. Приводятся статистические данные за последние периоды времени о востребованности на рынке программного обеспечения таких технологий, показаны тенденции их дальнейшего развития в ИТ-сфере.

Ключевые слова: программные технологии, web-продукты, мобильная разработка, программное обеспечение.

Мир информационных технологий (ИТ) никогда не стоит на месте – он динамично развивается согласно новым требованиям экономической и социальной деятельности современного общества. Особое место в текущее время занимают web - технологии и программные средства их разработки. Ежегодно появляются новые технологии для создания web-продуктов в малых и средних проектах, причём, акцент делается на возможности технологии быть использованной и для мобильных программных приложений [1],[3],[4]. Рассмотрим наиболее востребованные.

На первом месте следует отметить относительно новую технологию создания прогрессивных web-приложений.

Progressive Web Apps. PWA (Progressive Web Apps англ. прогрессивные веб-приложения) – это стремительно развивающаяся технология, популярная как у небольших компаний, так и у крупных ИТ гигантов, таких как Google, Samsung, Mozilla, Microsoft и др.

PWA позволяет без колоссальных ресурсов создавать простые мобильные приложения, основанные на каком-либо web-продукте. Например, если у вас есть свой сайт, интернет-магазин или иной web-проект, технология PWA позволит быстро, не затратно, создать на его основе мобильное приложение. Такое приложение может выполнять основные функции стандартного, в общем понимании, мобильного

приложения: работать в офлайн-режиме (благодаря сохранению данных в кэше устройства и обновлению новых данных, при наличии подключения к интернету), отправлять уведомления, обеспечить кроссплатформенность [4].

Если посмотреть на механизм работы данного вида приложения на мобильном устройстве, то он опирается на принципы работы стандартного мобильного приложения при работе с сайтом, но загрузка сайта происходит из самого устройства, а обновления уже подгружаются из сети во время использования приложения. Такой механизм повышает скорость развёртывания web-сайта на устройстве. Необходимо отметить качественные показатели данной технологии: PWA-разработки быстрые, надежные удобные, популярны у большого количества пользователей.

Анализ использования интернет- сервисами технологии PWA показал, что их популярность значительно выросла, после внедрения прогрессивных веб-приложений, так как основной задачей прогрессивных веб-приложений, помимо простоты разработки, является улучшение пользовательского опыта, чего часто не хватает стандартным мобильным приложениям. Так, для издания «The Washington Post», после перехода на PWA, посещение сайта выросло на 12%. Интернет-магазин «AliExpress» при помощи внедрения PWA увеличил конверсию на 104% (во всех браузерах); социальный интернет-сервис «Pinterest», благодаря технологии PWA, получил рост доходов от рекламы на 44%, а вовлеченность на 60%.

Некий «бум» PWA приходится на 2018 год; начиная с этого времени, по результатам данных сайта almanac.httparchive.org, наблюдается поступательный рост в использовании технологии. Можно сделать вывод, что за последние пять лет PWA востребована и прогрессивна. Но, конечно же, данной технологии в этом сегменте программного обеспечения составляют конкуренцию технологии, ориентированные на разработку мобильных нативных приложений. Нативные или собственные приложения (англ. native apps) - прикладные программы, которые разрабатываются под определённое устройство на определённой платформе. Например, приложения для IOS разрабатываются на языке Swift или Objective-C. Тоже самое как Java и Kotlin для Android-приложений. Нативные приложения имеют ряд преимуществ, таких как: более высокая оптимизация и нацеленность на конкретную разработку проекта, безотказность в размещении на популярных платформах App Store и Play Store и др.[3]. Поэтому,

рассматриваемая технологии PWA, в качестве разработки мобильных приложений, ориентированных на связь с программными web-продуктами, пока уступает по популярности в использовании, что и подтверждают статистические данные(statista.com). Сравнительный анализ двух технологий представлен диаграммой на временном интервале от 2018 до 2021 годов (рис. 1).

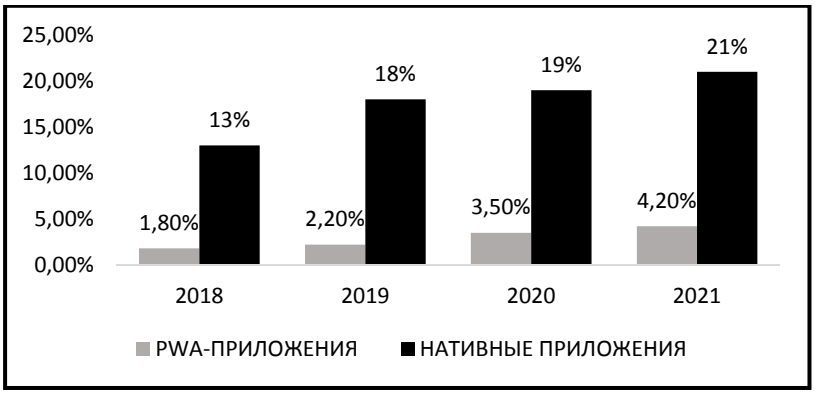


Рис. 1. Популярность использования (процент к базовому периоду 2017г.) нативных и PWA приложений

Следующей технологией, заслуживающей внимания для реализации web-приложений и востребованной на рынке программных продуктов, является **Single page application.**

SPA (Single page application англ. одностраничные веб-приложения) – это приложение или web-ресурс, использующее один HTML-документ как оболочку для всего функционала. Естественно, в SPA не используют один единственный HTML,CSS,JS файлы, они лишь динамически подгружаются по мере необходимости. Эта технология даёт ряд преимуществ, заключающихся в: отсутствии переходов, повышении производительности и скорости работы, оптимизации трафика, отличном UX/UI (User experience/user interface англ. пользовательский опыт и пользовательский интерфейс) [2].

Одностраничные web-приложения очень популярны сегодня и востребованы для разработки таких крупных сервисов, как: Google Disk, Google Maps, Gmail, Twitter, Trello.

Если говорить о перспективных направлениях развития новых и уже используемых технологиях в области мобильных приложений, web-сайтов и web-приложений, то необходимо отметить искусственный интеллект, облачные технологии, «гибридные технологии»[4].

Artificial Intelligence (AI - Artificial Intelligence англ. искусственный интеллект) – общее название для продукта, в функционале

которого присутствуют нейронные сети. Эксперты утверждают, что за AI-технологией будущее, эта технология уже используется в решении задач: бизнес-прогнозирования, аналитики различных данных, дизайне. Искусственный интеллект способен автоматизировать различные процессы, такие как: верстка, web-райтинг и много других рутинных процессов web-разработки.

Гибридная реальность (MR, англ. Mixed reality) - это термин для смеси виртуальной и дополненной реальности. Такая технология помогает повысить пользовательский опыт, ощутить реальность, но с помощью виртуального пространства. MR позволяет визуализировать тот или иной объект, действие, процесс, что повышает интерес пользователей к познанию реальности. Применяется технология на сегодняшний день в рекламе, web-продуктах, сфере развлечения, обучении. Например, сайт IKEA, благодаря технологии MR повысил свою конверсию: покупатель не выходя из дома может видеть покупаемые предметы мебели, рассмотреть их в пространстве, ощутить объём.

Выводы: Существующие и появляющиеся технологии разработки web-продуктов ориентированы на повышение пользовательского опыта и автоматизации создаваемых проектов. Происходит апробация соединения различных методов и подходов к разрабатываемым программным продуктам, ориентированным на новые потребности и тенденции развития общества.

Список использованных источников

1. Исаева Г.Н., Сидоров Ю.Ю. Использование мобильных-технологий для повышения эффективности взаимодействия программных систем Информационно-технологический вестник». - 2019. - №1(19). - С.74-80

2. Майкл Миковски, Джош Пауэлл. Разработка одностраничных веб-приложений: JavaScript End-to-end. — ДМК Пресс, 2018. — 512 с.

3. Нативные, гибридные и web-приложения в сравнении // Код доступ: https://medium.com/nuances-of-programming, [Дата обращения 06.04.2022]

4. Основные тренды веб-разработки 2021 // expinet.ru: Экспертная сеть expinet// Код доступ: https://expinet.ru/stati/osnovnye-trendy-veb-razrabotki-2021.html, [Дата обращения 06.04.2022]

ДИНАМИЧЕСКАЯ И ФУНКЦИОНАЛЬНАЯ МОДЕЛИ СИСТЕМЫ ЭЛЕКТРОННОГО ДОКУМЕНТООРБОРОТА

Булаева О.В., преподаватель кафедры информационных технологий и управляющих систем,
Технологический университет («МГОТУ»),
Россия, г. Королев

21 век – век высоких технологий. Быстрый обмен информацией это неотъемлемая часть современного мира. Для того, чтобы соответствовать этому требованию, нужны современные, качественные, надежные системы документооборота. В связи с этим была создана специальная система -«Система электронного документооборота».

Система электронного документооборота(СЭД) - автоматизированная многопользовательская система, сопровождающая процесс управления работой иерархической организации с целью обеспечения выполнения этой организацией своих функций.

Ключевые слова: динамическая модель, функциональная модель, системы электронного документооборота

Уже многие годы обычный бумажный способ передачи документов заменяется электронными организациями. В настоящее время электронные документы приобретают большую популярность, одно из главных качеств – сокращение времени, также нельзя не отметить возможность удаленно заниматься делопроизводством. СЭД (система электронного документооборота) очень много - функциональна, и с достаточной степенью надежности система выполняет требования как показано на рис. 1.

Сейчас очень ценится хранение важных документов, и СЭД (система электронного документооборота) как раз является надежным хранилищем данных. Она сохраняет всю информацию в специально созданных архивах. Так же, во избежание утери или порчи компьютерных файлов, информация хранится на двух или более дисках. Вдобавок система может поддерживать любой тип документов.

Использование системы электронного документооборота(СЭД) помогает в многих аспектах работы с документами таких как:

Рис. 1. Классификация СЭД

- **Использование меньшего кол-ва бумаги в организации.** Использование и хранение бумаги занимает большое кол-ва места в организации, заменив их на электронные документы можно освободить эти места под рабочие места для новых сотрудников и увеличить производительность предприятия
- **Меньше затрат на содержание документов.** Хранение бумажных документов требует большого пространства, по сравнению с электронными.
- **Удобность использования.** Электронные документы проще искать и систематизировать в отличие от бумажных.
- **Автоматизация.** При работе с бумажными документами тратиться огромное кол-во времени для передачи документов от одного сотрудника к другому.
- **Надежность документов.** Бумажные документы могут потеряться или испортиться при использовании в отличии от электронных

которые надежно хранятся в системе и которые легко найти нужный документ по поиску в системе.

- **Выше скорость документооборота.** Электронные документы доставляются почти мгновенно и всегда можно узнать получила ли вторая сторона документ.
- **Легкая работа с другими службами (Налоговая и т.д.).** Необходимые документы можно выгрузить из системы и отправить в инстанцию.

СУБД (система управления базами данных) позволяет не только создавать базы данных, но и осуществлять в них сортировку и поиск данных. Благодаря ядру, которое отвечает за управление данными во внешней и оперативной памяти и журнализацию, а также процессору языка БД (база данных), обеспечивающий поиск оптимального плана выполнения запросов из всех возможных вариантов для заданного запроса с целью уменьшения использования вычислительных ресурсов.

На рис. 2 представлена структура системы электронного документооборота.

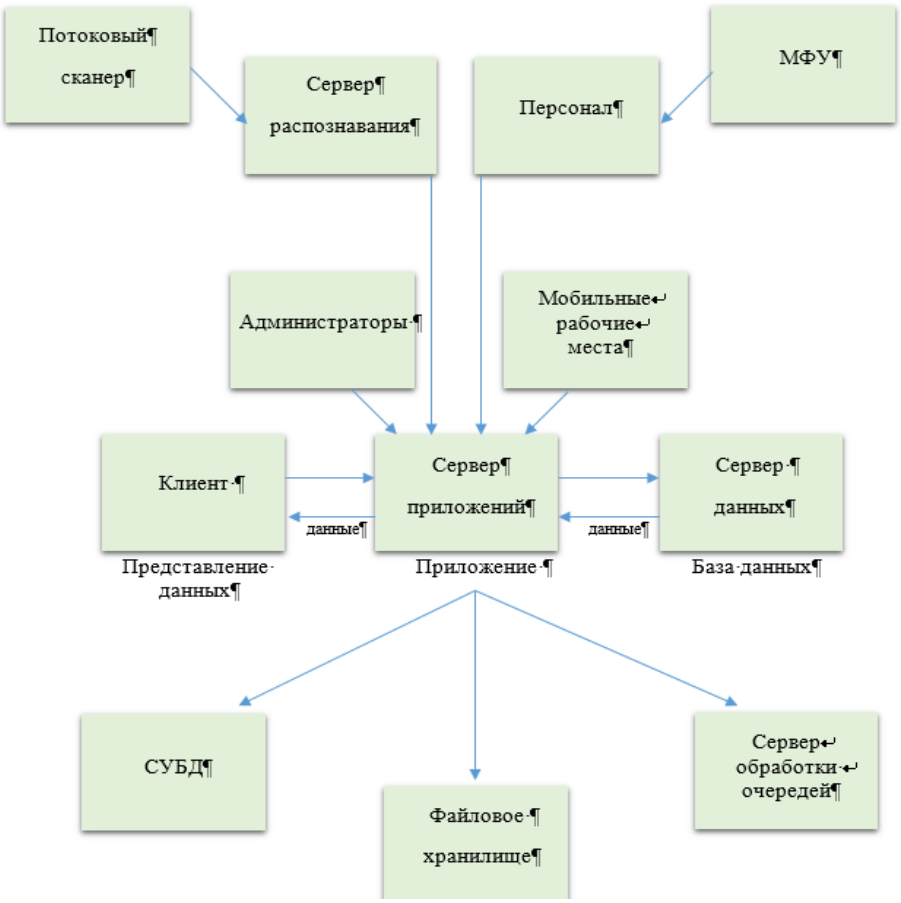


Рис. 2. Структура СЭД

Такая структура документооборота является легкой и доступной для тех пользователей, которые не часто пользуются СЭД.

Сервер очередей - отдельный процесс, который принимает сообщения от производителей и распределяет их между заказчиками сообщений. В качестве производителей и заказчиков сообщений могут быть разные процессы и службы.

На рис. 3 представлено взаимодействие разных систем в реализации фотохостинга.

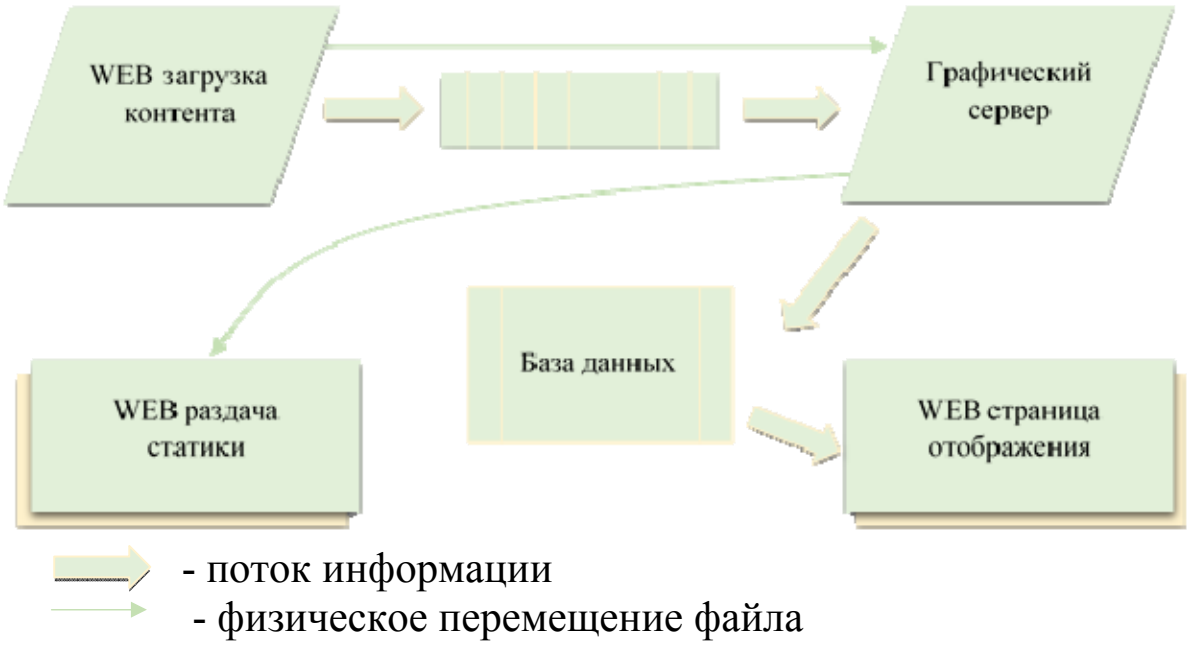


Рис. 3. Реализации фотохостинга

Такая система подходит для организаций с большим числом посещений разных файлов. Она работает по следующему принципу: после получения информации, сервер передает ее в виде сообщения на сервер очередей. Программа постоянно обновляет сервер очередей, для того чтобы принять следующую информацию о новом загрузочном материале и переводит ее в нужный формат.

На рис. 3 представлено взаимодействие разных систем в реализации фотохостинга. Такая система подходит для организаций с большим числом посещений разных файлов. Она работает по следующему принципу: после получения информации, сервер передает ее в виде сообщения на сервер очередей. Программа постоянно обновляет сервер очередей, для того чтобы принять следующую информацию о новом загрузочном материале и переводит ее в нужный формат.

Система Электронного документооборота(СЭД). Использование системы электронного документооборота(СЭД) поможет сократить множество аспектов таких как

- Сотрудники на 30% меньше тратят времени на согласование документов;
- В три раза снижаются затраты расходные материалы;
- До 25% растет производительность труда;
- До 80% меньше трат на хранение документов.

На рисунке 4 мы видим, что система электронного документооборота(СЭД) помогает уделять больше времени для работы над содержимым чем бумажный документооборот.

Рис. 4. Преимущества СЭД

Это происходит из–за того что руководитель может контролировать выполнением все работы своими работниками. Так же система электронного документооборота помогает оптимизировать процесс обучения новых сотрудников так как он помогает доставлять новые инструкции и положения значительно быстрее чем при информиро-

вании каждого сотрудника по отдельности. На рис. 5 мы можем заметить, что затраты на бумагу, тонер картридж и т.п. идут в пустую.

Рис. 5. Бесполезные затраты

Но не смотря на все плюсы системы электронного документооборота есть и минусы. один из таких минусов — это вирусы. То есть вероятность повреждения базы данных неизвестным вредоносным кодом. Решение этой проблемы поможет регулярное резервирование информации на неподключенных к сети устройствах.

Так же одна из проблем — это сложность адаптации сотрудников возрастной категории 40+ к цифровой форме взаимодействия. Так как более старшему поколению трудно даются цифровые технологии.

Еще одна из проблем это - высокая стоимость. Цена отечественной СЭД для малых предприятий колеблется в пределах 1000-10000 долларов

Подводя итог, можно сказать о том, что в современном развивающемся мире количество электронных документов стремительно растет. Эффективное функционирование каждой организации, независимо от ее профиля, находится в прямой зависимости от уровня

оперативной обработки документации и информации, скорости взаимодействия между организациями.

СЭД обеспечивает процесс создания управления и распространения электронных документов в компьютерных сетях, а также контроль и хранение документов в организации.

СЭД является одной из самых востребованных систем так как позволяет повысить эффективность управления организации предоставляя всю необходимую информацию, которая могла быть утеряна.

Список используемых источников

1. Ковалева, О.В. Особенности современных информационных систем, существенные с точки зрения безопасности / О.В. Ковалева // Эволюционные процессы информационных технологий: сб. труд. 4-й межвузовской научно-технической конференции с международным участием. – М.: Издательство «Научный консультант», 2019. - С.114-118.

2. Ковалева, О.В. Инновационные аспекты социально-экономического развития региона / О.В. Ковалева // Сборник статей VIII Ежегодной научной конференции аспирантов «МГОТУ». – М.: Издательство «Научный консультант», 2018. - С. 245-252.

3. Боев, В.Д. Компьютерное моделирование / В.Д. Боев. - СПб.: ВАС, 2014. — 432 с.

4. Чертовской, В. Д. Моделирование процессов адаптивного автоматизированного управления производством: монография / В. Д. Чертовской. - Санкт-Петербург: Лань, 2019. - 200 с.

5. Иванова, С. М. Теория информации. Моделирование интеллектуальных систем: учебное пособие / С. М. Иванова, З. В. Ильиченкова. - Москва: РТУ МИРЭА, 2020. - 65 с.

ОБЕСПЕЧЕНИЕ СИНХРОНИЗАЦИИ МНОГОКАНАЛЬНОГО СБОРА ДАННЫХ С РАЗЛИЧНОЙ СТЕПЕНЬЮ ДИСКРЕТИЗАЦИИ В МОМЕНТ РЕГИСТРАЦИИ В ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНОЙ СИСТЕМЫ НОВОГО ПОКОЛЕНИЯ

Елькин С.В., магистр группы ИМО-ПИ 21,
Жиделев М.А., магистр группы ИМО-ПИ 21,
Технологический университет («МГОТУ»),
Россия, г. Королев

Основная цель статьи – показать процесс синхронизации многоканального сбора данных с различной степенью дискретизации в момент регистрации в информационно-измерительной системы нового поколения, обеспечивающей всестороннее информационное обслуживание разработки высотных кислородно-водородных ЖРД на этапах контрольных, сертификационных и лётных испытаний, повышение точности и информативности результатов измерений, интенсификацию процессов обработки и анализа данных испытаний.

Ключевые слова: многоканальная измерительная система, кабель, измерения, космос, ракетный двигатель, крейт, КСВИ-106, регистрация параметрических данных, ЖРД, датчик.

Введение. Испытательный стенд В2 КСВИ-106 был введен в эксплуатацию в 1967 году. Предназначен для испытания жидкостных ракетных двигателей и ракета-носителей на компонентах: керосин, кислород и водород. Так же имеются рабочие места для калибровки расходомеров и проливки труб из различных композитных материалов. Испытательный стенд В2 имеет богатую историю. За все время существования были испытаны двигатели на жидкостном ракетном топливе не только советские и российские, но также и зарубежные [3].

Основной раздел. В общем виде информационно-измерительная система стенда В2 состоит из двух подсистем: подсистема сбора и обработки быстроменяющихся параметров и медленноменяющихся. Вся система должна быть объединена в одну компьютерную сеть для обмена полученными дынными.

Работа системы измерений. Во время проведения испытаний второй ступени ракетных двигателей идет параллельный, одновременный обмен с 20-ю компьютерами визуализации. Система измерений даёт возможность проводить замеры с различными внешними

параметрами. Давление может колебаться вакуумного 0 до 400 атмосфер. Температура внешней среды и рабочей жидкости может достигать 1500 градусов Цельсия. Имеет поддержку разного уровня криогенных жидкостей, пульсации. Все уровни измерительной системы обеспечиваются модулем искрозащиты [2].

Получение значений при измерении происходит по средствам разнообразных датчиков. Датчик представляет собой моноблочную конструкцию, включающую в себя чувствительный элемент в виде металла и первичный преобразователь сигнала. В ходе замеров внешняя среда определенным образом действует на сердцевину и она деформируется, первичный преобразователь сигнала преобразует деформацию пружины в сигнал переменного тока, который поступает на АРМ сбора для хранения.

Информация о метках времени на выходе из аппаратуры единого времени передается в формате IRIG-B от сервера единого времени, а также сигнал старта испытаний на расстояния до 350 метров, с наличием гальваноразвязки для всех единиц системы. Это все возможно при наличии в схеме подключения передатчика и приемника, с помощью которых и происходит передача сигнала на большое расстояние с высокой точностью.

Работа информационно-измерительной системы. Информационно-измерительная система является новейшим серийным продуктом компании «Лаборатория автоматизированных систем», предназначенная для проведения удаленных, точных замеров различных параметров, требуемых для исследования. Преимуществами данных информационно-измерительных систем являются:

– взаимодействие с базой данных стенда, благодаря чему можно создавать готовые конфигурации с использованием привычной терминологии отрасли;

– полное предоставления прав на взаимодействие с готовой конфигурацией, что дает возможность всячески ее изменять;

– единый пользовательский интерфейс для взаимодействия с измерительным оборудованием и каналами связи;

– возможность проводить измерительные работы с датчиками различного напряжения;

– программное обеспечение позволяет визуализировать полученные данные с датчиков, для дальнейшей обработки;

– возможность разделение ролей пользователей, администрирование.

Еденный пользовательский интерфейс представлен на рис. 1.

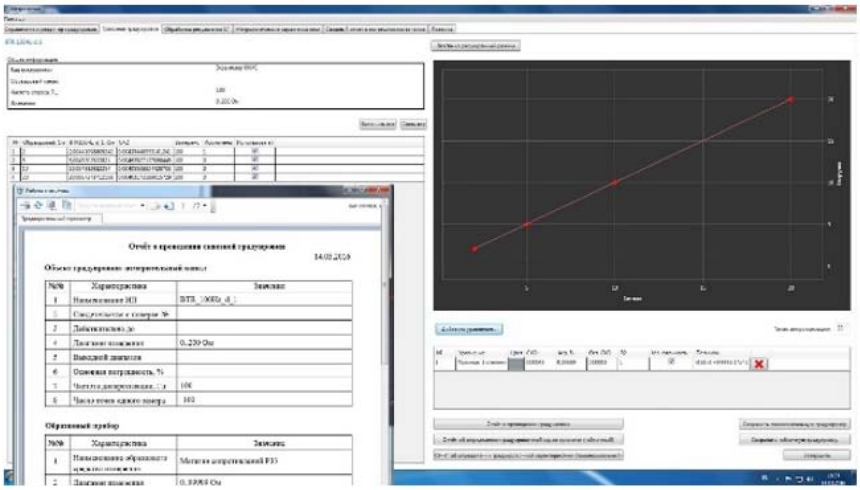


Рис. 1. Программное обеспечение L-Card

Аппаратная часть информационно-измерительной системы выполнена в модульном виде, что позволяет добавлять, изменять, убирать модули в процессе эксплуатации каналов. Модули системы используются для: измерения давления, расхода, температуры, вибрации и других частотных сигналов.

Все модули информационно-измерительной системы имеют дублирующие компоненты.

Для получения корректных данных при работе информационно-измерительной системы следует решить ряд вопросов с синхронизацией всех измерительных и обрабатывающих модулей системы. Для этого имеется модуль синхронизации с применением технологий GPS. Информационно-измерительная система включает в себя так же общий сервер, использующийся для централизованного доступа к результатам измерения со всех модулей.

Сервер выполняет следующие функции:

– хранит в базе данных все результаты испытаний;
– резервное копирование баз данных;
– динамическое присвоение IP-адресов;
– синхронизация времени полученного от спутников с временем на АРМ;
– предоставление единого удаленного доступа к АРМ.

Кроме того, синхронизация позволяет согласованно, буферизировано подключить высокоомные аналоговые сигналы, обеспечивает

работу с потенциометрическими дублированными датчиками и аналогово-цифрового преобразователя типа LTR11.

Расположение и устройство информационно-измерительной системы позволет использовать подключение дискретных сигналов по схеме «сухой контакт» с логическими портами системы. Схематичексое подключение элементом системы представлено на рис. 2.

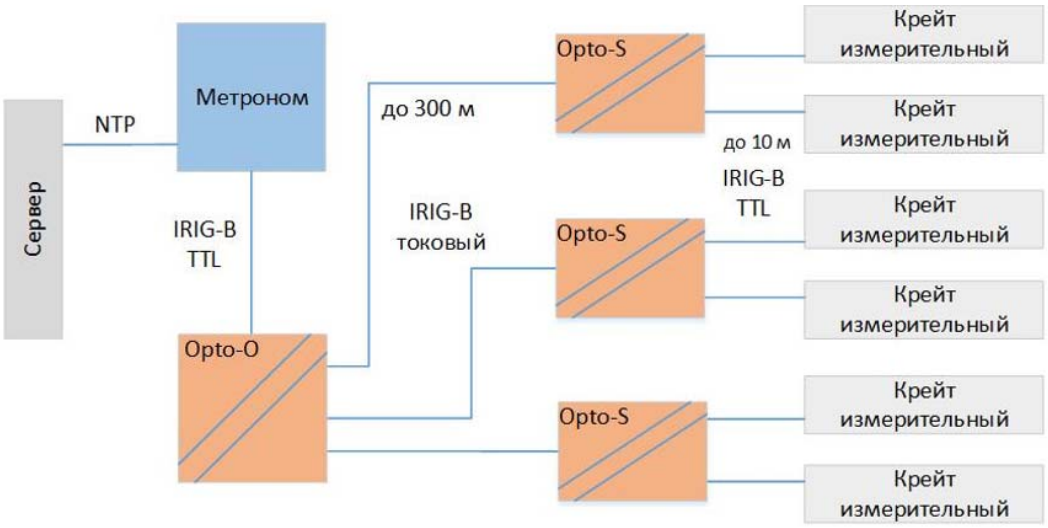


Рис. 2. Схематическое подключение сигналов

Обозреваемый информационно-программный комплекс успешно использовался при испытаниях не только холодных проливок, но и испытание ракетного двигателя работающего на кислородно-водородном топливе.

Информационно-измерительная система имеет 1423 каналов, при этом все они еще и дублируются, дабы максимально избежать потерь информации в случае аварии. Для дублирования сигналов с датчиков существует устройства раздвоения сигналов, которое раздваивает сигналы и направляет их на две системы: основную и дублирующую. Устройство раздвоения сигналов рассчитано на подключения до 16 различных датчиков. После раздвоения сигнал поступает на устройства усиления сигнала, где с помощью повторителя на 2 системы поступает сигнал с одним и тем же значением. Электропитание для дублирующей системы и основной осуществляется через блоки питания (резервного и основного) [2].

Измерительная система является не только многоуровневой, но и распределенной, при этом все модули исполнены в искробезопасном режиме. Стенд, на котором установлена система, имеет в себе

ряд стационарных датчиков, с которых на информационно-измерительный комплекс поступает информация о показаниях. После чего первичная информация поступает в бункер для дальнейшей обработки и структуризации в режиме реального времени.

Информационная система является уникальной и поэтому для нее были специально разработаны и запрограммированы аппаратные и программные продукты, такие как: платы для дублирования поступающего сигнала с датчиков. Главная задача плат дублирования – обособить сигналы друг от друга, чтобы избежать помех на линии передачи сигнала. Платы дублирования позволяют подключать датчики типа: дискретные, термопарные, сопротивления, потенциометрические.

Сейчас данные платы поставлены на конвейер и выпускаются в огромном количестве, для обеспечения потребностей различных отраслей.

Пример платы дублирования подключений представлен на рис. 3.

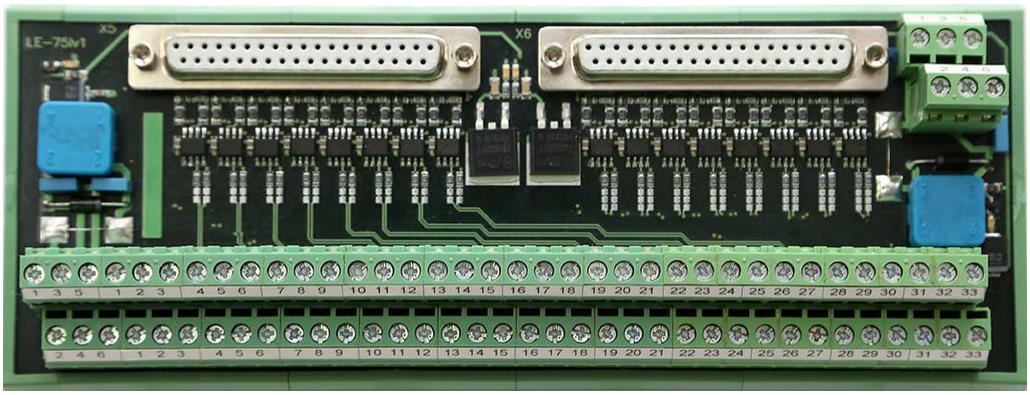


Рис. 3. Плата для дублирования подключений.

Для того, чтобы сигналы, поступавшие на основную и дублирующие системы существует в цепи устройства для согласования сигналов предназначенное для гальванической развязки и дублирования входных команд на основную и дублирующую системы. Одно устройство рассчитано на работу с 16 каналами связи. Строение каждого канала связи имеет 3 элемента: фильтр, буферный элемент и оптической пары кабеля. Запитка осуществляется при помощи двух блоков питания на 9 В и на 24 В [5 - 7]. На входя каждого канала связи имеется плавкий предохранитель, который защитит модуль в случае скачка напряжения. Для индикации работы модуля служат свето-

диоды. Структура устройства согласования сигналов представлена на рис. 4, а интерфейс подключения представлен на рис. 5.

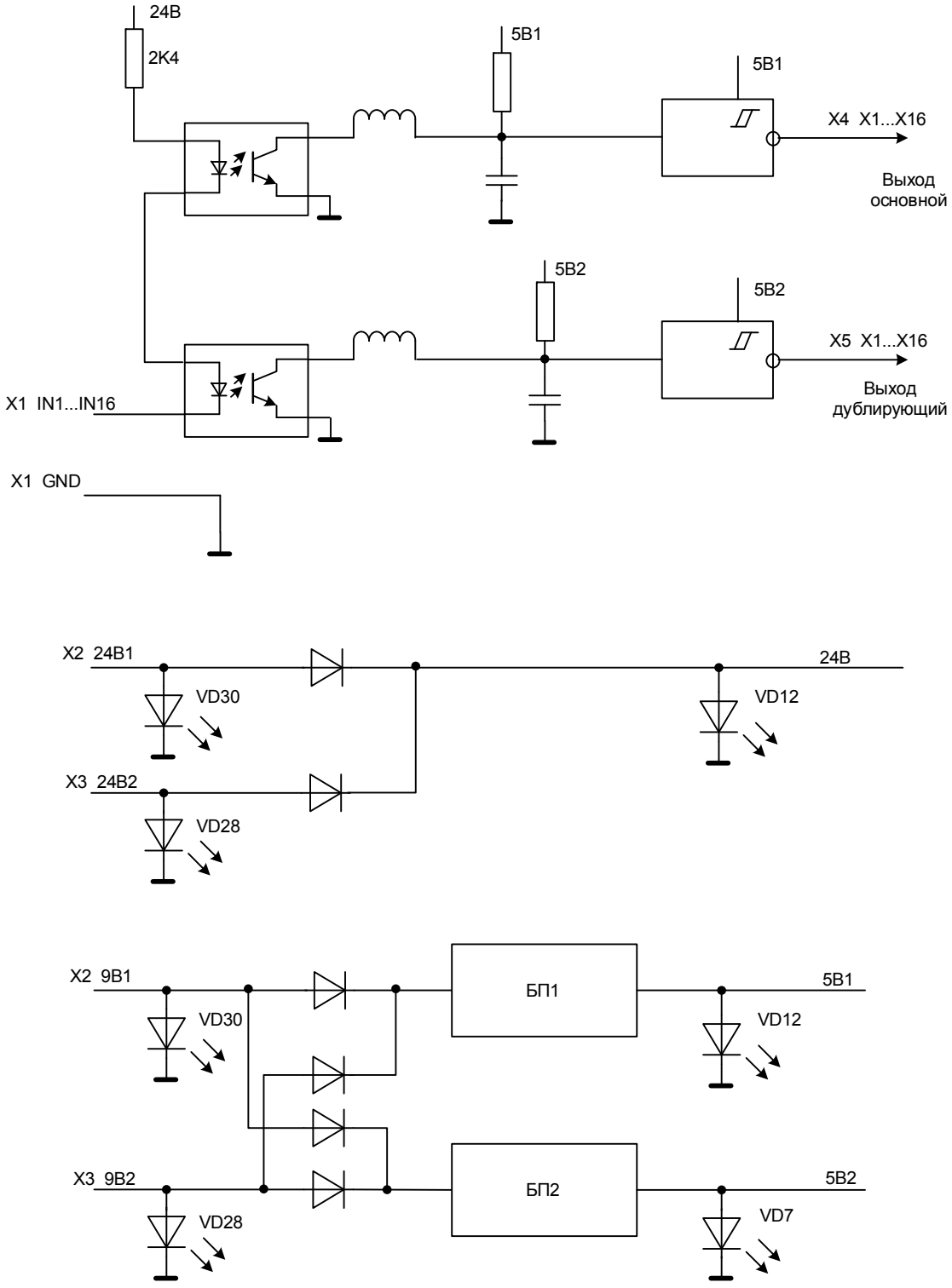


Рис. 4. Структурная схема устройства I-АНР3

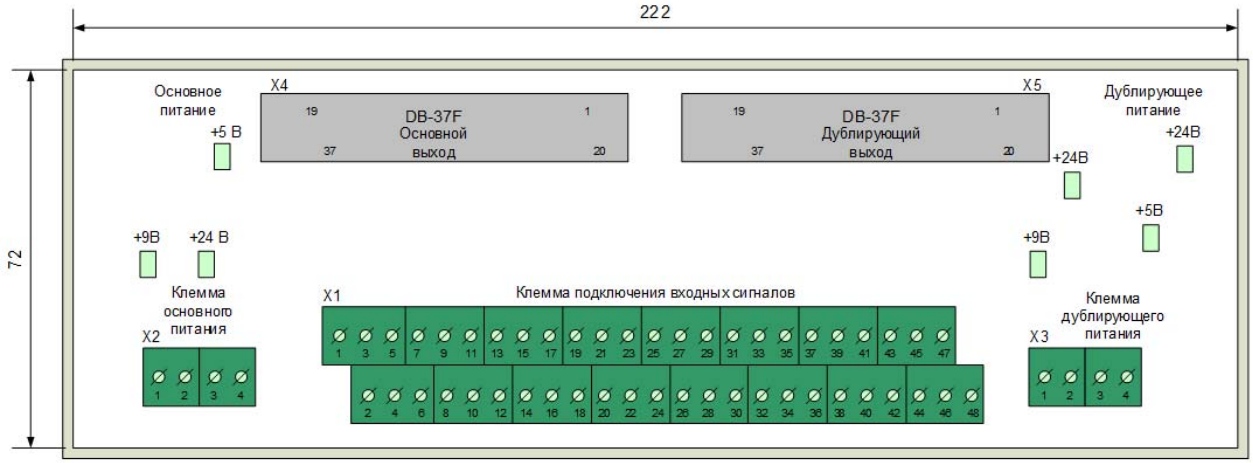


Рис. 5. Интерфейс подключения устройства I-AHP3

Заключение. Информационно-измерительную систему стенда В2 КСВИ-106 разработала компания «Лаборатория автоматизированных систем (АС)». Информационно-измерительная система является универсальной и может быть использована для других отраслей промышленности [2].

Список использованных источников

1. Справочники и руководства пользователя научно-производственного предприятия «Мера».

2. Разработка и производство электронного измерительного оборудования, 2021. [Электронный ресурс]. URL - https://www.lcard.ru/(дата обращения 18.01.2022).

3. ФКП «Научно-испытательный центр ракетно-космической промышленности», 2021. [Электронный ресурс]. URL- http://www.nic-rkp.ru/ (дата обращения 20.01.2022).

4. Руководство по эксплуатации датчиков давления, разрежения и разности давлений ADZ.

5. Артюшенко В.М. Сервис информационных систем в электротехнических комплексах. Монография / Москва, 2010.

6. Артюшенко В.М., Аббасова Т.С. Особенности резервирования источников бесперебойного питания компьютерного и телекоммуникационного оборудования // Электротехнические и информационные комплексы и системы. 2007. Т. 3. № 3. С. 20–23.

7. Артюшенко В.М., Гуреев А.К., Абраменков В.В. Енютин К.А. Мультимедийные гибридные сети. Москва, 2007.

АВТОМАТИЗАЦИЯ ПРОПУСКНОГО РЕЖИМА ПРЕДПРИЯТИЯ ЗА СЧЕТ ПРИМЕНЕНИЯ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОЙ СИСТЕМЫ

Жиделев М.А., магистр группы ИМО-ПИ 21,
Елькин С.В., магистр группы ИМО-ПИ 21,
Технологический университет («МГОТУ»),
Россия, Королев.

Основная цель статьи – показать на практике возможности технологий NFC/RFID в системах контроля и управления доступом. В качестве примера для оптимизации была использована СКУД предприятия ФКП НИЦ РКП. Учитывая исходные данные, было поставлено технической задание на проектирование новой системы. Был осуществлен выбор и обоснование выбора программной и аппаратной частей для реализации задач, поставленных в ТЗ. На основании технического задания и анализа программных и аппаратных комплексов было разработано программное обеспечение, удовлетворяющее поставленным задачам. Полученные результаты проведенной работы стали основанием эффективности информационной системы.

Ключевые слова: СКУД, NFC/RFID, КПП, JAVA, C#

Введение. Благодаря компьютерным технологиям происходит модернизация и оптимизация технических процессов, облегчающих жизнь человеку. С развитием технологий расширяется область применения и растут возможности вычислительных систем. Сложно представить деятельность человека без использования компьютеров в наше время.

Универсальным хранилищем информации являются базы данных. Для создания и взаимодействия с ними используются специальные комплексы программ, а именно системы управления базами данных. Всё это вместе взаимодействие с информацией, хранение, обработку и поиск. Например, можно записывать и хранить в базе данных информацию о сотрудниках предприятия и использовать эту технологию на контрольно-пропускном пункте для проверки. Благодаря данной технологии можно ускорить процесс прохождения через КПП и соответственно увеличить его пропускную способность.

Существует тенденция по внедрению информационных технологий, способствующих оптимизации контроля пропускного режима сотрудников на крупных государственных предприятиях. В свою

очередь, такая организация как ФКП “НИЦ РКП” тоже использует систему пропусков для ограничения доступа людей на закрытую территорию предприятия.

Тем не менее на предприятии в системе контроля временных и разовых пропусков используется устаревшая подсистема в виде бумажной картотеки, расположенной прямо на пропускном пункте. Оформление, выдача и проход по разовым пропускам может достигать часа или более по времени в зависимости от количества людей в очереди. Оптимизация данной системы приведет к:

Удобству работы с информацией. Благодаря использованию системы с электронной базой данных, будет значительно упрощена обработка информации.

Основной раздел. Анализ исходных данных. Перед тем, как приступить к разработке программного обеспечения и оптимизации пропускного режима предприятия, следует определиться с понятием контрольно-пропускного пункта, а именно как он работает в целом и в рамках предприятия в частности. В этом случае, мною будет разобрано функционирование КПП предприятия в рамках временных и разовых пропусков.

Понятие контрольно-пропускного пункта. В первую очередь обусловим саму концепция контрольно-пропускного пункта. Контрольно-пропускной пункт (КПП) – особо оснащенное место на объекте (учреждении, огороженной охранной зоной) с целью реализации контроля доступа на территорию людей или транспорта. Данное понятие включает в себя в том числе и КПП, находящиеся при комендантской службе.

КПП могут быть:

- Временными. В самом простом варианте могут представлять из себя шлагбаум с местом для размещения персонала;
- Постоянными. В этом случае КПП представляет из себя отдельно здание (к примеру, окопами или укрытиями), эстакадами досмотра, системой управления доступом и контроля и т.д.

Дежурство и контроль на КПП осуществляется в зависимости от характеристик охраняемого объекта.

Различают следующие типы пропусков [1]: Разовые; Временные; Материальные (для транспорта); Постоянные.

Анализ работы временных и разовых пропусков на предприятии. Рассмотрим процесс выдачи и контроля временных и разовых пропусков в ФКП “НИЦ РКП”. Разовые пропуска работают по следующему алгоритму:

1. В отделе кадров происходит оформление бланка с печатью, ФИО, подписью, отделом и датой посещения;

2. В кабинете возле КПП нужно предъявить бланк и паспорт, после этого делают разовый пропуск и относят всё на пропускной пункт (одновременно могут оформлять примерно до 4 человек);

3. Сотрудники пропускного пункта вызывают по очереди, производят проверку документов и допускают на предприятие;

4. Перед выходом с предприятия, необходимо указать дату убытия и поставить подпись начальника отдела;

5. На выходе с предприятия сотрудники пропускного пункта производят проверку пропуска и документов.

Значительными недостатками данной системы можно отметить высокое время ожидания и снижение пропускной способности КПП. В зависимости от количества людей, время ожидания прохода по временному пропуску может достигать часа и более.

Теперь рассмотрим работу временного пропуска:

1. Оформляется приказ на допуск на территорию предприятия;
2. Приносите документы для оформления пропуска на КПП;
3. Заказывается пропуск;
4. Пропуску присваивается номер, приносите документы в кабинет возле КПП, где сверяются данные, после чего пропуск с документами относятся на пропускной пункт;
5. Вызывают по очереди, проверяют документы, выдают пропуск, после чего можно свободно пройти на территорию предприятия;
6. На выходе предъявляется паспорт и пропуск, последний сдаётся на хранение в нумерованную картотеку;
7. При следующем посещении предъявляется также паспорт и номер пропуска.

Из-за устаревшего метода хранения, используемого при работе с временными пропусками, замедляется поиск информации. Также данный метод является менее надёжным, чем электронная база данных.

Использование новых информационных технологий позволило бы упростить и ускорить выдачу пропусков, а также повысить безопасность.

В результате анализа работы контрольно-пропускного пункта были выявлены следующие проблемы:

- Физическая картотека временных пропусков достаточно устарела, ручной поиск информации в ней занимает больше времени, чем могло бы быть с электронной базой данных;
- Из-за отсутствия электронной базы данных и технологичной системы контроля доступа, время, потраченное на выдачу разовых и временны пропусков может достигать до часу и более.
- Также, данная картотека является менее надёжной, чем электронная база данных;
- Из-за отсутствия автоматизированного процесса, время, которое приходится на первичную проверку временных пропусков и проверку разовых пропусков достаточно велико;

Данные трудности появляются из-за устаревания нынешней информационной организации и невысокой пропускной способности контрольно-пропускного пункта. Применение современных информационных технологий может решить большинство этих проблем.

Выбор аппаратно-программных средств разработки и эксплуатации ИС. В современном мире большинство КПП частично или полностью оборудовано специальными системами проверки пропусков. Данные системы содержат как программную, так и аппаратную составляющие, например, систему турникетов и запись информации в базы данных.

Благодаря этому происходит увеличение скорости прохождения через КПП и оптимизация безопасности.

Технологии, используемые на КПП. В настоящее время средства электронного доступа, они же электронные пропуска (ЭП), использующиеся в системах контроля доступа, делятся на две основных группы: контактные и бесконтактные.

Контактным пропускам необходим непосредственный контакт с устройствами считывания. Это приводит к механическим повреждениям и быстрой поломке.

Бесконтактные типы пропусков срабатывают на расстоянии от считывателя (для определенных моделей оно составляет до 1 м). Благодаря этому они считаются более долговечными и надежными [1].

Кроме варианта работы, пропуска различают типом чипа, формой и исполнением: толстые и тонкие карты, большие и маленькие брелоки, браслеты.

У бесконтактных ЭП существует два стандарта: EmMarine и MiFare. Я рассмотрю подробно каждый из них чуть позже.

Электронные пропуска могут работать и без специального программного обеспечения.

Многие современные компании и корпорации уже перешли на использование электронных пропусков. Развитие данных технологий идет быстрыми темпами и дает потребителю широкие возможности для выбора. В табл. 1 проведем сравнительную характеристику технологий, используемых при контроле пропускного режима и выберем наиболее подходящую для выполнения поставленных задач ВКР.

Таблица 1. Сравнительная характеристика технологий бесконтактной передачи данных

	NFC/RFID	**Штрихкод/QR-код**	**Магнит**
Надежность	+	-	-
Безопасность	+	-	-
Перспективность	+	+	-

Таким образом были выбраны наиболее новые и перспектиные технологии NFC и RFID.

Технологии RFID и NFC. Технология радиочастотной идентификации (RFID) основана на системе состоящей из двух основных компонентов: меток и устройств считывания. Устройства считывания, они же Reader'ы представляют из себя устройства у которых есть в наличии одна или несколько антенн, которые образуют радиочастотные поля, в которых осуществляется обмен данными с RFID-метками. Такие метки могут работать в пассивном и активном режиме. Пассивные метки запитаны от аккумуляторов считывателей, активные - от батареек. Такие метки могут хранить от серийных номеров до больших блоков данных (страниц информации). RFID считыватели бывают мобильными и стационарными. Системы считывания также могут быть интегрированы в архитектуру кабинета, помещения или здания.

Благодаря большому диапазону работы метки с чипом RFID являются идеальным вариантом для большинства крупных компаний [5]. На сегодняшний день карты с чипом RFID применяют во многих отраслях. Большинство из нас используют такие карты регулярно.

Области использования RFID карт. На сегодняшний день карты с чипом RFID применяют во многих отраслях. Большинство из нас используют такие карты регулярно. Рассмотрим основные места, где применена RFID-технология.

1. Пластиковые карты с чипом RFID применяют для оплаты проезда в общественном транспорте. В момент прикладывания (контакта) чипа и устройства считывания происходит верификация

и процесс списания средств.

2. Карты с чипами RFID используют в больших и средних компаниях в системах контроля доступа (СКУД).

3. В пропускных системах школ и университетов тоже используют технологии поддерживающие карты с чипом RFID.

4. В гостиницах и отелях зачастую используют данную технологию для заселения постояльцев. Такие карты служат ключом в номер и могут быть средством оплаты.

5. Крупные фитнес залы используют карты с чипом RFID для контроля доступа посетителей в тренажерный комплекс. На таких картах может храниться информация о клиентах и время посещения.

6. Крупные торговые сети используют данную технологию в качестве дисконтных карт.

7. На станциях АЗС карты с чипами RFID учувствуют в накопительных системах. Покупатели могут копить и расплачиваться баллами за услуги, предоставляемые на АЗС.

8. Система оплаты проезда в транспондерах также использует технологию карт с чипом RFID. При проезде через него, происходит автоматическое считывание информации и оплата.

9. Данная технология используется для бесконтактной оплаты товаров и услуг банковскими картами оснащенными чипами RFID. Для безопасности предусмотрены ограничения списаний средств.

10. Также данную технологию используют некоторые автомобильные производители в противоугонных системах.

Типы RFID карт. На данный момент существует большое количество различных карт с чипами RFID, все они соответствуют определенным стандартам [6]. Эти стандарты определяет “Международная Организация по Стандартизации” (ISO) при участии “Международной Электротехнической Комиссии” (International Electrotechnical Commision). Сейчас используются два основных вида карт с чипами RFID. А именно MIFARE и HID.

- MIFARE — применяются для идентификации личности, а также для проведения платежей. Включают в себя восемь стандартов с различными чипами и характеристиками. Бывают бесконтактными.
- HID — используются в большинстве сфер деятельности человека. В частности такие карты используются при контроле

доступа в помещения закрытого типа. На такие карты можно не однократно перезаписывать информацию.

Что такое NFC. Near Field Communication (NFC) - «коммуникация ближнего поля» технология беспроводной передачи данных малого радиуса действия. Данная технология позволяет осуществлять обмен данными между устройствами, расположенными на 10 сантиметрах друг от друга.

Устройства NFC работают на частоте 13.5 МГц. Такие системы зачастую формируются из двух основных устройств, а именно считывателей и меток. Благодаря считывателю формируется радиочастотное поле в котором можно осуществлять взаимодействие с метками или с другими считывателями. Считыватели работают в режиме активной коммуникации, а метки – в пассивной. [3]

Отличия RFID от NFC. В таблице 2. проведем отличительную характеристику данных технологий.

Таблица 2. Характеристика частот чипов RFID

	RFID	**NFC**
Связь	односторонняя	двусторонняя
Частота	13.56 МГц	13.56 МГц
Радиус считывания	От 1 до 4м	10см
Функционал	Чтение/запись	Чтение/запись/оплата/обмен данными P2P

Проведя сравнительную характеристику, в качестве технологии передачи данных, используемой в СКУД, была выбрана технология NFC. Благодаря своей перспективности и малого радиуса работы данная технология идеально подходит для спроектированной системы контроля доступа.

Технологии NfcA и Ndef. NfcA класс предоставляет доступ API (программный интерфейс) для Android.

Формат обмена данными NFC (NDEF) - это стандартизированный формат данных, который может использоваться для обмена информацией между любым совместимым устройством NFC и другим устройством или тегом NFC. Формат данных состоит из сообщений NDEF и записей NDEF. Стандарт поддерживается форумом NFC и находится в свободном доступе для ознакомления, но для загрузки требуется согласие с лицензионным соглашением.. Каждая NDEF запись содержит две части:

- Тип записи (record type) - указывает тип данных в записи
- Данные записи (payload)

Две эти записи описывают алгоритм, который необходимо совершить устройству при прикосновении к NFC метке. NDEF поддерживает как простые так и сложные наборы действий, это зависит то установленного ПО для устройств NFC. Главной особенностью NDEF формата является отсутствие необходимости в установке специального ПО на устройства поддерживающие NFC технологии. На метки можно записывать сразу несколько записей. При этом многие приложения работают только с первой записью.

NDEF (формат обмена данными NFC) - это мало весящий двоичный формат, используемый для инкапсуляции типизированных данных. Он указан форумом NFC для передачи и хранения с помощью NFC, однако он не зависит от транспортировки.

NDEF определяет сообщения и записи. Запись NDEF содержит типизированные данные, такие как носитель типа MIME, URI или пользовательская полезная нагрузка приложения. Сообщение — NDEF-это контейнер для одной или нескольких записей NDEF.

Когда устройство Android получает сообщение NDEF (например, путем считывания метки NFC), оно обрабатывает его через механизм отправки, чтобы определить действие для запуска. Тип первой записи в сообщении имеет особое значение для отправки сообщения, поэтому тщательно разработайте эту запись [4].

Выбор устройств, поддерживающих технологию NFC

Использование Mifare в СКУД. Технология **Mifare** основана на популярном стандарте бесконтактной карты ISO 14443, это позволяет совмещать карты Mifare с банковскими картами и мобильными устройствами [3]. **Mifare** включает в себя большое количество продуктов, способных работать в системах контроля доступа.

Идентификатор Mifare содержит идентификационный номер - так называемый UID-номер и перезаписываемую память, он не защищен от чтения и не является секретным и иногда даже написан снаружи на карточке. А вот доступ к памяти защищен. Чтение и запись возможна только при знании ключей доступа, а передаваемые между картой и считывателем данные защищены.

Считыватель как Mifare может читать UID, а может читать данные из памяти. Большинство дешевых считывателей могут читать только UID, что плохо, так как UID не защищен и можно по-прежнему сделать дубликат карты.

Чтобы считыватель читал из памяти, требуется настройка и подготовка карт. И в считыватель, и в карты должен быть занесен некий секрет для данного конкретного внедрения. Это может немного усложнять процедуру подготовки карты и считывателя. Для выполнения этой процедуры нужно запустить определенную программу и прогнать по очереди карты, прежде чем выдавать их сотрудникам. Это программное обеспечение уже встроено в базовые комплекты программного обеспечения для контроллеров СКУД[5].

Из-за того, что не у всех котроллеров есть поддержка работы с технологией Mifare, нужно ответственно подходить к выбору контроллеров и считывателей. При использовании в системах СКУД контроллеры и считыватели должны быть настроены на работу с Mifare.

Идентификаторы Mifare отличаются более высокой степенью защиты и стоят немного дороже чем идентификаторы EM Marine

Идентификаторы формата Mifare необходимо правильно использовать. Необходима настройка карты и считывателя.

Карты с неоригинальным чипом зачастую используются в малых СКУД. Любые риски и ошибки минимальны при их использовании.

Выбор NFC метки. Для реализации пропускной деятельности необходимо выбрать устройство, служащее пропуском. Так как была выбрана технология NFC, то в качестве пропусков будут использоваться NFC метки. Существует множество таких меток, однако я буду использовать именно NFC Mifare Ultralight. Благодаря низкой себестоимости и доступности мой выбор пал именно на неё.

Выбор считывающего устройства. Перед тем как приступить к выбору самого считывателя необходимо изучить ПО, на которых они работают.

Выбор ПО для USB NFC считывателя

На данный момент существует две прошивки на которых работают USB NFC считыватели. А именно CDC и HID. Рассмотрим каждый из них отдельно и выберем наиболее подходящий для решения задач, поставленных в дипломной работе.

В табл. 3 проведем сравнительную характеристику данных прошивок и выберем наиболее подходящую для выполнения поставленных задач дипломной работы.

Таблица 3. Сравнительная характеристика прошивок CDC и HID

	CDC	**HID**
Возможность управлять устройством с помощью скриптов и сторонних программ	+	-
Возможность задавать формат выводимых данных с помощью строки форматирования	+	-
Работа со встроенными драйверами	+	-

Таким образом был выбран протокол CDC для считывателя USB NFC благодаря простоте работы с устройством.

Выбор аппаратной составляющей. Для реализации работы NFC меток с компьютером и базами данных существуют специальные считыватели NFC меток, работающие через USB порты. В данный момент на рынке существует множество устройств поддерживающих данную технологию. Рассмотрим подробнее самые популярные и доступные из них.

В табл. 4 проведем сравнительную характеристику данных считывателей и выберем наиболее подходящий для выполнения поставленных задач дипломной работы [6].

Таблица 4. Сравнительная характеристика считывателей ODRFID, ODRFID-M/N/E и ODRFID-E

	ODRFID	**ODRFID-M/N/E**	**ODRFID-E**
Небольшая цена	+	-	-
Наличие на рынке	+	+	+
Поддержка Ultralight	+	+	-
Поддержка CDC	+	+	+

Таким образом, был выбран настольный USB NFC считыватель ODRFID благодаря поддержке работы с NFC метками технологии Ultralight и небольшой стоимости.

Выбор операционной системы для мобильного приложениюю Современный рынок операционных систем смартфонов делится на два крупных лагеря. А именно Android OS и iOS. Рассмотрим каждую из них по отдельности и выберем наиболее перспективную и подходящую для реализации поставленных задач диссертационной работы[7].

В табл. 5 приведен сравнительный анализ характеристик операционных систем Android OS и iOS.

Таблица 5. Сравнительная характеристика операционных систем Android OS и iOS

	Android OS	**iOS**
Доступность	+	-
Быстрый эмулятор	+	-
Большое сообщество разработчиков	+	-
Хороший фреймворк	+	-
Понятная документация и отзывчивая служба поддержки	+	-
Платформа Open source	+	-

Таким образом, проводя сравнительную характеристику, была выбрана **Android OS** в качестве операционной системы для разработки мобильного приложения. В дальнейшем я буду использовать эмуляторы и смартфон на базе **Android OS.**

Выбор среды разработки и языка программирования для мобильного приложения. Мобильные приложения принято разрабатывать в специальных средах разработки IDE (программных комплексах, строго ориентированных на проектирование и сборку приложений). Так как в качестве операционной системы была выбрана **Android OS**, то наиболее подходящей средой разработки приложения для данной ОС будет **Android Studio**. Данная IDE хороша тем, что имеет встроенный эмулятор, облегчающий отладку приложений и понятный, интуитивный интерфейс.

Выбор языка программирования мобильного приложения

Чтобы создать приложение для операционной системы Android необходимо выбрать не только среду разработки IDE, но и определенный язык программирования, на котором будет написана программа. Существуют несколько языков подходящих для разработки мобильных приложений. Так как в качестве среды разработки мною была выбрана IDE Android Studio, это значительно сужает выбор языков программирования. В данной среде используются два основных языка программирования Java и Kotlin, а языки C/C++ и C# как вспомогательные. Так как Kotlin представляет из себя улучшеную версию Java, то естественно мой выбор пал именно на него. Благодаря простому синтаксису и большой библиотеки данный язык отлично подойдет для разработки мобильного приложения.

Выбор среды разработки и языка программирования для компьютерного приложения. Для разработки компьютерного приложения не подойдет среда разработки Android Studio, следовательно, необходимо выбрать специальную IDE, ориентированную на создание компьютерных

программ и подключение к ним баз данных. В качестве такой среды разработки отлично подойдет **Microsoft Visual Studio.**

Особые инструменты разработки позволяют новичкам лучше ориентироваться в коде. Так, например, существует опция загорающейся желтой лампочки, которая появляется рядом со строчками, которые можно оптимизировать. При нажатии на нее появляются подсказки, которые помогают понять, что можно поменять для оптимизации кода. Безусловно, автоиспраление и автозаполнение строк при написании в ней тоже присутствует.

Выбор языка программирования компьютерного приложения. Как и при разработке мобильного приложения, при разработке приложения для Windows OS необходимо выбрать не только IDE, но и язык программирования, который поддерживает среда разработки и который будет удовлетворять всем современным требованиям. В качестве языка программирования для разработки программы для Windows OS был выбран C#.

Обзор инструментов и систем управления базами данных. В современном мире базы данных управляется с помощью СУБД, системами управления базами данных, которые позволяют взаимодействовать с базой данных и создавать структуру БД, заполнять её информацией, редактировать содержимое и отображать его. В качестве системы управления подойдет **MySQL**. Мой выбор пал на данную систему благодаря ее быстродействию, поддержке в MS Visual Studio и простой установке и настройке.

Данная СУБД распространяется как под коммерческой лицензией, так и под лицензией на свободное программное обеспечение. Создатели MySQL зачастую добавляют новые возможности по заказам лицензированных пользователей. Благодаря этому система не стоит на месте и развивается. MySQL имеет приличное количество функций в бесплатной версии для реализации, простая документация позволит разобраться в работе СУБД.

Выбор инструмента. Чтобы осуществлять редактирование и управление БД на MySQL необходимо иметь специальное ПО. В качестве такого ПО выступают инструменты управления базами данных. Так как ранее мною была выбрана система баз данных на основе MySQL, то лучшим инструментом управления станет **MySQL Workbench.** Данная среда хорошо подходит для архитекторов и разработчиков БД. В таблице 6 проведем сравнительную характеристику ПО, ориентированного на работу с БД на MySQL и выберем наиболее

перспективное и подходящее для решения поставленных задач дипломного проекта.

Таблица 6. Сравнительная характеристика MySQL Workbench, phpMyAdmin и DataGrip

	MySQL Workbench	**phpMyAdmin**	**DataGrip**
Бесплатная	+	+	-
Работа в офлайн режиме	+	-	+
Совместимость с Windows	+	+	+
Активная поддержка	-	+	+
Интуитивное управление	+	-	+
Можно работать без знания PHP	+	-	+

Таким образом, проводя сравнительную характеристику, был выбран MySQL Workbench в качестве визуального инструмента для осуществления работы с базой данных на MySQL.

Заключение. В аналитической части данной работы был проведён анализ работы контрольно-пропускного пункта в целом и работа временных и разовых пропусков, в частности. Были обнаружены проблемы, которые можно исправить путём разработки новой системы контроля и учета временных и разовых пропусков.

Также был произведён сравнительный анализ сред разработки, выбор подходящего оборудования и СУБД для реализации проекта. А именно в качестве основной технологии передачи данных была выбрана технология NFC-RFID. Были рассмотрены принципы работы технологии NDEF. В качестве устройства представляющего пропуск была выбрана специальная метка типа Mifare Ultralight и USB NFC ODRFID в качестве устройства выполняющего роль считывателя. В качестве операционной системы на базе которой будет создано приложение была выбрана Android OS. Была выбрана среда разработки Android Studio и язык программирования Java для разработки мобильного приложения. В качестве среды разработки компьютерного приложения была выбрана Microsoft Visual Studio и язык программирования C#. Был произведен обзор систем управления создания и управления БД. Для разработки базы данных была выбрана СУБД MySQL. В качестве системы управления была выбрана MySQLWorkbench. Данная система представляет собой чрезвычайно

удобное средство для управления СУБД MySQL. Оно позволяет достаточно эффективно управлять локальным сервером даже малознакомым с SQL людям.

Благодаря своей универсальности, с помощью технологии NFC (Near Field Communication) можно осуществлять контроль доступа на предприятия закрытого типа. Внедрение таких технологий в системы контроля доступа позволяет не только ускорить процесс выдачи и поверки пропусков, но и обезопасить контрольно-пропускные пункты предприятий. Спроектированная СКУД позволила внедрить передовые технологии в области хранения и обротки информации в лице системы баз данных. В свою очередь они заменили устаревшие бумажные носители информации. В будущем данная система рекомендована к внедрению на предприятие ФКП НИЦ РКП.

Список использованных источников

1. Коряковский А.В. Информационные системы предприятия: Учебное пособие. - М.: НИЦ ИНФРА-М, 2016. С. 280 – 283.

2. Медведев М.А. Разработка информационных систем. Учебное пособие. - М.: Флинта, Изд-во Урал. ун-та, 2017. С.60 – 64.

3. Елисеев Н. Технология NFC – возможности и применения. Научная статья, выпуск в журнале Электроника НТБ #6/2011, С. 1 –3.

4. Ревазов Х.Ю. Тавасиев Д.А. Команов П.А. Основной принцип работы NFC-устройств и их безопасность. Научная статья, Изд-во ISSN 2020, С. 1-2.

5. Бондаренко Р. Технология NFC - связь на близком расстоянии [Электронный ресурс] / Р.Бондаренко. -2011. URL: http://www.russianelectronics.ru/leader-r/review/2187/doc/57689/.

6. Прилуцкий А. Технология NFC: что, зачем и когда [Электронный ресурс] / А. Прилуцкий. 2013. URL: http://www.hardnsoft.ru/academy/technology/28916/.

7. Ярчук А.В. Операционные системы мобильных устройств. Научная статья в журнале Вестник МГУП имени Ивана Федорова 2015 С. 1-2.

8. Маркин А.В. Построение запросов и программирование на SQL. Учебное пособие / А.В. Маркин. - М.: Диалог-Мифи, 2016. С 383- 384.

АНАЛИЗ ОСОБЕННОСТЕЙ ВОЛС НА ПРИМЕРЕ ИНТЕРАКТИВНОЙ СИСТЕМЫ КАБЕЛЬНОГО ТЕЛЕВИДЕНИЯ

Евдокимова Д.В., инженер,
ОАО «Метрострой», Россия, г. Москва

В статье рассмотрены вопросы, связанные с кратким анализом особенностей построения ВОЛС на примере системы интерактивного кабельного телевидения.

Ключевые слова: волоконно-оптическая линия связи, оптический передатчик, оптический приемник, оптический усилитель.

Неуклонное увеличение абонентов, подключенных к одной головной станции (ГС) с одновременным увеличением транслируемых каналов в диапазоне, приводит к увеличению потерь по коаксиальным магистралям, что влечет за собой частое включение магистральных усилителей [1-3]. При числе усилителей большем 7–9, как правило, не удается реализовать требуемые качественные параметры сигнала (отношение сигнал/шум – S/N и уровень интермодуляционных искажений второго – CSO или третьего – CTB порядков) в силу конечного значения динамического диапазона усилителей [4, 5].

Для решения такой задачи все шире используются волоконно-оптические линии связи (ВОЛС). Это вид связи, при которой информация передается по оптическим волокнам, часто именуемым «оптическое волокно» (Fiber). ВОЛС считается самой совершенной средой для передачи широкополосной информации на значительные расстояния [6-9]. Особенностями ВОЛС являются:

– широкополосность оптических сигналов, обусловленная высокой частотой несущей ($f_o \approx 10^{14}$ Гц). Физически это означает, что в предельном случае по одной оптической линии можно передать тысячи телевизионных программ, 10 миллионов телефонных разговоров или цифровую информацию со скоростью порядка 10^{12} бит/с (или Терабит/с);

– малое погонное затухание сигнала в волокне. Типовые значения затуханий в волоконно-оптическом кабеле (ВОК) не превышает 0,4 дБ/км на длине волны 1310 нм и 0,25 дБ/км на длине волны 1550 нм;

– волокно изготовлено из кварца, основу которого составляет двуокись кремния, широко распространенного, а потому и недорогого материала в отличие от меди;

– ВОЛС устойчивы к электромагнитным помехам;

– передаваемая информация по ВОЛС защищена от несанкционированного доступа. Ее нельзя подслушать неразрушающим способом. Всякие воздействия на волокно легко регистрируются методом мониторинга целостности линии. Естественно, что теоретически существуют способы обойти защиту от мониторинга, но затраты на их реализацию будут столь велики, что превзойдут стоимость перехваченной информации;

– долговечность (сохранение свойств в определенных пределах), превышает 25 – 30 лет, что позволяет проложить волокно один раз;

– стеклянные волокна – не металл, следовательно, они безопасны в электрическом отношении. Такие кабели можно монтировать на мачтах существующих линий электропередач, как отдельно, так и встраивая их в фазовый провод, экономя значительные финансовые средства;

– в ВОК используются одномодовые и многомодовые волокна. Для трансляции ТВ сигналов применимы только одномодовые волокна, обладающие существенно лучшими характеристиками по затуханию, частотной дисперсии и полосе пропускания;

– число оптических жил в ВОК колеблется в больших пределах и обычно составляет 16 – 32 для средних и крупных СКТ;

– недостаток ВОЛС заключается в том, что для монтажа оптических волокон требуется прецизионное, а потому дорогое, технологическое оборудование. Следовательно, при обрыве ВОК затраты на восстановление выше, чем при работе с медными кабелями.

Несмотря на отмеченный недостаток ВОЛС все шире используются для трансляции ТВ сигналов вплоть до каждого дома и даже до абонента.

Варианты стандартного построения ВОЛС представлены на рис. 1. [1].

Вариант *а* – используется при значительной протяженности магистрали; *б* – при наличии одного передатчика; *в* – при удалениях отдельных районов.

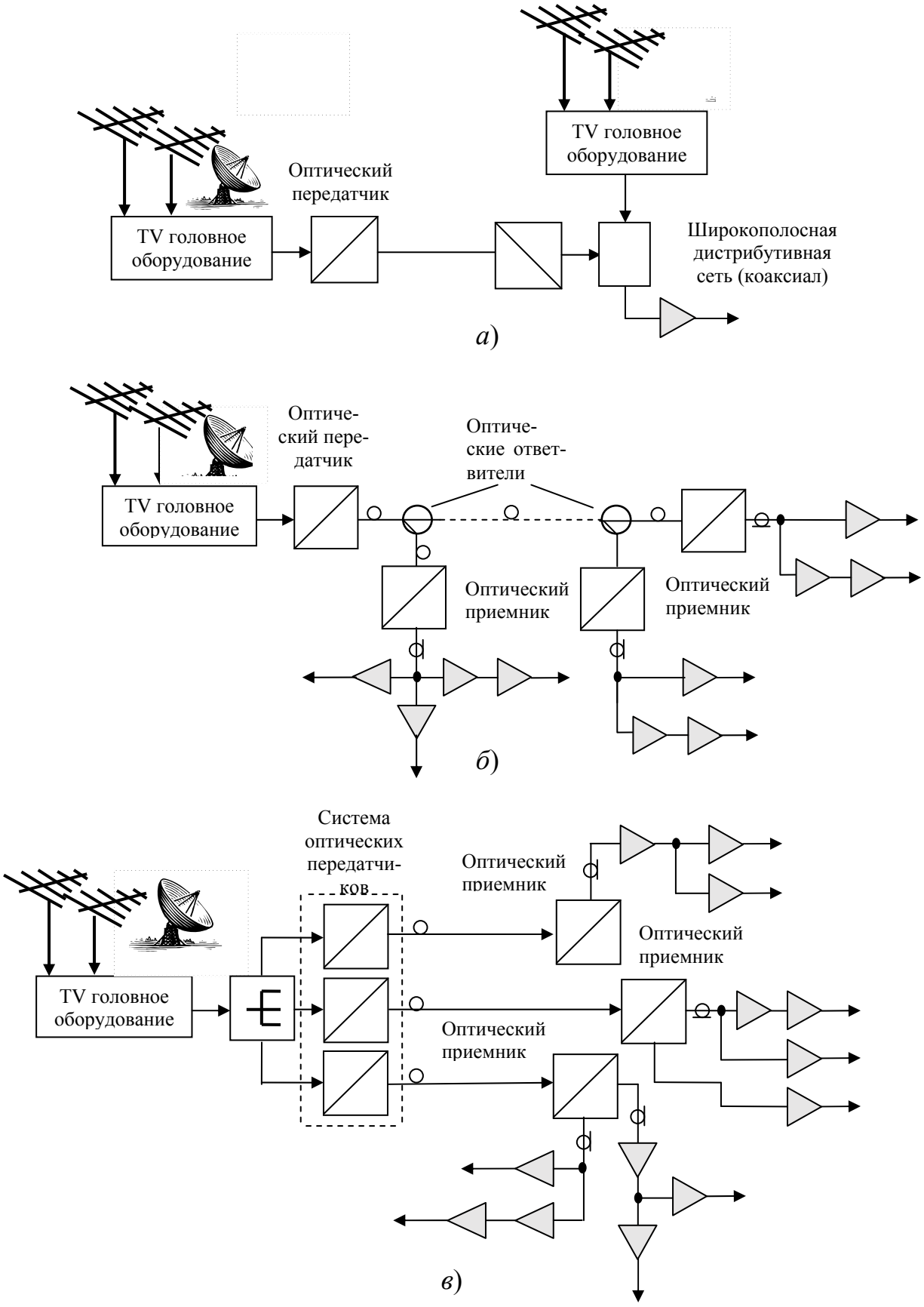


Рис. 1. Варианты стандартного построения ВОЛС, где: *а* – от центральной ГС к местной распределительной станции; *б* – с оптическим цепным распределением; *в* – веерное распределение

Список используемых источников

1. Артюшенко, В. М. Выбор кабельного оборудования с учетом их электротехнических характеристик / В.М. Артюшенко, В.А. Корчагин // Вестник Ассоциации ВУЗов туризма и сервиса. – 2008. - №1. – С.55-58.

2. Артюшенко В.М., Гуреев А.К., Абраменков В.В. Енютин К.А. Мультимедийные гибридные сети. Москва, 2007.

3. Артюшенко В.М., Маленким А.В. Количественная оценка электромагнитного влияния однопроводных линий электрического оборудования // Электротехнические и информационные комплексы и системы. 2008. Т. 4. № 1-2. С. 29-32.

4. Артюшенко В.М. Защита структурированных кабельных систем от внешних электромагнитных воздействий // Теоретические и прикладные проблемы сервиса. 2005. № 3 (16). С. 20-27.

5. Артюшенко В.М., Енютин К.А., Буткевич М.Н. Анализ эффективности уменьшения межкабельных переходных помех в экранированных кабельных системах // Электротехнические и информационные комплексы и системы. 2009. Т. 5. № 1. С. 19–23.

6. Артюшенко, В. М. Анализ систем управления космическим летательным аппаратом / В.М. Артюшенко, М.И. Видов // Информационные технологии. Радиоэлектроника. Телекоммуникации. – 2011. – №1. – С.18-29.

7. Артюшенко В.М., Кучеров Б.А. Анализ энергетических характеристик линий корпоративной сети спутниковой связи // Информационно-технологический вестник. 2014. № 1 (1). С. 13-19.

8. Артюшенко В.М., Воловач В.И. Особенности отражения зондирующих сигналов радиотехнических устройств обнаружения от протяженных объектов сложной формы // Школа университетской науки: парадигма развития. 2012. № 2-1 (6). С. 42-46.

9. Артюшенко В.М., Кучеров Б.А. Оценка экономической эффективности использования автоматизированной системы распределения средств управления космическими аппаратами в условиях ресурсных ограничений // Вестник Поволжского государственного университета сервиса. Серия: Экономика. 2013. № 5 (31). С. 131-136.

СОВРЕМЕННЫЙ ПОДХОД К РАЗРАБОТКЕ SPA ПРИЛОЖЕНИЙ НА ФРЕЙМВОРКЕ ANGULAR

Руя М.А., магистр группы ИМО-ПИ 21,
Гунина Е.В., магистр группы ИМО-ПИ 21,
Технологический университет («МГОТУ»),
Россия, Королев.

В работе рассматриваются проблемы, связанные с современным подходом к разработке SPA приложений на фреймворке ANGULAR.

Ключевые слова: web приложения, фронтенд разработчики, браузер.

Сегодня почти каждый бизнес, от малого до крупного, должен иметь свой сайт, для большей продаваемости своих услуг, привлечения новых клиентов и заказчиков. До сих пор 46% небольших компаний не имеют своего web сервиса, однако у 24% из них не растет прибыль в отличие от остальных.

Но мало просто запустить сайт и продолжать развивать свой бизнес в интернете, самое важное подойти к этому делу ответственно. Нужно найти хорошего веб-дизайнера, который продумает все до мелочей, распишет как будут работать будущие сервисы и чем сайт будет продавать себя. После того как все вышеперечисленные вопросы закрыты нужно нанимать разработчиков. Для создания любого web приложения нужны фронтенд разработчики, которые отвечают за видимую пользователю оболочку и как она будет взаимодействовать с браузером, и бэк-енд разработчики, которые подготовят для первых все данные с которыми нужно работать.

Миллиардер и один из самых успешных людей на планете Билл Гейтс однажды сказал: «Если вашего бизнеса нет в Интернете – вас нет в бизнесе». Даже при условии спроса на выпускаемую продукцию, услугу и конкурентную стоимость продукта, но при отсутствии сайта в Сети – ваш бизнес неумолимо движется к банкротству. Таковы реалии современного рынка. Сейчас эра информационных технологий и сеть интернет переживает самые лучшие времена и необычайную востребованность. У любой современной компании существует сайт и это не только один из элементов престижа, но и новые возможности заработка, клиенты и заказчики.

Первые компьютерные сети — военные и гражданские — на целые десятилетия предшествовали первым веб-сайтам. Однако сайтам

тоже нужно уделить немного внимания — в конце концов, именно благодаря им мы можем свободно общаться и получать информацию со всех концов планеты. Сегодняшние веб-страницы (а также лежащие в их основе протоколы, языки разметки и кодирования) заставляют данные, передаваемые по ссылкам, обретать доступную форму. Благодаря этому информация становится понятной конечному пользователю. Первая концепция Интернета была создана для нужд вооруженных сил США. Такая сеть должна была пережить Третью мировую войну и обеспечить бесперебойную связь между удаленными командными центрами и частями.

В далеком 1969 была создана ARPANET — академическая сеть, объединившая университеты. Затем следовало развитие USENET, который соединил два академических центра, но имел первые дискуссионные группы. И это было достижение — сеть перестала быть «практичной», превратившись в платформу для общения. Веб-сайты или, скорее, идеи для них, были заблокированы решениями Американского национального научного фонда, которые не разрешали использовать Интернет в чисто коммерческих целях. По мнению чиновников той эпохи, Интернет должен был использоваться только в образовательных, научных и военных целях. Однако этот маленький парадокс не помешал развитию сети в западном мире.

Первые сайты были созданы не в Америке, а в ЦЕРН — Европейской организации ядерных исследований. Фактически, это историческое событие произошло в Швейцарии. И хотя сегодня можно сказать, что это не ядерная технология, общение с помощью компьютеров всерьез захватывало умы европейских ученых и стратегов. Веб-сайты были созданы благодаря проекту WorldWideWeb (W3) Тимом Бернерсом-Ли и Робертом Кайо.

Время шло и технологии не стояли на месте, начали появляться первые web страницы в сети интернет, поисковые службы и каталоги существующих сайтов. На рис. 1 показано, какой был рост web-сайтов.

Но все они были похожи друг на друга потому что тогдашний web сайт состоял только из HTML разметки. Но все изменилось в 1996 году, когда миру разработки был представлен CSS. В переводе на русский - Каскадные таблицы стилей считались и остаются языком программирования, позволяющий разукрашивать сайт, позиционировать элементы на странице и отличать один web сайт от другого. Не менее важным событием в 1996 году стало появление Nokia 9000 —

первого телефона, подключенного к Интернету, на экране которого можно было просматривать веб-сайты.

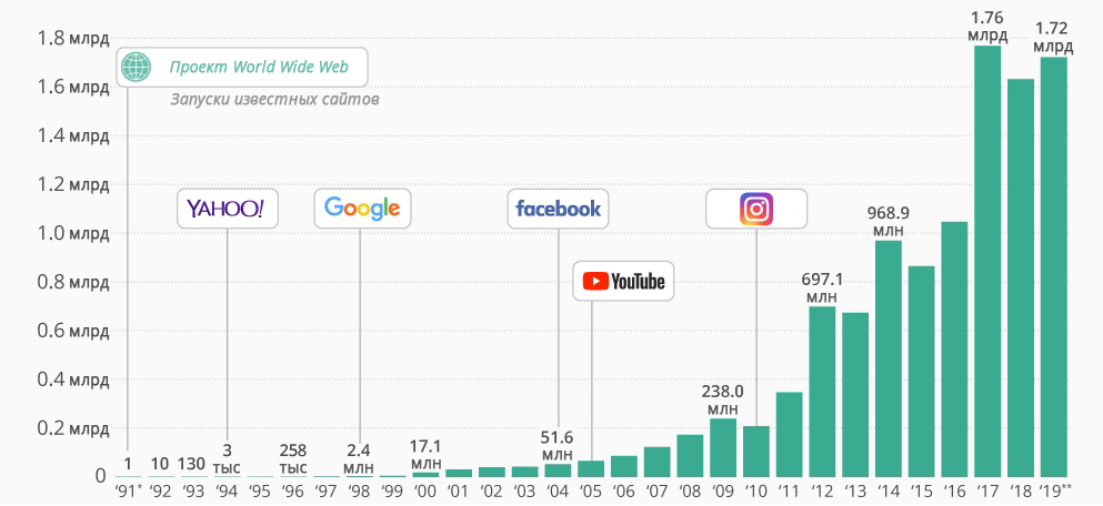


Рис. 1. График роста web сайтов

Также в те года был создан один из лучших, на тот момент, браузер NetScape (рис.2), а позже, в 1995 году, Брендон Эйх из Netscape Communications, вдохновленный Java, Scheme и Self, разработал язык программирования JavaScript. Но никаких сходств, кроме названия, javascript и java не имели. Брендан Эйх просто решил воспользоваться ажиотажем вокруг языка java и это получилось.

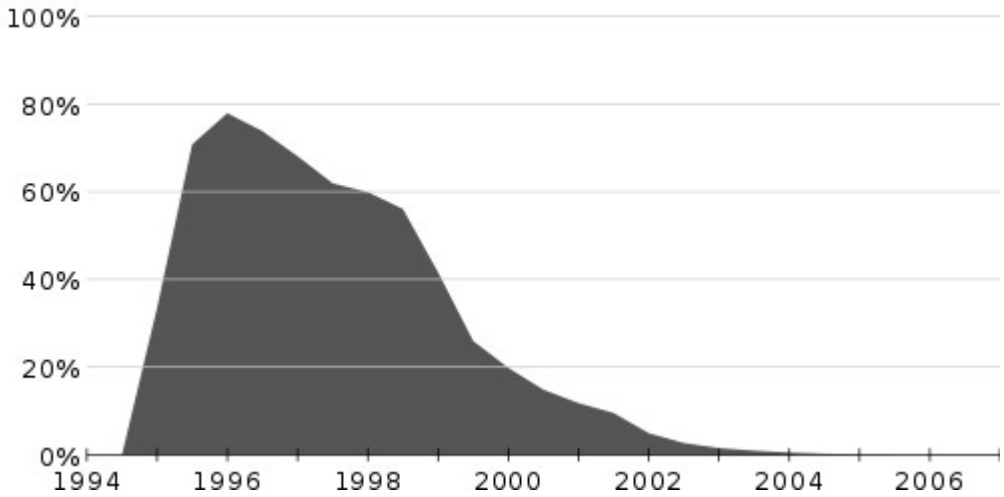


Рис. 2. График популярности Netscape

Mocha от Netscape (позже JavaScript) стремился превратить Интернет в полноценную платформу приложений. Кроме того, при использовании вместе с их продуктом сервера приложений LiveWire он обеспечит изоморфную разработку с одним и тем же языком, исполь-

зуемым как на клиенте, так и на сервере. В конце концов, JavaScript стал единственным мостом между пользователем и браузером, вместе с HTML и CSS. Именно эти три технологии являются опорными пунктами всех сайтов в сети интернет.

Интернет разрастался и если в 2000-ых годах пользователей измеряли десятками тысяч, то к 2005 году их количество измерялось миллионами, а с ними увеличивалось и количество web сайтов разных тематик. На рис. 3, можем увидеть, как росло число пользователей в интернете.

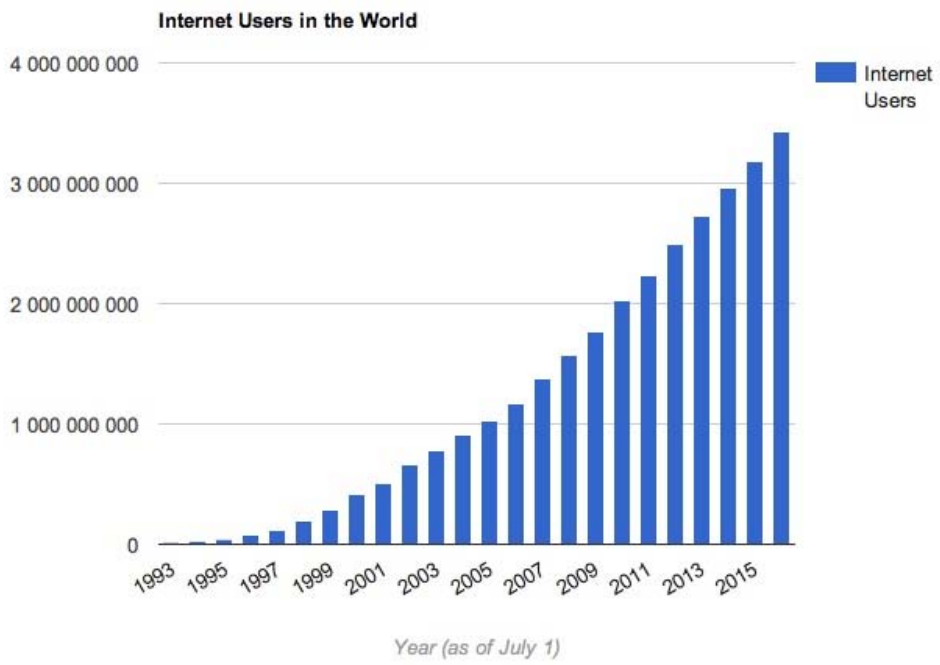


Рис. 3. График роста пользователей сети интернет

Программисты разрабатывали сайты сложнее и высоконагруженнее с каждым днем, и начинали находить минусы разработки сайта только на javascript. Тогда и начали появляться библиотеки (надстройки над javascript) и готовые CMS системы. Но библиотеки не уходили сильно далеко от своего родителя, а готовые CMS были достаточно узки в использовании. Исходя из этого начали появляться первые фреймворки для javascript, благодаря которым стало возможно продумывать качественную архитектуру будущего сайта или web приложения и делать ее высоконагруженной.

В начале 2000-х годов JavaScript был в основном в зачаточном состоянии и в основном использовался для выполнения основных изменений на странице. Основные моменты включали наведение курсора мыши, выпадающие меню и прокрутку текста — вещи, которые

разработчики считают само собой разумеющимися сегодня с помощью CSS. В то время Internet Explorer доминировал в среде веб-браузеров, а с 1999 года он включал оболочку библиотеки, которую Microsoft разработала для своего собственного продукта электронной почты Outlook. Симпатичный, но устрашающе названный объект XMLHttpRequest со временем стал стандартизированным для всех браузеров и стал воротами к тому, как мы сегодня воспринимаем большую часть Интернета. Важно отметить, что этот XMLHttpRequest позволял отправлять запросы на сервер и обрабатывать ответы без необходимости обновлять браузер или выполнять полный круговой обход. До этого такие вещи, как щелчок по вкладке или отправка формы, означали, что сервер обрабатывал этот запрос и решал, как отобразить ответ, а браузер отключался и в конечном итоге отображал результат.

Разработчики ухватились за функциональность и увидели потенциал для создания реальных приложений для замены рабочего стола в Интернете. Асинхронный Javascript и XML, сокращенно AJAX, были придуманы для описания этой новой возможности.

JQuery. Технически jQuery не была первой средой JavaScript, но ее популярность резко возросла после ее выпуска в 2006 году. Целью jQuery было решение многих проблем, с которыми разработчики сталкивались из-за тонких различий в реализации веб-браузеров, и она абстрагировала большую часть функций, которые хотели разработчики, в чистый и простой в освоении фреймворк.

Имея потенциал для создания приложений, использующих удобство Интернета, разработчики создавали все более и более крупные решения, которые проверяли ремонтопригодность jQuery. Такие продукты, как Gmail, продемонстрировали, чего можно достичь, но стало ясно, что могут потребоваться более удобные для предприятий инструменты.

AngularJS. В 2010 году Джереми Ашкенас выпустил Backbone, первый фреймворк, предназначенный для создания одностраничных приложений. Джереми видел, каким грязным может стать огромное приложение jQuery, и хотел найти более чистый подход, чтобы исправить тысячи селекторов и переплетенных обработчиков событий. Интересно, что Backbone не требовал jQuery, это был независимый фреймворк, но при наличии jQuery можно было включить определенные функции.

Примерно в то же время Адам Абронс и Мишко Хевери создали AngularJS, который вскоре перешел под опеку Google, когда Хевери устроился на работу в компанию. Angular был первым фреймворком, предоставившим полную архитектуру для разработки интерфейсных приложений.

Одной из основных функций AngularJS была двунаправленная привязка данных, которая позволяла привязывать данные модели к HTML-разметке и обновлять изменения в режиме реального времени. Разработчики назвали это «автомагией». Angular также поддерживал внедрение зависимостей и возможность создавать повторно используемые компоненты.

Angular. Новый выпуск AngularJS, выпущенный 14 сентября 2016 года и известный как Angular 2, был полностью переписанным предыдущим, полностью основанным на новых спецификациях ECMAScript версии 6 (официально ECMAScript 2015). Подобно переписыванию ядра ASP.NET, «революция» принесла такое количество критических изменений на уровне архитектуры, обработки конвейера HTTP, жизненного цикла приложения, управления состоянием, что перенос старого кода на новый был практически невозможен: несмотря на сохранение его прежнее название, новая версия Angular представляла собой совершенно новый фреймворк, практически не имеющий общего с предыдущим.

Решение не делать Angular 2 обратно совместимым с AngularJS ясно продемонстрировало намерение команды автора принять совершенно новый подход: не только в синтаксисе кода, но и в их образе мышления и разработке клиентского приложения. Новый Angular был очень модульным, основанным на компонентах, поставляется с новой и улучшенной моделью внедрения зависимостей и множеством шаблонов программирования, о которых его старший брат никогда не слышал.

Вот краткий список наиболее важных улучшений, представленных в Angular 2:

- Семантическое версионирование: Angular 2 — это первый выпуск, использующий семантическое управление версиями, также известное как SemVer: универсальный способ управления версиями различных выпусков программного обеспечения, помогающий разработчикам отслеживать происходящее без необходимости копаться в деталях журнала изменений. SemVer базируются на 3 -х числах - XYZ - где X обозначает основную версию, Y обозначает малую версию, и

Z обозначает патч - релиз. Более конкретно: число X, представляющее основную версию, увеличивается, когда несовместимые изменения API вносятся в стабильные API; число Y, представляющее минор версия, увеличивается при добавлении функций, совместимых с предыдущими версиями; число Z, представляющее выпуск исправления, увеличивается, когда исправляется ошибка обратной совместимости. Такое улучшение легко недооценить, но оно необходимо для большинства современных сценариев разработки программного обеспечения, где непрерывная поставка (CDE) имеет первостепенное значение, а новые версии выпускаются с большой частотой.

- TypeScript: Если вы опытный веб-разработчик, вы, вероятно, уже знаете, что такое TypeScript. Если вы этого не сделаете, давайте просто скажем, что TypeScript — это расширение JavaScript, созданное Microsoft, которое позволяет использовать все функции ES2015 и добавляет мощные возможности. Проверка типов и объектно-ориентированные функции во время разработки (такие как объявления классов и типов): исходный код TypeScript может быть затем «преобразован» в стандартный код JavaScript, понятный всем браузерам.

- Рендеринг на стороне сервера: Angular 2 поставляется с Angular Universal, технологией с открытым исходным кодом, которая позволяет внутреннему серверу запускать приложения Angular и предоставлять клиенту только полученные статические HTML-файлы. В двух словах, сервер выполнит первый проход страницы для более быстрой доставки клиенту, а затем немедленно обновит клиентский код. У SSR есть свои предостережения, такие как требование Node.js, установленного на хост-компьютере, для выполнения необходимых шагов предварительного рендеринга, а также наличия там всей папки node modules, но это может значительно увеличить время отклика приложения для типичного интернет-браузера, таким образом устранение известной проблемы с производительностью AngularJS.

- Angular Mobile Toolkit: Набор инструментов, специально разработанный для создания высокопроизводительных мобильных приложений.

- Интерфейс командной строки: новый интерфейс командной строки, представленный в Angular 2, может использоваться разработчиками для создания компонентов, маршрутов, сервисов и каналов с помощью команд консоли/терминала вместе с простыми тестовыми оболочками.

- Компоненты: Это основные строительные блоки Angular 2, полностью заменяющие контроллеры и области действия AngularJS, а также поднимающие большинство задач, ранее охватываемых прежними директивами: данные приложения, бизнес-логика, шаблоны и стили приложения Angular 2 могут быть созданы с помощью компонентов.

Angular 4. 23 марта 2017 года Google выпустила Angular 4: цифра 3 была полностью пропущена, чтобы объединить все основные версии многих компонентов Angular, которые до этой даты разрабатывались отдельно — например, Angular Router, который уже имел версию 3. x в то время. Начиная с Angular 4, вся Angular Framework была объединена в один и тот же шаблон MAJOR.MINOR.PATCH SemVer.

Новая основная версия принесла ограниченное количество критических изменений, таких как: новая и улучшенная система маршрутизации, поддержка TypeScript 2.1+ (и требования), а также некоторые устаревшие интерфейсы и теги. Также было внесено немало улучшений, в том числе:

- Подборка опережающих времен. Angular 4 компилирует шаблоны на этапе сборки и соответствующим образом генерирует код JavaScript. Это огромное архитектурное улучшение по сравнению с режимом Just in Time, используемым в AngularJS и Angular 2, где приложение компилируется во время выполнения, т. е. при запуске приложения: не только приложение работает быстрее, поскольку клиенту не нужно ничего компилировать, но он сбрасывает / ломает во время сборки, а не во время выполнения для большинства ошибок компонентов, что приводит к более безопасным и стабильным развертываниям.
- Пакет анимаций NPM. Все существующие анимации и эффекты пользовательского интерфейса, а также новые, были перемещены в специальный пакет @angular/animations вместо того, чтобы быть частью @angular/code: умный ход, позволяющий не анимированным приложениям отказаться от этой части. кода, поэтому он намного меньше и, возможно, быстрее.

Среди других заметных улучшений: новый валидатор форм для проверки действительных адресов электронной почты, новый интерфейс ParamMap для параметров URL в модуле HTTP-маршрутизации, улучшенная поддержка интернализации и т. д.

Angular 5. Выпущенный 1 ноября 2017 года Angular 5 включает поддержку TypeScript 2.3, еще один небольшой набор критических изменений, множество улучшений производительности и стабильности и несколько новых функций, таких как:

- Новый HTTP клиентский API. Начиная с Angular 4.3, модуль @angular/http был отложен в пользу нового пакета @angular/common/http с улучшенной поддержкой JSON, перехватчиками и неизменяемыми объектами запроса/ответа и другими вещами. Переключение было завершено в Angular 5, при этом предыдущий модуль устарел, а новый рекомендован для использования во всех приложениях.
- API передачи состояния. Новая функция, позволяющая передавать состояние приложения между сервером и клиентом.
- Новый набор событий маршрутизатора для более детального контроля над жизненным циклом HTTP: ActivationStart, ActivationEnd, ChildActivationStart, ChildActivationEnd , GuardsCheckStart , GuardsCheckEnd , ResolveStart и ResolveEnd .

Ноябрь 2017 года также стал месяцем выпуска моей книги по ASP.NET Core 2 и Angular 5, в которой рассказывается о большинстве вышеупомянутых улучшений.

Angular 6. Выпущенный в апреле 2018 года Angular 6 был в основном служебным выпуском, больше ориентированным на улучшение общей согласованности фреймворка и его набора инструментов, чем на добавление новых функций. Так что кардинальных изменений не было. Поддержка RxJS 6, новый способ регистрации провайдеров, новый инъекционный декоратор, улучшенная поддержка Angular Material (компонент, специально созданный для реализации материального дизайна в пользовательском интерфейсе на стороне клиента Angular), дополнительные команды/обновления CLI и так далее.

Angular 7. Angular 7 вышел в октябре 2018 года, и это определенно было серьезное обновление, как мы можем легко догадаться, прочитав слова, написанные Стивеном Флуином — руководителем отдела по связям с разработчиками в Google и известным представителем Angular — в официальном блоге разработчиков Angular после официального выпуска:

«Это основной выпуск, охватывающий всю платформу, включая базовую структуру, Angular Material и CLI с синхронизированными основными версиями. Этот выпуск содержит новые функции для на-

шей цепочки инструментов и позволил запустить несколько крупных партнеров».

Вот список новых функций:

- Простое обновление: благодаря заделу, сделанному с версией 6, команда Angular смогла сократить шаги, необходимые для обновления существующего приложения Angular с более старой версии до самой последней. Подробную процедуру можно просмотреть, посетив веб-сайт https://update.angular.io, невероятно полезное интерактивное руководство по обновлению Angular, которое можно использовать для быстрого восстановления необходимых шагов — команд CLI, обновлений пакетов и т. д. — которые необходимо выполнить. сделано для обновления существующего приложения Angular с более старой версии Angular до самой последней.
- Подсказки CLI: интерфейс командной строки Angular был изменен, чтобы предлагать пользователям, как при выполнении общих команд, таких как ng new или ng add @angular/material, чтобы помочь разработчикам обнаружить встроенные функции, такие как маршрутизация, поддержка SCSS и так далее.
- Angular Material & CDK: дополнительные элементы пользовательского интерфейса, такие как: виртуальная прокрутка, компонент, который загружает и выгружает элементы из DOM на основе видимых частей списка, что позволяет создавать очень быстрые возможности для пользователей с очень большими прокручиваемыми списками; CDK-родная поддержка перетаскивания; улучшенные элементы выпадающего списка; и больше.
- Партнерские запуски: Улучшена совместимость с рядом сторонних проектов сообщества, таких как: Angular Console , загружаемая консоль для запуска и запуска проектов Angular на вашем локальном компьютере; AngularFire , официальный пакет Angular для интеграции с Firebase; Angular для NativeScript , интеграция между Angular и NativeScript — фреймворк для создания нативных приложений для iOS и Android с использованием JavaScript и/или клиентских фреймворков на основе JS; некоторые интересные новые специфичные для Angular функции для StackBlitz , онлайн-среды IDE, которую можно использовать для создания проектов Angular и React, таких как редактор с вкладками и интеграция с языковой службой Angular и так далее.

- Обновленные зависимости: добавлена поддержка TypeScript 3.1, RxJS 6.3 и Node 10, хотя предыдущие версии все еще можно использовать для обратной совместимости.

Angular 8. Angular 8, который был выпущен 29 мая 2019 года и на данный момент является самой последней версией. Новый выпуск в основном посвящен Ivy, долгожданному новому компилятору/среде выполнения Angular: несмотря на то, что он является текущим проектом со времен Angular 5, версия 8 является первой, которая официально предлагает переключатель времени выполнения для фактического согласия на использование Ivy, что возможно, станет средой выполнения по умолчанию, начиная с Angular 9.

Чтобы включить Ivy, просто добавьте enableIvy": true свойство в angularCompilerOptions раздел в файле tsconfig.json приложения. Мы поговорим об этом подробнее в следующих главах, когда мы фактически выполним переключение, чтобы увидеть, как наш код будет работать с новым компилятором/средой выполнения.

Другие заметные улучшения и новые функции включают в себя:

- Поддержка Bazel: Angular 8 поддерживает Bazel, бесплатный программный инструмент, разработанный и используемый Google для автоматизации создания и тестирования программного обеспечения: он может быть очень полезен для разработчиков, стремящихся автоматизировать конвейер доставки, поскольку позволяет выполнять инкрементную сборку и тестирование и даже возможность настройки удаленных сборок (и кэширования) на сборочной ферме.
- Маршрутизация: маршрутизатор Angular теперь принимает новый синтаксис для объявления маршрутов с отложенной загрузкой, используя синтаксис import() из TypeScript 2.4+ вместо того, чтобы полагаться на строковый литерал: старый синтаксис был сохранен для обратной совместимости, но будет возможно скоро упал.
- Рабочие службы: введена новая стратегия регистрации, позволяющая разработчикам выбирать, когда регистрировать своих рабочих, а не делать это автоматически в конце жизненного цикла запуска приложения; также возможно обойти сервисного работника для определенного HTTP-запроса, используя новый ngsw-bypass заголовок.
- API рабочей области. Новый и более удобный способ чтения и изменения конфигурации рабочей области Angular вместо ручного изменения angular.json файла.

В разработке на стороне клиента сервис-воркер — это сценарий, который браузер запускает в фоновом режиме для выполнения любых действий, не требующих ни пользовательского интерфейса, никакого-либо взаимодействия с пользователем.

В новой версии также были внесены некоторые заметные критические изменения — в основном из-за Ivy — и удалены некоторые давно устаревшие пакеты, такие как @angular/http, который был заменен на @angular/common/http начиная с Angular 4.3, а затем официально объявлен устаревшим в 5.0.

SPA приложение. Цель SPA (Single Page Application) — сделать приложения пригодными для использования практически на любом устройстве.

В настоящее время каждое устройство (настольный компьютер, ноутбук или мобильное устройство) под управлением Windows, Linux, Android или IOS включает браузер, с помощью которого пользователь может просматривать веб-страницы. При развертывании современных бизнес-приложений не лучше ли использовать этот браузер в качестве клиента? Вместо того, чтобы развертывать толстые клиентские программы на устройстве каждого пользователя? Принимая во внимание разнообразие поддерживаемых аппаратных платформ и операционных систем, а также другие соображения безопасности? Очевидно, ответ «ДА». Кроме того, это особенно верно для приложений SaaS, которые должны работать на как можно большем количестве платформ.

Но, с точки зрения конечного пользователя, просмотр веб-страниц или использование бизнес-приложений — это два совершенно разных опыта.

- Веб-серфинг подразумевает переход с одной веб-страницы на другую, с одного контента на другой, где пользователь может ощущать последовательные полные обновления страниц, не расстраиваясь.
- Однако использование бизнес-приложения требует гораздо большей гибкости и быстрой интерактивности. Как правило, в традиционном бизнес-приложении действия пользователя не подразумевают полного обновления страницы приложения. Пользователь чувствует, что он остается в пределах одной среды приложения.

Одностраничное приложение (SPA) — это веб-приложение, состоящее из одной HTML-страницы. Вместо обновления всей страницы после каждого взаимодействия с пользователем, как в случае тра-

диционного многостраничного приложения (MPA), только данные, которые должны быть обновлены, запускают частичное обновление.

Например, когда вы просматриваете электронную почту Google, вы не замечаете существенных изменений во время навигации. Боковая панель и заголовок остаются нетронутыми, когда вы просматриваете свой почтовый ящик.

И это ключ к тому, чтобы дать пользователю представление о том, что он использует бизнес-приложение. Пользователь остается в этом гибком и очень интерактивном интерфейсе.

И SPA, и MPA основаны на протоколе HTTP.

В традиционной архитектуре MPA клиент/сервер каждый щелчок пользователя запускает HTTP-запрос к серверу. Результатом этого нового запроса является полное обновление страницы, даже если часть содержимого остается прежней, что можно увидеть на рис. 4:

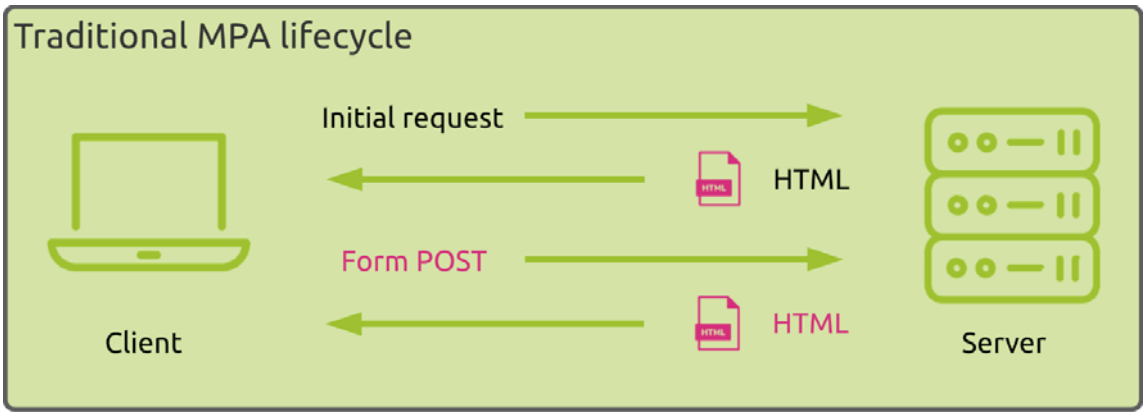


Рис. 4. Жизненный цикл MPA-приложения

С другой стороны, ядро SPA основано на Ajax, наборе методов разработки, которые позволяют клиенту отправлять и получать данные с сервера асинхронно (в фоновом режиме), не мешая отображению и поведению веб-страницы. Ajax позволяет веб-страницам и, соответственно, веб-приложениям динамически изменять содержимое без необходимости перезагрузки всей страницы.

Чтобы это произошло, SPA сильно зависит от сценариев JavaScript, которые запускаются в браузере клиента. Фреймворки JavaScript, такие как React, Vue, Angular и Ember, несут ответственность за обработку тяжелой работы на стороне клиента.

Заключение. Несмотря на некоторые проблемы, упомянутые выше, внедрение архитектуры SPA, по-видимому, является способом удовлетворить некоторые из основных требований, предъявляемых к современным бизнес-приложениям, а именно:

- Обеспечение плавного и плавного взаимодействия с пользователем
- Быстрый процесс разработки
- Гибкий дизайн для быстрой адаптации к новым требованиям пользователей
- Поддержка любого устройства, любой операционной системы
- Гарантия хорошего взаимодействия с пользователем в условиях медленной сети

Эта архитектура особенно подходит для приложений SaaS.

С другой стороны, мониторинг производительности таких приложений является сложной задачей, поскольку архитектура SPA выдвигает большую часть логики приложения на периферию. Мониторинг производительности SPA требует мониторинга не только производительности клиентских устройств, но и всех вызовов API, выполняемых к серверным службам (которые могут быть вашими или размещаться у третьих сторон и могут включать другие типы связи, такие как разрешение DNS и подключения к CDN). Другими словами, мониторинг такой среды требует полной видимости устройств конечных пользователей (типы устройств, ОС, браузер и т. д.), местонахождения конечных пользователей и производительности сетевого подключения, вызовов API (идентификация запрошенных сторонних служб, связанных с ними характеристик, а также статус завершения).

Список использованных источников

1. Миковски Майкл С., Разработка одностраничных веб-приложений, 2014. – 152 с.

2. Мациевский Н.С. Реактивные веб-сайты. Клиентская оптимизация в алгоритмах и примерах: Учебное пособие / Н.С. Мациевский, Е.В. Степанищев, Г.И. Кондратенко — М.: Интернет-Университет Информационных Технологий: БИНОМ. Лаборатория знаний, 2010. — 336 с.

3. Мациевский Н. Разгони свой сайт. Методы клиентской оптимизации веб-страниц. - М.: Интернет-Университет Информационных Технологий: БИНОМ. Лаборатория знаний, 2013.

4. Флэнаган Д. Javascript. Подробное руководство. - 2012

5. Сообщество IT-специалистов HTML и CSS [Электронный ресурс] URL: https://habr.com/ru/

АНАЛИЗ АКТУАЛЬНОСТИ ПЕРЕХОДА СЕРВЕРОВ ЦОД НА НОВЫЙ ТИП ПАМЯТИ DDR5

Теодорович Н.Н., к.т.н, доцент,
Свербеев А. Ю., Михайлов Д. А.,
Суходольский Г. А., бакалавры гр. ИБО ЗИ – 20,
Технологический университет («МГОТУ»),
Россия, Королев.

В статье проведен анализ актуальности перехода серверов ЦОД на новый тип памяти DDR5.

Ключевые слова: ЦОД, ОЗУ, DDR5.

Введение. В центрах обработки данных (дата-центрах) хранятся и обрабатываются огромные объемы информации для различных компаний - от поисковиков до финансовых организаций, проводящих финансовые операции особой важности.

Серверы дата-центра - единая многокомпонентная система информационной инфраструктуры, включающая серверное оборудование, обеспечивающая обработку и хранение информации. Все оборудование ЦОД спроектировано для обеспечения максимальной отказоустойчивости, стабильности и мощности оборудования, ведь даже минутная остановка работы серверов повлечет за собой огромные финансовые убытки для компании.

Серверная оперативная память играет важную роль в стабильности работы машины. Если во время обработки финансовых операций или конфиденциальных данных произойдет сбой, последствия могут оказаться катастрофическими. Во избежание этого, производство планок ОЗУ жестко контролируется, чтобы добиться высокого качества продукции, ведь она должна выдерживать высокие нагрузки в течение длительного периода времени.

В серверах используется не специальная серверная оперативная память, но она обязательно должна поддерживать технологию ECC (Error Correction Code) - код коррекции ошибок, который позволяет автоматический распознавать и исправлять ошибки одиночных битов в памяти, способные вызывать критические сбои при высокой интенсивности вычислений.

DDR5 — это новое, 5-е поколение синхронной динамической оперативной памяти с удвоенной скоростью передачи данных (Double

Data Rate Synchronous Dynamic Random Access Memory), также называемая DDR5 SDRAM. Разработка началась в 2017 году. Память DDR5 обладает новыми функциями для повышения производительности, снижения энергопотребления и более высокой целостности данных для вычислительных систем следующего десятилетия. Память DDR5 была представлена в 2021 г.

DDR5 поддерживается на данный момент такими процессорами, как:

Intel:

- Поколения ядер Sapphire Rapids, например, Intel Xeon Scalable; (серверный процессор)
- Поколения ядер Alder Lake, например, Intel Core i9-12900K (для ПК)
- AMD:
- Поколения ядер, например, AMD EPYC Genoa; (серверный процессор)
- Поколения ядер Zen 3+, Zen 4, например, Ryzen 7 6800U (для ПК)

Так как основным потребителем новой памяти в ближайшее время выступит серверный сегмент, компания Intel, доминирующая на рынке серверных процессоров в течение многих лет, активно участвует в разработке новых типов материнских плат, поддерживающих новый стандарт памяти.

В пользовательском сегменте начало массового перехода пользователей к DDR5 памяти ожидается в 2023 году, а к 2026 году новая память, предположительно, будет занимать до 90% мирового компьютерного рынка и вытеснит актуальный на данный момент стандарт DDR4.

Сравнение с предшественником. Преимущества нового поколения ОЗУ приведены в табл. 1:

Таблица 1. Преимущества нового поколения ОЗУ

Поколение	**DDR5**	**DDR4**
Частота	5200 МГц	3200 МГц
Макс. Плотность ядра	64 Гбит	16 Гбит
1	2	3
Макс. Размер UDIMM	512 Гб	128 Гб
Макс. Скорость передачи	6,4 Гб/с	3,2 Гб/с
Каналов	2	1
Ширина	64-бит(2x32)	64-бит

Поколение	DDR5	DDR4
Банки	4	4
Группы банков	8/4	4/2
Длина пакета	BL16	BL8
Напряжение	1,3 В	1,5 В

Сравнение производилось оперативной памяти DDR4-3200 МГц и DDR5- 5200МГц. Результаты показаны на рисунках 1 – 6.

Первой тестировалась программа AIDA 64 - утилита, которая позволяет узнать сведения об аппаратных и программных компонентах компьютера. Проверялась скорость чтения, записи и копирования обеих планок памяти (рис.1, 2):

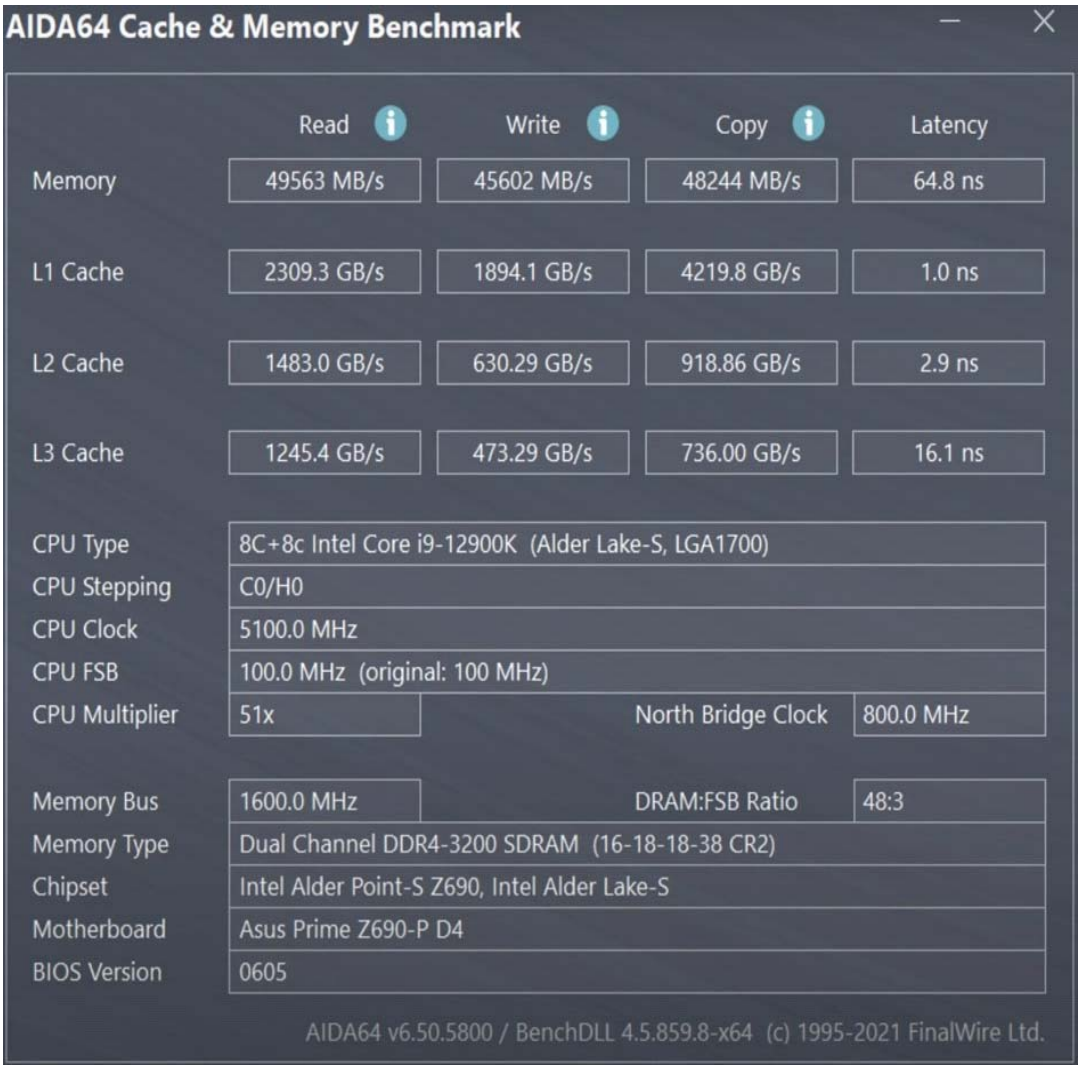


Рис. 1. DDR4 3200 МГц

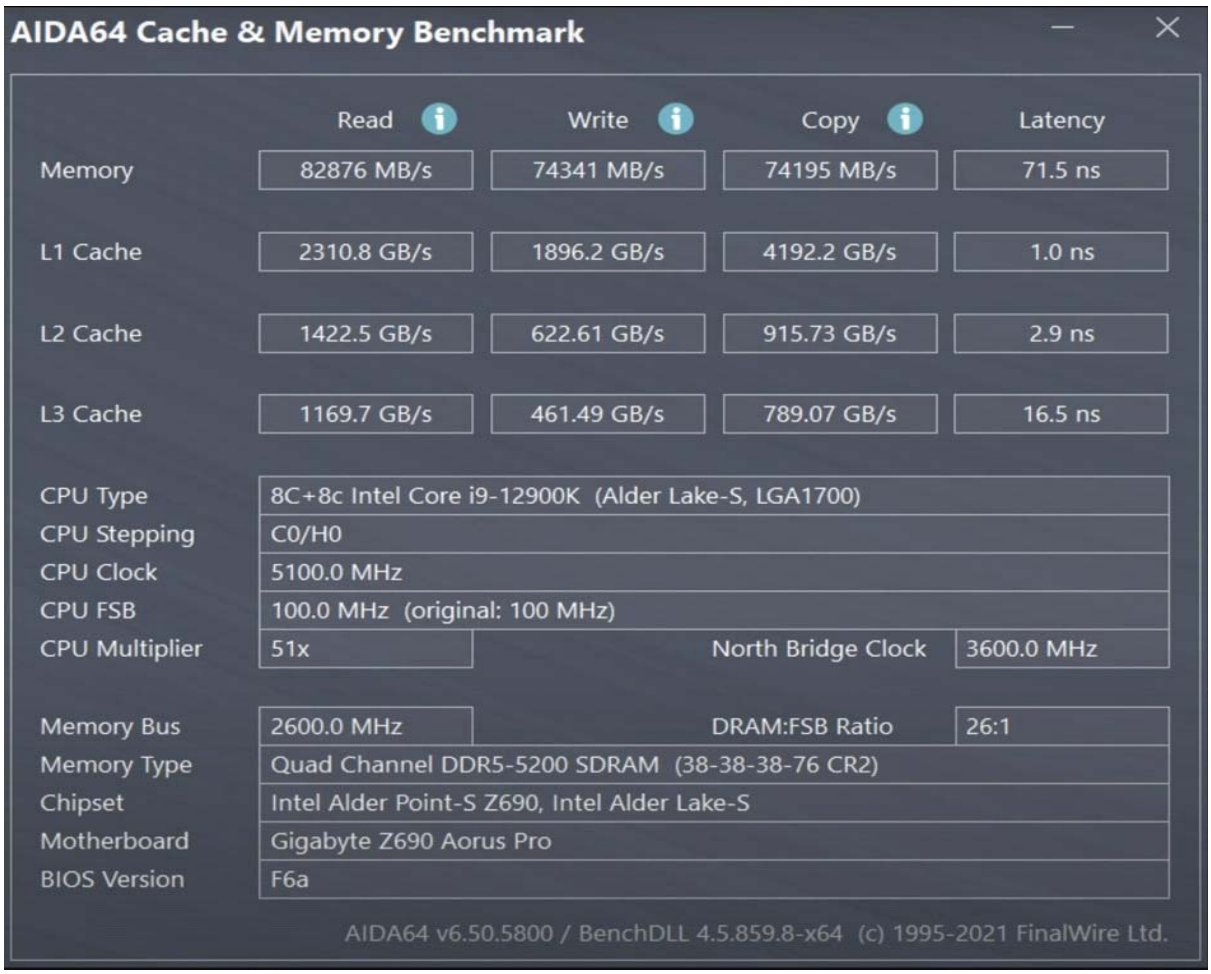


Рис.2. DDR5 5200МГц

Как видно, DDR5 быстрее в 1,6 раза, но при этом латентность (некая величина в наносекундах, представляющая собой совокупность частоты и таймингов памяти, а также частоты процессора) у старого поколения лучше. Это объясняется тем, что с ростом частоты, растет и тайминг (Row Active Time (tRAS) - минимальное время, которое дается контроллеру для работы со строкой (время, в течение которого она может быть открыта для чтения или записи), после чего она закроется.), то производительность падает, а у DDR5 тайминг 38-38-38-72 такт шины, в то же время у DDR4 16-18-18-38 такт шины, следовательно, при всей своей скорости обработки DDR5 проигрывает в производительности DDR4.

Ниже на рис. 3, 4 представлены сведения о работе двух поколений памяти в архиваторе и программе визуализации.

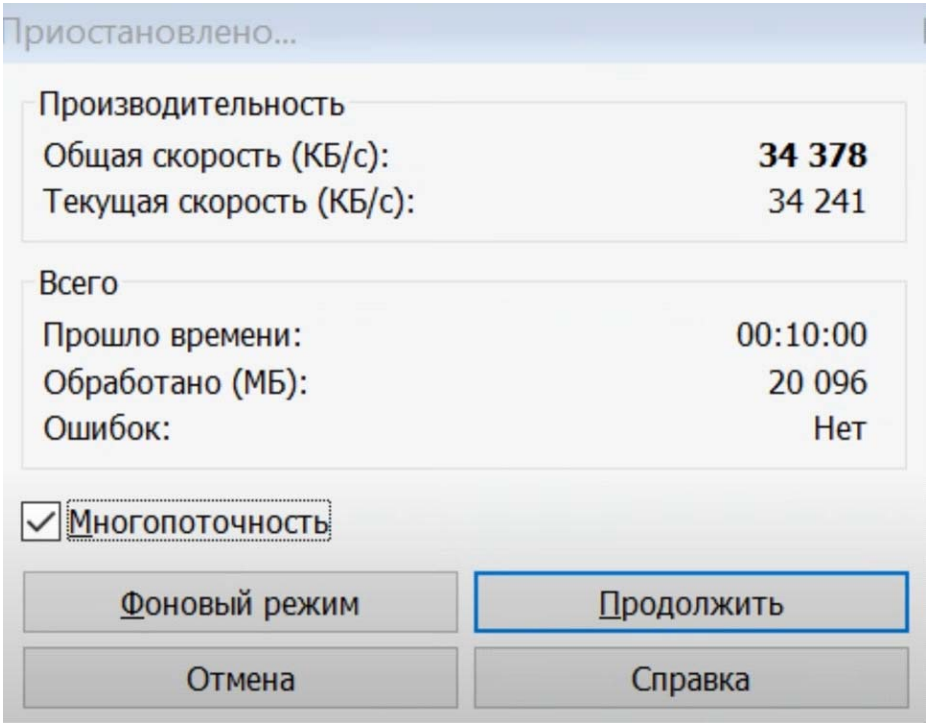


Рис.3. DDR4 3200 МГц

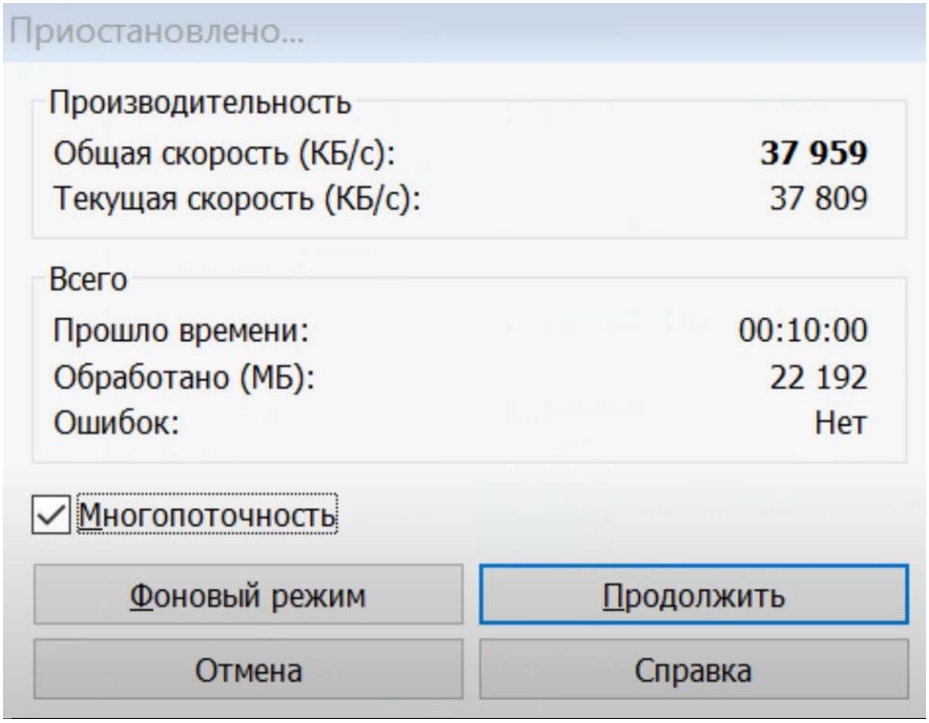


Рис. 4. DDR5 5200МГц

В архиваторе DDR5 показал себя лучше на 10% лучше, чем DDR4. Это незначительный прирост, при том, что скорость выше в 1,65 раз.

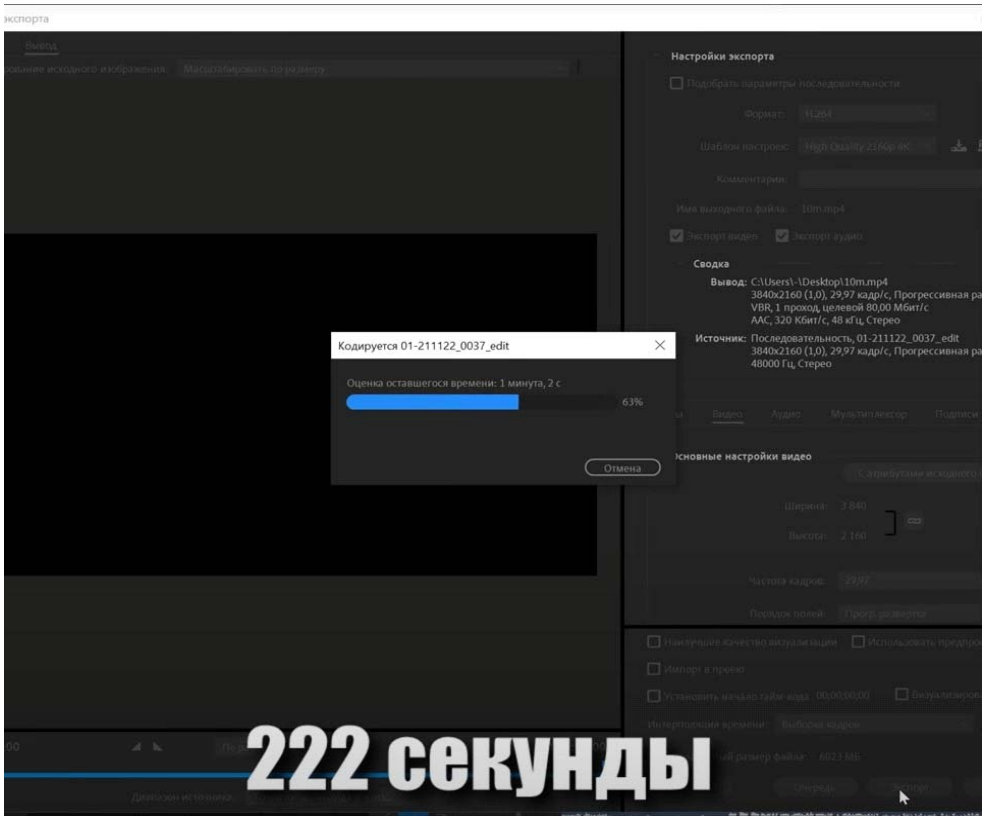


Рис. 5. DDR4 3200 МГц

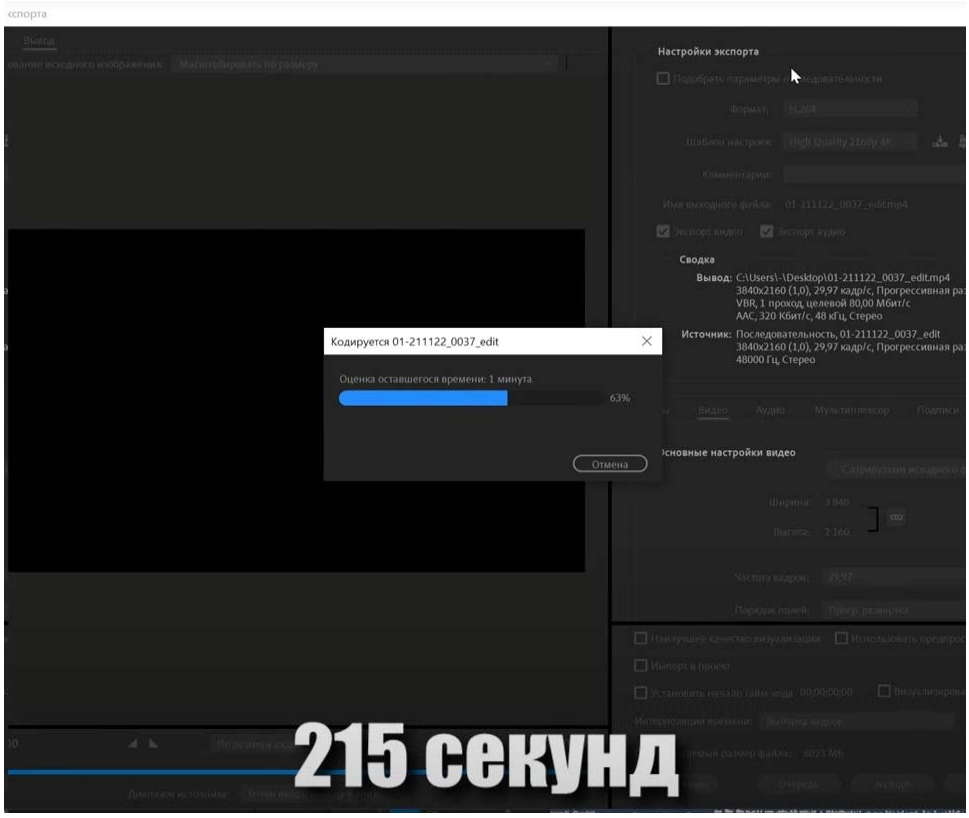


Рис. 6. DDR5 5200МГц

Средства визуализации также показали небольшое улучшение в скорости работы всего на всего в 4% (рис. 5, 6).

DDR5 имеет два канала передачи данных, по 40 бит на каждый поток в отличии от DDR4 с одним 64-битным каналом. Длина пакета для каждого канала составит 16 байт (BL16), вместо 8 байт (BL8) у DDR4. За одну операцию каждый канал передает 64 байта данных. В результате DDR5 при одинаковой скорости выполняет две 64-байтовые операции, в то время как DDR4 только одну. В итоге эффективная пропускная способность DDR5 увеличилась вдвое, по сравнению с DDR4.

Заявленный вольтаж является ложным - не 1,3 В, а 1,6 В, то есть на 0.1 В больше, чем и у DDR4, и на 0,3 В больше, чем заявлено в характеристиках. Скорее всего это связанно с тем, что новая память плохо оптимизирована, и ей предстоит еще дорабатываться. Для компаний это является важным показателем, так как это влечет за собой огромные затраты на электроэнергию, ведь сервера работают безостановочно, из-за чего даже разница в 0,1 Вольт существенна.

Цена за флагманскую версию нового поколения памяти (128 Гб) составляет порядка 420 тыс. рублей, а флагман прошлого поколения (128 ГБ) стоит 230 тыс. рублей. Практически в два раза дороже, чем предшественник.

Анализируя вышесказанное, можно сказать, что на данный момент переход ЦОД на DDR5 выглядит неоправданным из-за высокой цены и отмеченных недостатков.

Список используемых источников:

1. Исаева Г. Н., Теодорович Н. Н., Басова С. А. Региональные проблемы внедрения и распространения систем защищаемого электронного документооборота // Интернет-журнал «НАУКОВЕДЕНИЕ» Том 9, №3 (2017) http://naukovedenie.ru/PDF/54TVN317.pdf (доступ свободный).

2. Роганов А. А., Теодорович Н. Н. Тенденции развития облачных технологий // Современные информационные технологии / Под науч. ред. В.М. Артюшенко. М.: Научный консультант, 2015. С. 125-132.

3. Сидорова, Н. П., Логачева, Н. В., Добродеев, В. Ю. Информационные технологии оперативного анализа данных / Н. П. Сидорова, Н. В. Логачева, В. Ю. Добродеев // Информационно-технологический вестник. - 2014. - Т. 01. - № 1. - С. 64-74.

4. Теодорович, Н. Н., Роганов, А. А. Тенденции развития облачных технологий // Современные информационные технологии под

науч. ред. докт. техн. наук, проф. В. М. Артюшенко // М.: "Научный консультант. - 2015. -. С. 125-132.

5. Abbasova, T. S., Sidorova, N. P., Teodorovich, N. N. & Abbasov, E. M. Evaluation of Telecommunications Electromagnetic Compatibility with the Use of Three-Dimensional Modeling Technology [Text] // Modern Applied Science. - 2016. - Vol. 10, - No. 10, - pp.224-230. ISSN 1913-1844; E-ISSN 1913-1852. Published by Canadian Center of Science and Education. DOI: 10.5539/mas.v10n10p224

6. Горбатова, И.А., Саитова К.М. Перспективы развития оперативной памяти компьютера // Мой шаг в науку. Материалы IV Всероссийской научно-практической конференции. Отв. редактор Э.Р. Сайдимова. – 2021. – . С. 346-347

7. Пащенко Д.С., Комаров Н.М., Мохов А.И. Верхнеуровневая модель оценки стратегических рисков и бюджетирования цифровой трансформации на промышленном предприятии // Управление финансовыми рисками. 2021. № 1. С. 8-23.

8. Душкин, Р.В. Модель распределенных вычислений для организации программной среды, обеспечивающей управление автоматизированными системами интеллектуальных зданий / Р.В. Душкин, А.И. Мохов // Компьютерные исследования и моделирование. – 2021. – . – Т. 13, № 3. – С. 557-570.

9. Что такое центр обработки данных (ЦОД) [Электронный ресурс]. – Режим доступа: https://timeweb.com/ru/community/articles/chto-takoe-centr-obrabotki-dannyh. – Дата доступа: 20,03.2022.

К ВОПРОСУ ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ВИРУС-МАЙНЕР

Теодорович Н.Н., к.т.н, доцент,
Суходольский Г.А., Григорьева М.В.,
Свербеев А.Ю., студенты группы ИБО-ЗИ-20
Технологический университет («МГОТУ»),
Россия, г. Королев

В статье рассмотрены вопросы, связанные с вирус-майнер.

Ключевые слова: компьютерные программы; компьютерные угрозы; информационная безопасность; вирус; майнер; защита.

Ведение. «Майнинг» становится всё более актуальной темой в наше время, однако она всё ещё не так широко раскрыта и распространена [1]. Другое дело вирус-майнер, мало кто о них слышал, но каждый может быть причастен к добыче «виртуальных денег», даже не подозревая об этом.

Так называемые «вирус-майнеры» — вирусы, использующие компьютеры для добычи валюты и передачи ее владельцу этих ПО, что в свою очередь может привести к повреждению техники и потере данных, что уже является угрозой информационной безопасности.

Основная часть. Для дальнейшего понимания статьи требуется обратиться к теоретической базе.

Компьютерный вирус — вид вредоносного программного обеспечения, отличающийся репликацией и распространением своих копий по различным каналам связи, а также способностью внедряться в код других программ, в системные области памяти, в загрузочные секторы. Но это лишь одно из многих определений [2].

Компьютерный вирус — разновидность компьютерной программы, способной создавать свои копии (необязательно совпадающие с оригиналом) и внедрять их в файлы, системные области компьютера, компьютерных сетей, а также осуществлять иные деструктивные действия.

Майнинг — это добыча криптовалюты. Процесс работает благодаря технологии блокчейн — выстроенная по определённым правилам непрерывная последовательная цепочка блоков (связный список), содержащих информацию. В каждом из них записано определенное число транзакций.

Вирус-майнер — это вредоносное программное обеспечение, основной целью которого является майнинг, внедряется в системы частных пользователей, но в отличии от других троянов, объектом майнера являются аппаратные ресурсы компьютера, а не данные его владельца.

Майнеры делятся на два типа: криптоджейкинг и классический.

Криптоджейкинг — такой тип вируса существует в виде скрипта в коде интернет-страниц, они не распространяются в виде отдельных ПО, а существуют только в пределах сайтов. При посещении таких страниц аппаратные ресурсы компьютерных систем начинают добывать криптовалюту. Часто встречается такое, что сайт предупреждает о криптоджейкинге. Это делается для получения дохода с ресурса, предоставляемого на “бесплатной основе”, и является аналогом рекламных постов, занимающих полезное пространство, для владельца сайта. В таком случае владелец ПК сам решает, согласен он на такие условия или нет, что освобождает такой вид майнера от статуса “вредоносный”.

Классический майнер — это обычная майнер-программа, которую используют для добычи криптовалюты на майнинг-фермах, однако она может распространяться отдельно и в комплекте с любой другой программой. Используя аппаратные ресурсы не принадлежащие владельцу данного ПО, злоумышленник имеет возможность получать валюту за счёт чужого оборудования. Как правило, такие вирусы работают в фоновом режиме и автоматически запускаются во время загрузки компьютера, не выдавая себя.

Тенденция такова, что количество атак майнинг-вирусами с каждым днём становится больше в разы. Именно поэтому важно уже сейчас обратить внимание на защиту своих устройств. Для того, чтобы обезопасить компьютерную систему от вируса-майнера, следует соблюдать основные правила компьютерной безопасности. В первую очередь, следует установить антивирус. Однако такой защиты недостаточно. Требуется соблюдение трех правил: регулярное обновление программного обеспечения и операционной системы, установленной на компьютерной системе; предотвращение установки подозрительного ПО с файлами-распаковщиками; использование прав пользователя за компьютером, вместо прав администратора.

Существует несколько сигналов того, что компьютерная система заражена вирус-майнером:

- перегревы CPU (центрального процессора) и GPU (графического процессора);
- чрезмерная работа системы охлаждения;
- полная загрузка всех ядер процессора и видеокарты;
- медленная работа системы.

Раньше майнеры было просто найти в диспетчере задач. Они существовали в виде процессов, которые сильно нагружают систему, но современные вирусы научились скрывать свои слабые места и теперь при открытии диспетчера задач, такие процессы отключаются и продолжают работу только после того, как за нагрузкой системы перестают следить. Однако майнер легко вычислить по температуре комплектующих, если CPU и GPU загружены минимально а их температура зашкаливает, это явный признак вирусной программы-майнера.

Для поиска вируса-майнера раньше использовали встроенную системную программу - диспетчер задач. Программы использующие свободные ресурсы компьютера выдавали себя нагрузкой на CPU и GPU, которую фиксировал диспетчер, однако сейчас вредоносное ПО автоматически отключается при его запуске.

В данной ситуации мы можем обнаружить такие программы с помощью монитора ресурсов. Для его вызова необходимо открыть системное окно “выполнить”. Сделать это можно через поиск приложений или через комбинацию клавиш “Win + R”. Далее следует вписать команду “resmon” . В открывшемся окне можно оценить использование ресурсов сети, дисков, центрального и графического процессоров. В графе “Состояние” можно увидеть, какие программы выполняются прямо сейчас, а какие приостановили свою работу).

Далее нужно удалить такие программы, но лучше это доверить профессионалу, ведь компоненты Windows, входящие в список образов ПО, тоже могут быть приостановлены за ненадобностью.

Вторым способом справиться с вирус-майнерами является покупка и установка антивирусных программ. Существуют бесплатные версии такого ПО, но в большинстве своём они не могут даже обнаружить новую угрозу. Платная версия антивируса полностью справляется со своей задачей. ПО обнаруживает и устраняет почти любой современный вирус-майнер. Разработка и обновление таких программ, как и вирусов происходит постоянно, что дает возможность на приличном уровне противостоять такого вида вирусам.

Заключение. За счет повышения уровня информатизации, компьютер стал частью жизни почти каждого человека. Это привело к

росту желания получить ценные ресурсы неправомерным путем. Постоянно развивающиеся компьютерные угрозы заставляют каждого задуматься о безопасности своей информации. Для обеспечения этой самой безопасности необходимо придерживаться рекомендаций специалистов или руководствоваться пунктами "об информационной безопасности", изложенными в Положении каждой компании.

Периодический анализ новых угроз и заинтересованность в сохранении информации и ресурсов могут гарантировать надежную защиту от угроз со стороны большей части злоумышленников.

Список используемых источников

1. Майнинг - последние новости сегодня [Электронный ресурс] URL: https://www.rbc.ru/crypto/tags/?tag=Майнинг.

2. Компьютерные вирусы : учебное пособие. — Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2015 — Часть 1 — 2015. — 62 с. — Текст : электронный // Лань : электронно-библиотечная система.

3. Компьютерные вирусы и вредоносное ПО [Электронный ресурс] URL: https://www.kaspersky.ru/resource-center/threats/computer-viruses-and-malware-facts-and-faqs

4. Наиболее часто обнаруживаемые семейства вредоносных программ для крипто-майнинга, поражающие корпоративные сети по всему миру с января по июнь 2020 года [Электронный ресурс] URL: https://www.statista.com/statistics/325252/cryptomining-malware-global/.

5. Статистика кибербезопасности 2021 года. Полный список статистики, данных и тенденций [Электронный ресурс] URL: https://purplesec.us/resources/cyber-security-statistics/.

6. Теодорович Н.Н., Исаева Г.Н. К вопросу о создании защищенной системы управления контентом // Современные информационные технологии / Под науч. ред. В.М. Артюшенко. М.: Научный консультант, 2018. С. 84-89.

7. Теодорович Н.Н., Дмитриева Е.А., Кравчени М.С. Разработка и обоснование проекта развития информационного портала МГОТУ как инструмента управления знаниями университета. Современные информационные технологии / Под ред. В.М. Артюшенко. М.: Научный Консультант, 2017. - С. 63-68.

8. Теодорович Н. Н. Основы теории комплексных систем безопасности // Приборы и системы. Управление, контроль, диагностика. 2010. № 8. С. 16-20.

ПРОЕКТИРОВАНИЕ ИНФОРМАЦИОННО-УПРАВЛЯЮЩЕЙ СИСТЕМЫ ДЛЯ СТЕНДА 1А ПОДРАЗДЕЛЕНИЯ ИС-101 С ИСПОЛЬЗОВАНИЕМ ТРЕХКАНАЛЬНОЙ СХЕМЫ ДЛЯ ОГНЕВЫХ ИСПЫТАНИЙ ДВИГАТЕЛЬНЫХ УСТАНОВОК

Гунина Е. В., магистр группа ИМО-МП-21,
Руя М.А., магистр группа ИМО-МП-21,
Технологический университет («МГОТУ»),
Россия, г. Королев

Основная цель статьи – показать состав технических и программных средств информационно-управляющих систем (ИУС) для холодных и огневых испытаний ступеней РН и ЖРД тягой до 250 тс на компонентах топлива АТ+НДМГ и отработки перспективных ДУ ракетных блоков тягой до 500 тс.

Ключевые слова: система управления изделием (СУИ), система управления стендом (СУС), контроля, диагностики и отображения параметров (СКДО), система управления электропитанием (СУЭП), трехканальная схема

Введение. Информационно-управляющая система стенда ИС-101 включает:

– систему управления изделием (СУИ), обеспечивающую подачу компонентов топлива, газов и рабочих сред на борт стендового блока посредством управления элементами автоматики обвязки изделия;

– систему управления стендом (СУС), обеспечивающую управление отсеками и щитовыми и аварийную защиту стенда;

– систему контроля, диагностики и отображения параметров (СКДО), обеспечивающую формирование интегрированного информационного потока систем управления и измерения, обработку по заданным алгоритмам и отображение прямых и производных параметров на автоматизированных рабочих местах разработчиков изделия и ведущих испытание;

– систему управления электропитанием (СУЭП) аппаратурой ИУС и исполнительными элементами стендового оборудования стенда.

Основной раздел. Рассмотрим каждую составляющую информационно-управляющей системы отдельно.

Система управления стендом. Система управления стендом предназначена для:

– управления в ручном и автоматическом режимах исполнительными

– элементами (ИЭ) типа электропневматических клапанов (ЭПК) и двигателей постоянного тока;

– искробезопасного приема сигналов с датчиков давления, температуры, углового положения и контактных датчиков;

– выдачи в стендовые системы команд синхронизации и обменных команд;

– оперативного ввода и проверки циклограмм и алгоритмов управления, а также – их корректировки при необходимости;

– выполнения заданных циклограмм и алгоритмов в автоматическом– режиме с тактом 10 мс;

– регистрации принимаемых с датчиков сигналов и выдаваемых на ИЭ – команд с частотой 100 Гц;

– отображения на экранах персональных электронно-вычислительных – машин (ПЭВМ) автоматизированных рабочих мест (АРМ) операторов и ведущих инженеров состояния элементов автоматики и значений измеряемых параметров стенда в виде мнемосхем, таблиц, графиков, индикаторов и т.д.;

– регистрации, оперативной обработки информации, и представления– результатов в виде таблиц, графиков на экране монитора, в электронном и бумажном виде.

Структурная схема СУС представлена на рис. 1.

СУС является двухуровневой распределенной системой. На самом нижнем уровне находятся контроллеры управления, а также устройства связи с объектом. Соответственно на уровне выше находятся места оператора с автоматизированной системой, операторов СУС,АРМ сервер СУС и устройства организации локальной вычислительной сети.

Аппаратура нижнего уровня СУС (контроллеры управления и устройства связи с объектом испытания) монтируется в двух приборных стойках (стойке СУС 1 и стойке СУС2) расположенных в помещении аппаратуры управления в бункере стенда ИС-101.

АРМ СУС расположены в пультовой бункера стенда ИС-101. Средства связи с сервером СУС смонтированы в стойке сетевых коммутаторов, расположенной в пультовой бункера стенда ИС-101.

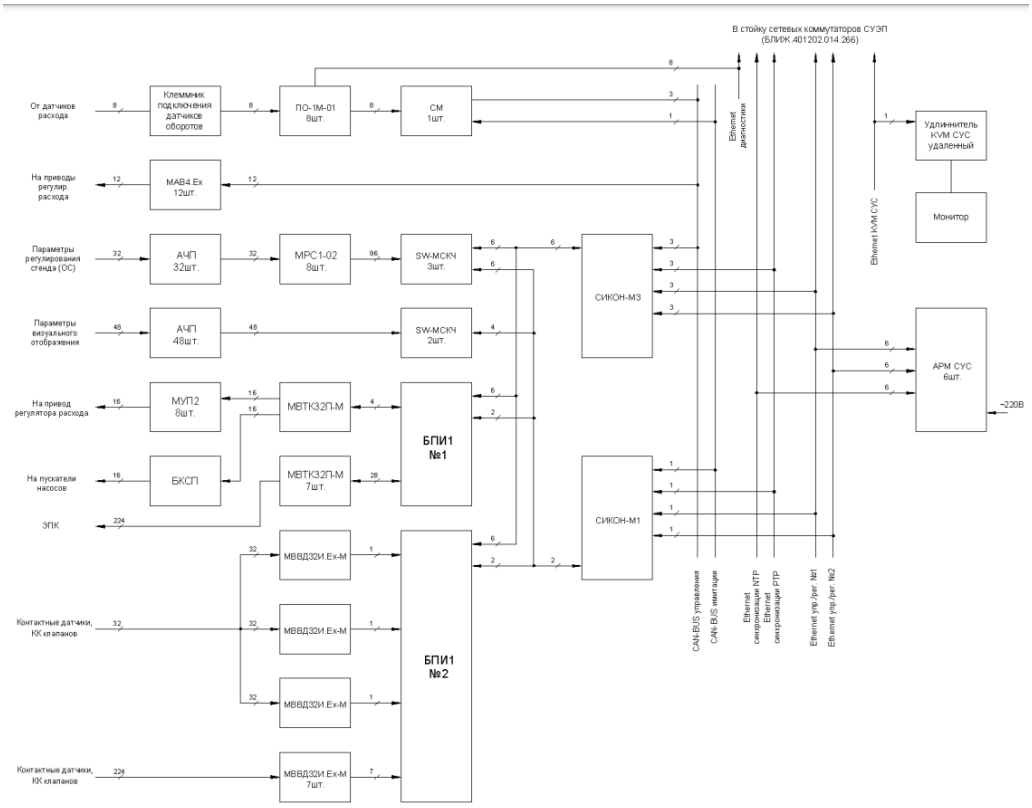


Рис. 1. Структурная схема СУС

Связь между верхним и нижним уровнями осуществляется посредством линий высокоскоростной связи (ЛВС) «Ethernet».

СУС выполнена по трехканальной схеме. Центральными устройствами системы являются управляющий трехканальный СИКОН-М3 и регистрирующий одноканальный СИКОН-М1, которые:

– организуют работу аппаратуры системы;

– реализуют циклограммы испытания и алгоритмы управления исполнительными элементами стенда;

– обеспечивают функции контроля, регистрации и имитации фактического исполнения управляющих команд;

– обеспечивают прием ручных команд от оператора СУС и передачу телеметрии о текущем состоянии системы и стенда на АРМ СУС для отображения и регистрации.

Работа каждого контроллера обеспечивается управляющей программой, организующей цикличное выполнение задачи. Период времени, определяющий цикл работы контроллера называется тактом управляющей программы. Каждый такт контроллера состоит из фиксированной последовательности шагов: опроса входов, обработки рабочих программ и выдачи управляющих сигналов на исполнительные элементы. Длительность такта контроллеров СУС составляет 10 мс.

Контроллер СИКОН-М3 имеет три независимых канала. Аппаратной основой каждого канала являются: процессорный модуль МП530 и тыловой модуль ввода/вывода ТВВ, подключенные к общей для всех трех каналов генмонтажной плате.

Одноканальный контроллер СИКОН-М1 выполняет функции контроля, имитации и регистрации фактического исполнения команд управляющего контроллера. Аппаратной основой контроллера регистрации, как и контроллера управления, является процессорный модуль МП530 и тыловой модуль ввода/вывода ТВВ, объединенные генеральной монтажной платой. Процессорные модули управляющего и регистрирующего контроллеров одинаковы по аппаратному исполнению и отличаются в составе СУС лишь программным обеспечением, определяющим функциональные особенности модуля и его уникальный сетевой адрес, формируемом при определении конфигурации системы [1].

Система управления изделием. Система управления изделием предназначена для:

– управления в ручном и автоматическом режимах исполнительными элементами (ИЭ) типа электропневматических клапанов (ЭПК), пиропатронов (ПП), пироклапанов (ПК) и двигателей постоянного тока;

– искробезопасного приема сигналов с датчиков давления, температуры, углового положения и контактных датчиков;

– выдачи в стендовые системы команд синхронизации и обменных команд;

– оперативного ввода и проверки циклограмм и алгоритмов управления, а также – их корректировки при необходимости;

– выполнения заданных циклограмм и алгоритмов в автоматическом режиме с тактом 10 мс;

– регистрации принимаемых с датчиков сигналов и выдаваемых на ИЭ команд с частотой 100 Гц;

– отображения на экранах персональных электронно-вычислительных машин (ПЭВМ) автоматизированных рабочих мест (АРМ) операторов и ведущих инженеров состояния элементов автоматики и значений измеряемых параметров стенда в виде мнемосхем, таблиц, графиков, индикаторов и т.д.;

– регистрации, оперативной обработки информации, и представления результатов в виде таблиц, графиков на экране монитора, в электронном и бумажном виде.

Структурная схема СУИ представлена на рис. 2.

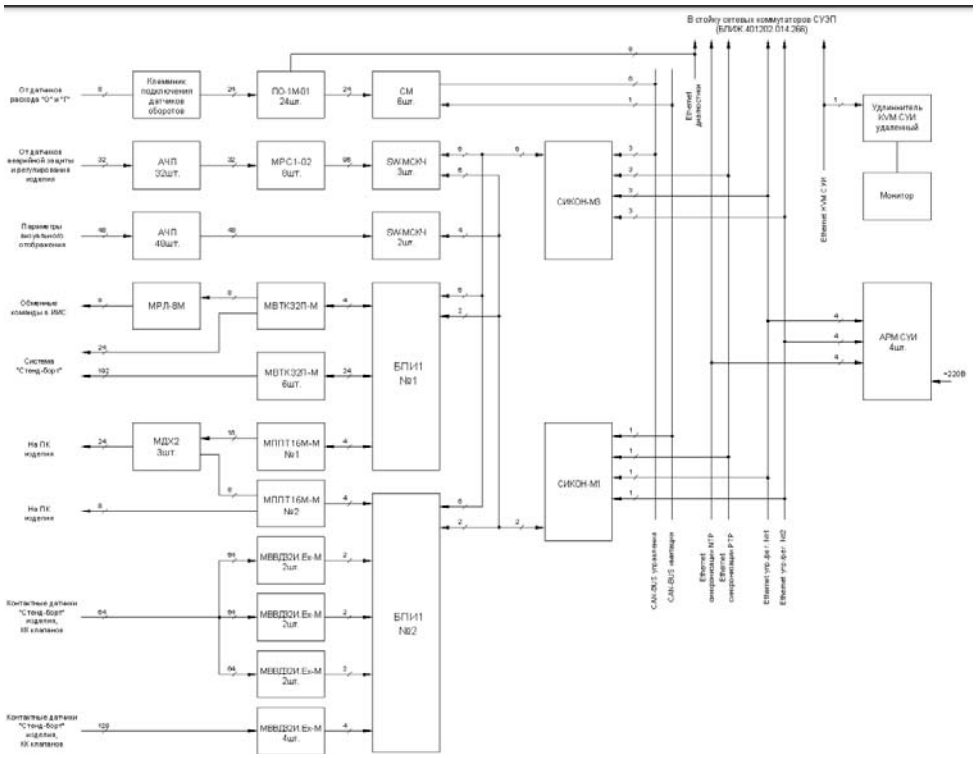


Рис. 2. Структурная схема СУИ

СУИ является двухуровневой распределенной системой. Нижний уровень состоит из контроллеров управления и устройств связи с объектом. Верхний уровень включает в себя АРМ операторов СУИ,АРМ сервер СУИ и устройства организации локальной вычислительной сети.

Аппаратура нижнего уровня СУИ (контроллеры управления и устройства связи с объектом испытания) монтируется в двух приборных стойках (стойке СУИ 1 и стойке СУИ2) расположенных в помещении аппаратуры управления в бункере стенда ИС-101.

АРМ СУИ расположены в пультовой бункера стенда ИС-101. Средства связи с сервером СУИ смонтированы в стойке сетевых коммутаторов, расположенной в пультовой бункера стендаИС-101.

Связь между верхним и нижним уровнями осуществляется посредством линий высокоскоростной связи (ЛВС) «Ethernet».

СУИ выполнена по трехканальной схеме, представленной на рис. 3.

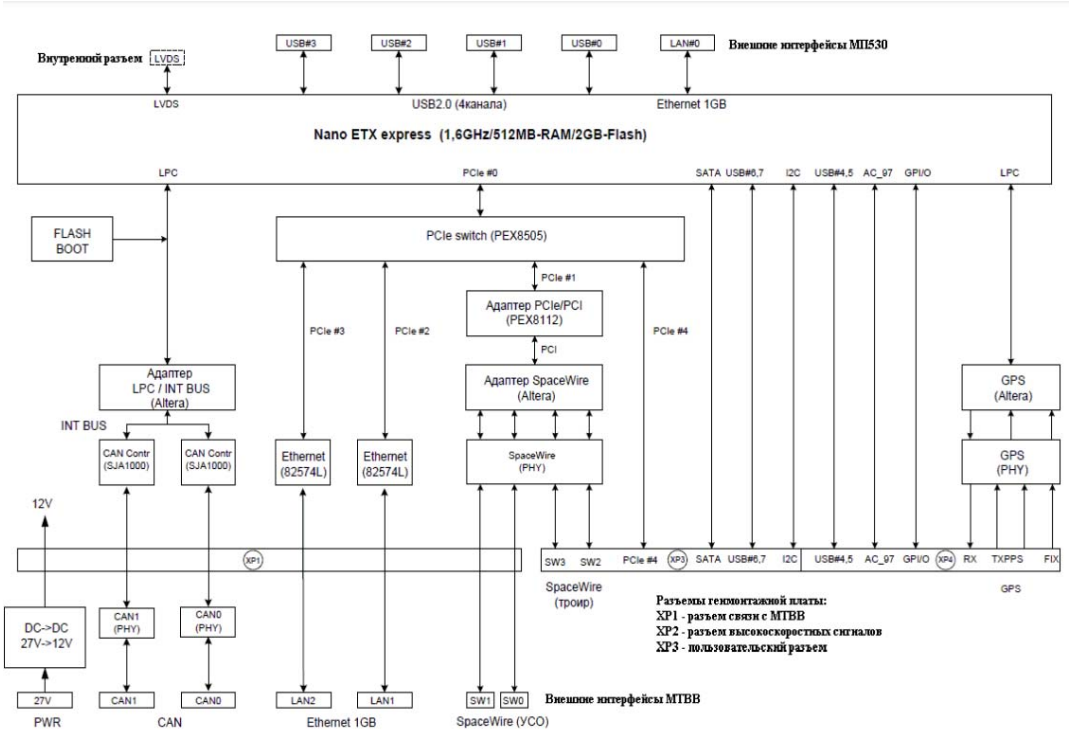


Рис. 3. Трехканальная схема СУИ

Центральными устройствами системы являются управляющий трехканальный СИКОН-М3 и регистрирующий одноканальный СИКОН-М1, которые:

– организуют работу аппаратуры системы;

– реализуют циклограммы испытания и алгоритмы управления исполнительными элементами стенда;

– обеспечивают функции контроля, регистрации и имитации фактического исполнения управляющих команд;

– обеспечивают прием ручных команд от оператора СУИ и передачу телеметрии о текущем состоянии системы и стенда на АРМ СУИ для отображения и регистрации.

СКДО предназначена для подготовки и проведения холодных и огневых стендовых испытаний агрегатов и двигательных установок I и II ступеней и огневых стендовых испытаний двигательной установки II ступени, включающих четыре и более жидкостных ракетных двигателей, на высококипящих компонентах ракетного топлива (несимметричный диметилгидразин в качестве горючего + азотный тетраоксид в качестве окислителя) в составе ракетных блоков в части системы управления [2].

Система контроля, диагностики и отображения параметров. Система контроля, диагностики и отображения параметров предназначена для:

– объединения информационных потоков стендовых систем;

– ведения, а также измерения показателей, обрабатывания и внешнего визуального отображения полученной информации о работоспособности стенда и изделия в удобной для восприятия форме;

– регистрации объединенного потока данных с частотой не выше 2 Гц;

– осреднения параметров СИ и СУ для обеспечения отображения их с заданной частотой обновления;

СКДО включает в себя одну ориентированную автономную систему, смонтированную в стойке. Центральными устройством системы является сервер-мост, который объединяет информационные потоки ИУС и СИ, усредняет и выдает в сеть СКДО поток информации на АРМ СКДО для отображения на визуальных формах. Схема СКДО представлена на рис. 4.

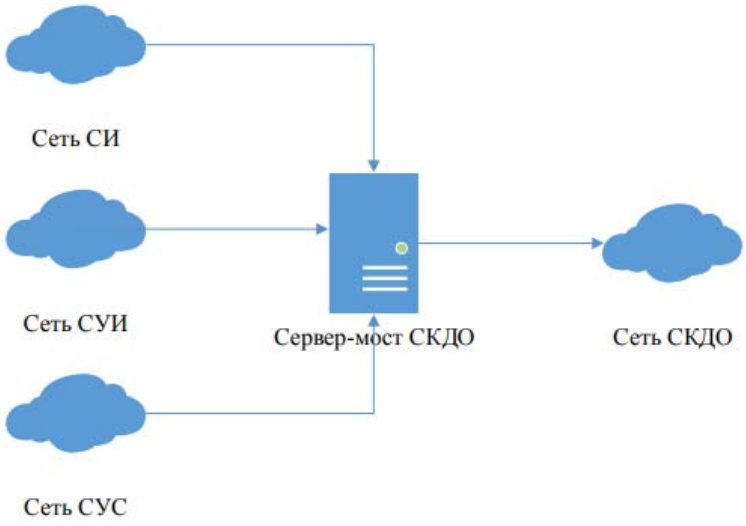


Рис. 4. Схема объединения информационных потоков

Сервер-мост СКДО представлен в виде сервера формата 1U, устанавливаемого в стойку сетевого оборудования – стойку приборную СО.

Визуальное отображение мнемосхем, таблиц и графиков на экранных формах с текущими значениями параметров стенда и изделия выполняется на базе ПЭВМ АРМ СКДО, подключенного к сети СКДО. К АРМ СКДО, в зависимости от расположения в бункере 1А, подключаются либо экраны СКДО, либо мониторы LCD.

Концентратором информационного потока сети СКДО является коммутатор СКДО. Коммутатор принимает поток от сервера-моста и раздает его 12-ти подключенным АРМ [3].

Система управления электропитанием предназначена для дистанционной коммутации цепей подачи электропитания.

Система управления электропитанием. Система управления электропитанием обеспечивает непрерывный автоматизированный контроль параметров электропитания аппаратуры системы управления стендом, системы управления изделием и исполнительных элементов стендового оборудования стенда ИС-101 ФКП «НИЦ РКП».

Питание системы СУЭП осуществляется от двух стендовых независимых источников переменного напряжения: ~220В №1 (далее ввод №1) и ~220В №2 (далее ввод №2).

Ввод №1 питает шкаф источника питания TIS 600-124 UDS (далее TIS) №1, №3 и №5 через встроенные в них фильтры TDK-Lambda RSEN-2010 №1, №3 и №5 соответственно. Ввод №2 питает TIS №2 и №4 через фильтры RSEN-2010 №2 и №4 соответственно.

Выводы 24В TIS №1, №2 и TIS №3, №4 попарно объединенные через диодную развязку для обеспечения резервирования, заведены на клеммники «Uавт СУС вх» и «Uавт СУИ вх» соответственно. Вывод 24В TIS №5 заведен напрямую на клеммник «Uавт СУЭП вх» и не резервирован.

Напряжения 24В Uавт с клеммников «Uавт СУС вх» и «Uавт СУИ вх», модулями коммутации питания МКП3-01 №1 и №2, коммутируются на клеммники «Uавт СУС вых» и «Uавт СУИ вых» соответственно, откуда доступны для использования СУС и СУИ.

Структурная схема СУЭП представлена на рис. 5.

Запуск СУЭП осуществляется при включении стойки СУЭП путем перевода, самовозвратного тумблера включения в положение «ВКЛ». При этом напряжение Uавт с клеммника «Uавт СУЭП вх» коммутируется МКП-01 №3 на клеммник «Uавт СУЭП вых», а с него питает все потребители СУЭП. (Выключение стойки СУЭП производится переводом самовозвратного тумблера в положение «ВЫКЛ»).

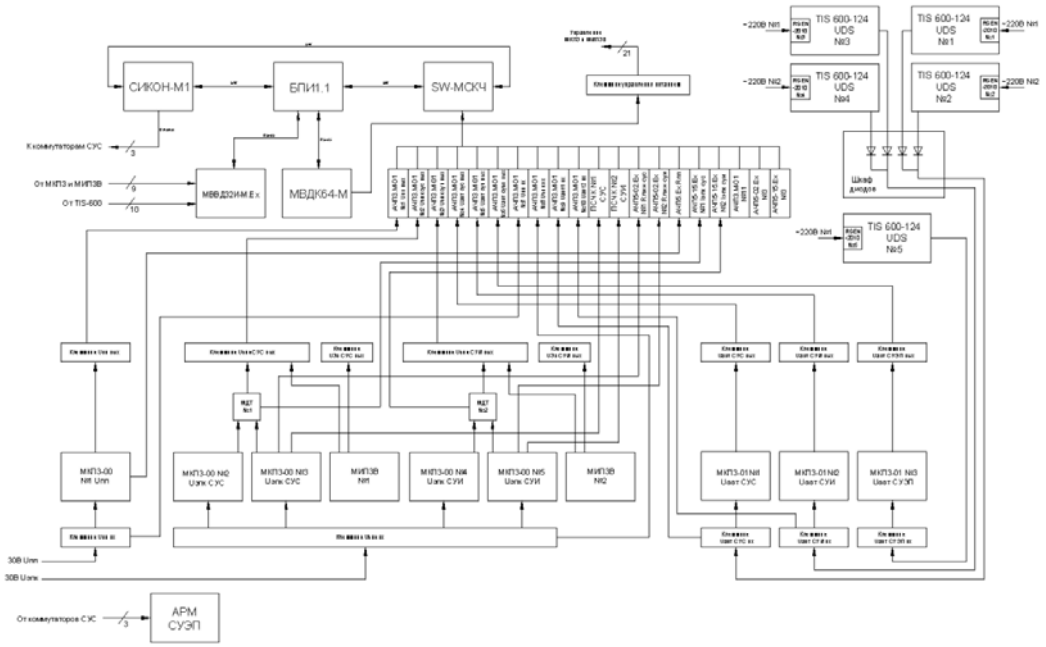


Рис. 5. Структурная схема СУЭП

Безопасные 3-вольтовые напряжения U3в, используемые системами СУС и СУИ для проверок, преобразуются из 24В Uавт СУЭП и коммутируются модулями источника питания 3В МИП3В №1 и №2 на клеммники «Uэпк СУС вых», «U3в СУС вых» и «Uэпк СУИ вых», «U3в СУИ вых» соответственно.

Строгую последовательность коммутации питаний на выходные клеммники обеспечивают аппаратные блокировки, реализованные управляющими цепями МКП3-00, МКП3-01 и МИП3В СУЭП.

Текущее состоянии электропитания СУЭП, подаваемое для информационноизмерительных систем и систем управления, определяется состоянием шкафов источника питания TIS 600-124 UDS, модулей МКП3-00, МКП3-01 и МИП3В посредствам приема от них дискретных сигналов типа «сухой контакт», модулем искрозащитным дискретного ввода МВВД32И-М.Ех.

МВВД32И-М.Ех периодически опрашивается блоком преобразования интерфейсов БПИ1.1 по интерфейсу RS-485, на предмет изменения состояния дискретных сигналов. Текущие значения напряжений Uавт, Uэпк, Uпп и U3в на входных и выходных клеммниках СУЭП определяются аналого-частотными преобразователями АЧП3.М-01.

Текущие значения потребляемых исполнительными элементами СУС и СУИ токов преобразованные на шунтах модулей МДТ определяются АЧП5-15.Ех. Значения сопротивления линий ИЭ и целост-

ности ПС СУС и СУИ при проверках определяются АЧП5-02.Ех и АЧП5.Ех соответственно. Значения сопротивлений изоляции ИЭ СУС и СУИ при проверках определяются преобразователем сопротивления в частоту-код ПСЧК. Перечисленные АЧП и ПСЧК преобразуют измеренные физические величины в частотные сигналы и отправляют их модулю связи с контроллером частотному SW-МСКЧ, который в свою очередь, определив частоту полученных сигналов, преобразует ее в цифровой код.

Информация о состоянии дискретных сигналов полученная модулем БПИ1.1, а также оцифрованная информация о значениях физических параметров полученная SW-МСКЧ, по высокоскоростной сети «SpaceWare» (SW) передается контроллеру СИКОН-М1, который использует ее в работе внутренних алгоритмов управления СУЭП и трансляции по дублированной сети Ethernet для регистрации и отображения на мониторе автоматизированного рабочего места АРМ оператора СУЭП в бункер управления.

Отображение текущего состояния СУЭП и выдачу команд управления, осуществляется средствами программы «Пульт СУЭП, запускаемой на АРМ оператора СУЭП в бункере управления. Команды оператора с АРМ СУЭП поступают по сети Ethernet контроллеру СИКОН-М1. Контроллер, получив команду оператора и выполнив проверку ее корректности и совместимости с текущим состоянием системы, передает ее по SW через БПИ1.1 модулю вывода дискретных команд МВДК64-М, который, в свою очередь, через клеммник управления питанием воздействует на цепи управления модулей МКП3 и МИП3В[4].

СУИ выполнена по трехканальной схеме. Центральными устройствами системы являются управляющий трехканальный СИКОН-М3.

Работа каждого контроллера обеспечивается управляющей программой, организующей цикличное выполнение задачи. Период времени, определяющий цикл работы контроллера называется тактом управляющей программы. Каждый такт контроллера состоит из фиксированной последовательности шагов: опроса входов, обработки рабочих программ и выдачи управляющих сигналов на исполнительные элементы. Длительность такта контроллеров СУИ составляет 10 мс. Контроллер СИКОН-М3 имеет три независимых канала. Аппаратной основой каждого канала являются: процессорный модуль МП530 и

тыловой модуль ввода/вывода ТВВ, подключенные к общей для всех трех каналов генмонтажной плате.

Каждый контроллер имеет еще два интерфейса SW, выведенные на разъемы генмонтажной платы, что позволяет соединять три контроллера крейта СИКОН-М3 «в кольцо» для обмена и выравнивания информации между каналами. В результате управляющая программа в каждом из контроллеров выполняет операцию сравнения состояния регистров соседних каналов со своим и, в зависимости от результата, устанавливает признаки «ошибка слева», «ошибка справа» в соответствующих битах телеграммы запроса к блоку преобразования информации БПИ1, отправляемой по внешнему интерфейсу SW каждый такт.

Одним из устройств, включенных в «кольца» SW является блок преобразования информации БПИ1, являющийся «мостом» между интерфейсом SW и шиной RS-485. БПИ1 обеспечивает дискретный ввод/вывод контроллеров, выполняя трансляцию «канал в канал» управляющих команд модулям дискретного вывода МВТК32П-М, а также прием информации от модулей ввода дискретных сигналов МВВД32И-М.Ex. Кроме того, БПИ1 содержит модули переключения каналов, реализующие мажоритарную функцию «два из трех» при наличии признака «ошибка» одного из каналов в поступающих от контроллеров телеграммах, и выдачу выровненной командной информации в три канала модулей вывода дискретных сигналов.

Аппаратной основой каждого из четырех каналов БПИ1 являются объединенные общей генмонтажной платой модуль связи SW-IO интерфейса SW и модуль МПК485, предназначенный для обмена информацией по шине RS-485 с модулями ввода/вывода дискретных сигналов. Как и в контроллере управления, генмонтажная плата является общей для всех каналов, что позволяет реализовывать мажоритарную функцию. Входной информацией для алгоритмов управления являются параметры стенда, характеризующие его текущее состояние и измеряемые датчиками, имеющими на выходе аналоговые сигналы (потенциометрические датчики, термопары и термосопротивления, датчики напряжения), частотные (датчики расходов) и дискретные сигналы (контактные датчики давления, положения). Прием дискретных сигналов с контактных датчиков для троированного реализован с помощью 10 модулей искрозащищенных дискретного ввода МВВД32И-М.Ex объединенных интерфейсами RS485.

Сигналы потенциометрических датчиков давления принимаются преобразователями АЧП2-06.Ex. Сигналы токовых датчиков (от 4 до 20 мА) принимаются преобразователями АЧП4-01.Ex. Сигналы датчиков сопротивления (от 0 до 100 Ом) принимаются преобразователями АЧП5-02.Ex. Напряжение постоянного тока (от 0 до 5 В) преобразуется в частоту посредством АЧП2-11.Ex. Выходные частотные сигналы с АЧП предназначенные для троированного контроллера размножаются с помощью 8 четырехканальных модулей распределения сигналов МРС1-02 на три направления и передаются в каждый канал контроллера управления через соответствующие модули связи с контроллером частотные SW-МСКЧ. SW-МСКЧ использует для связи с контроллерами кольцевую сеть SW.

Кольцевая сеть SW каждого канала трехканального контроллера включает только один соответствующий SW-МСКЧ. Каждый SW-МСКЧ рассчитан на прием 32-х частотных сигналов, и может обеспечить работу в режиме имитации входных частотных сигналов, значения которых задаются регистрирующим контроллером. Это дает возможность имитировать значения параметров стенда при отладке алгоритмов управления. В СУИ предусмотрено 24 ПО1-М-01 для обеспечения троированного ввода частотного сигнала от 8 датчиков оборотов.

Для связи ПО1-М-01 с контроллерами предназначен связной модуль СМ. СМ может передать в контроллер информацию от 8 ПО-1-М. СМ соединен с управляющим и регистрирующим контроллерами по соответствующему интерфейсу CAN. Интерфейс CAN предназначенный для регистрирующего контроллера, может использоваться им для имитации сигналов с датчиков оборотов при отладке алгоритмов управления. По завершении обработки входной информации с датчиков стенда в соответствии с заданными алгоритмами управления, реализованными специальным ПМО СУИ, в контроллере управления СИКОН-М3 вырабатываются управляющие сигналы на исполнительные элементы стенда.

Формирование силовых управляющих сигналов на ЭПК, двигатели приводов и реле осуществляется семью модулями вывода дискретными троированными силовыми МВТК32П-М, имеющими по 32 выходных канала управления. Троированные модули выполнены на бесконтактных ключах (коммутируемый ток до 4А), реализующих функцию аппаратного мажоритирования «два из трех» на основе ко-

манда, принимаемых от трех каналов контроллера управления через БПИ1.

Управление ПС реализовано на базе двух модулей полумостовых преобразователей троированных 16-ти канальных МППТ16М-М с бесконтактными силовыми ключами. Каждый МППТ16М-М обеспечивает двуполярную коммутацию (коммутацию обоих полюсов питания) команд управления по 32-м выходным каналам дублирующих нитей пиросредства (ПС) к выходным соединителям модуля МППТ16М-М. Модуль содержит диагностические цепи, обеспечивающие контроль наличия напряжения на ПС после срабатывания силовых ключей, что позволяет выполнять проверки циклограммы испытания без стыковки с ПС изделия.

Заключение. Таким образом, за счет введения троированной архитектуры систем СУИ и СУС повышается надежность и точность управления приводами за счет автоматического переключения на исправный канал при управлении нерезервированной нагрузкой (резервированной дублированием) и уменьшается влияние дестабилизирующих факторов на точность управления. Но автоматическе переключение на исправный канал происходит не всегда, поэтому информация проходит по трем каналам одновременно и по результатам двух совпавших результатов информация считается истинной.

Список использованных источников

1. Система управления стендом. Руководство по эксплуатации БЛИЖ.401202.012.266 РЭ. 2018 г.

2. Система управления изделием. Руководство по эксплуатации БЛИЖ.401202.011.266 РЭ. 2018 г.

3. Система контроля, диагностики и отображения параметров. Формуляр БЛИЖ.401202.013.266 ФО. 2018 г.

4. Система управления электропитанием. Руководство по эксплуатации БЛИЖ.401202.014.266 РЭ. 2018 г.

ИСПОЛЬЗОВАНИЕ ХРАНИЛИЩА СТОЛБЦОВ В ORACLE ДЛЯ АНАЛИЗА ДАННЫХ В OLAP СИСТЕМАХ

Емельянов Е.Г., аспирант,
Логачева Н.В., к.т.н., доцент,
Технологический университет («МГОТУ»),
Россия, г. Королев

Рассматривается проблема использования хранилища столбцов в Oracle для анализа данных в OLAP системах. Поставлен вопрос о эффективности данного решения в OLAP системах современных хранилищ данных

Ключевые слова: OLAP, ETL, Oracle IM

Рост объемов обрабатываемой в интеллектуальных системах управления информации и соответствующее повышение требований к производительности и надежности инфраструктуры вынуждает архитекторов искать оптимальные способы использования хранилищ данных, в частности, для фиксации, оперативного поиска и обработки данных, для регламентированной аналитической обработки. В данной работе рассматривается один из возможных путей решения поставленных задач применительно к ПО Oracle, т.к. в настоящее время значительная доля OLAP-систем используют именно этот инструмент обработки данных.

Хранилище столбцов Oracle в памяти (IM column Store) в базе данных Oracle обеспечивает повышенную производительность как для специальных запросов, так и для анализа данных в реальном времени. База данных транзакций в реальном времени используется для предоставления мгновенных ответов на запросы, что позволяет легко использовать одну и ту же базу данных для транзакций OLTP и аналитики хранилища данных.

Традиционная аналитика имеет определенные ограничения или требования, которыми необходимо управлять, чтобы получить хорошую производительность для аналитических запросов. Необходимо знать шаблоны доступа пользователей, а затем настроить свои структуры данных, чтобы обеспечить оптимальную производительность для этих шаблонов доступа. Необходимо настроить существующие индексы, материализованные представления и кубы OLAP. Некоторые витрины данных и базы данных отчетов имеют сложный ETL и, следовательно, нуждаются в специальной настройке. Так же необхо-

димо найти баланс между выполнением аналитики устаревших данных и замедлением операций OLTP в производственных базах данных.

Хранилище столбцов IM — это дополнительная область в SGA, в которой хранятся копии таблиц, разделов таблиц и отдельных столбцов в сжатом столбчатом формате, оптимизированном для быстрого сканирования. Столбчатый формат легко поддается векторной обработке, что позволяет выполнять агрегирование, объединение и некоторые типы поиска данных быстрее, чем традиционные форматы на диске. Столбчатый формат существует только в памяти и не заменяет формат кэша на диске или в буфере. Вместо этого он дополняет буферный кэш и предоставляет дополнительную, согласованную с транзакциями копию таблицы, которая не зависит от формата диска.

Хранилище столбцов IM позволяет базе данных Oracle выполнять сканирование, объединение и агрегирование намного быстрее, чем при использовании исключительно дискового формата. Больше всего выигрывают бизнес-приложения, специальные аналитические запросы и рабочие нагрузки хранилища данных. Чистые базы данных OLTP, которые выполняют короткие транзакции с использованием поиска по индексу, выигрывают меньше.

Хранилище столбцов IM легко интегрируется с базой данных Oracle. Все существующие функции базы данных, включая функции высокой доступности, поддерживаются без необходимости внесения изменений в приложения. Таким образом, настроив хранилище столбцов обмена мгновенными сообщениями, вы можете мгновенно повысить производительность существующих аналитических рабочих нагрузок и специальных запросов.

Oracle Optimizer знает о хранилище столбцов IM, что позволяет базе данных Oracle беспрепятственно отправлять аналитические запросы в хранилище столбцов IM, в то время как запросы OLTP и DML отправляются в хранилище строк.

Преимущества, предлагаемые хранилищем столбцов IM для сред хранилищ данных:

1. Более быстрое сканирование большого количества строк и применение фильтров, использующих такие операторы, как =,<,> и IN.

2. Более быстрый запрос подмножества столбцов в таблице, например выбор 5 из 100 столбцов.

3. Улучшена производительность соединений за счет преобразования предикатов в таблицах небольших измерений в фильтры в большой таблице фактов.

4. Эффективное агрегирование с использованием преобразования VECTOR GROUP BY и обработки массива векторов.

5. Сокращение места для хранения и значительно меньшие накладные расходы на обработку, поскольку при использовании хранилища столбцов IM требуется меньше индексов, материализованных представлений и кубов OLAP.

Таким образом, предлагаемая методика для повышения эффективности использования хранилищ данных позволяет решить поставленные задачи.

Список используемых источников

1. Гребенюк Н. А., Гребенюк Е. И. Технические средства информатизации: Ек.: ИД «Академия» 2021 г. 272 стр.

2. Максимов Н.В., Попов И.И., Голицына О.Л. Информационные системы: учебное пособие. М.: ИНФРА-М, 2020 г. 496 стр.

3. Аверченков В. И. Информационные системы: учебное пособие 4-е изд., стер. - М.: Флинта , 2020. 128

РАСПРЕДЕЛЕНИЯ ВЕРОЯТНОСТЕЙ БЕЛОГО ГАУССОВСКОГО ШУМА И АДДИТИВНОЙ СМЕСИ ДВУМЕРНЫХ НЕГАУССОВСКИХ ПОМЕХ

Воловач В.И., д.т.н.
Поволжский государственный университет сервиса («ПВГУС»),
Россия, г. Тольятти

Рассмотрены вопросы, связанные с нахождением двумерной плотности распределения вероятностей (ПРВ) аддитивной смеси активных полосовых негауссовских помех с белым гауссовским шумом. Получены зависимости ПРВ аддитивной смеси активной полосовой негауссовской помехи и белого гауссовского шума от величины дисперсии шума и отношения мощности активной помехи к мощности шума.

Ключевые слова: плотности распределения вероятностей, активная полосовая аддитивная помеха, бимодальный характер распределения.

Актуальность решаемой задачи. В статистической радиотехнике, радиолокации, радионавигации, в теории связи и автоматического управления широкое распространение получила прикладная теория случайных процессов. Как правило, рассматриваются модели, в которых принимаемые сигналы описываются в виде аддитивной смеси полезного сигнала и гауссовского шума [1, 2]. Довольно часто, на практике, в реальных условиях полезные сигналы подвержены воздействию аддитивной смеси активных полосовых помех, имеющих негауссовский характер распределения, с белым гауссовским шумом [3, 4]. Для синтеза и анализа информационно-измерительных систем обрабатывающих такие сигналы, необходимы математические модели, позволяющие близко к реальности моделировать плотности распределения вероятностей (ПРВ) таких смесей [5].

Рассмотрим ПРВ двумерных активных полосовых помех имеющих ярко выраженный негауссовский характер распределения.

ПРВ мгновенных значений двумерных активных полосовых негауссовских аддитивных помех. Пусть на полезный сигнал воздействует активная узкополосная помеха $n_A(t)$. В этом случае, в точке приема на полезный сигнал, будет оказывать влияние так называемая суммарная помеха, которая может быть представлена в виде аддитивной смеси активной негауссовской помехи и белого гауссовского шума

$$n(t) = A_0\cos[\omega_0 + \Phi(t) + \theta] + \xi(t) = n_A(t) + \xi(t), \quad (1)$$

где A_0 – амплитуда активной аддитивной помехи; $\Phi(t) = K_{\text{ФМ}}\eta(t)$ – при фазовой модуляции или $\Phi(t) = K_{\text{ЧМ}}\int_0^t \eta(t_1)d\,t_1$ – при частотной модуляции, здесь $K_{\text{ФМ}}$, $K_{\text{ЧМ}}$ – крутизна соответствующей модуляционной характеристики; $\eta(t)$ – модулирующий шум, который будем считать гауссовским; θ – начальная фаза, имеющая равномерное распределение на интервале (0, 2π); $\xi(t)$ – внутриприемный белый гауссовский шум.

В этом случае двумерную ПРВ активной аддитивной помехи $W_2(n_1, n_2)$ для сечений n_1, n_2 отстоящих на интервал $t_2 - t_1$, определяют по формуле

$$W_2(n_1^*, n_2^*) = \sum_{K=0}^{\infty} \varepsilon_K r_U^{K^2} L_K(n_1^*)L_K(n_2^*)\cos[K\omega_0(t_1 - t_2)],$$

где $n_i^* = n_i/A_0$, i = 1, 2; $\varepsilon_0 = 1$; $\varepsilon_K = 2\forall K \geq 1$; $r_u(t_1 - t_2)$ – огибающая коэффициента корреляции модулированной составляющей; $\forall$ – математическое обозначения условия, которое верно для всех обозначенных элементов (читается как «для всех…», «для каждого…», «для любого…»); $L_K(n) = \frac{1}{2\pi}\sqrt{\frac{\alpha}{\pi}}\int_{-\pi}^{\pi}\exp\{-\alpha(n - \cos\varphi)^2\}\cos(\text{К}\varphi)d\varphi$.

Здесь $\alpha = A_0^2/2\sigma_\xi^2$ – отношение мощности модулированной составляющей к мощности внутреннего шума $\xi(t)$.

Заметим, что поскольку

$$\int_{-\infty}^{\infty} L_K(x)\,dx = \frac{1}{2\pi}\int_{-\pi}^{\pi}\cos(\text{К}\varphi)\,d\varphi = \begin{cases}1 & \text{при} \quad K = 0\\ 0 & \text{при} \quad K = 1,2\text{’}\end{cases}$$

то есть, при К = 0 выполняется условие нормировки, $L_K(x)$ является одномерной ПРВ аддитивной смеси (1). Следовательно

$$L_0(n) = \frac{1}{2\pi}\sqrt{\frac{\alpha}{\pi}}\int_{-\pi}^{\pi}\exp\{-\alpha(n - \cos\varphi)^2\}d\varphi = W_1(n).$$

Начальные моменты, в этом случае, могут быть определены исходя из выражения $m_{2K} = \frac{(2K-1)!}{2^K}\frac{L_K(-\alpha)}{\alpha^K}$, где $L_K(z) = \text{e}^z\frac{1}{K!}\frac{d^K}{dz^K}(\text{e}^{-z}z^K)$ - полином Лагерра.

Для функции $L_K(n)$ имеет место рекуррентная формула

$$L_{K+1}(x) = \frac{1}{\alpha}\frac{dL_K(x)}{dx} + 2xL_K(x) - L_{K-1}(x), \forall K \geq 1;$$

$$L_1(x) = \frac{1}{2\alpha}\frac{dL_0(x)}{dx} + xL_0(x).$$

Учитывая, что

$$\lim L_K(x) = \begin{cases} \frac{T_x(x)}{\pi\sqrt{1-x^2}} & |x| < 1 \\ 0 & |x| \geq 1 \end{cases},$$

где $T_x(x)$ – полином Чебышева первого рода, двумерную ПРВ можно представить в виде

$$W_2(n_{A1}, n_{A2}) = \frac{1}{(\pi A_0)^2} \sum_{K=0}^{\infty} \varepsilon_K r_U^{K^2} \frac{T_K\left(\frac{n_{A1}}{A_0}\right) T_K\left(\frac{n_{A2}}{A_0}\right)}{\left\{\left(1-\frac{n_{A1}^2}{A_0^2}\right)\left(1-\frac{n_{A2}^2}{A_0^2}\right)\right\}^{0,5}} \cos\{K\omega_0\}(t_2 - t_2). \quad (2)$$

В отсутствие модуляции ($r_U = 1$) полученная формула (2) совпадает с известным выражением для двумерной ПРВ гармонического колебания с равномерно распределенной начальной случайной фазой [2].

Аналитическое выражение для ПРВ аддитивной смеси (1), в случае одновременной амплитудной и частотной модуляции шумом очень громоздко, и поэтому здесь не приводится.

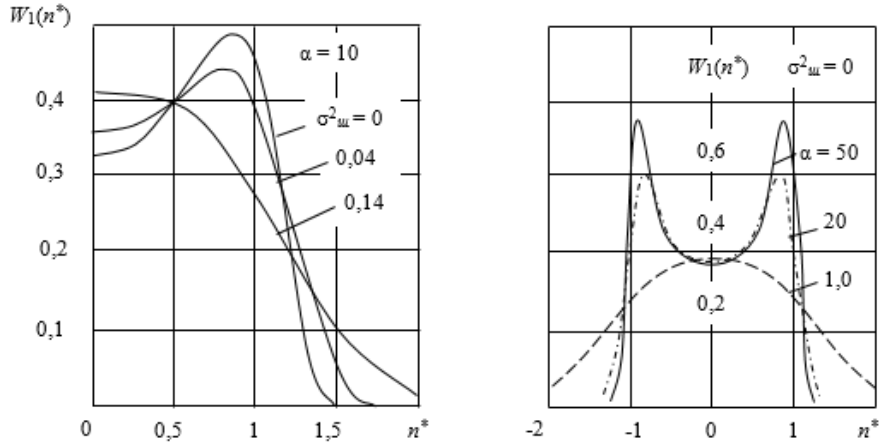
Одномерная ПРВ смеси, нормированная к A_0, при независимости шумов, модулирующих амплитуду и частоту, может быть найдена исходя из выражения

$$W_1(n^*) = \frac{1}{\pi}\sqrt{\frac{\alpha}{\pi}} \int_{-\pi}^{\pi} \frac{\exp\left\{-\alpha \frac{(x-\sin\vartheta)^2}{1+2\sigma_{\text{ш}}^2 \alpha \sin^2\vartheta}\right\}}{\left(1+2\sigma_{\text{ш}}^2 \alpha \sin^2\vartheta\right)^{0,5}} d\vartheta,$$

где $\sigma_{\text{ш}}^2$ – дисперсия шума, модулирующего амплитуду.

На рис. 1 приведены кривые, иллюстрирующие зависимость ПРВ $W_1(n^*)$ от дисперсии шума и параметра α (отношение мощности модулированной составляющей к мощности внутреннего шума $\xi(t)$) играющего, в данном случае, роль аналогичную роли отношения сигнал/шум.

Заметим, что характерной особенностью ПРВ активных помех с частотной модуляцией является их бимодальный характер. Введение амплитудной модуляции или добавление аддитивного гауссовского шума сглаживает эту бимодальность. При $\sigma_{\text{ш}}^2 = 0$ плотность распределения вероятностей $W_1(n^*)$ вырождается в $W_1(n)$, соответствующую плотности распределения вероятностей аддитивной смеси гауссовского шума и синусоидального колебания с частотной модуляцией.



а) *б*)

Рис. 1. Зависимости плотности распределения вероятностей аддитивной смеси активной полосовой негауссовской помехи и белого гауссовского шума от величины: *а* – $\sigma_{\text{ш}}^2$, при $\alpha = \text{const}$; б – α, при $\sigma_{\text{ш}}^2 = \text{const}$

Выводы. Таким образом, рассмотрены вопросы, связанные с нахождением плотности распределения вероятностей двумерных активных полосовых негауссовских помех, воздействующих на полезный сигнал, при наличии белого гауссовского шума. Получены зависимости плотности распределения вероятностей аддитивной смеси активной полосовой негауссовской помехи и гауссовского шума от отношения мощности модулированной составляющей помехи к мощности белого шума и величины его дисперсии.

Список использованных источников

1. Тихонов В.И. Нелинейное преобразование случайных процессов. – М.: Радио и связь, 1986. – 296 с.

2. Артюшенко В. М. Обработка информационных параметров сигнала в условиях аддитивно-мультипликативных негауссовских помех. М.: ФГБОУ ВПО ФТА, Изд-во «Канцлер», 2014. 298 с.

3. Воловач В. И. Методы и алгоритмы анализа радиотехнических устройств ближнего действия. – М.: Радио и связь, 2013. – 228 с.

4. Артюшенко В.М., Воловач В.И. Использование эллиптически симметричной модели плотности распределения вероятности для описания негауссовских помех // Радиотехника. 2016. №6, – С.113-117.

5. Артюшенко В.М., Воловач В.И. Измерение информационных параметров сигнала в условиях воздействия аддитивных негауссовских коррелированных помех // Автометрия – 2016. Т52. – №6. – С.22-28.

РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ ПЕРЕДВИЖЕНИЯ КРОСС-ПЛАТФОРМЕННОЙ САМОХОДНОЙ УСТАНОВКИ «MUS»

Коротчиков Б.О., магистр группа ИМО-МП-20,
Орлов А.Д., магистр группа ИМО-МП-20,
Технологический университет («МГОТУ»),
Россия г. Королев

В данной статье рассмотрен вопрос разработки программного обеспечения для передвижения кросс-платформенной самоходной установки «MUS». Предложена методика и алгоритмы проектирования программного обеспечения для кросс-платформенной самоходной установки не требующая больших затрат по времени и дополнительного специализированного программного обеспечения. Обоснована причина создания данного программного обеспечения. Разработаны и представлены алгоритмы алгоритмы автоматического и ручного управления. В качестве примера показаны фрагменты кода автоматического передвижения. При помощи данной программы возможно построить сложные задачи, включающие в себя циклы и множественные повторы, а также динамические переходы к различным частям кода управляющей программы.

Ключевые слова: программирование роботов, робототехника, программа, самоходная установка, методы, алгоритм, робот

Современные роботы ежедневно получают те или иные усовершенствования, происходит развитие всех их составляющих. Чаще всего подвергаются усовершенствованию такие составляющие как: механика, кинематика, программное обеспечение управления и обработки изображения, системы управления.

Очевидно, в последнее время уделяется все больше и больше внимания развитию систем и программ управления, механика и кинематика за последние 15 лет не потерпела особых изменений, чего нельзя сказать о программном обеспечении (ПО) и системах управления.

Сделанный упор на разработку микропроцессорных плат привел к удешевлению, доступности, универсальности разрабатываемых систем управления роботами, что в свою очередь повлияло на появление новых программ управления. Появилась потребность в разработке программного обеспечения к системам управления нового поколения и модернизации уже существующего ПО. Зачастую современные системы управления базируются на микропроцессорной ос-

нове. Данные системы имеют достаточную гибкость для обеспечения большинства потребностей, а также поддерживают различные языки программирования и стандарты ввода-вывода. Поэтому разработка программ управления для данных систем актуальна и на данный момент, разработчик имеет выбор среди множества программных продуктов и систем разработки.

1. Постановка задачи. Авторами предлагается методика разработки программы обработки потокового видеоизображение и управления кросс-платформенной самоходной установки «MUS». Разработанная программа включает в себя локальное и удаленное управление, передачу видеопотока в реальном времени, автоматическое передвижение из пункта А в пункт Б [2].

2. Методика разработки программы управления. 1. Функции, которые должна выполнять разрабатываемая система (локальное и удаленное управление, автоматическое управление, передача потокового видео и т. д.)

2. Разработка структуры программы, разбивка данной структуры на отдельные блоки согласно требуемым функциям.

3. Выбор языка программирования, модулей, драйверов и необходимых библиотек

4. Написание программного кода в среде разработки

Программа MUS v1.0 состоит из нескольких модулей. При создании данной программы использовалось не большое количество специальных библиотек, что позволяет получить большую стабильность и универсальность работы текущего программного обеспечения при применении обновлений.

Программный код для распознавания объектов на видео реализован на языке программирования Python. Использована библиотека OpenCV [1].

Система управления реализована при помощи языка Arduino C, который представляет собой язык C++ с фреймворком Wiring [3].

3. Формы и функции программного обеспечения. Программа служит для управления кросс-платформенной самоходной установкой «MUS» и поддерживает два режима: 1) ручное управление 2) автоматическое передвижение по заданным координатам из точки А в точку Б. Изначально рассматривается самостоятельное передвижение самоходной установки по заданным координатам, однако если что-то идет не так, оператор всегда имеет возможность вмешаться в систему управления и взять полное управление всеми функциями на себя[3].

Наблюдение за движением установки происходит при помощи камеры, что позволяет находить интересующие нас предметы а также достаточно точно позиционировать текущее местоположение робота и его возможное отклонение от заданного маршрута [1].

```
import cv2
import numpy as np
from imutils.video import VideoStream
import imutils
from time import sleep

# название окна подстройки
WINDOWNAME = "Настройка тона"

# минимальный размер контуров пятна
BLOBSIZE = 1500

# константы насыщенности и яркости
S_MIN = 29
S_MAX = 255
V_MIN = 148
V_MAX = 255

# цвет прямоугольника (B, G, R)
RECTCOLOR = (0, 255, 0)

# толщина линии прямоугольника
RTHICK = 2

# определяем функцию проверки размера пятна
def checkSize(w, h):
    if w * h > BLOBSIZE:
        return True
    else:
        return False

# определяем пустую функцию
def empty(a):
    pass

# определяем размеры кадра
frameSize = (320, 240)

# создаём объект видео потока
```

```
    vs = VideoStream(src=0, usePiCamera=True, resolution=frameSize, framerate=32).start()

    # ждём окончания инициализации видеопотока
    sleep(2)

    # создаём окно с ползунком
    cv2.namedWindow(WINDOWNAME)
    cv2.resizeWindow(WINDOWNAME, 500, 100)
    cv2.createTrackbar("Hue", WINDOWNAME, 0, 180, empty)

    while True:

        # получаем кадр изображения
        image = vs.read()

        # получаем максимальный и минимальный тон из значения ползунка
        h_min = cv2.getTrackbarPos("Hue", WINDOWNAME) - 10
        h_max = cv2.getTrackbarPos("Hue", WINDOWNAME) + 10

        # определяем границы цвета в HSV
        lower_range = np.array([h_min, S_MIN, V_MIN])
        upper_range = np.array([h_max, S_MAX, V_MAX])

        # конвертируем изображение в HSV
        hsv = cv2.cvtColor(image, cv2.COLOR_BGR2HSV)

        # создаём маску выбранного цвета
        thresh = cv2.inRange(hsv, lower_range, upper_range)

        # побитово складываем оригинальную картинку и маску
        bitwise = cv2.bitwise_and(image, image, mask=thresh)

        # показываем картинку маски цвета
        cv2.imshow("bitwise", bitwise)

        # удаляем цвет из маски
        gray = cv2.cvtColor(bitwise, cv2.COLOR_BGR2GRAY)

        # ищем контуры в картинке
        contours, _ = cv2.findContours(gray, cv2.RETR_EXTERNAL, cv2.CHAIN_APPROX_NONE)

        # если контуры найдены...
        if len(contours) != 0:
```

```
            # выводим найденные контуры
            #cv2.drawContours(image, contours, -1, 255, 1)

            # находим контуры бОльшего размера
            c = max(contours, key = cv2.contourArea)

            # получаем координаты прямоугольника, в который они вписаны
            x,y,w,h = cv2.boundingRect(c)

            # если прямоугольник достаточного размера...
            if checkSize(w, h):

                # выводим его
                cv2.rectangle(image, (x, y), (x+w, y+h), RECTCOLOR, RTHICK)

        # Показываем картинку с квадратом выделения
        cv2.imshow("Image", image)

        # Если была нажата клавиша ESC
        k = cv2.waitKey(1)
        if k == 27:

            # прерываем выполнение цикла
            break

    # закрываем все окна
    cv2.destroyAllWindows()

    # останавливаем видео поток
    vs.stop()
```

Для обеспечения перемещения данного робота будет использована система передвижения заимствованная у пауков. За реализацию системы будет отвечать плата “Troyka Cap”[3].

Заключение. Разработанная программа полностью соответствует поставленной задаче. Данные решения можно использовать для проектирования программного обеспечения современных роботов различных типов. Переход на видеоизображение способствует дополнительным возможностям модернизации (реализации компьютерного зрения). В созданном программном обеспечении существует возможность реализации большого количества дополнительных функций: условные переходы, автоматическая установка геолокации

при триггере, дополнительные данные с подключаемых датчиков и т.д.

Список использованных источников

1. AI и Python-компьютерное зрение – [Электронный ресурс] https://russianblogs.com/article/2813948268/

2. OpenCV Python – [Электронный ресурс] https://pypi.org/project/opencv-python/

3. Ленти Д. Изучение робототехники с помощью Python – 2019 - С. 55 – 70

МОНЕТИЗАЦИЯ ИГР С ПОМОЩЬЮ МОДЕЛИ FREE-TO-PLAY

Шумилин М.П., бакалавр гр. ИСТ-18-2,
Технологический университет («МГОТУ»),
Россия, г. Королев

В статье рассматриваются вопросы, затрагивающие монетизацию игр с помощью модели FREE-TO-PLAY.

Ключевые слова: браузерные игры, модель прибыли «Free-to-Play».

Множество существующих на сегодняшний день игр делятся на две больше группы. Игры, в которых надо платить чтобы в них играть и двигаться дальше по сюжету, и те, которые бесплатны с самого начала их использования. Такие игры используют модель прибыли «Free-to-Play», иначе играй бесплатно.

Free-to-Play, как один из видов монетизации, пришел в Россию из Азии, и, на сегодняшний день, очень популярен среди разработчиков игр. Данная модель является одной из самой прибыльной по сравнению с другими. Неоспоримо, дополнительный контент и подписки на получение наград немного выигрывают на фоне Free-to-Play, только пользователи желают и требуют, чтобы игры стали общедоступными для каждого.

Free-to-Play произвела эволюцию среди систем торговли контентом для игр онлайн-сервисов с более долгим сроком жизни, сменив место ежемесячной подписки. Это произошло из-за того, что подписка ограничивала доступ к продаже контента игрокам и стимулировала более дорогой порог вступления в игру. Такая модель монетизации позволила создать несколько отличных решений для разработчиков. Это лучшая продажа контента пользователю, более широкий ассортимент продукта, который значительно помог пополнить количество продаж игр. К тому же, значительно понизился порог входа, по-другому, с помощью данной модели, игры стали более доступными для людей с ограниченными денежными ресурсами.

В России среди множества игр, модель Free-to-Play начали использовать больше всего браузерные игры, разработка некоторых потребляет не так много ресурсов. Но в связи с ростом пользователей в сети Интернет начали создаваться русскоязычные версии востребо-

ванных Free-to-Play игр. Сегодня количество онлайн игр, которые были разработаны в России более 30 штук, но с каждым днем их становиться все больше.

Среди разработчиков есть мнение, что существует правильный и не правильный Free-to-Play. Но также есть вариант, сделать эту модель монетизации более легче, где пользователь платит за более веселое прохождение, но сам контент игры не зависит от состояния кошелька игрока.

Когда в играх дело доходит до создания и расчетов игровой экономики, разработчик должен всегда давать пользователю продукта возможность влиять на данную ему экономику (различные механики, скидки в честь выхода игры). Цены на контент при такой модели чаще всего поднимаются и в начале таких акций пользователь думает, что ему выдается скидка, но, на самом деле, он приобретает товар за ту же стоимость, что была и раньше. Тут уже работает психика, пользователь начинает думать, что такая акция может быть только раз и если он ее не использует, то будет в будущем жалеть об этом.

Описанный выше способ очень активно стали применять в играх, которые специализируются только для пользователей PC, за короткий промежуток времени разработчики часто стали использовать его. Но, к сожалению, данный метод еще не нашел свое место в мобильных играх, поэтому сегодня у разработчиков есть возможность реализовать этот способ для большей прибыли проекта.

Почему модель монетизации Free-to-Play так активно используется? Во время становления данного подвида монетизации критики не замечали ее и не придавали никакого значения, но Free-to-Play имеет свои преимущества по сравнению с другими, а это:

- *Демократизация.*

Используя такую модель, разработчик сможет охватить более большую аудиторию, ведь все пользователи игр желают получать удовольствие от приложения и быть принятыми в центре сообщества, даже не заплатив за нее

- *Игры как увлечение.*

Для модели Free-to-Play принято говорить, что игра должна иметь постоянное развитие, так как пользователи с более большей вероятностью начинают понимать, что игра нечто особенное, что не похоже на другие игры в данном сегменте. И игроки начинают участвовать различных турнирах, повышать свои навыки чтобы занимать

все более высокие строчки в таблице рейтинга, люди начинают говорить, что игра становиться их хобби, местом отдыха.

- *Лучшее соответствие бизнес-модели сервиса.*

Разработчик должен создавать различные события, в которых игрок обязан выполнять цепочку заданий для получения главной награды (редкого предмета, доступа к тайной комнате в локации). Разработчик заинтересован в создании контента для получения прибыли.

- *Более эффективная монетизация внимания.*

Есть взаимосвязь, между тем сколько пользователь проводит времени в игре и тем сколько он вкладывает финансов в нее. Получение прибыли с одного игрока ничем не ограничена, разве только материальным положением.

Прибыль и финансовые показатели

Сначала разберемся с показателями, которые чаще всего разработчики внедряют в игровой процесс, а именно:

- **Удержание**. **Показатель, который дает понять автору продукта, как долго человек остается пользователем контента, обычно принимают за «dX», где X – переменная, которая считает количество дней с начала регистрации,** а само значение представляет собой процент установленных копий игры, которые были использованы за данное количество дней. Другими словами, если удержание d40 составляет 20%, то получается, что 20% установивших игру себе на ПК использовали ее и на 40-ой день
- **Вовлеченность**. **Существует много способов как ее рассчитать, но для более легкого расчета обычно смотрят на время, которое игрок тратит на нахождение в игре (сеанс) и количество сеансов в день (сколько раз игрок заходит в игру в течении дня)**
- **Коэффициент конверсии**. Количество пользователей который начали платить за дополнительный контент.
- **Активные пользователи в день (DAU)**. Среднее количество игроков за один день
- **Средний доход на активного пользователя в день .**Общий доход, полученный от игроков за день, разделенный на количество игроков в игре. Данный параметр зависит от типа игры: одни приносят меньше 2$ в сутки другие – 4$ и больше.
- **Общая ценность (LTV)**. Показатель среднего дохода с одного пользователя за весь период игры.

Удержание и вовлеченность — самые важные показатели!

Если так произойдет, что удержание начнет резко падать, то пользователи перестанут приносить доход, так как игрок чаще всего после длительного отсутствия в игре не видит смысла возвращаться и начинать все сначала, поэтому он переходит на другой проект.

Если же разработчику удалось вернуть в строй игрока, который давно не играл, то показатель монетизации будет определяться вовлеченностью пользователя в данный проект.

Оптимизация доходов, очень важна как для разработчика, так и для компании, которая спонсирует проект. Но, если первоначально обратить слишком много внимания на показатели прибыли и их какое-то улучшение, то разработчик придет к тому, что показатели будут не самыми оптимистичными. На математическом языке это называют оптимизацией локальных максимумов. Главная цель вообще любой игры – «глобальные максимумы» как мы можем видеть на рис. 1.

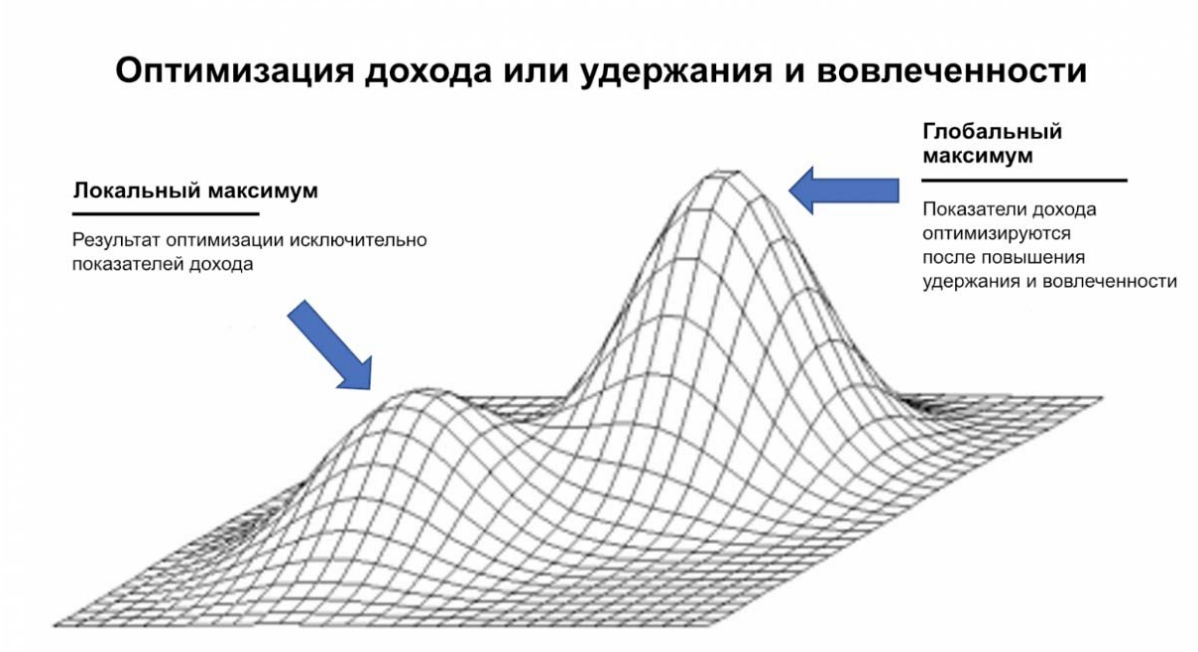


Рис. 1. Оптимизация дохода или удержания и вовлеченности

Проблема, из-за которой показатели бывают не слишком радостные очень проста – достаточно лишь посмотреть на игру как на систему некоторых ограничений. Всегда существовало то, что ограничивает рост или как-то влияет на возможности разработчика для дальнейшего развития проекта.

Время – деньги.

Говоря простым языком, не время приносит деньги, а внимание к игре и вовлеченность. Все игры, существующие сегодня, – это бизнес, который как любой бизнес превращает внимание в прибыль. В

тех же премиум-играх, за которые пользователь должен внести фиксированную сумму, чтобы только получить возможность играть, разработчик сможет получить больше прибыли от дополнительного контента (иначе DLC) в продолжения сюжета, чтобы пользователь и дальше использовал продукт.

Метафора напряжения

В физике напряжение – это «давление», движущая сила, которая заставляет электроны перемещаться по проводящей цепи.

В компьютерных играх так же существует свое «напряжение», которое выступает роли игрового цикла.

По времени проведенным в игре, пользователь сталкивается с различными вариантами монетизации: купить редкую валюту чтобы получить доступ к сундуку, повышение показателей героя для более быстрого прохождения локации, получить предмет, который невозможно получить бесплатно. Возможность игрока участвовать в таких вариантах монетизации и количество взаимосвязанных покупок – и является экономической напряжённостью внутри игры.

Данный критерий можно сравнить с экономической концепцией оборачиваемости денег. Мне напряжение нравится больше, оно выглядит как целостная метафора, которая имеет в себе различные вариации оказываемого давления на пользователей, которые в свою очередь приобретают товары во время прохождения игры.

Как и в случае электричества, напряжение со временем может меняться. Многие игры с этой точки зрения выглядят так, как представлено на рис. 2.

Рис. 2. Экономическое напряжение в игре

Если уж так произошло, что игрок все-таки покинул игру, то экономическое напряжение для него становится равным нулю, то есть с данного пользователя вы больше не заработаете, так как он перестал быть игроком вашего проекта. Если же у вас есть другой проект, который вы можете ему предложить, то возможно данного пользователя можно будет завлечь в него.

Есть игры, которые очень востребованы, выглядят зачастую лучше, чем та которую мы видели с вами на графике выше. В данных проектах, очень сильно развито удержание игрока, чтобы он мог тратить больше времени на нахождение в игре, поэтому в данных играх экономическое напряжение больше.

В заключении хочется отметить, что модель Free-to-Play игр очень разнообразна и существует много ее подвидов. Разработчикам игр, которые будут основаны на данном методе монетизации следует придерживаться правил, чтобы в вашу игру было весело играть и создавать игры, в которые пользователь заходит на минуту, но остается там на часы. Игры с данной моделью монетизации востребованы и будут занимать свое место в игровой индустрии.

Список используемых источников

1. Как работает монетизация [Электронный ресурс] URL: https://vc.ru/marketing/280943-kak-rabotaet-monetizaciya-v-mobilnyh-igrah#:~:text=Монетизация%20игры%20построена%20таким%20образом,д. (дата обращения:02.03.2022).

2. 59 способов монетизации игры: как сделать свой проект прибыльным Статьи редакции [Электронный ресурс] URL: https://vc.ru/flood/35119-59-sposobov-monetizacii-igry-kak-sdelat-svoy-proekt-pribylnym дата обращения:05.03.2022).

3. Стратегия монетизации для игр [Электронный ресурс] URL: https://admob.google.com/intl/ru/home/games/ (дата обращения:09.02.2022).

4. «Фритуплей» — зачем нужна и как работает [Электронный ресурс] URL: https://igrasan.ru/statejnik/frituplej-zachem-nuzhna-i-kak-rabotaet/ (дата обращения:13.01.2022).

5. Хороший плохой фритуплей [Электронный ресурс] URL: https://gdcuffs.com/good-bad-free-to-play/ (дата обращения:15.03.2022).

6. F2p, что это? [Электронный ресурс] URL: https://pr-nsk.ru/f2p-chto-eto/ (дата обращения:28.03.2022).

Научное издание

ЭВОЛЮЦИОННЫЕ ПРОЦЕССЫ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Сборник трудов по материалам
7-й всесоюзной научно-технической конференции
4 апреля 2022 г.

Сдано в набор 20.04.2022. Подп. в печ. 27.04.2022.
Формат 60×88/16. Бумага офсетная.
Усл.печ.л. 10,2 Тираж 500 экз.

ISBN 978-5-907477-53-7

Издательство Научный консультант
123007, г. Москва, Хорошевское ш., 35к2, офис 508.
Тел.: +7 (926) 609-32-93, +7 (499) 195-60-77 www.n-ko.ru keyneslab@gmail.com