СибАК
www.sibac.info

ISSN 2310-4066

XLV СТУДЕНЧЕСКАЯ МЕЖДУНАРОДНАЯ НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ

№8(44)

НАУЧНОЕ СООБЩЕСТВО СТУДЕНТОВ XXI СТОЛЕТИЯ. ТЕХНИЧЕСКИЕ НАУКИ

г. НОВОСИБИРСК, 2016

СибАК
www.sibac.info

НАУЧНОЕ СООБЩЕСТВО СТУДЕНТОВ XXI СТОЛЕТИЯ. ТЕХНИЧЕСКИЕ НАУКИ

Электронный сборник статей по материалам XLV студенческой международной заочной научно-практической конференции

№ 8 (44)
Сентябрь 2016 г.

Издается с Октября 2012 года

Новосибирск
2016

УДК 62
ББК 30
Н 34

Председатель редколлегии:

Дмитриева Наталья Витальевна – д-р психол. наук, канд. мед. наук, проф., академик Международной академии наук педагогического образования, врач-психотерапевт, член профессиональной психотерапевтической лиги.

Редакционная коллегия:

Ахмеднабиев Расул Магомедович – канд. техн. наук, доц. Полтавского национального технического университета им. Ю. Кондратюка.

Ахметов Сайранбек Махсутович – д-р техн. наук, проф. Евразийского национального университета им. Л.Н. Гумилева, г. Астана, академик РАЕН, действительный член (академик) Национальной инженерной академии Республики Казахстан, советник президента Казахстанского университета инновационных и телекоммуникационных систем (КазУИТС), заместитель председателя Западно-Казахстанского филиала НИА РК, руководитель Отделения научной школы «Устойчивое инновационное развитие в инновации» Международного государственного университета природы, общества и человека «Дубна» в КазУИТС, г. Уральск.

Елисеев Дмитрий Викторович – канд. техн. наук, доцент, бизнес-консультант Академии менеджмента и рынка, ведущий консультант по стратегии и бизнес-процессам, «Консалтинговая фирма «Партнеры и Боровков»

Н 34 «Научное сообщество студентов XXI столетия. Технические науки»: Электронный сборник статей по материалам XLV студенческой международной научно-практической конференции. – Новосибирск: Изд. АНС «СибАК». – 2016. – № 8 (44)/ [Электронный ресурс] – Режим доступа. – URL: http://www.sibac.info/archive/Technic/8(44).pdf.

Электронный сборник статей по материалам XLV студенческой международной научно-практической конференции «Научное сообщество студентов XXI столетия. Технические науки» отражает результаты научных исследований, проведенных представителями различных школ и направлений современной науки.

Данное издание будет полезно магистрам, студентам, исследователям и всем интересующимся актуальным состоянием и тенденциями развития современной науки.

ББК 30
ISSN 2310-4066
© АНС «СибАК», 2016 г.

Оглавление

Секция «Архитектура, Строительство» 6

ВЫБОР ТЕХНОЛОГИИ УСТРОЙСТВА СТОЛБЧАТЫХ ЖЕЛЕЗОБЕТОННЫХ ФУНДАМЕНТОВ В ТРУДНОДОСТУПНЫХ РЕГИОНАХ ДЛЯ МАЛОЭТАЖНОГО ДОМОСТРОЕНИЯ 6
Малышев Леонид Сергеевич
Кабанов Евгений Анатольевич
Погодин Денис Алексеевич

ОЗЕЛЕНЕНИЕ ТРАМВАЙНОГО ПОЛОТНА 10
Хайруллин Ильназ Илдарович
Логинова Ольга Анатольевна

Секция «Информационные технологии» 16

АВТОМАТИЗАЦИЯ ДЕЯТЕЛЬНОСТИ ИНСПЕКТОРА ОТДЕЛА АНАЛИЗА, ПЛАНИРОВАНИЯ И КОНТРОЛЯ ПОЛИЦИИ 16
Айкожаев Нурислам Муратович
Жуматаева Жанат Есиркеповна

ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ ТЕХНОЛОГИИ «ИСКУССТВЕННЫЙ НОС» В РАКЕТНО-КОСМИЧЕСКОЙ ОТРАСЛИ 22
Айкожаев Нурислам Муратович
Есеналиева Наргиз Айдаровна
Жуматаева Жанат Есиркеповна

ПРОЕКТИРОВАНИЕ ИНФОРМАЦИОННЫХ МОДЕЛЕЙ АИС ОТДЕЛА ИНФОРМАЦИОННОГО ОБЕСПЕЧЕНИЯ ШТАБА ПОЛИЦИИ 27
Айкожаев Нурислам Муратович
Шестопалова Ольга Львовна

АНТИВИРУСЫ: АНАЛИЗ ПРОИЗВОДИТЕЛЬНОСТИ И ЭФФЕКТИВНОСТИ 35
Бурцев Игорь Алексеевич
Кукаева Евгения Борисовна

ПРОГНОЗИРОВАНИЕ ЭНЕРГОПОТРЕБЛЕНИЯ ПРЕДПРИЯТИЯ РАКЕТНО-КОСМИЧЕСКОЙ ОТРАСЛИ 40
Кириченко Юлия Николаевна
Шудабаева Арай Казымбековна
Жуматаева Жанат Есиркеповна

ПЕРСПЕКТИВЫ РАЗВИТИЯ МОБИЛЬНЫХ СЕТЕЙ ПЯТОГО ПОКОЛЕНИЯ 5G 46
Дмитриев Егор Андреевич
Танаев Иван Владимирович
Швейкин Владислав Витальевич
Завгородний Станислав Дмитриевич

ОБЗОР УГРОЗ И ТЕХНОЛОГИЙ ЗАЩИТЫ WI-FI СЕТЕЙ 51
Федоров Сергей Александрович
Битюцкая Наталья Ивановна

РАЗРАБОТКА WEB-ПРИЛОЖЕНИЯ ДЛЯ УЧЕТА ВЫПУСКНИКОВ ТЕХНИКУМА 59
Щелканов Константин Олегович
Валеев Михаил Владимирович

Секция «Математика» 65

КРИПТОГРАФИЯ НА ОСНОВЕ КОДОВ ИСПРАВЛЕНИЯ ОШИБОК 65
Дмитриев Егор Андреевич
Танаев Иван Владимирович
Швейкин Владислав Витальевич
Завгородний Станислав Дмитриевич

АЛГОРИТМ ОБУЧЕНИЯ МНОГОСЛОЙНОЙ НЕЙРОННОЙ СЕТИ МЕТОДОМ ОБРАТНОГО РАСПРОСТРАНЕНИЯ ОШИБКИ 70
Дмитриев Егор Андреевич
Танаев Иван Владимирович
Швейкин Владислав Витальевич
Завгородний Станислав Дмитриевич

РАСШИРЕННЫЙ АЛГОРИТМ ДИФФИ-ХЕЛЛМАНА 75
Андросова Татьяна Евгеньевна
Курочкин Владислав Михайлович
Додонова Наталья Леонидовна

ПРИМЕНЕНИЕ ЭЛЛИПТИЧЕСКИХ КРИВЫХ В КРИПТОГРАФИИ 81
Швейкин Владислав Витальевич
Танаев Иван Владимирович
Дмитриев Егор Андреевич
Завгородний Станислав Дмитриевич

ПРИМЕНЕНИЕ ТЕОРИИ ЧИСЕЛ В АЛГОРИТМЕ ШИФРОВАНИЯ RSA 86
Швейкин Владислав Витальевич
Завгородний Станислав Дмитриевич
Танаев Иван Владимирович
Дмитриев Егор Андреевич

Секция «Моделирование» **92**

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ДВИЖЕНИЯ КОСМИЧЕСКОЙ ТРОСОВОЙ СИСТЕМЫ В НЕЦЕНТРАЛЬНОМ ГРАВИТАЦИОННОМ ПОЛЕ ЗЕМЛИ 92
Сахибназарова Виктория Бахтиёровна

Секция «Ресурсосбережение» **97**

ВЛИЯНИЕ ЧЕЛОВЕЧЕСКОЙ ДЕЯТЕЛЬНОСТИ НА ЖИЗНЕННО ВАЖНЫЕ РЕСУРСЫ И СТАБИЛЬНОСТЬ ЭКОСИСТЕМ 97
Дубленных Филипп Дмитриевич
Кобзева Ирина Олеговна

ВОЗМОЖНОСТЬ И ПЕРСПЕКТИВА ИСПОЛЬЗОВАНИЯ ОТХОДОВ ТЕПЛОЭНЕРГЕТИКИ В ПРОИЗВОДСТВЕ ЗАПОЛНИТЕЛЯ ДЛЯ КОНСТРУКЦИОННЫХ БЕТОНОВ 102
Сумарокова Любовь Сергеевна
Фомина Ирина Викторовна

СЕКЦИЯ

«АРХИТЕКТУРА, СТРОИТЕЛЬСТВО»

ВЫБОР ТЕХНОЛОГИИ УСТРОЙСТВА СТОЛБЧАТЫХ ЖЕЛЕЗОБЕТОННЫХ ФУНДАМЕНТОВ В ТРУДНОДОСТУПНЫХ РЕГИОНАХ ДЛЯ МАЛОЭТАЖНОГО ДОМОСТРОЕНИЯ

Малышев Леонид Сергеевич
студент магистратуры, инженерно-строительный факультет ВоГУ, РФ, г. Вологда
E-mail: lokiwish@list.ru

Кабанов Евгений Анатольевич
научный руководитель, кандидат технических наук, доцент ВоГУ, РФ, г. Вологда

Погодин Денис Алексеевич
научный руководитель, кандидат технических наук, доцент ВоГУ, РФ, г. Вологда

Применение наиболее технологичных методов устройства свайных фундаментов значительно сокращают продолжительность строительства, а также позволяют быстрее и дешевле получить конечный качественный результат. Выбор эффективного способа строительства позволит оптимизировать экономическую и техническую часть проекта [5].

Возникла значимая и новая технологическая строительная проблема - исследование свайных фундаментов с целью выявления наиболее эффективного метода технологии устройства при малоэтажном строительстве [6].

Анализ существующих технологий устройства фундаментов позволяет выявить имеющие принципиальное значение проблемы, которые должны быть учтены при подготовке и производстве монтажных работ:

- стоимость материалов для каждого из сравниваемых методов;
- себестоимость транспортных расходов на устройство фундамента;
- уменьшение объема транспортных грузов;

- уменьшение продолжительности, трудоемкости и стоимости строительства [3].

Одной из основных проблем при выборе технологии устройства фундамента является стоимость материалов. При строительстве свай используется большое количество стали, бетона, гидроизолирующих материалов, песчано-гравийной смеси, закладных деталей, арматуры и др. Также стоит учитывать, что расход бетона трубобетонных свай значительно ниже, нежели у буронабивных свай. Однако при использовании трубобетона будет уже больший расход стали. От цены используемых материалов зависит большая часть сметной стоимости [1,2].

Не менее важной проблемой является себестоимость фундамента, она зависит от многих факторов. Например, особенность фундамента. Характерность буронабивной сваи с башмаком заключается в том, что в пробуренную скважину опускают обсадную трубу, имеющую на конце свободно опертый чугунный башмак, оставляемый в грунте после погружения обсадной трубы на требуемую глубину. Порционно загружая бетонную смесь, регулярно ее уплотняя и постепенно извлекая трубу из скважины, получают готовую набивную бетонную сваю. Принципиальное отличие трубобетонных свай в том, что обсадная труба длиной до 40...50 м имеет в нижней части жестко закрепленный башмак. После достижения дна скважины труба остается там, не извлекается, а заполняется бетонной смесью. Поэтому себестоимость зависит от объема проводимых работ [7].

Важный вопрос, это и перемещение значительного количества грузов. Транспортные и связанны с ними погрузочно-разгрузочные работы влияют на стоимость и трудоемкость строительства объектов и составляют в среднем 20 ... 25% общей стоимости и трудоемкости строительной продукции [3]. Столь значительный удельный вес транспортных работ требует оптимальных решений при выборе направления грузопотоков, транспортных средств, а также комплексной механизации всего транспортного процесса — погрузки, перемещения, выгрузки. При этом необходимо стремиться к уменьшению

расстояния перевозок грузов, избегать перегрузок, рационально использовать в погрузочно-разгрузочных операциях основные монтажные механизмы строительной площадки. Так же расходы на транспортировку зависят от объема и веса материалов.

Касаясь темы продолжительности строительства буронабивных и трубобетонных свай, применение данных технологий уменьшает объем земляных работ, сокращает количество арматуры, уменьшает количество свай, дает возможность работать круглосуточно в три смены [4]. Мобильность буровой техники обеспечивает высокие темпы работ: сокращается продолжительность свайных работ, и строительство обходится дешевле. При создании проектов и строительстве малоэтажных домов наиболее целесообразно использовать малозаглубленные фундаменты, которые наряду с надежностью позволяют значительно сократить расход материалов и снизить трудозатраты. Поэтому использование двух сравниваемых типов будет актуально в строительстве.

Преимущества свайных фундаментов вытекают из недостатков других фундаментов, например, ленточных, одним из которых, если не основным, является их недостаточная прочность на пучинистых грунтах. Такие типы почв занимают в России чуть ли не большую часть её территории. Поэтому, принимая решение о типе будущего фундамента, необходимо учитывать — тип грунта, глубину промерзания и уровень грунтовых вод в месте будущего строительства. При глубине промерзания, находящейся ниже уровня грунтовых вод, почва под домом может вспучиваться, с усилием до 15 т/кв. м. Единственным верным решением для этого случая может служить свайный фундамент, ведь сваи, заложенные ниже уровня промерзания почвы, не выдавливаются вверх. Еще одним преимуществом свайных фундаментов, а особенно буронабивных свай, является их более низкая по отношению к другим стоимость благодаря уменьшению количества земляных работ и значительному уменьшению объёма заливаемого в основание бетона.

Недостатком буронабивных и трубобетонных свай является трудоёмкость. Так при применении трубобетонных свай необходимо сделать уширенную

бетонную пяту, а если свая буронабивная нужно сделать внутреннюю опалубку. Для опалубки в сухих грунтах вполне достаточно использовать свернутый и закреплённый в виде трубы гидроизол. Он позволяет защитить бетон сваи от грунтовых вод и промерзания. При высоком уровне грунтовых вод в качестве опалубки сваи можно использовать металлические или асбоцементные трубы подходящего диаметра [4].

Несмотря на перечисленные выше проблемы, технология устройства столбчатых железобетонных фундаментов является неотъемлемой частью современного строительства, а, следовательно, решение данных проблем является наиболее актуальной задачей технологического проектирования.

Список литературы:

1. Кикин, А. И. К проблеме прочности стальных труб, заполненных бетоном / А. И. Кикин, Р. С. Санжаровский, В. А. Трулль // Известия вузов. Строительство и архитектура. - 1977. - № 6. - С. 3-7.
2. Кикин, А. И. Конструкции из стальных труб, заполненных бетоном / А. И. Кикин, Р. С. Санжаровский, В. А. Трулль. - Москва: Стройиздат, 1974. - 144 с.
3. МДС 81-35.2004 Методика определения стоимости строительной продукции на территории Российской Федерации (с Изменениями от 16.06.2014). [Электронный ресурс] – Режим доступа. – URL: http://docs.cntd.ru/document/1200035529 (дата обращения: 23.09.2016)
4. СНиП 1.04.03-85* Нормы продолжительности строительства и задела в строительстве предприятий, зданий и сооружений. Часть I. (Общие положения. Раздел А (подразделы 1-6)). [Электронный ресурс] – Режим доступа. – URL: http://docs.cntd.ru/document/1200000622 (дата обращения: 23.09.2016)
5. СП 24.13330.2011 Свайные фундаменты. Актуализированная редакция СНиП 2.02.03-85. [Электронный ресурс] – Режим доступа. – URL: http://docs.cntd.ru/document/1200084538 (дата обращения: 23.09.2016)
6. СП 30-102-99 Планировка и застройка территорий малоэтажного жилищного строительства. [Электронный ресурс] – Режим доступа. – URL: http://docs.cntd.ru/document/1200004849 (дата обращения: 23.09.2016)
7. СП 63.13330.2012 Бетонные и железобетонные конструкции. Основные положения. Актуализированная редакция СНиП 52-01-2003 (с Изменениями N 1, 2). [Электронный ресурс] – Режим доступа. – URL: http://docs.cntd.ru/document/1200095246 (дата обращения: 23.09.2016)

ОЗЕЛЕНЕНИЕ ТРАМВАЙНОГО ПОЛОТНА

Хайруллин Ильназ Илдарович
магистрант, кафедра автомобильные дороги, мосты и тоннели, КГАСУ, РФ, г. Казань

Логинова Ольга Анатольевна
научный руководитель, канд. технических наук, КГАСУ, РФ, г. Казань
E-mail: loginova@kgasu.ru

Как и в любом большом городе, в Казани одной из главных проблем являются пробки на дорогах. Это вызвано, главным образом, недостаточной пропускной способностью улиц и дорог, а также неудовлетворительным качеством покрытия и неправильностью организации движения на отдельных участках.

Наиболее наглядно эту проблему пробок может продемонстрировать в час пик улица Ломжинская, которая находится в Советском районе г.Казани. Дело в том, что эта улица не может справиться с потоком автомобилей, которые едут в поселок Вознесенское. Кроме того сказывается качество покрытия на улице Ноксинский спуск, который является основной улицей, соединяющий город с поселком.

Для решения этой проблемы в выпускной работе запроектирована улица, которая соединяет Большое Казанское Кольцо (БКК) и поселок Вознесенское.

Проектируемая улица находится в г. Казани Республики Татарстан. Улица в административном отношении проходит по территории Советского района Казани, по незастроенной территории, между улицами Минская и Закиева. В геоморфологическом отношении, объект расположен на левобережье р. Волги, на левом водораздельном склоне долины р. Ноксы. Протяженность участка от БКК (ПК 0+00) до ул. Ю.Фучика (ПК 7+00), которую пересекает проектируемая дорога – 700 м.

В соответствии с заданием и СП «Градостроительство» [1], проектируемая улица относится к магистральной улице районного значения. Основное назначение магистральной улицы районного значения – это транспортная

и пешеходная связь между жилыми районами, а так же между жилыми и промышленными районами, общественными центрами; выходы на другие магистральные улицы.

Ширина улицы составляет 54,0 метра, интенсивность автомобилей учётом перспективы 9500 авто/сут., интенсивность пешеходов – 6000 чел/сут. На данной улице (ул. Азинский лес) необходимо предусмотреть движение общественного транспорта в виде автобусов и трамваев (рис.1).

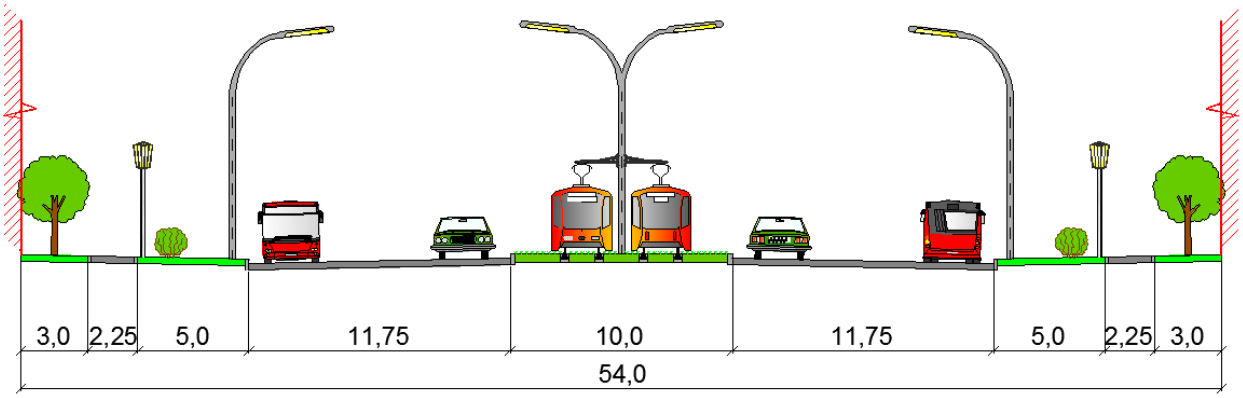

Рисунок 1. Расчетный поперечник улицы

В современных городах большую роль играет общественный транспорт. Он оказывает огромное влияние на город и его жителей. Хорошо организованное движение общественного транспорта улучшает транспортное состояние городов, привлекает туристов, особенно если общественный транспорт работает в ночное время и проходит по значительной территории города и его исторической части.

В то же время, транспорт несет с собой ряд негативных явлений: шум, загазованность и вибрации. Широкое использование трамваев позволяет решить ряд таких проблем.

Устройство трамвайных путей в одном уровне с проезжей частью, влечет за собой их асфальтирование или бетонирование. Это приводит к ряду неблагоприятных экологических последствий. Увеличивается поверхностный сток ливневых вод, который во время проливных дождей может перегрузить канализационную систему города. Увеличиваются расходы на очистку сточных

вод. Уменьшается приток грунтовых вод, уменьшается уровень испарений и воздушная влажность. Увеличивается содержание пыли в окружающей среде. Возрастает уровень шума, не только за счет увеличения числа автомобильного транспорта, но большого числа поверхностей и плотной застройки, которые отражают звук, а не поглощают его.

С 80-х годов двадцатого века в странах Западной Европы стали применять озеленение трамвайных путей. Такая конструкция трамвайного пути получила название «Green Track». Это можно встретить в Барселоне, Франкфурте, Милане, Сент-Этьене, Страсбурге и Варшаве. Практический эффект от реализации такого решения жители городов почувствовали сразу.

Основными задачами озеленения трамвайных путей являются:

1. Снижение уровня шума. Высаженная на одном уровне с головкой рельса растительность уменьшает уровень шума до 3 дБ.

2. Снижение уровня вибрации за счет поглощения импульсов газоном и прирельсовыми профилями.

3. Снижение уровня загазованности. Зеленая растительность выделяет кислород, поглощая углекислый газ.

4. Уменьшение объема поверхностного стока ливневых вод в результате поглощения растительностью части воды.

5. Уменьшение температуры рельсов вследствие того, что нагреву подвергается только верхняя часть рельса, а остальная часть находится под конструктивными слоями. Таким образом, уменьшается вероятность аварии из-за образования волнистых путей.

6. Снижение температуры окружающего воздуха. Вместо привычного бетона между трамвайными путями используется газонная трава, которая отражает большую часть света, тем самым меньше нагревается сам и меньше нагревает окружающий воздух.

7. Улучшение психологического состояния населения. Зеленая растительность оказывает положительное психофизиологическое воздействие на человека. «Зеленые» трамвайные пути уменьшает утомляемость водителя

трамвая, тем самым, уменьшая вероятность возникновения аварийной ситуации.

Решение озеленять выделенное трамвайное полотно или нет, конечно же, принимают городские власти. И если оно принято, то это влечет за собой дополнительные затраты на реконструкцию.

В данной работе для уменьшения шума и вибрации трамвайные пути устраивают из железобетонных рельсовых модулей «PREFArails» [2].

Сначала в слое песка устраивается дренаж из гофрированной трубы для сбора грунтовых вод, которые собираются в водосборных колодцах и сбрасываются в канализационную систему. Это необходимо для исключения вспучивания обводненных слоев основания вследствие их промораживания и оттаивания. Поверх уплотненного слоя песка укладывается слой из щебня, который уплотняется и заклинивается щебнем из более мелкой фракции. Слой песка и щебня является основанием для устройства рельсовых модулей. После этого в пространство между модулями досыпается щебень, устраивается выравнивающий слой из песка. Песок накрывается специальной антикорневой изоляцией PLANTER-life. На изоляцию укладываются газонные решетки Eco Pro, заполненные субстратом с семенами [3]. В этом случае газон будет находиться в одном уровне с головкой рельса (рис.2).

Рисунок 2. Газон на одном уровне с головкой рельса

Другой вариант - создания «Green Track». Это устройство газона у подошвы рельса. Но такое решение эстетически и технически проигрывает первому варианту. В качестве растительности могут бить использованы газонные травы, очиток или искусственная трава (рис.3) [4, 7].

Рисунок 3. Газон у подошвы рельса

Как и любая растительность, газонная трава нуждается в уходе, а именно в орошении и скосе. Для орошения проектируются системы автоматического полива Gardena (рис.4), а для скоса травы используется специальная газонокосилка (рис.5) [5, 6].

Рисунок 4. Система автоматического полива Gardena

Рисунок 5. Газонокосилка

Список литературы:

1. СП 34.13330.2012 Автомобильные дороги. Актуализированная редакция СНиП 2.05.02-85* [Текст] / М.: Госстрой России, 2013.
2. ADVANTAGES OF THE PREFArails ENCASED RAIL SYSTEM. [Электронный ресурс]. - Режим доступа. - URL: http://www.prefarails.eu/en/articles/21/les-atouts-du-systeme-de-voie-noyee-prefarails (дата обращения: 03.06.16).
3. Green Tram Tracks. [Электронный ресурс]– Режим доступа. - URL: http://www.urbantrack.eu/images/site/publications/FinalConference/presentations/07_ASP_Grassed%20Track.pdf (дата обращения: 03.06.16).

4. Effect and Function of Green Tracks. [Электронный ресурс]– Режим доступа. - URL: http://www.gruengleisnetzwerk.de/images/downloads/effects.pdf (дата обращения: 03.06.16).
5. Paris Tramways Install Turf. [Электронный ресурс] – Режим доступа. – URL: http://www.hunterindustries.com/sites/default/files/styles/colorbox_gallery/public/sprays-running.png?itok=mZnD3SF5 (дата обращения: 03.06.16).
6. Train Ticket Europe Blog. [Электронный ресурс] – Режим доступа. – URL: http://train-ticket.blogspot.ru/2014/06/tour-de-france-of-tramways-brest.html (дата обращения: 03.06.16).
7. Urban Track Innotrans. 2008. [Электронный ресурс] – Режим доступа. – URL: https://www.yumpu.com/en/document/view/26673434/urbantrack-innotrans-2008-ttk-unife (дата обращения: 03.06.16).

СЕКЦИЯ

«ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ»

АВТОМАТИЗАЦИЯ ДЕЯТЕЛЬНОСТИ ИНСПЕКТОРА ОТДЕЛА АНАЛИЗА, ПЛАНИРОВАНИЯ И КОНТРОЛЯ ПОЛИЦИИ

Айкожаев Нурислам Муратович
студент, кафедра Б12-ИТИиУ, филиал «Восход» МАИ,
Республика Казахстан, г. Байконур
E-mail: nurislam.aykozhaev@mail.ru

Жуматаева Жанат Есиркеповна
научный руководитель, к.т.н., кафедра Б12-ИТИиУ, филиал «Восход» МАИ,
Республика Казахстан, г. Байконур

Отдел анализа, планирования и контроля (АПК) подразделения штаба Управления министерства внутренних дел (УМВД) России осуществляет информационно-аналитическую деятельность по выработке своевременных, обоснованных и рациональных управленческих решений начальника Главного управления (ГУ) дел в сфере охраны правопорядка и борьбы с преступностью, а также при реализации других функций Главного управления. Обеспечивает разработку плана основных организационных мероприятий Главного управления на основе систематического анализа состояния преступности и охраны общественного порядка на территории области, результатов деятельности Главного управления и иных факторов, определяющих оперативную обстановку. Координирует работу подразделений ГУ и отделений внутренних дел по выявлению и внедрению передового опыта [1].

Автоматизация деятельности инспектора отдела АПК полиции необходима для сокращения значительных объемов документооборота и наведения порядка в документировании. В настоящее время в Органах внутренних дел особую актуальность приобретают правильная организация работы с управленческими документами.

Разрабатываемая система предназначена для внедрения в подразделение штаба УМВД Российской Федерации. Пользователем системы будет инспектор отдела АПК полиции.

Одним из основных этапов проектирования какой-либо системы является проектирование функциональных моделей.

Информационная модель – модель объекта, представленная в виде информации, описывающей существенные для данного рассмотрения параметры и переменные величины объекта, связи между ними, входы и выходы объекта и позволяющая путём подачи на модель информации об изменениях входных величин моделировать возможные состояния объекта [2].

Разработанные информационные модели позволят более наглядно представить основные процессы, входные и выходные данные, необходимые для функционирования будущей системы.

Для проектирования информационных моделей используется инструментальное средство – Ramus Educational (кроссплатформенная система моделирования и анализа бизнес-процессов).

Главная цель построения контекстной диаграммы заключается в том, чтобы сделать требования к системе ясными и понятными на каждом уровне детализации, а также разбить эти требования на части с точно определенными отношениями между ними.

На рисунке 1 представлена контекстная диаграмма системы, в которой определены входные и выходные потоки данных.

Входными данными являются: статистические данные из отдела информационного обеспечения, планы мероприятий из ГУ МВД РФ, нормативно-правовые документы из ГУ МВД РФ, годовой план взаимодействия подразделений и служб из ГУ МВД РФ, проблемные вопросы из оперативных совещаний.

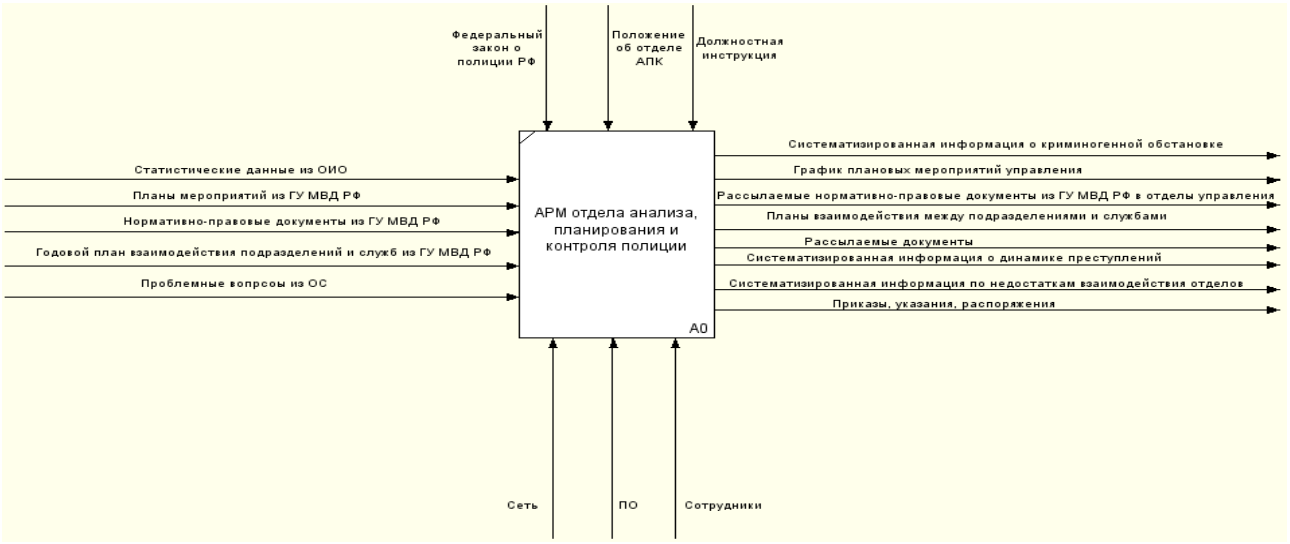

Рисунок 1. Контекстная диаграмма системы

Выходными данными являются: систематизированная информация о криминогенной обстановке, график плановых мероприятий управления, рассылаемые нормативно-правовые документы из ГУ МВД РФ в отделы управления, планы взаимодействия между подразделениями и службами, рассылаемые документы, систематизированная информация о динамике преступлений, систематизированная информация по недостаткам взаимодействия отделов, приказы, указания, распоряжения.

После построения контекстной диаграммы следующим шагом является построение диаграммы нулевого уровня, более подробно иллюстрирующей процессы, протекающие в системе.

Изображение контекстной диаграммы нулевого уровня показано на рисунке 2.

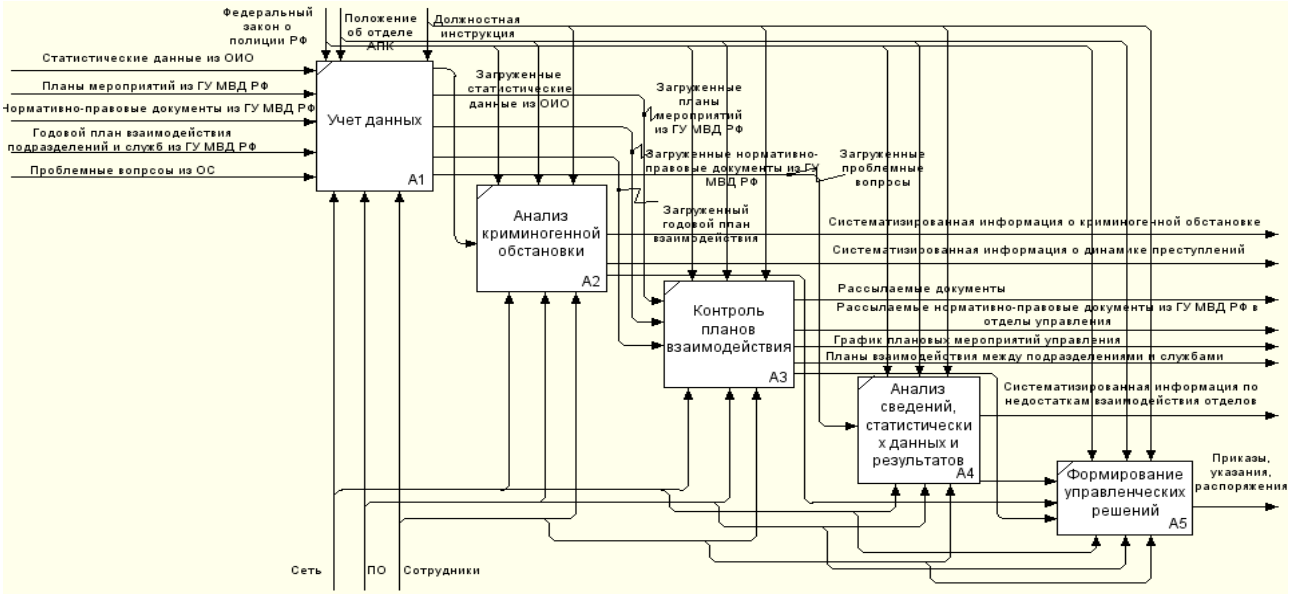

Рисунок 2. Диаграмма нулевого уровня

Диаграмма нулевого уровня включает в себя следующие подсистемы:

- подсистема «Учет данных»;
- подсистема «Анализ криминогенной обстановки»;
- подсистема «Контроль планов взаимодействия»;
- подсистема «Анализ сведений, статистических данных и результатов»;
- подсистема «Формирование управленческих решений».

Данные подсистемы отражают основные направления деятельности отдела АПК полиции.

Следующим шагом является построение диаграмм декомпозиции основных её подсистем.

Для того чтобы провести более детальное моделирование подсистемы «Анализ криминогенной обстановки», необходимо выполнить ее декомпозицию.

Диаграмма декомпозиции процесса подсистемы «Анализ криминогенной обстановки» представлена на рисунке 3.

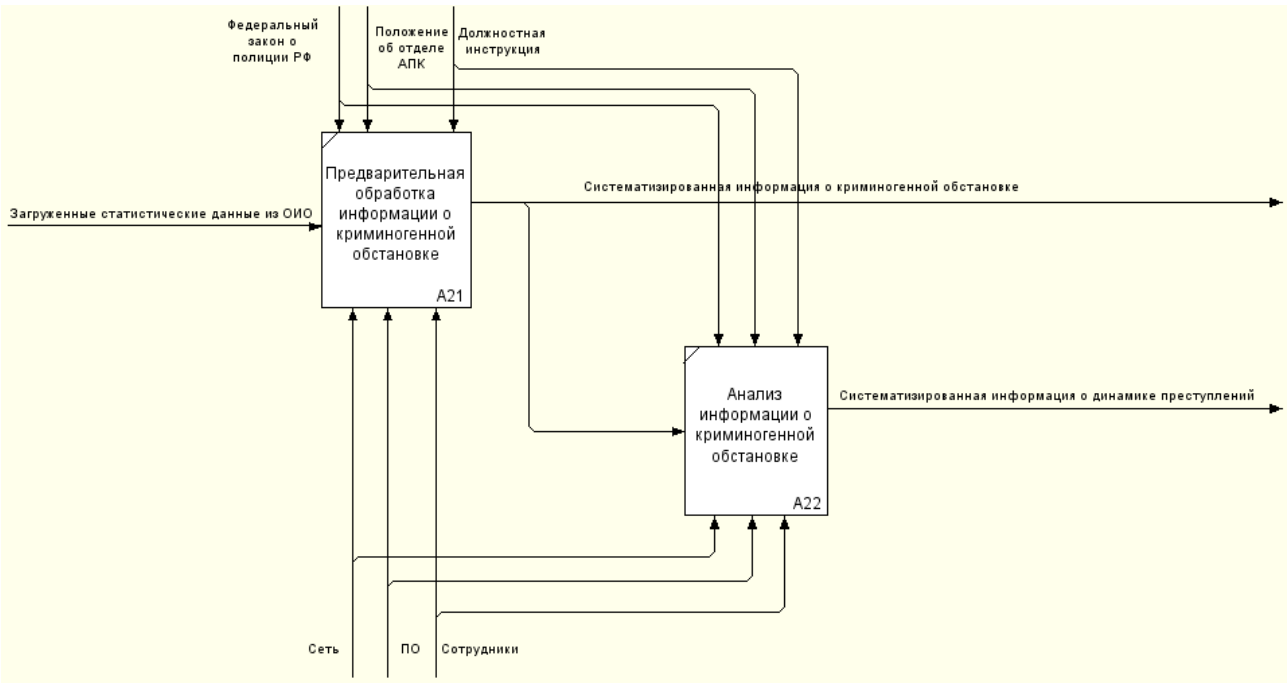

Рисунок 3. Диаграмма декомпозиции подсистемы «Анализ криминогенной обстановки»

На рисунке 4 представлена декомпозиция блока А4 – «Анализ сведений, статистических данных и результатов».

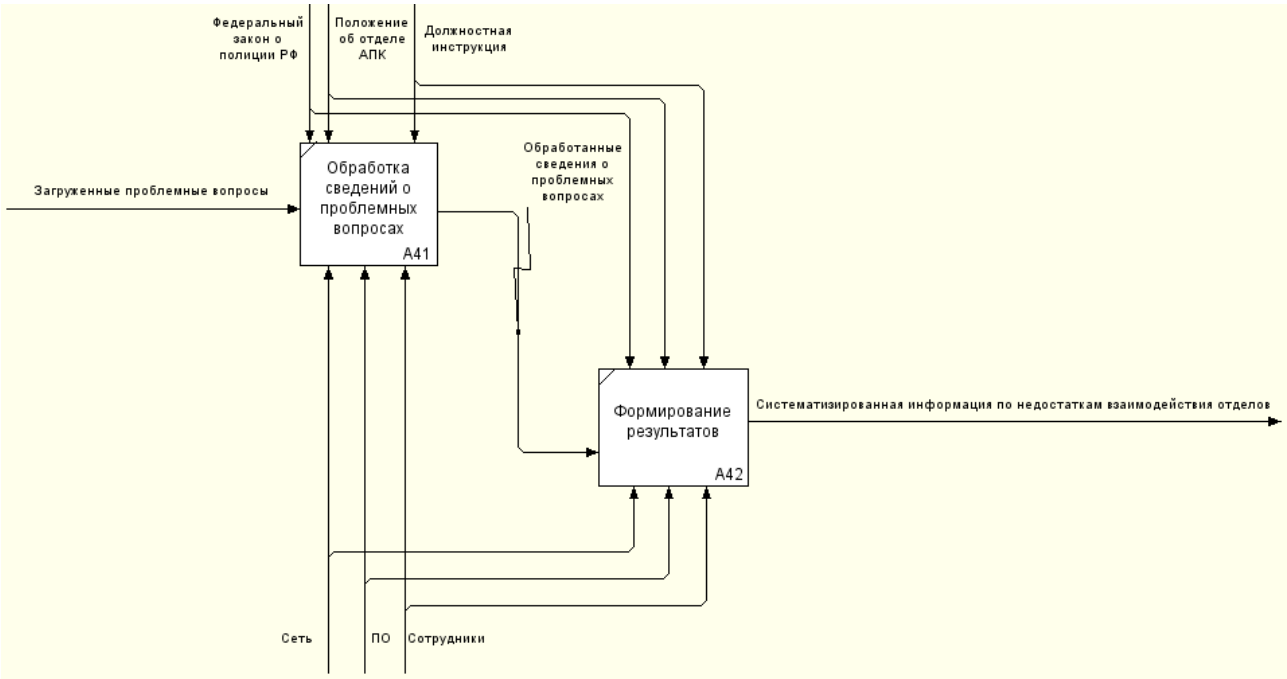

Рисунок 4. Диаграмма декомпозиции подсистемы «Анализ сведений, статистических данных и результатов»

Создание проектируемой системы обеспечит уменьшение трудоемкости работы, выполняемой инспектором отдела АПК, сокращение времени

на обработку информации, снижение влияния «человеческого фактора» на весь процесс, уменьшение риска потери информации, сокращения частоты появления ошибок, а также увеличение достоверности данных.

Список литературы:

1. Сайт МВД России: сайт – [Электронный ресурс] – Режим доступа.URL:https://54.мвд.рф/gumvd/struktura/sp/item/418092 (дата обращения: 16.09.2016).
2. Энциклопедия Википедия: сайт – [Электронный ресурс] – Режим доступа.URL:https://ru.wikipedia.org/wiki/Информационная_модель(дата обращения: 16.09.2016).

ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ ТЕХНОЛОГИИ «ИСКУССТВЕННЫЙ НОС» В РАКЕТНО-КОСМИЧЕСКОЙ ОТРАСЛИ

Айкожаев Нурислам Муратович
студент, кафедра Б12-ИТИиУ, филиал «Восход» МАИ,
Республика Казахстан, г. Байконур
E-mail:nurislam.aykozhaev@mail.ru

Есеналиева Наргиз Айдаровна
студент, кафедра Б12-ИТИиУ, филиал «Восход» МАИ,
Республика Казахстан, г. Байконур

Жуматаева Жанат Есиркеповна
научный руководитель, к.т.н., кафедра Б12-ИТИиУ, филиал «Восход» МАИ,
Республика Казахстан, г. Байконур

Известный древнегреческий философ Аристотель первым выделил пять основных чувств человека: слух, зрение, обоняние, вкус и осязание. Чувство обоняния не считают одним из важнейших чувств, так как с помощью обоняния человек получает информацию небольшого размера. Тем не менее чувство запаха наиболее загадочное и непредсказуемое, так как тесно связано с психологическим аспектом восприятия окружающей среды.

Подобно вкусу, обоняние – химическое чувство, так как рецепторы тесно связаны с сигналами, поступающими от молекул. Когда молекулы, находящиеся в воздухе, попадают на носовые рецепторы, человек начинает чувствовать запах. Без нормального функционирования обонятельного аппарата человек перестает чувствовать ароматы большинства продуктов питания, и, следовательно, не может различить одни продукты питания от других.

Всем известно, что запах и вкус тесно связаны между собой. Обоняние и запах – это чувства гораздо более сложные и влияющие на жизнь людей в большей степени, чем считалось, и вероятно, что ученые, которые занимаются их исследованием, совершат много новых открытий.

Человеческий нос – объект изучения многих инженеров и ученых, которые пытаются понять, каким образом функционирует нос. Большой интерес

к обонянию человека возник вследствие новых открытий в сфере создания искусственного (электронного) носа.

Электронный нос – мультисенсорное цифровое устройство, которое предназначено для анализа воздушной среды посредством систематизации запахов. На сегодняшний день технология искусственного носа не может заменить обонятельную систему человека, но область использования этой технологии довольно обширна.

Обонятельная система человека обширно применяется в целях производства, например, для контроля разнообразных продуктов питания. Натренированный нос человека, тщательно исследовав запахи продуктов питания, таких, как зерно, мясо, молоко, алкоголь, может в дальнейшем установить их пригодность или непригодность. Таким же образом определяют перспективен ли тот или иной парфюмерный запах, находят поддельные косметические средства. Также запахи принимаются во внимание и докторами при определении некоторых болезней: брюшной тиф, золотуха, пневмония или диабет, вызывают специфичное дыхание или жидкие выделения с присущими запахами, которые могут быть замечены умелыми врачами.

Если искусственный интеллект электронного носа сможет различать запахи таким образом, то в этом случае электронный нос смог бы справится с той же работой, вдобавок значительно лучше.

Трудность заключается в том, что обонятельная система человека крайне субъективная: весьма часто разные люди по-разному чувствуют одинаковые запахи. Электронный нос устраняет эту трудность, бесспорно определяя некий «стандарт» для всех запахов, например точно устанавливая запах испорченного мяса.

На сегодняшний день различные макеты электронного носа уже массово используются в промышленности. Например, в агрокомплексе Швеции искусственный нос используется для независимого контроля качества зерна. Другие вариации электронного носа помогают контролировать испарения вредных для здоровья человека химических веществ.

Есть несколько причин, из-за которых применение искусственного носа более целесообразно, а именно:

- обнаружение различных составляющих носит объективный характер;
- вдыхание через нос токсичных веществ опасно для человека;
- обнаружение химических веществ, которые не имеют запаха (т.е. человеческий нос не в состоянии обнаружить их);
- способность действовать в условиях непригодных для функционирования человеческого носа.

Для понимания принципа действия электронного носа, необходимо уточнить, каким образом возникает запах: иногда его создает какое-либо одно химическое вещество, но чаще – комбинация множества различных химических компонент. Электронный нос должен реагировать на определенную концентрацию требуемых молекул и их комбинаций [1, с. 19].

Существуют два принципиально разных подхода к реализации электронного носа:

- с использованием методов газовой хроматографии и масс-спектрометрии;
- с использованием нейросетевых методов и алгоритмов [1, с. 19-20].

Хроматографы и масс-спектрометры являются электронным носом лишь частично, так как использование этих методов не даёт возможность регистрировать запахи, а лишь наличие различных химических компонент.

Применение нейросетевого подхода имеет свои преимущества, такие как:

- снижение стоимости, что является следствием замены редких и дорогостоящих сенсоров на мультисенсорную комбинацию;
- возможность обнаружения большего числа химических составляющих;
- снижение временных затрат.

Недостаток использования нейросетевых технологий заключается в том, что для нормального функционирования электронного носа необходимо настроить его на нужные запахи, т.е. предварительно обучить нейронную сеть.

В настоящее время без космической навигации, метеорологии, связи и космических технологий уже немыслимо существование человека.

Создаются новые космодромы, ракетно-космические комплексы, разрабатываются космические технологии.

На начальном этапе освоения космоса не изучались экологические проблемы региона, состояние экосистемы и ее устойчивость к антропогенным загрязнениям. В результате возникли регионы, где загрязнение среды, вызванное хозяйственной и космической деятельностью человека, превышает допустимые нормы и наносит непоправимый ущерб и биосфере, и почве, и, в конечном итоге, элементу этой биосферы – человеку. Как следствие, сократилась продолжительность жизни в загрязненных регионах, возросла частота сердечно-сосудистых и раковых заболеваний.

Ярким примером такого региона на территории Республики Казахстан является космодром Байконур.

Промышленное освоение этого региона, как хозяйственное, так и космическое привело к отчуждению и засорению обширных земельных площадей, при чем часть из них подвергается загрязнению токсичными компонентами ракетных топлив.

Пуски ракет-носителей приводят к значительному загрязнению озонового слоя атмосферы Земли и истощению ионосферы.

Наибольшую экологическую опасность представляют ситуации, связанные с аварийными проливами компонентов токсичных ракетных топлив.

Загрязненная почва может быть причиной заражения воды рек и открытых водоемов (озер, прудов) вследствие поступления космического ракетного топлива с талыми и ливневыми стоками, а также источником загрязнения трав, культурных растений, которые являются продуктами питания домашних животных и человека.

В районах аварийных проливов топлива, происходит испарение космического ракетного топлива. Высококипящие компоненты в газообразном или парообразном состоянии перемешиваются с воздухом и образуют облако,

которое распространяется по направлению ветра, образуя на своем пути очаг заражения.

При аварийном проливе ракетно-космического топлива на территории города Байконур, создаются межправительственные комиссии Республики Казахстан и Российской Федерации по ликвидации последствий аварии. Под совместным руководством этих двух стран осуществляется поиск, сбор и вывоз с мест падения фрагментов ракеты-носителя.

Таким образом, для анализа воздушной среды, воды и почвы при авариях ракеты-носителя может быть использована технология искусственного носа, которая облегчит работу межправительственных комиссий путем повышения точности исследований воздушной среды и снижения временных затрат на исследования. Также данная технология позволяет проводить исследования без участия человека.

Список литературы:

1. Круг П.Г. Нейронные сети и нейрокомпьютеры: Учебное пособие по курсу «Микропроцессоры». – М.: Издательство МЭИ, 2002. – 176 с.

ПРОЕКТИРОВАНИЕ ИНФОРМАЦИОННЫХ МОДЕЛЕЙ АИС ОТДЕЛА ИНФОРМАЦИОННОГО ОБЕСПЕЧЕНИЯ ШТАБА ПОЛИЦИИ

Айкожаев Нурислам Муратович
студент, кафедра Б12-ИТИиУ, филиал «Восход» МАИ,
Республика Казахстан, г.Байконур
E-mail:nurislam.aykozhaev@mail.ru

Шестопалова Ольга Львовна
научный руководитель, канд. техн. наук, доцент, декан факультета «Испытания летательных аппаратов», ИО зав. кафедрой «Информационные технологии испытаний и управления» филиала «Восход» МАИ,
Республика Казахстан, г. Байконур

Данная автоматизированная информационная система отдела информационного обеспечения (АИС ОИО) штаба полиции предназначена для внедрения в Управление министерства внутренних дел России. Пользователями системы будут сотрудники отдела информационного обеспечения штаба полиции [1].

Разработанные информационные модели АИС ОИО штаба полиции позволят более наглядно представить основные процессы, входные и выходные данные, необходимые для функционирования АИС ОИО штаба полиции.

Информационная модель – модель объекта, представленная в виде информации, описывающей существенные для данного рассмотрения параметры и переменные величины объекта, связи между ними, входы и выходы объекта и позволяющая путём подачи на модель информации об изменениях входных величин моделировать возможные состояния объекта [4].

Главная цель построения контекстной диаграммы заключается в том, чтобы сделать требования к АИС ОИО штаба полиции ясными и понятными на каждом уровне детализации, а также разбить эти требования на части с точно определенными отношениями между ними.

На рисунке 1 представлена контекстная диаграмма работы АИС ОИО штаба полиции, в которой определены входные и выходные потоки данных.

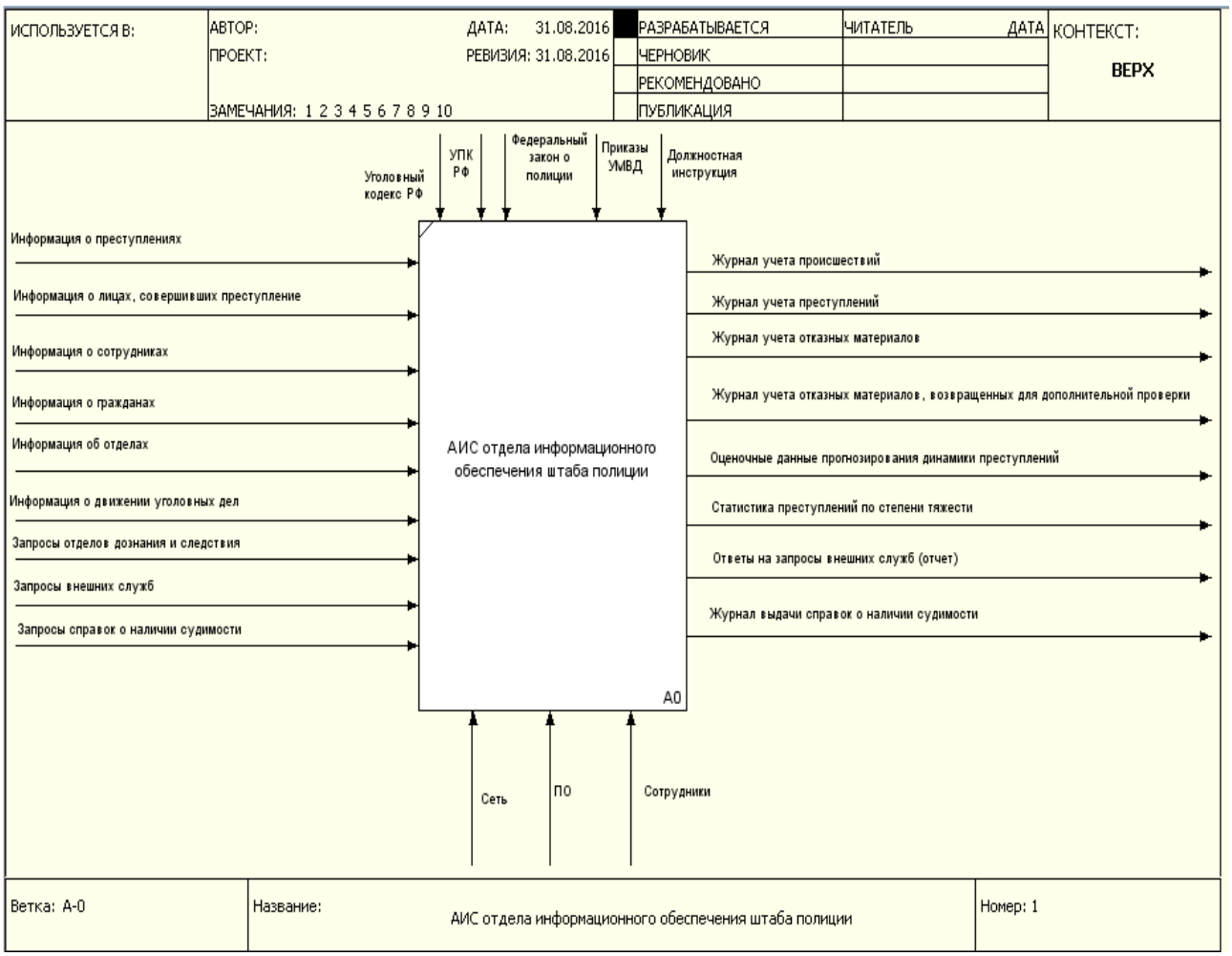

Рисунок 1. Контекстная диаграмма работы АИС ОИО штаба полиции

Входная информация:

- информация о преступлениях;
- информация о лицах, совершивших преступление;
- информация о сотрудниках;
- информация о гражданах;
- информация об отделах;
- информация о движении уголовных дел;
- запросы отделов дознания и следствия;
- запросы внешних служб;
- запросы справок о наличии судимости.

К выходным данным АИС ОИО штаба полиции относятся:

- журнал учета происшествий;

- журнал учета преступлений;
- журнал учета отказных материалов;
- журнал учета отказных материалов, возвращенных для дополнительной проверки;
- оценочные данные прогнозирования динамики преступлений;
- статистика преступлений по степени тяжести;
- ответы на запросы внешних служб (отчет);
- журнал выдачи справок о наличии судимости.

К управлению относится:

- Уголовный Кодекс РФ – основной источник уголовного права, однако по значимости главным источником уголовного права, как и всех других отраслей права, является Конституция Российской Федерации, в которой содержатся нормы, имеющие в том числе и уголовно-правовое значение [3];
- Уголовно-процессуальный кодекс РФ – это основополагающий нормативно-правовой акт в сфере уголовно-процессуального права, который устанавливает базисные принципы и порядок уголовного судопроизводства [2];
- Федеральный закон «О полиции»;
- Приказы УМВД;
- Должностная инструкция.

К механизму относится:

- сеть;
- программное обеспечение;
- сотрудники.

Следующим шагом после построения контекстной диаграммы является построение диаграммы нулевого уровня.

Изображение контекстной диаграммы нулевого уровня показано на рисунке 2.

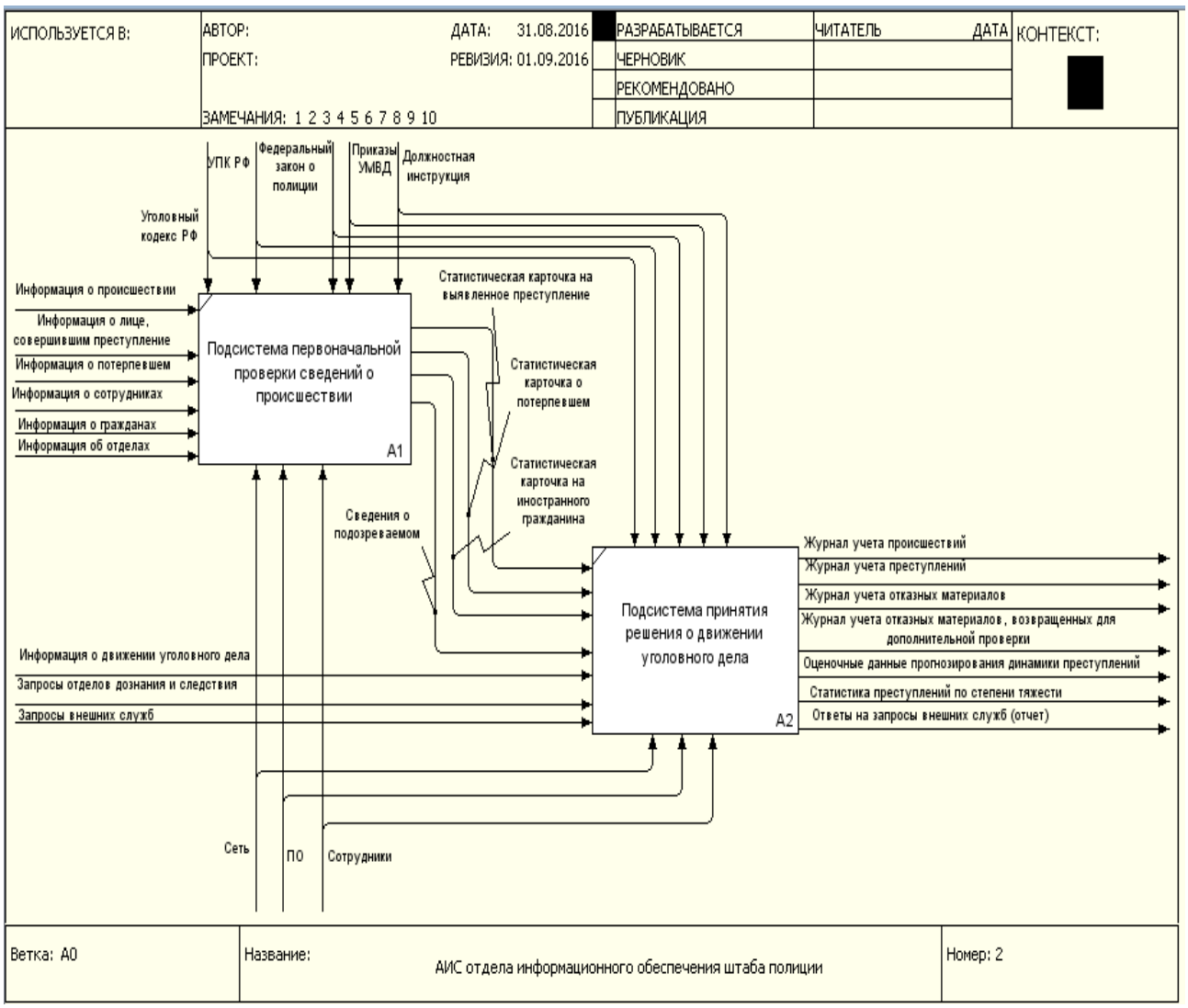

Рисунок 2. Диаграмма нулевого уровня АИС ОИО штаба полиции

Контекстная диаграмма нулевого уровня строится путем декомпозиции контекстной диаграммы нулевого уровня и содержит следующие подсистемы:

- подсистема первоначальной проверки сведений о происшествии;
- подсистема принятия решения о движении уголовного дела.

Данные процессы отражают основные направления деятельности отдела информационного обеспечения штаба полиции, автоматизированные в АИС ОИО штаба полиции.

Следующим шагом является построение диаграмм декомпозиции основных её процессов.

На рисунке 3 представлена декомпозиция блока А1 – «Подсистема первоначальной проверки сведений о происшествии».

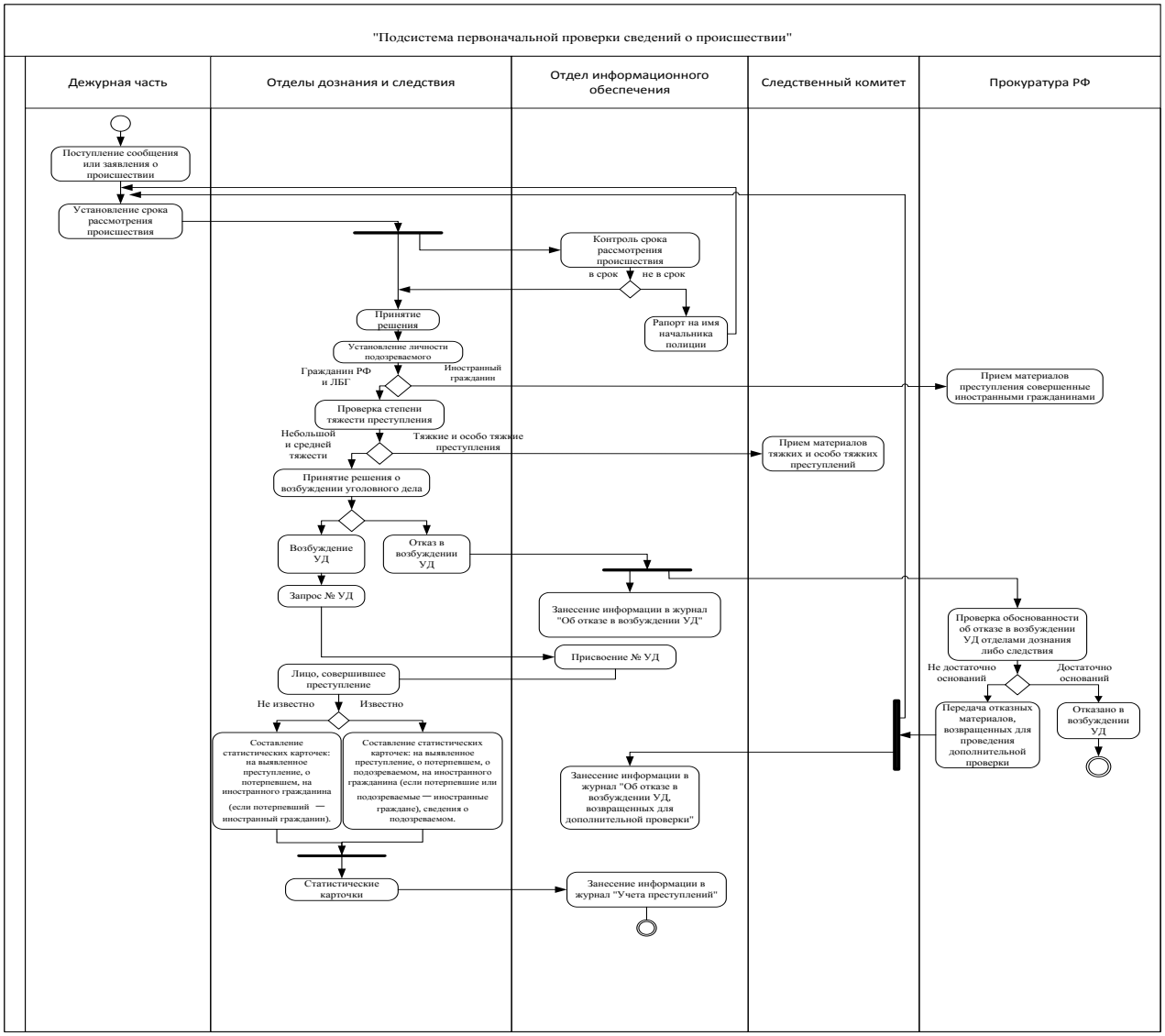

Рисунок 3. Декомпозиция «Подсистемы первоначальной проверки сведений о происшествии»

В подсистеме первоначальной проверки сведений о происшествии происходит установление срока рассмотрения происшествия начальником полиции или его заместителем и заносится в книгу учета происшествий. Далее отдел информационного обеспечения контролирует выставленный срок, при не соблюдении срока рассмотрения происшествия отделом дознания либо следствия, отдел информационного обеспечения пишет рапорт на имя начальника полиции. Если дело рассмотрено в выставленные сроки, происходит установление личности подозреваемого, если установлено, что подозреваемый гражданин иностранного государства, то дело передается в Прокуратуру РФ. В случае когда гражданин России и ЛБГ (лицо без

гражданства) дело рассматривается отделом дознания, либо следствия. Далее происходит проверка степени тяжести преступления, тяжкие и особо тяжкие преступления переходят в Прокуратуру РФ. Небольшой и средней тяжести рассматриваются отделами следствия и дознания. Следующим этапом является принятие решения о возбуждении уголовного дела. При отказе в возбуждении уголовного дела, отдел информационного обеспечения фиксирует информацию об отказе в возбуждении в журнале «Об отказе в возбуждении уголовного дела». Материалы преступления переходят в Прокуратуру, где происходит проверка обоснованности об отказе в возбуждении уголовного дела отделами дознания либо следствия. При не достаточных обоснованиях Прокуратура возвращает материалы преступления для дополнительной проверки, отдел информационного обеспечения заносит эти данные в журнал «Об отказе в возбуждении уголовного дела, возвращенных для проведения дополнительной проверки». При возбуждении уголовного дела, отделы дознания либо следствия делают запрос номера уголовного дела в отдел информационного обеспечения. Далее отделы дознания либо следствия выставляют статистические карточки, если лицо, совершившее преступление, не известно выставляются: статистическая карточка на выявленное преступление, статистическая карточка о потерпевшем и криминалистическая карта на иностранного гражданина (если потерпевший – гражданин другого государства). Иначе, если лицо совершившее преступление известно, составляются: статистическая карточка на выявленное преступление, статистическая карточка о потерпевшем, карточка на подозреваемого, криминалистическая карта на иностранного гражданина (если потерпевшие или подозреваемые иностранные граждане) и сведения о подозреваемом. Отдел информационного обеспечения заносит информацию со статистических карточек в журнал «Учета преступлений».

На рисунке 4 представлена декомпозиция блока А2 – «Подсистема принятия решения о движении уголовного дела».

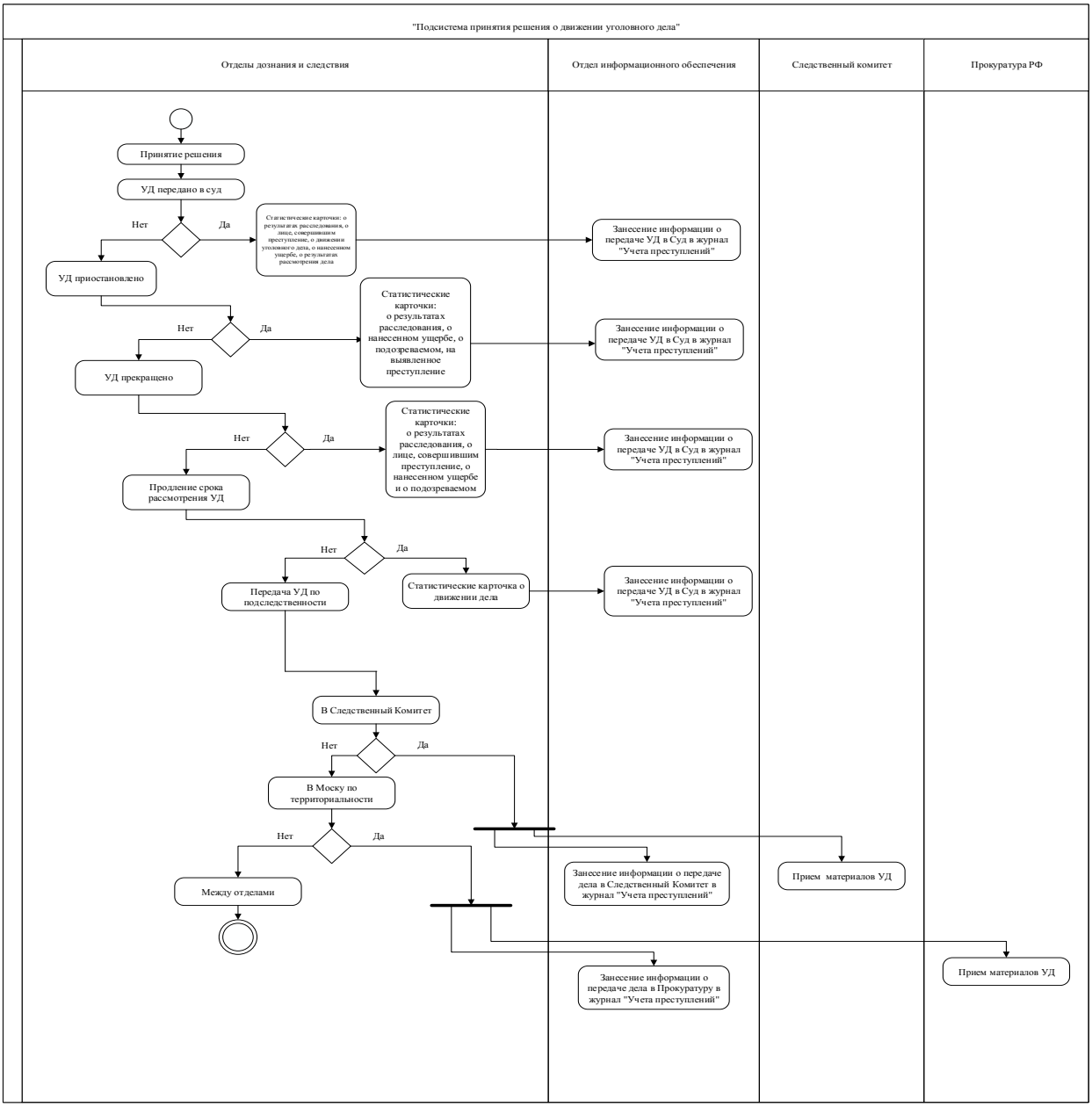

Рисунок 4. Декомпозиция «Подсистемы принятия решения о движении уголовного дела»

В подсистеме «Принятия решения о движении уголовного дела» уголовное дело может быть: передано в суд, приостановлено, прекращено, продлен срок рассмотрения и дело может быть передано по подследственности. При передаче дела в суд выставляются статистические карточки: о результатах расследования, о лице, совершившим преступление, о движении уголовного дела, о нанесенном ущербе, о результатах рассмотрения дела, информация заносится отделом информационного обеспечения в журнал «Учета преступлений». При приостановлении уголовного дела выставляются статистические карточки: о результатах расследования, о нанесенном ущербе, о подозреваемом,

на выявленное преступление (при переквалификации преступления), информация заносится отделом информационного обеспечения в журнал «Учета преступлений». При прекращении уголовного дела выставляются статистические карточки: о результатах расследования, о лице, совершившим преступление, о нанесенном ущербе и о подозреваемом, информация заносится отделом информационного обеспечения в журнал «Учета преступлений». При продлении срока рассмотрения уголовного дела выставляется карточка о движении дела, информация заносится в журнал «Учета преступлений». При передаче уголовного дела по подследственности дело может быть передано Следственный Комитет, в Москву по территориальности и между отделами. При передаче дела в Следственный Комитет материалы дела передаются в Следственный Комитет и заносится информация в журнал «Учета преступлений». При передаче дела по территориальности в Москву материалы дела передаются в Прокуратуру РФ и информация заносится в журнал «Учета преступлений». Уголовное дело может быть передано из отдела дознания в следственный отдел и наоборот.

Создание проектируемой системы обеспечит уменьшение трудоемкости работ выполняемых отделом информационного обеспечения, уменьшение времени обработки информации, уменьшение влияния «человеческого фактора» на весь процесс, уменьшение риска потери информации, уменьшение частоты появления ошибок, а также увеличение достоверности данных.

Список литературы:

1. Айкожаев Н.М. Математическая модель прогнозирования динамики преступлений: Международная научно-практическая конференция (Новосибирск, 26 июля 2016 г.). - С.1-5.
2. Последняя действующая редакция с комментариями: сайт – [Электронный ресурс] – Режим доступа. – URL: http://stupkrf.ru/ (дата обращения: 11.09.2016).
3. Электронная библиотека: сайт – [Электронный ресурс] – Режим доступа. – URL: http://www.bibliotekar.ru/ugolovnoe-pravo-4/7.htm (дата обращения: 11.09.2016).
4. Энциклопедия Википедия: сайт – [Электронный ресурс] – Режим доступа.URL:https://ru.wikipedia.org/wiki/Информационная_модель (дата обращения: 01.09.2016).

АНТИВИРУСЫ: АНАЛИЗ ПРОИЗВОДИТЕЛЬНОСТИ И ЭФФЕКТИВНОСТИ

Бурцев Игорь Алексеевич
студент предметно-цикловой комиссии естественно-научных и математических дисциплин,
РФ, Республика Калмыкия, г. Элиста

Кукаева Евгения Борисовна
научный руководитель, преподаватель предметно-цикловой комиссии естественно-научных и математических дисциплин, Калмыцкого филиала «Московского государственного гуманитарно-экономического университета»
РФ, Республика Калмыкия, г. Элиста
E-mail: evgenika_kykaeva@mail.ru

Быстродействие и ресурсоемкость антивируса для большинства пользователей являются одними из наиболее важных характеристик наряду с качеством самой защиты. На эти характеристики многие пользователи обращают внимание в первую очередь при выборе и покупке антивируса [1]. В ходе исследования проводилось тестирование. Цель тестирования - выявить, какие антивирусы наименее используют аппаратные ресурсы компьютера, и при этом достаточно эффективны [2]

Каждый день появляются тысячи новых вредоносных программ. Соответственно, ни один антивирус не способен гарантировать 100% защиту компьютера, поэтому у любого пользователя будет риск заражения даже с установленной антивирусной защитой. Помимо качественной защиты, на антивирус возлагается быстродействие и ресурсоемкость [3].

В процессе тестирования были измерены и сравнены параметры, которые влияют на восприятие пользователем скорости работы антивируса.

Исследование проводилось на базе Калмыцкого филиала «Московского государственно гуманитарно-экономического университета» с целью определения самого популярного антивируса был проведен опрос студентов и сотрудников филиала. По результатам опроса были выявлены наиболее популярные среди респондентов следующие антивирусные продукты от известных производителей:

1. Avast Internet Security
2. Avira Antivirus Premium
3. Kaspersky CRYSTAL 17.0.0.611
4. Dr.Web Security Space 11.0
5. ESET NOD32 SmartSecurity 9.0.377.1
6. Norton Internet Security

В ходе тестирования использовались только пробные версии, которые ограничены по времени использования. Тестирование антивирусных средств велось по следующим параметрам:

1. Объем установочного файла.
2. Время установки.
3. Время, загрузка ЦП и памяти при тестировании папки Windows.
4. Время, загрузка ЦП и памяти при тестировании папки с вирусами.
5. Количество идентифицированных вирусов и % срабатывания.
6. Простота установки и настройки.

Тестирование велось на двух платформах, имеющихся в филиале.

Характеристики платформ представлены в таблице 1.

Таблица 1.

Характеристики тестовых платформ

№	Компоненты	Платформа 1	Платформа 2
1	Процессор	Intel Celeron D 326 2,8 ГГц	Intel Celeron Dual Core E3300 2,5ГГц
2	Память (ОЗУ)	1 Гб	1Гб (2*512 Мб)
3	Видеокарта	GeForce 8600 GT 256 Мб	Inyel GMA (встроенная)
4	Жесткий диск	WD 500 Гб	500 Гб Seagate
5	ОС	Windows XP SP2	Windows 7

При тестировании на компьютерах были установлены стандартные программные пакеты. Процесс тестирования антивирусных средств занял несколько дней. Результаты перепроверялись и корректировались. Для выявления уровня загрузки оперативной памяти, файла подкачки, виртуальной памяти использовался программный пакет Everest Ultimate Edition 5.50 компании Lavalys Consulting Group.

Таблица 2.

Результаты тестирования антивирусов на платформе 1.

№	Антивирус/Тест		Avast Internet Security	Avira Antivirus Premium	Kaspersky CRYSTAL 17.0.0.611	Dr.Web Security Space 11.0	ESET NOD32 SmartSecurity	Norton Internet Security
1.	Объем установочного файла (Мб)		133,8	145	170,5	198,6	69,8	158,7
2.	Время установки (с)		135	455	148	233	55	137
3.	Загрузка	ОЗУ (Мб)	400	497	524	432	460	554
		Файл подкачки (Мб)	695	356	442	589	498	289
		Виртуальная память (Мб)	609	684	899	1025	819	688
4.	Тестирование антивирусом папки Windows	ОЗУ (Мб)	473	324	530	565	371	370
		Файл подкачки (Мб)	364	345	616	508	624	455
		Виртуальная память (Мб)	788	875	1281	897	694	1066
		ЦП (%)	43	58	73	100	35	53
		Затраченное время в сек.	186	255	128	446	342	125
5.	Время, загрузка ЦП и памяти при тестировании папаки с вирусами	ОЗУ (Мб)	344	528	535	332	434	627
		Файл подкачки (Мб)	309	542	639	332	236	420
		Виртуальная память (Мб)	753	1170	1374	764	770	1147
		ЦП (%)	44	40	48	100	80	50
		Затраченное время в сек.	3500	37	1340	76	1353	37
6.	Количество идент. вирусов		7155	6783	6884	7101	5608	4982
7.	Простота установки и настройки		1	2	2	3	4	3
	% срабатываний		98,4%	93,4%	94,6%	89,3%	72,3%	79,4%

Результаты тестирования на 2 платформе здесь не приведены – отличие только показателями, ввиду отличия аппаратных платформ. При тестировании учитывалась суммарная нагрузка антивирусного ПО на аппаратные ресурсы вместе с операционной системой и программным обеспечение. Выяснить нагрузку чисто антивируса было сложно, так как при запуске антивируса работало множество процессоров, принадлежащих антивирусу, поэтому было

легче посчитать суммарную нагрузку. Также учет суммарной нагрузки позволяет оценить в полной мере нагрузку на аппаратуру и учесть конечные параметры аппаратных средств.

Для тестирования папки с вирусами использовался набор с вирусами, общим количеством 7100 различных учебных вирусов. Перед копированием папки с вирусами, конечно же, отключалась антивирусная защита. Проникновение при этом вирусов в систему минимальны – в папке находились четыре архива с вирусами.

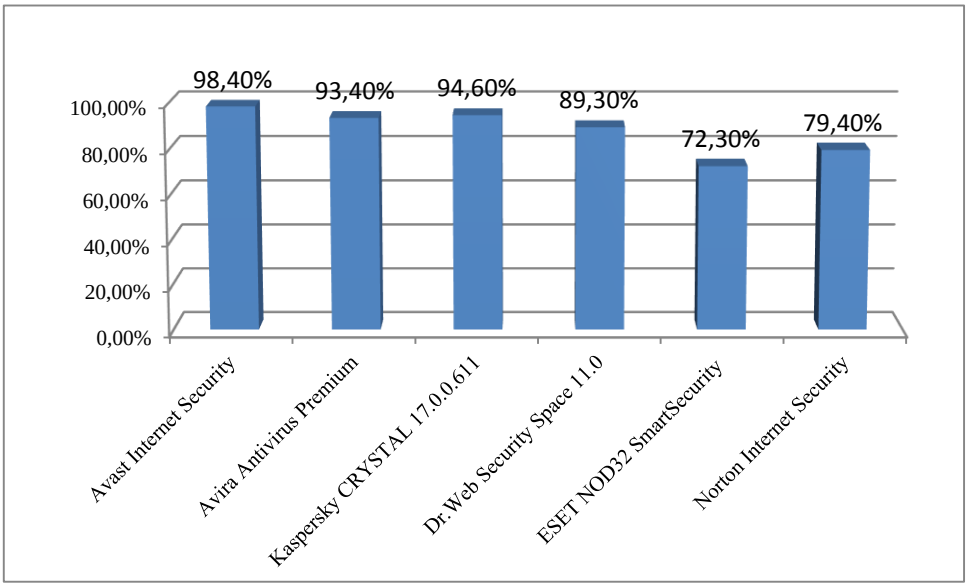

Диаграмма 1. %срабатывания угрозами

Из этой диаграммы видно, что наибольший процент срабатываний угроз антивирусных средств Avast Internet Security- 98,4%, наименьший у ESET NOD32 SmartSecurity-72,3%. Если говорить о количественно соотношении зафиксированных угроз, можно заключить, что наибольшее количество идентифицированных угроз наблюдается у Avast Internet Security-7155, наименьший у Norton Internet Security- 4982.

При тестировании антивирусом папки с вирусами, можно увидеть наименьшую нагрузку на ОЗУ демонстрирует Dr.Web Security Space 11.0- 332 Мб, а наибольшую- Norton Internet Security- 627 Мб.

Полученные в ходе тестирования результаты дают ясное представление об эффективности и быстродействии популярных на рынке антивирусных

продуктов, что важно для построения эффективной системы защиты информации.

Анализируя результаты тестирования можно сделать выводы: наиболее лучшие результаты показал антивирус Avast Internet Security, не считая длительности проверки.

Сравнивая результаты представленного теста с другими, любой пользователь компьютера может сделать рациональный выбор в пользу того или иного антивирусного обеспечения.

Список литературы:

1. Безмалый В.Ф. Угрозы домашнему компьютеру/ В. Безмалый // Журнал Компьютер Пресс.- №11.М.-2012.-125 с.
2. Грибков А., Багликов В. К вопросу обнаружения компьютерных атак и вредоносного заражения // Журнал "Information Security/ Информационная безопасность".- №5,М. - 2014.-135 с.
3. Лопатин, В.Н. Информационная безопасность России: Человек, общество, государство. Серия: Безопасность человека и общества. М.: 2013. - 428 с.

ПРОГНОЗИРОВАНИЕ ЭНЕРГОПОТРЕБЛЕНИЯ ПРЕДПРИЯТИЯ РАКЕТНО-КОСМИЧЕСКОЙ ОТРАСЛИ

Кириченко Юлия Николаевна
студент, кафедра Б12-ИТИиУ, филиал «Восход» МАИ,
Республика Казахстан, г. Байконур
E-mail:kiri4enko.uiliya@mail.ru

Шудабаева Арай Казымбековна
студент, кафедра Б12-ИТИиУ, филиал «Восход» МАИ,
Республика Казахстан, г. Байконур

Жуматаева Жанат Есиркеповна
научный руководитель, к.т.н., кафедра Б12-ИТИиУ, филиал «Восход» МАИ,
Республика Казахстан, г. Байконур

Данная работа посвящена проблеме прогнозирования энергопотребления на предприятии ракетно-космической отрасли. Целью прогнозирования является определение будущего объема энергопотребления, на основе которого затем составляется план закупа электроэнергии. В настоящее время процесс прогнозирования выполняется вслепую, без применения каких-либо математических методов. Применение математической модели позволит наиболее точно спрогнозировать, а, следовательно, запланировать объемы энергопотребления, что сократит расходы предприятия.

На сегодняшний день существует огромное количество методов прогнозирования. Наибольшей популярностью пользуются: метод экспертных оценок, экстраполяция, моделирование, экономическое прогнозирование, метод регрессионного анализа.

Основой метода экспертных оценок является профессиональный опыт одного или нескольких специалистов, осуществляющих прогноз. Достоинством данного метода является его простота, но в то же время, прогнозирование производится специалистом, который может неправильно понять вопросы.

Идея метода экстраполяции заключается в исследовании прошлых и настоящих тенденций развития предприятия с целью дальнейшего

их прогнозирования. Недостаток данного метода в том, что при большом объеме данных прогноз может быть ошибочным.

Суть регрессионного анализа заключается в определении связи между некоторой характеристикой Y наблюдаемого явления (объекта) и величинами $x_1, x_2, \ldots, x_n$, которые обуславливают изменения Y. Переменная Y называется зависимой переменной (результативным признаком), влияющие переменные $x_1, x_2, \ldots, x_n$ называются факторами (факторными признаками).

Различают линейную и нелинейную регрессии. В зависимости от числа взаимосвязанных признаков регрессия бывает парной и множественной. Если рассматривается связь между результативным и факторным признаками, то регрессия называется парной, в противном случае она называется множественной (многофакторной) регрессией.

Задачами регрессионного анализа являются: установление зависимости между признаками, составление уравнения регрессии и оценка его параметров.

Регрессионный анализ используется в основном при среднесрочном и долгосрочном прогнозировании.

При прогнозировании энергопотребления объектами предприятия ракетно-космической отрасли температура воздуха рассматривается как влияющий фактор. Следовательно, для прогнозирования будет использована парная регрессия.

Уравнение парной регрессии можно записать в следующем виде:

$$y = a_0 + a_1 x \tag{1}$$

Для оценки неизвестных параметров $a_1, a_2, \ldots, a_n$ используется метод наименьших квадратов. Данный метод основан на предположении о независимости наблюдений и нахождении параметров уравнения (a_0, a_1), при которых сумма квадратов отклонений фактических значений результативного признака от теоретических, полученных по выбранному уравнению регрессии, сводится к минимуму:

$$S = \sum_{i=1}^{n} (y_i - \bar{y}_x)^2 \rightarrow min \tag{2}$$

Для определения параметров линейной парной регрессии составляется система нормальных уравнений следующего вида:

$$\begin{cases} na_0 + a_1 \sum_{i=1}^{n} x_i = \sum_{i=1}^{n} y_i \\ a_0 \sum_{i=1}^{n} x_i + a_1 \sum_{i=1}^{n} {x_i}^2 = \sum_{i=1}^{n} x_i y_i \end{cases} \quad (3)$$

где n - объем исследуемой совокупности, a_0 – усредненное влияние неучтенных в уравнении факторных признаков на результативный признак, a_1 – коэффициент регрессии, который показывает, на сколько в среднем изменяется значение результативного признака при увеличении факторного признака на единицу собственного измерения [1].

Пусть имеются данные о среднемесячной температуре воздуха и об объеме энергопотреблении на объекте предприятия ракетно-космической отрасли за 2015 год (таблица 1).

Таблица 1.

Зависимость энергопотребления и температуры воздуха

Месяц	**Объем энергопотребления, (кВт·ч,Y_i)**	**Среднемесячная температура воздуха, (°C, X_i)**
Январь	51202	-6,8
Февраль	62179	-6,9
Март	50851	4,6
Апрель	56800	15,2
Май	44211	23,45
Июнь	42802	29,2
Июль	49713	29,85
Август	49376	28,6
Сентябрь	39276	21,1
Октябрь	46288	11,2
Ноябрь	44315	2,3
Декабрь	58454	-4
Всего	595467	147,8

Предполагается, что рассматриваемые признаки связаны линейно. Строится расчетная таблица для нахождения параметров линейного уравнения (1) объема энергопотребления (таблица 2).

Таблица 2.

Расчетная таблица для определения параметров линейного уравнения регрессии

Месяц	Объем энергопотребления (кВт·ч,Y_i)	Среднемесячная температура воздуха,(°С,X_i)	X^2	XY
Январь	51202	-6,8	46,24	-348174
Февраль	62179	-6,9	47,61	-429035
Март	50851	4,6	21,16	233914,6
Апрель	56800	15,2	231,04	863360
Май	44211	23,45	549,9025	1036748
Июнь	42802	29,2	852,64	1249818
Июль	49713	29,85	891,0225	1483933
Август	49376	28,6	817,96	1412154
Сентябрь	39276	21,1	445,21	828723,6
Октябрь	46288	11,2	125,44	518425,6
Ноябрь	44315	2,3	5,29	101924,5
Декабрь	58454	-4	16	-233816
Всего	595467	147,8	4049,515	6717977

На основе расчетов составляется система нормальных уравнений (4):

$$\begin{cases} 12a_0 + 147{,}8a_1 = 595467 \\ 147{,}8a_0 + 4049{,}515a_1 = 6717977 \end{cases} \quad (4)$$

Далее система уравнений (4) решается методом Гаусса, откуда a_0=53026,94, a_1= -276,43. Следовательно, уравнение (1) для прогнозирования энергопотребления предприятия ракетно-космической отрасли примет вид (5):

$$\bar{y}_x = 53026{,}94 - 276{,}43x \quad (5)$$

По значению коэффициента регрессии можно сделать вывод о том, что при увеличении среднемесячной температуры воздуха на 1°С, объем энергопотребления (кВт·ч) уменьшится в среднем на 276,43 кВт·ч.

Для сравнения фактических и теоретических значений результативного признака строится таблица 3.

Таблица 3.

Сравнение фактических и теоретических значений результативного признака

Месяц	Объем энергопотребления (кВт·ч,Y_i)	Среднемесячная температура воздуха, (°C, X_i)	$\bar{y}_x$
Январь	51202	-6,8	54906,66
Февраль	62179	-6,9	54934,31
Март	50851	4,6	51755,36
Апрель	56800	15,2	48825,2
Май	44211	23,45	46544,66
Июнь	42802	29,2	44955,18
Июль	49713	29,85	44775,5
Август	49376	28,6	45121,04
Сентябрь	39276	21,1	47194,27
Октябрь	46288	11,2	49930,92
Ноябрь	44315	2,3	52391,15
Декабрь	58454	-4	54132,66
Всего	595467	147,8	595466,9

По полученным данным для наглядности строятся графики, представленные на рисунке 1.

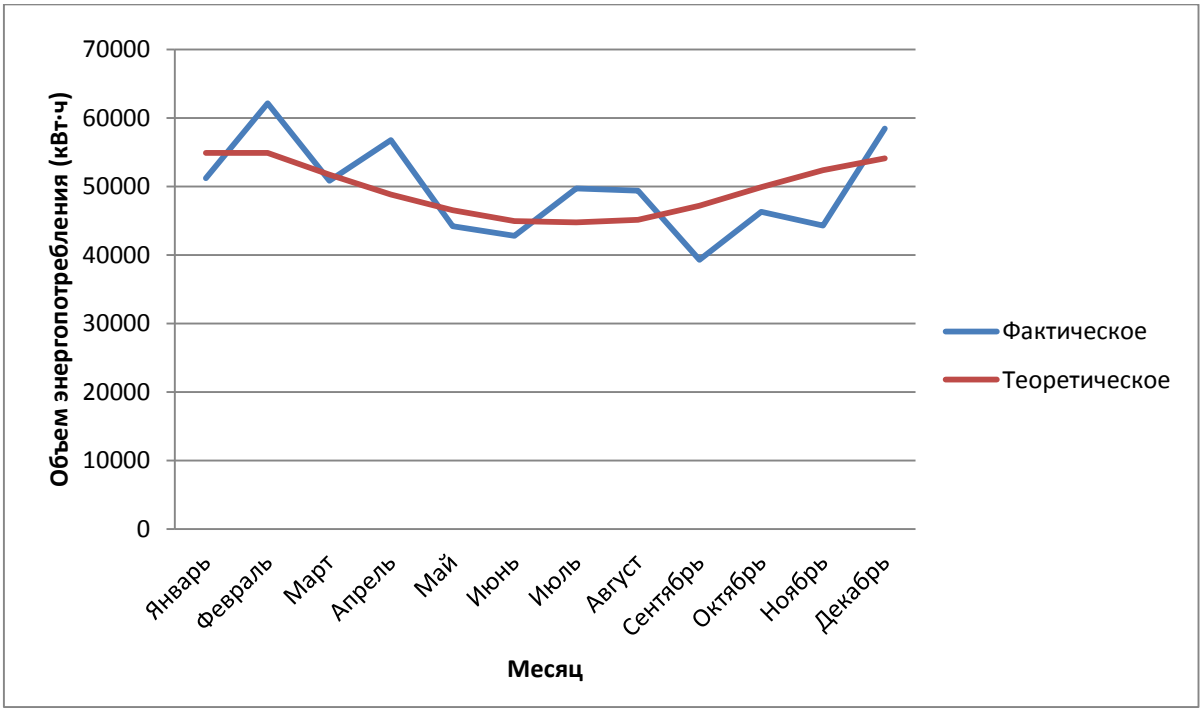

Рисунок 1. Сравнение фактических и теоретических значений результативного признака

Исходя из полученных результатов, можно сделать вывод о том, что теоретические значения результативного признака близки к фактическим, следовательно, полученное уравнение (5) можно использовать для расчета планируемого объема энергопотребления, но для того, чтобы добиться большей точности, можно, помимо температуры, учитывать и другие факторы: сезонность, влажность, освещенность и т.д.

В целом, полученные результаты оправдали ожидания.

Список литературы:

1. Минашкин В.Г., Шмойлова Р.А., Садовникова Н.А., Моисейкина Л.Г., Рыбакова Е.С. ТЕОРИЯ СТАТИСТИКИ: Учебно-методический комплекс. – М.: Изд. Центр ЕАОИ. 2008. – 296 с.

ПЕРСПЕКТИВЫ РАЗВИТИЯ МОБИЛЬНЫХ СЕТЕЙ ПЯТОГО ПОКОЛЕНИЯ 5G

Дмитриев Егор Андреевич
студент, факультет информатики СНИУ им. Королёва,
РФ, г. Самара
E-mail: pritstant@yandex.ru

Танаев Иван Владимирович
студент, факультет информатики СНИУ им. Королёва,
РФ, г. Самара
E-mail: killabeeez@mail.ru

Швейкин Владислав Витальевич
студент, факультет информатики СНИУ им. Королёва,
РФ, г. Самара
E-mail: xelle163@gmail.com

Завгородний Станислав Дмитриевич
студент, факультет информатики СНИУ им. Королёва,
РФ, г. Самара
E-mail: stas1885@mail.ru

Введение

Общение между людьми всегда было очень важным. Если при встрече двух человек им достаточно использование только их голоса, то при удалении на большое расстояние появляется необходимость использования специальных устройств.

Так в 1876 году был изобретен телефонный аппарат Александром Бэллом, что позволило вести удаленное общение, но накладывало необходимость нахождения рядом со стационарным телефоном. Более 100 лет единственной возможностью организации телефонной связи для обычных людей являлись проводные линии.

Для большей мобильности в координировании спецслужб многие страны вели разработку систем радиосвязи, которые не зависели от проводов. Впоследствии эти наработки перекочевали в повседневную жизнь.

На данный момент развитие мобильной связи включает в себя 4 поколения: 1G, 2G, 3G, 4G. Причем стандарты поколений делятся на аналоговые (сети 1G) и цифровые (сети 2G, 3G и 4G).

Сейчас ведутся активные разработки в области создания новой сети пятого поколения 5G.

Возможности применения сети 5G

Ожидается создание новых сервисов в IT-сфере, телекоммуникаций, автомобильной индустрии, образования и многих других секторах за счет подключения через 5G сети множества устройств, устанавливающих миллиарды соединений. Кроме того, пятое поколение мобильной сети позволит улучшить качество работы уже функционирующих сервисов, в которых используются большие объемы трафика.

Помимо планшетов и смартфонов в сетях пятого поколения появятся автомобили, камеры видеонаблюдения, телевизоры, метеорологические датчики, датчики "умных" электрических сетей и т д.

Рисунок 1. Иллюстрация разнообразных объектов, подключенных к беспроводной сети 5G

Появление в повседневной жизни сетей пятого поколения позволит вывести приложения дополненной и виртуальной реальности на новый уровень. Так в образовательных целях можно будет создавать виртуальны модели вселенной или музеи прямо в школах и университетах.

Применение сети 5G найдут и в транспортной области. Оснастив автомобили сенсорами для считывания всевозможной информации о ситуациях на дороге: рядом расположенных автомобилей, метеорологических условий, знаков дорожного движения, состояния асфальтового покрытия, управление транспортным средством можно будет перевести в полностью автоматический режим.

Рисунок 2. Будущее взаимодействие автомобилей

Помимо комфорта вождения откроются также новые возможности для обеспечения безопасности на дорогах на более высоком уровне. Например, если автомобиль совершает экстренное торможения, то он посылает сообщение другим участникам дорожного движения. Получив данное уведомление, они в свою очередь в автоматическом режиме совершают так же торможение или перестраиваются в свободную полосу во избежание столкновения.

Архитектура сетей 5G

Многие эксперты считают, что сети пятого поколения 5G будут не "сота-ориентированными", а "устройство-ориентированными". При сотовой связи операторская сеть состоит из сот - базовых станций, которые обеспечивают связь некотором радиусе охвата. Устройство, которое находится внутри этого радиуса действия, создает исходящие и нисходящие каналы свзяи, а также контролирует соединение и объем трафика. Базовая станция в свою очередь управляет самой сотой, внутри которой находятся устройства абонентов.

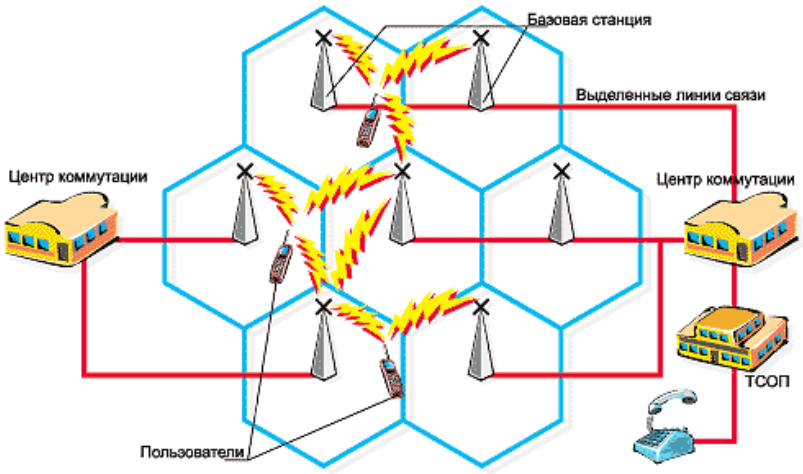

Рисунок 3. Иллюстрация сотовой сети

В сетях 5G обмен между устройствами будет осуществляться одновременно множественными потоками информации с узлами различных типов. Их задача будет заключаться в обслуживании этих устройств в определенные моменты.

В "устройство-ориентированных" сетях устройства будут обмениваться напрямую между собой, а через ядро 5G сети будет проходить только сигнальный трафик.

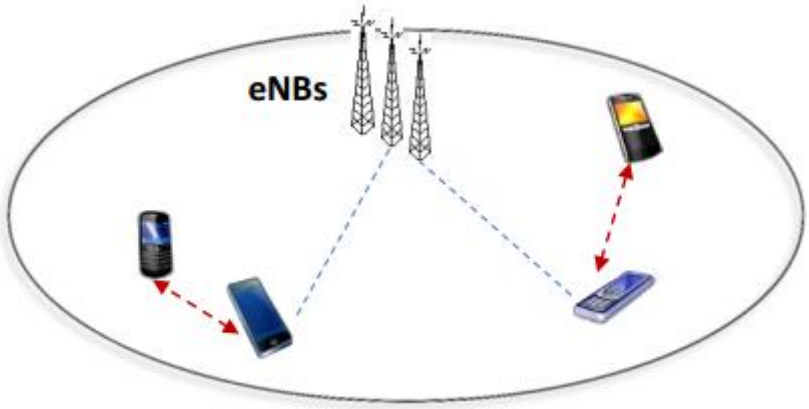

Рисунок 4. Иллюстрация "устройство-ориентированной" сети

Благодаря такой технологии появится уникальная возможность переносить передачу данных в нелицензируемую область спектра для дополнительной разгрузки сети.

Предположительные сроки запуска

Ожидается, что сети пятого поколения для коммерческого использования появится уже в 2020 году, если будут выделены необходимые спектры частот. При этом начать тестирование первых в мире 5G сетей операторы смогут в крупных городах уже в 2018-2019 годах, как только появится необходимое оборудование.

Список литературы:

1. METIS Deliverable D 2.4, “Proposed solutions for new radio access”, 28 February 2015
2. METIS Deliverable D 8.4, “METIS final project report”, 30 April 2015

ОБЗОР УГРОЗ И ТЕХНОЛОГИЙ ЗАЩИТЫ WI-FI СЕТЕЙ

Федоров Сергей Александрович
студент, кафедра ИБСиТ ИСТиД (филиала) СКФУ,
РФ, г. Пятигорск
E–mail: sergio26russian@yandex.ru

Битюцкая Наталья Ивановна
научный руководитель, канд. физико-математических наук
доцент кафедры ИБСиТ ИСТиД (филиала) СКФУ,
РФ, г. Пятигорск

С появлением в современном мире компактных устройств для работы в Интернете перед разработчиками встала новая задача - обеспечить доступ к сети в местах, находящихся на удаленном расстоянии от кабельного интернета. Именно так и появились сети, работающие по радиоканалу и позволяющие людям посетить различные сетевые ресурсы при использовании карманных персональных компьютеров (далее КПК).

Беспроводные сети являются новым шагом в развитии технических средств доступа к сети. Их развитие продолжается и в настоящее время. Согласно исследованию американской организации Juniper Research, проведенному в 2015 году: «Все большая доля мобильного трафика со смартфонов и планшетов будет передаваться не через сети 2G/3G/4G, а именно через Wi-Fi. В течение четырех ближайших лет у сотовых операторов во всем мире останется лишь 40% трафика. А к 2020 году ожидается увеличение объема передачи данных по сетям 802.11 с 30 000 петабайт до 115 000 петабайт. Такая тенденция будет активнее реализовываться на территории Северной Америки и Европы» [15].

На основе таких исследований можно сделать вывод, что увеличение, как охвата сетей, так и количества пользователей, требует достаточно серьезных вложений в защиту Wi-Fi комплексов.

В качестве основы Wi-Fi сетей лежит группа международных стандартов семейства IEEE 802, которые регулируют работу локальных вычислительных сетей (далее LAN) и сетей, расположенных в мегаполисах (далее MAN).

Службы и протоколы данного семейства стандартов работают на двух нижних уровнях семиуровневой сетевой модели OSI: канальном и физическом.

Физический уровень определяет метод передачи данных, которые представлены в виде двоичных комбинаций, от одного устройства к другому.

Канальный уровень предназначен для обеспечения взаимодействия сетей на физическом уровне и применения способов контроля над возникающими ошибками. Согласно спецификации IEEE 802 данный уровень разделен на два подуровня: MAC (англ. Media Access control) и LLC (logical link control).

Основным стандартом, управляющим Wi-Fi сетями, является IEEE 802.11, в который входят дополнительные стандарты, представленные таблице 1.

Таблица 1.

Стандарты беспроводной связи Wi-Fi [1-7]

№ п/п	Название стандарта	Скорость передачи данных Мб/с	Частота передачи сигнала (Ггц)	Год принятия стандарта	Примечание
1	2	3	4	5	6
1	IEEE 802.11	2	2,4	1997	Первый стандарт
2	IEEE 802.11a	54	5	1999	Первые рабочие продукты выпущены в 2001 году. Теоретическая разработка
3	IEEE 802.11b	11	5.4	1999	Изменен способ поддержки частоты (в сравнении с первоначальным стандартом)
4	IEEE 802.11c	54	5,4	2001	Изменена работа с мостами
5	IEEE 802.11d	54	5,4	2001	Используется только для роуминга
6	IEEE 802.11e	54	5,4	2005	Улучшен пакетный режим
7	IEEE 802.11g	54	5,4	2003	В качестве замены 802.11b
8	IEEE 802.11h	54	5	2004	Создан для работы в Европе
9	IEEE 802.11i	54	5-5.5	2005	Новый тип защиты от несанкционированного доступа, названный WPA
10	IEEE 802.11j	54	5	2005	Предназначен для работы в Японии
11	IEEE 802.11n	600	2.5-5	2009	Совместим с a/b/g
12	IEEE 802.11p	54	2.6-3.7	2008	Предназначен для использования транспортными средствами
13	IEEE 802.11t	54	2.5-5.5	2007	Используется для тестирования

14	IEEE 802.11w	54	2.5-5.5	2011	Защищает от редактирования фреймы
15	IEEE 802.11y	54	3.65-3.7	2012	Работает в радиусе 5 км
16	IEEE 802.11ac	От 433 до 6770	5	2014	Новейший стандарт совместим с IEEE 802.11n
17	IEEE 802.11ad	До 7000	60	2016	Находится в разработке

Но прежде чем создавать систему защиты информации в Wi-Fi сетях, нужно получить представление о самом нарушителе. Чтобы понять это, необходимо составить потенциальную модель нарушителя.

Нарушителей принято подразделять на три основные категории:

1. *Любопытные*. Они выполняют взлом ради своего самоутверждения или забавы. Большинство из них не представляют серьезной угрозы безопасности сети, а некоторые могут даже сообщить администратору о найденных ими уязвимостях. Эти люди при должном внимании к своим навыкам и умениям смогут вырасти в неплохих специалистов по информационной безопасности.

2. *Охотники за каналами связи*. Эти люди представляют несколько другую когорту участников информационного обмена. Интерес этих лиц направлен на попытку пользования чужими сетями для передачи различного контента в сеть. Чаще всего данные имеют не совсем законный характер. Согласно международному законодательству любая попытка проникновения в чужую сеть имеет за собой серьезные последствия вплоть до тюремного заключения.

3. *Преступники*. Третья категория самая опасная. Её представители умеют и знают, каким образом лучше всего осуществить подобный взлом. Их беспроводные сети привлекают анонимностью, наличием внеполосных каналов доступа. В компании, имеющей большое количество устройств, подключенных к сети, очень сложно отследить, через какое устройство произошла передача данных. Самые сильные атаки они совершают группой лиц, имеющих довольно хорошее образование в области компьютерных технологий и не понаслышке знакомых с принципами радиофизики [9].

Для создания системы защиты Wi-Fi сетей необходимо иметь представление о различных видах атак, которые могут применяться нарушителями.

Атакой на систему называется действие или совокупность действий злоумышленника, направленных на получение доступа к информационной системе [13].

Для удобства понимания сути атак их обычно объединяют в различные группы, исходя из общих свойств:

1. Атака на настройки параметров канального уровня в сетях 802.11.

Одна из таких атак - атака на настройку режима экономии энергии. Злоумышленник подменяет устройство клиента, которое находится в состоянии так называемого «спящего» режима, осуществляя сбор кадров. После того как клиент примет кадры, точка доступа очистит буфер и, таким образом, клиент не получит своих кадров. Этот способ реализации, но уже с подделкой кадров осуществляется при применении карты индикации трафика, которая сообщит клиенту об отсутствии новых пакетов. Такая атака сложна в реализации из-за выполнения операции по перекрытию доступа настоящих TIM кадров к атакуемым хостам [14].

2. DoS атаки.

Применяются в качестве одного из способов проникновения в сеть. Из-за физической природы радиоволн, как средства передачи информации, и конструктивных особенностей протоколов IEEE 802.11 они не могут быть защищены от атак на физическом уровне. Такие атаки в свою очередь подразделяются на несколько видов:

- *Атака на физический уровень* (глушение) – такая операция приводится в исполнение при помощи специально сконструированного передатчика или беспроводной карты, которые забивают канал связи несанкционированным трафиком. Основной недостаток такой операции в обязательном требовании к расположению передатчика в непосредственной близости к атакуемой сети.

- *Затопление сеанса связи поддельными фреймами* - такая атака, как и глушение, практически неотразима. В отличие от предыдущего вида атак, здесь помимо аппаратной части присутствует программная, представленная программой Vodill.Эта программа как раз и генерирует фальшивые фреймы, отправляя их через основной передатчик [11].
- *Атака при помощи неправильно сформированных кадров аутентификации* - в этом случае злоумышленник посылает кадры с запросом на аутентификацию, причем в самом кадре записаны адрес точки, адрес клиента и неизвестный для такой точки доступа алгоритм аутентификации. В результате точка доступа может выдать сообщение: «Получен кадр аутентификации с неожиданным номером транзакции». В результате этого соединение прерывается.
- *Заполнение буфера точки доступа*.
- *Чрезмерное количество запросов на соединение*. Такая операция может происходить в случае постоянного изменения MAC адресов подключаемого устройства.
- *Атака путем удаления кадров.*
- *Изменение контрольной суммы избыточного кода* (далее CRC32) заставляет точку доступа отвергнуть запрос на подключение. Осуществление атаки возможно лишь в случаях отправления искаженного кадра одновременно с настоящим отправителем или же в тот момент, когда абонент отправляет последние четыре байта кадра, запустить шумовые помехи. Защита от такой атаки довольно проблематична [12].
- *DoS-атака, основанная на циклическом переборе идентификаторов EAP*. Extensible Authentication Protocol (далее EAP, расширяемый протокол аутентификации) используется в популярных механизмах аутентификации WPA и WPA2PSK. Идентификатор EAP, который имеет диапазон (0-255), должен быть уникален только в пределах одного порта, но некоторые точки доступа могут отказывать новым абонентам в возможности подключения [14].

3. Атаки на систему аутентификации.

Атака на фильтрацию MAC–адресов. Для совершения такой атаки требуются следующие действия по анализу сетевого трафика для поиска MAC–адресов: проверка наличия в сети выбранного хоста и ожидание его выхода из сети. Иногда допускается и нахождение в одной сети с клиентом, чей адрес используется, в таком случае требуется отключить протокол ARP (протокол определения адреса) и отказаться от использования межсетевого экрана. Необходимо также производить наблюдение за отправлением пакетов с этого хоста и сообщений об отсутствии доступа к порту по протоколу ICMP (протокол контроля сообщений), чтобы избежать срабатывания системы IDS (система обнаружения вторжений). Иногда злоумышленник может отключить атакуемый хост, применяя способ подмены своего MAC–адреса на адрес атакуемого хоста.

Рассмотрим основные способы защиты от вторжений в сетях IEEE802.11. Не существует систем абсолютной защиты Wi-Fi сетей. Для обеспечения безопасности в таких сетях нужно принимать следующие меры:

- уменьшить зону радиопокрытия (правильно, если сигнал не будет выходить за пределы контролируемой зоны);
- установить новый пароль администратора (отличный от установленного по умолчанию);
- включить фильтрацию по MAC–адресам;
- изменить стандартный идентификатор сети (SSID) и периодически его изменять;
- активизировать внутрисетевое шифрование;
- изменять в установленные сроки ключи шифрования;
- установить межсетевые экраны и антивирусы;
- обеспечить реализацию алгоритмов фильтрации трафика на межсетевых экранах;
- учредить специальную схему резервирования оборудования и резервного копирования программного обеспечения, установленного в сети;

- производить периодический контроль за оборудованием, работающим в сети.

Все эти меры должны быть описаны в политике безопасности предприятия и иметь возможность реализации на оборудовании любого типа (сейчас реализация данных требований возможна практически на всех устройствах).

В данной статье рассмотрены различные угрозы информационной безопасности беспроводных сетей IEEE 802.11 и способы защиты от них. Некоторые из видов атак до сих пор не имеют качественного способа противодействия. В недалеком будущем, скорее всего, появятся новые стандарты безопасности для Wi-Fi сетей, которые позволят поднять общую планку безопасности [14].

Список литературы:

1. 802.11-1999 - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications.
2. 802.11a-1999 - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: High-speed Physical Layer in the 5 GHz Band.
3. 802.11b-1999 - Part 11: WLAN MAC and PHY specifications: Higher-Speed Physical Layer Extension in the 2.4 GHz Band.
4. 802.11b-1999_Cor1-2001 - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications. Amendment 2: Higher-speed Physical Layer (PHY) extension in the 2.4 GHz band — Corrigendum 1.
5. 802.11d-2001 - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications. Amendment 3: Specification for operation in additional regulatory domains.
6. 802.11F-2003 - IEEE Trial-Use Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11™ Operation.
7. 802.11g-2003 - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 4: Further Higher Data Rate Extension in the 2.4 GHz Band.
8. Вишневский В.М., Ляхов А.И., Портной С.Л. и др. Широкополосные беспроводные сети передачи информации. - М.: Техно сфера, 2005. - 592 с.
9. Владимиров А.А. Wi-фу: «боевые» приемы взлома и защиты беспроводных сетей. - М.: НТ-Пресс, 2005. - 463 с.

10. Лукацкий А.В. Обнаружение атак. - СПб.: БХВ-Петербург, 2001. - 367 с.
11. Мерит М., Полино Д. Безопасность беспроводных сетей./ Пер. с англ. А.В.Семенова. - М.: Компания АйТи, ДМК Пресс, 2004. - 288 с.
12. Педжман Р., Лиери Д. Основы построения беспроводных локальных сетей стандарта 802.11. - М: Вильямс, 2004. - 294 с.
13. Приходько А.Я. Словарь-справочник по информационной безопасности. - М.: Синтег, 2001. - 124 с.
14. Щербаков В.Б., Ермаков С.А. Безопасность беспроводный сетей: стандарт IEEE 802.11. - М: РадиоСофт, 2010. - 255 с.
15. Wi-Fi to Carry up to 60% of mobile traffic by 2019// Hamphir UK.–2015– [Эл. ресурс] – Режим доступа. – URL: http://www.juniperresearch.com/press/press-releases/wifi-to-carry-60pc-of-mobile-data-traffic-by-2019 (дата обращения 15.09.2016)

РАЗРАБОТКА WEB-ПРИЛОЖЕНИЯ ДЛЯ УЧЕТА ВЫПУСКНИКОВ ТЕХНИКУМА

Щелканов Константин Олегович
студент техникума информационных технологий, экономики и права Кемеровского института (филиала) РЭУ им. Г.В. Плеханова, РФ, г. Кемерово
E-mail: kschelkanov@icloud.com

Валеев Михаил Владимирович
научный руководитель, преподаватель Техникума информационных технологий, экономики и права Кемеровского института (филиала) РЭУ им. Г.В. Плеханова, РФ, г. Кемерово

Учебное заведение в сегодняшние дни – это сложный учебно-хозяйственный комплекс с многочисленными внешними и внутренними связями. И управление техникумом, его информационными потоками, учебным процессом, документооборотом и прочими процессами представляет собой сложную систему, мелкие и крупные задачи которой тесно связаны между собой.

Наиболее трудоемкими являются процессы, связанные с обработкой документов – сбор, накопление, преобразование, отображение, хранение, передача и вывод. Ускорить данные процессы и облегчить труд персонала и сотрудников техникума позволяют автоматизированные электронные системы. Практически все современные виды деятельности немыслимы без использования современных информационных средств и компьютерных технологий.

Основная цель функционирования учебной части – удовлетворение потребностей в обучении или повышении квалификации с использованием новых образовательных технологий и качественного обеспечения учебного процесса. Предметом деятельности учебной части является:

- осуществление образовательного процесса;
- формирование отчетности;
- проведение различных работ;

- осуществление контроля над учебным процессом.

Проанализировав работу учебной части, удалось выявить, что информация о выпускниках хранится в неудобном и разрозненном виде. В связи с этим появилась необходимость автоматизации этого процесса. Было принято решение о разработке и внедрении нового WEB-приложения, подходящего под конкретную область применения.

Выделим «узкие» места, которые необходимо устранить в дальнейшем:

- хранение информации о выпускниках в бумажном виде;
- сложный процесс обработки данных о выпускниках;
- потеря информации о выпускниках;
- создание ошибочных дубликатов информации о выпускниках;
- увеличение времени на поиск конкретных сведений о выпускниках.

Используя методику, определим, какие объекты и процессы будут принадлежать предметной области. Проект будет внутренним и частично внешним: обмен информацией и документами происходит между сотрудниками учебной части, часть информации доступна сторонним пользователям. Проект будет автоматизировать процесс учета выпускников техникума. Проект будет предназначен для сотрудников учебной части и сторонних посетителей (например, выпускников техникума или просто других заинтересованных лиц). Проект предназначен для следующих действий: представления информации о выпускниках всех выпусков по образовательному направлению техникума в удобной форме для всех пользователей, предоставлять возможность связи для выпускников. Проект не будет учебным, не будет интегрирован с другими системами, так же он не будет внедрен в других подразделениях техникума.

Одной из задач учебной части является взаимодействие с выпускниками. Необходимо сохранять и поддерживать в актуальном виде информацию о выпускниках, которую можно условно разбить на следующие группы (рисунок 1):

- Личная информация;

- Контактная информация;
- Информация об образовании, полученном в техникуме;
- Информация об образовании в других учебных организациях;
- Информация о карьере.

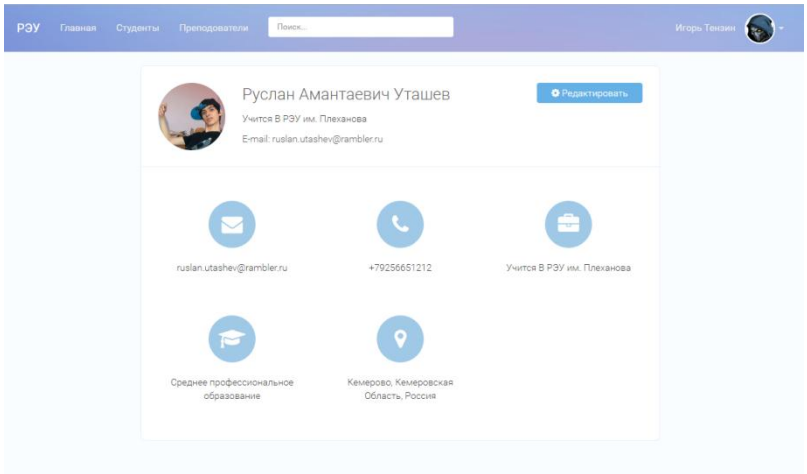

Рисунок 1. Информация о выпускниках техникума

Благодаря информационным технологиям, информацию о выпускниках можно хранить в электронном виде. В отличие от существующего на данный момент, бумажного – это позволит не только отображать данные из базы данных, но и редактировать их, систематизировать и создавать различные отчётные документы о выпускниках. Кроме того, это позволить осуществлять быстрый поиск по базе данных и создавать отчеты при помощи конструктора, которые упростят работу и сократят затрачиваемое на это время.

После рассмотрения имеющихся готовых решений, было принято решение о разработке и внедрении нового WEB-приложения, подходящего под конкретную область применения. Преимущества WEB -приложения:

- централизованное хранение данных;
- отсутствие специальных требований к аппаратной платформе;
- мобильность и удаленная работа;
- контроль и отчетность исполнения;
- кроссплатформенность.

WEB-приложение позволит:

- оперативно обновлять информацию о выпускниках;

- сократить время на поиск и обработку информации;
- установить связи с выпускниками университета;
- привлечь выпускников к участию в проф. ориентационной работе;
- сократить случаи потери информации;
- избежать создания дубликатов;
- позволит искать конкретную информацию в базе данных;
- сократить материальные затраты учебной части;
- сократить временные затраты учебной части;
- автоматизировать составление отчетности;
- получать быстрый доступ ко всей информации, хранящейся на сервере.

WEB -приложение предназначено для повышения оперативности и качества работы учебной части. Основным назначением WEB-приложения является организация работы с информацией и данными о выпускниках техникума. В рамках использования WEB-приложения на данный момент автоматизируются следующие процессы (рисунок 2):

- добавление информации о выпускнике;
- редактирование информации о выпускнике;
- удаление информации о выпускнике;
- поиск выпускников;
- добавление информации о группе;
- редактирование информации о группе;
- удаление информации о группе;
- поиск групп;
- добавление информации о мероприятиях;
- редактирование информации о мероприятиях;
- удаление информации о мероприятиях;
- просмотр участников мероприятий;
- запись на участие в мероприятиях;
- поиск мероприятий;

- получение сообщений обратной связи;
- поиск сообщений;
- приглашение новых пользователей;
- регистрация новых пользователей;
- удаление пользователей;
- блокирование/ разблокирование пользователей;
- редактирование личной информации пользователя;
- поиск пользователей;
- получение отчетных документов;
- сортировка результатов поиска.

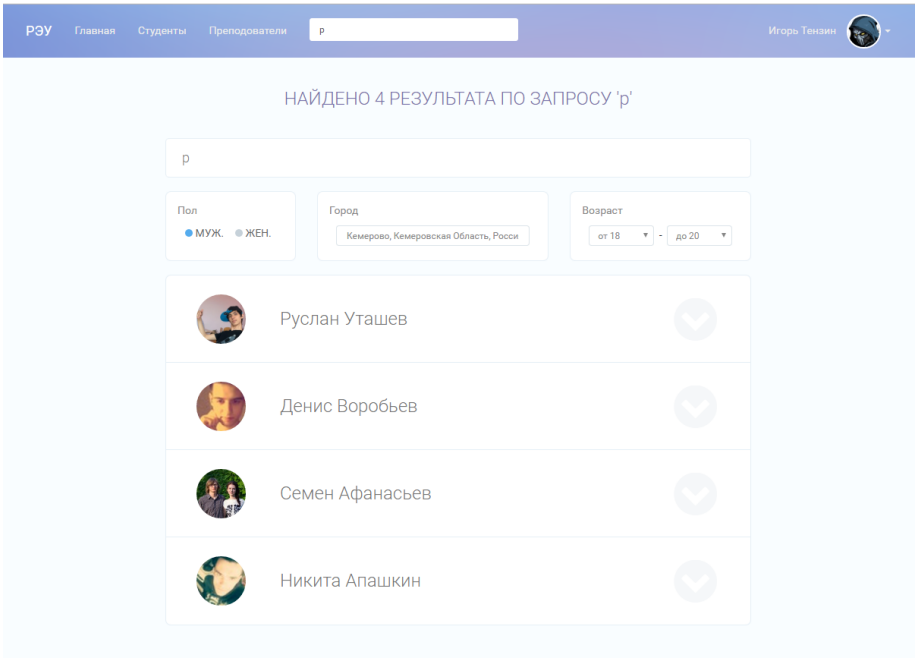

Рисунок 2. Поиск по запросу

Все данные WEB-приложения должны храниться в структурированном виде под управлением реляционной СУБД. Исключения составляют файлы данных, предназначенные для просмотра и скачивания (изображения, видео, документы и т.п.). Такие файлы сохраняются в файловой системе, а в базе данных размещаются имя файла, на который будет ссылаться система.

Сторонние пользователи имеют доступ только к общедоступной части сайта. Доступ к административной части имеют пользователи с правами

администратора. К ограниченной административной части имеют доступ только пользователи с правами редактора. Доступ к закрытой части должен осуществляться с использованием уникального логина и пароля. Приглашение на регистрацию выдается пользователем с правами администратора.

Перед разработкой WEB-приложения, была оценена эффективность от его создания и внедрения в учебную часть. Был применен метод «Информационная экономика». Вывод, который можно сделать после оценки, это то, что проект не потребует дополнительных технических средств.

В области бизнеса проект повысит эффективность работы сотрудников техникума за счет более эффективной работы во всех показателях, установленных на предыдущем этапе проектирования. В области технологий дополнительные инвестиции не потребуется, так как необходимые для системы сервисы и оборудование уже используются. Техникум оснащен ими в достаточной мере для осуществления и дальнейшего поддержания данного проекта.

Список литературы:

1. Измайлов Д.Г., Применение метода «Информационная экономика» при оценке эффективности разработки WEB-приложения «Гильдия выпускников» для кафедры Прикладной информатики / Курсовая работа, 2015
2. Измайлов Д.Г., Разработка WEB-приложения «Гильдия выпускников» для кафедры Прикладной информатики / Дипломная работа, 2015.

СЕКЦИЯ
«МАТЕМАТИКА»

КРИПТОГРАФИЯ НА ОСНОВЕ КОДОВ ИСПРАВЛЕНИЯ ОШИБОК

Дмитриев Егор Андреевич
студент, факультет информатики СНИУ им. Королёва,
РФ, г. Самара
E-mail: pritstant@yandex.ru

Танаев Иван Владимирович
студент, факультет информатики СНИУ им. Королёва,
РФ, г. Самара
E-mail: killabeeez@mail.ru

Швейкин Владислав Витальевич
студент, факультет информатики СНИУ им. Королёва,
РФ, г. Самара
E-mail: xelle163@gmail.com

Завгородний Станислав Дмитриевич
студент, факультет информатики СНИУ им. Королёва,
РФ, г. Самара
E-mail: stas1885@mail.ru

Введение

При передаче под влиянием помех, а также в процессе хранения информации могут возникать ошибки. Для обнаружения и исправления ошибок используются специальные корректирующие коды (коды обнаружения и исправления ошибок).

Для этого во время процессов записи или передачи к информативным данным добавляют контрольное число (особым образом структурированную избыточную информацию), а при чтении или приеме оно используется при проверке или исправлении ошибок. Количество ошибок, поддающихся исправлению, лимитировано и полностью зависит от выбранного применяемого кода.

В отличии от кодов исправления ошибок, коды их обнаружения могут только проверить существование ошибки, но не исправить. Но обнаружить их могут и используемые коды исправления, так как они принадлежат одним классам кодов.

$К_{об} > К_{исп}$, где $К_{об}$ - количество обнаруженных ошибок, а $К_{исп}$ - исправленных.

На основании кодов исправления ошибок существуют криптосистемы с открытыми ключами. Самыми распространенными являются алгоритмы шифрования McEliece и Niederreiter.

Криптосистема McEliece

Криптосистема с открытыми ключами McEliece была разработана Робертом Мак-Элисом в 1978 году. В ней впервые использовалась рандомизация в процессе зашифровки. Кроме того, основанием алгоритма является сложность процесса декодирования полных линейных кодов.

Открытый ключ получается путем перемножения производящей матрицы G на невырожденные случайные матрицы S и P. В качестве закрытого ключа выступает код исправления ошибок, количество которых равно t, а также применяется эффективный алгоритм декодирования. Обычно в алгоритме оперируют двоичные коды Гоппа.

McElice с использованием кодов Гоппы до сих пор не поддается криптоанализу.

Алгоритм работы McEliece

Криптосистема использует 3 этапа:

1) Генерация ключа, выдающего открытый и закрытый ключ.

а) Выбирается двоичный (n,k) - линейный код C, который исправляет t ошибок. Для кода C вычисляется k x n производящая матрица G.

б) Генерируются случайные n x n матрица перестановки P и невырожденная k x k матрица S.

в) Высчитывается k x n матрица G"=SGP.

г) Закрытый ключ представляет собой набор (S,G,P), а открытый ключ пару (G",t).

2) Шифрование передаваемого сообщения.

а) Сообщение m представляется в виде последовательности бинарных символов длины k.

б) Вычисляется вектор c"=mG".

в) Генерирование случайного вектора z длины n, содержащий в себе t единиц.

г) Вычисляется зашифрованное сообщение c=c" + z.

3) Расшифровка принятого зашифрованного сообщения.

а) Вычисление обратных матриц P^{-1} и S^{-1}.

б) Вычисление $c'=c\,P^{-1}$.

в) Используется алгоритм расшифровки для кода C (двоичные коды Гоппа легко декодируются с помощью алгоритма Петерсона), для получения m' из c'.

г) Вычисление исходного сообщения $m=m'S^{-1}$.

Пример работы McEliece

Пусть используется (7,4) код Хемминга, исправляющий все единичные ошибки.

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \quad S = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix}$$

$$P = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

Рисунок 1. G - производящая 4 x 7 матрица, S - случайная невырожденная 4 x 4 матрица, P - случайная 7 x 7 матрица перестановки.

Далее высчитывается 4 x 7 матрица G"= SGP, являющаяся частью открытого ключа.

$$\hat{G} = SGP = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}$$

Рисунок 2. Матрица G".

Пусть необходимо послать сообщение m = (1101), тогда сначала генерируется вектор z с весом 1. Например, z = (0000100). Затем вычисляется зашифрованный текст c = mG" + z = (0110010) + (0000100) = (0110110).

Для расшифровки сообщения используются обратные матрицы P^{-1} и S^{-1}.

$$P^{-1} = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix} \qquad S^{-1} = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

Рисунок 3. Обратные матрицы P^{-1} и S^{-1}.

Сначала вычисляется $c'=cP^{-1}$= (1000111). Далее с помощью быстрого алгоритма декодирования (алгоритма Хэмминга) расшифровывается c'. Синдромом c' является $(1110)^T$, значит в 7 позиции произошла ошибка. Сообщение будет y' = (1000110). Отбрасывая лишние биты у y', получается сообщение m' = (1000). Так как производящая матрица G была выбрана верно, а так же зная, что m' = (1000) и m'=mS, можно найти исходное сообщение $m=m'S^{-1}$=(1000)=(1101).

Недостатки криптосистемы McEliece

На данный момент эта криптосистема не получила широкого применения в силу некоторых недостатков. Например, размер открытого ключа слишком большой (при использовании кодов Гоппы открытый ключ будет 2^{19} бит), шифротекст в разы длиннее исходного сообщения, система сильнее подвержена ошибкам при передаче сообщения, а так же не может быть использована для аутентификации.

Перспективы использования McEliece

Учеными неустанно ведутся разработки по созданию квантовых компьютеров. Естественно рано или поздно они достигнут в этом успеха, и будут созданы квантовые компьютеры.

Нынешние системы шифрования построены на сложных математических задачах, которые требуют очень длительного перебора для нахождения решения. Это поиск дискретных логарифмов, криптография на основе эллиптических кривых, разложение целых чисел на простые множители. Простые компьютеры не могут справиться с ними за приемлемое время, однако это не будет проблемой для квантовых компьютеров.

Как только их работоспособность перейдет в полную силу, всей современной популярной криптографии с открытыми ключами придет конец. RSA, DH, ECC, DSA и другие криптоалгоритмы для обмена цифровых подписей и ключей утратят свою силу.

Такие алгоритмы уже существуют и хорошо изучены. Они не зависят от квантовых вычислений, а значит их можно считать квантово-устойчивыми. Таким алгоритмом как раз является McEliece, который в последнее время считается наиболее перспективным кандидатом на роль пост-квантовой криптосистемы.

Список литературы:

1. Jesse R. Robert McEliece. Москва, издательство “Книга по требованию”, 2012

АЛГОРИТМ ОБУЧЕНИЯ МНОГОСЛОЙНОЙ НЕЙРОННОЙ СЕТИ МЕТОДОМ ОБРАТНОГО РАСПРОСТРАНЕНИЯ ОШИБКИ

Дмитриев Егор Андреевич
студент, факультет информатики СНИУ им. Королёва,
РФ, г. Самара
E-mail: pritstant@yandex.ru

Танаев Иван Владимирович
студент, факультет информатики СНИУ им. Королёва,
РФ, г. Самара
E-mail: killabeeez@mail.ru

Швейкин Владислав Витальевич
студент, факультет информатики СНИУ им. Королёва,
РФ, г. Самара
E-mail: xelle163@gmail.com

Завгородний Станислав Дмитриевич
студент, факультет информатики СНИУ им. Королёва,
РФ, г. Самара
E-mail: stas1885@mail.ru

Основные определения

Определение 1 Градиент – вектор, указывающий направление наибольшего возрастания некоторой величины от одной точки пространства к другой (скалярного поля).

Определение 2 Градиентный спуск – метод нахождения локально максимума (минимума), который заключается в движении по направлению градиента (антиградиента).

Введение

В последнее время все больше и больше приобретают популярность так называемые искусственные нейронные сети. С их помощью можно достичь аппроксимации фактически любой функции. Самым сложным и крайне важным этапом создания сети является её обучение. В данной работе будет рассмотрен один из методов обучения нейронной сети – метод обратного распространения ошибки.

Постановка проблемы

Необходимо ознакомиться с математической моделью многослойной нейронной сети. Рассмотреть метод обратного распространения ошибки.

Нейронные сети

Модель искусственных нейронных сетей была заимствована от модели биологической нейронной сети человека. В отличие от искусственных нейронных сетей, биологические утроены гораздо сложнее и способны выполнять куда более серьезные задачи. В целом модель искусственной нейронной сети описывать поведение биологической.

Нейронные сети – это функции от n-мерного аргумента, а значение – вектор размерности m. Самая простейшая модель нейрона – персептрон. (Рис.1)

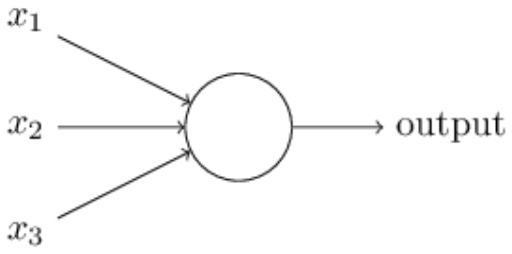

Рисунок 1. Модель персептрона

Аргументом является 3 – мерный вектор над полем (0, 1). Выходом является элемент поля (0,1). К нейрону от входного вектора идут ребра w, имеющие свои весовые коэффициенты. Также нейрон обладает смещением b, которое влияет на величину выхода.

$$output = \begin{cases} 0, if\ w \cdot x + b \leq 0 \\ 1, if\ w \cdot x + b > 0 \end{cases}$$

Более сложной является модель нейрона – сигмоида. В целом сигмоид очень напоминает персептрон за исключением, что компоненты входного вектора и выхода принимают значения на отрезке от [0;1], причем выход – это значение функции $Q(\sum_j w_j x_j) = \frac{1}{1+\exp(-\sum_j w_j x_j)}$. Многослойная нейронная состоит из нескольких слоев сигмоидальных нейронов. (Рис. 2)

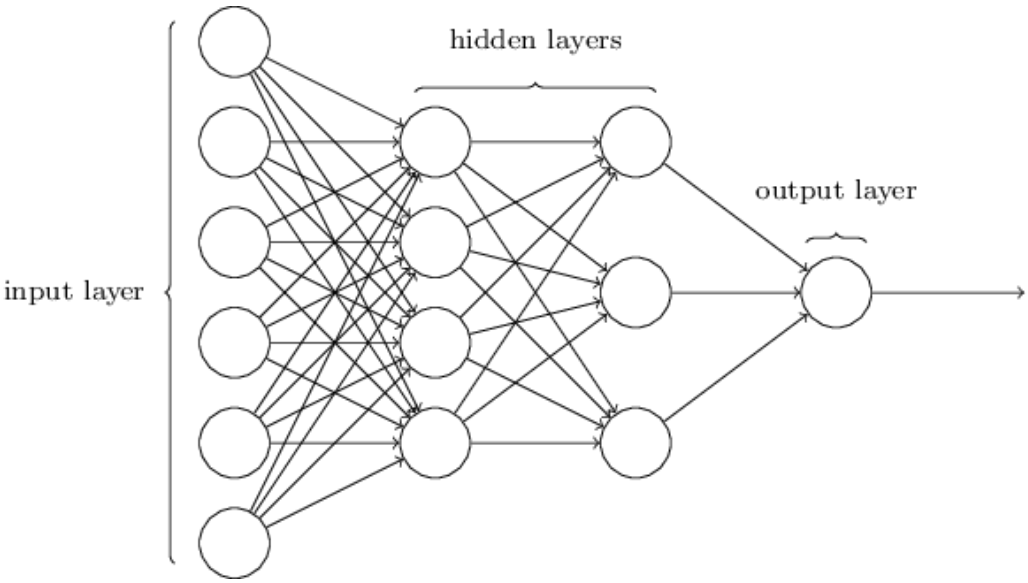

Рисунок 2. Многослойная нейронная сеть

Обучение нейронной сети

Для того, чтобы нейронная сеть выполняла определенную задачу, например, классификация объектов, необходимо подобрать значения весовых коэффициентов и смещений нашей нейронной сети. Метод обучения с учителем заключается в том, что на вход сети мы подаем вектор, а на выходе пытаемся получить желаемый вектор. Критерием определения результата будет является функция стоимости, которая определяет меру близости выходных значений многослойной сети от желаемого вектора. Введем функции стоимости $C(w,b) = \frac{1}{2n}\sum_x (y(x) - a)^2$. Функция C – среднеквадратичное отклонение выходного вектора от желаемого вектора, n – количество обучающих векторов. Основная идея заключается в нахождении градиента функции стоимости ∇C и движении сторону антиградиента -∇C . Данный метод называется <u>методом градиентного спуска</u>. Чтобы найти градиент функции, а в дальнейшем и антиградиент, мы должны найти частные производные $\frac{\partial C}{\partial w}$ и $\frac{\partial C}{\partial b}$ от всех весов и смещений нейронной сети. Отыскав все частные производные в начальной точке отправления, для продвижения к оптимальному решению, нужно произвести шаг в сторону антиградиента $w_k \to w_k' - \eta \frac{\partial C}{\partial w}$ и $b_l \to b_l' - \eta \frac{\partial C}{\partial b}$, где $\eta -$ коэффициент, длина шага. Иногда появляется сложность в подборе

коэффициента, так как при выборе слишком большого шага, можно перескочить локальный минимум, а при выборе слишком маленького, обучение требует слишком много времени. Основная сложность при вычислении градиента – является в нахождение градиента при использовании очень большого числа обучающих векторов, так как для вычислении градиента, мы должны найти отклонении нейронной сети от всех векторов и затем продвинуться на маленький шаг. В системах с использованием нейронных для обучения применяются порядка сотен тысяч обучающих выборок, что ведет к очень сильному увеличению времени. Поэтому вместо обычного градиента используется стохастический градиент. Например, имеем выборку порядка из ста тысячи векторов, используя псевдо случайное распределение, отбираем из выборки десятки или более векторов в зависимости от вычислительных ресурсов и находим приближенный градиент. Теория стохастического градиента дает условия сходимости метода стохастического градиентного спуска.

Перейдем непосредственно к описанию самого алгоритма.

1) Проинициализируем веса случайным образом. Чаще всего берётся нормальное распределение с нулевым математическим ожиданием и единичным среднеквадратичным отклонением.

2) Затем на входной слой подаем вектор и находим значения нейронов на других слоях $Q(\sum_j w_j x_j) = \frac{1}{1+\exp(-\sum_j w_j x_j)}$.

3) Для выходных нейронов считаем величину ошибки

$\delta_k = -a_k(1 - a_k)(y_k - a_k)$.

4) Для внутренних слоев $\delta_j = -a_j\left(1 - a_j\right)\sum_k \delta_k w_{jk}$.

5) Изменить значения $w' = w - \eta\delta_j a_i$, $b' = w - \eta\delta_j$ где i – индекс родительского слоя.

Так как значения ошибок нейронов предшествующих слоёв зависят от значений следующих слоев, то алгоритм называется метод обратного распространения ошибок.

Заключение

В данной работе бы рассмотрены модели искусственных нейронных сетей и метод обучения – обратное распространение ошибок.

Список литературы:

1. Круглов В., Борисов В. Москва, искусственные нейронные сети. Издательство “Горячая Линия – Телеком”, 2001
2. Хайкин С. Нейронные сети. Москва, издательский дом Вильям, 2008

РАСШИРЕННЫЙ АЛГОРИТМ ДИФФИ-ХЕЛЛМАНА

Андросова Татьяна Евгеньевна
студент, кафедра геоинформатики и информационной безопасности,
Самарский университет,
РФ, г. Самара
E-mail: androsovatati@mail.ru

Курочкин Владислав Михайлович
студент, кафедра геоинформатики и информационной безопасности,
Самарский университет,
РФ, г. Самара
E-mail: vlad555.95@mail.ru

Додонова Наталья Леонидовна
научный руководитель, кандидат физико-математических наук,
доцент кафедры прикладной математики, Самарский университет,
РФ, г. Самара

Сегодня мир вокруг нас превратился в один большой рынок, в котором электронные платежи заставили многие компании по-новому взглянуть на торговлю. Количество различных выгод и преимуществ, которые получила промышленность с помощью последних технологий, невероятно велико. Но весь этот технологический прогресс предъявляет все более строгие требования к безопасности, для того, чтобы защитить конфиденциальные данные от посторонних субъектов и различных перехватчиков информации. При этом, главным средством передачи важной информации остается сеть Интернет - место, где любой злоумышленник может представиться добропорядочным человеком. Следственно, очень важно разобраться в различных уязвимостях и в том, какие меры нужно предпринять, чтобы предотвратить перехват данных или их утерю. В настоящее время такими мерами являются различные криптографические и стеганографические методы, списки доступа, протоколы безопасности и прочее.

Криптография - наука и искусство сокрытия данных от несанкционированных субъектов при передачи этих данных по незащищенным каналам.

Методы шифрования обычно разделяют на три категории: симметричное шифрование, ассиметричное и хэш-функции.

Первыми были придуманы симметричные ключи. Суть состоит в том, что используется только один ключ для шифрования на стороне отправителя и расшифровывания на стороне получателя. Процесс расшифровывания является обратным процессу шифрования и обычно этот метод является самым быстрым. Однако, основная проблема заключается в том, каким образом безопасно передать ключ через сеть. Ведь если злоумышленник сможет перехватить его, то расшифровать любое сообщение не составит для него никакого труда.

Проблема передачи ключей исследовалась Уитфилдом Диффи и Мартином Хеллманом в Массачуссетском Технологическом университете США в 1976. Изобретенный ими алгоритм сейчас известен как «Алгоритм Диффи-Хеллмана» и используется для безопасного обмена разделенным секретом между двумя сторонами в режиме реального времени при передаче через незащищенную сеть. Согласование ключа - метод, при котором устройства, соединенные через сеть, устанавливают между собой разделенный секрет без обмена секретной информацией, а только лишь посредством обмена открытыми ключами. Оба устройства при получении открытого ключа выполняют некоторые вычисления при помощи своего закрытого ключа для того, чтобы получить разделенный секрет [2, с. 647 - 649]. В силу того, что алгоритм разрабатывался в первую очередь для обеспечения безопасности, он до сих пор широко используется и с течением времени был исследован многими авторами и сильно видоизменился.

Мы хотим предложить алгоритм, основанный на алгоритме Диффи-Хеллмана, в котором будет предложена новая техника для обмена ключами. В таком "Расширенном алгоритме Диффи-Хеллмана" будут использоваться цифровые изображения для генерации случайных чисел, которые необходимы при обмене ключами через незащищенные сети.

Введение

После публикации алгоритма Диффи-Хеллмана в 1976 г. представления о двухстороннем обмене ключами через незащищенную сеть кардинально изменились. Цель алгоритма состоит в том, чтобы позволить пользователям безопасно обмениваться ключами, которые впоследствии будут использоваться для шифрования.

На текущий момент безопасности алгоритма Диффи-Хеллмана может быть уже недостаточно. Возникает вопрос, как можно его улучшить?

Цель работы: предложить способ улучшения алгоритма Диффи-Хеллмана.

Задачи:

1. Разобрать принцип работы алгоритма Диффи-Хеллмана.
2. Выяснить, каким образом можно его улучшить.
3. Разработать приложение с реализацией предложенного алгоритма.

Алгоритм Диффи-Хеллмана

Алгоритм Диффи-Хеллмана используется для безопасного обмена разделенным секретом между двумя сторонами в режиме реального времени при передаче через незащищенную сеть. Согласование ключа - метод, при котором устройства, соединенные через сеть, устанавливают между собой общий ключ без обмена секретной информацией, а только лишь посредством обмена открытыми ключами. Оба устройства при получении открытого ключа выполняют некоторые вычисления при помощи своего закрытого ключа для того, чтобы получить общий ключ.

Алгоритм может быть описан следующим образом:

1. Обе стороны A и B соглашаются об использовании двух констант p и g. p является простым числом, а число g называется генератором.

2. A и B выбирают свои закрытые ключи a и b такие, что они являются случайными числами меньше p.

3. Пусть $g^a \ mod \ p$ и $g^b \ mod \ p$ - публичные ключи сторон A и B соответственно.

4. Затем A и B проводят обмен своими публичными ключами через незащищенную сеть.

5. Сторона A вычисляет $(g^b \ mod \ p)^a \ mod \ p$, что равносильно $g^{ba} \ mod \ p$.

6. Сторона B вычисляет $(g^a \ mod \ p)^b \ mod \ p$, что равносильно $g^{ab} \ mod \ p$.

7. Общий ключ K теперь может быть теперь вычислен как $K = g^{ba} \ mod \ p = g^{ab} \ mod \ p$ [1, с. 64 – 65].

Основное содержание работы

Основная идея, которая делает алгоритм Диффи-Хеллмана стойким и безопасным - использование случайных чисел.

Случайные последовательности бывают двух типов:

1. Настоящие случайные

2. Псевдослучайные

В данной работе мы хотим предложить расширенный алгоритм Диффи-Хеллмана, который отличается от оригинального следующим:

1. Используется новый простой и эффективный способ для генерации настоящих случайных чисел с помощью цифровых изображений.

2. Имеются предложения по способу вычисления общего секретного ключа.

Генерация настоящих случайных чисел с помощью изображений

Защищенность алгоритма Диффи-Хеллмана может быть повышена, если включить в процесс генерации ключей настоящие случайные числа. Для генерации таких чисел могут быть использованы небольшие изображения. Безопасность такого алгоритма, по сравнению с тем, что использует псевдослучайные числа, будет повышена. Значение каждого пикселя изображения может быть получено с помощью простых функций любого из языков программирования, например, Java и представлено в виде строки. Чтобы представить изображение в двоичном виде, RGB значение должно быть получено для каждого пикселя.

Генерация случайного числа происходит следующим образом:

1. Выбираем любое изображение (или создаем его с использованием любого графического редактора).

2. Представляем изображение в двоичном формате.

3. Составляем матрицу из двоичных чисел.

4. Значение p может быть получено конкатенацией строк таблицы.

5. Значение g может быть получено конкатенацией столбцов таблицы.

6. Теперь остается только передать изображение второй стороне, где необходимо будет проделать то же самое.

Изменения в процедуре вычисления ключей

Второй шаг в расширенном алгоритме Диффи-Хеллмана - произвести некоторые математические вычисления для генерации ключей, которыми будет происходить обмен.

Модифицированный алгоритм может быть представлен следующим образом:

1. Сторона А использует следующие ключи:

* Закрытый ключ XA = $a * b * c$;

* Публичный ключ $YA = gXA\ mod\ p$

* Секретный ключ $K1 = YBXAmod\ p$.

2. Сторона В использует следующие ключи:

* Закрытый ключ X$B = a + b + c$;

* Публичный ключ $YB = gXB\ mod\ p$

* Секретный ключ $K1 = YAXBmod\ p$.

3. Значения p и g получены при помощи способа, представленного выше; a, b, c выбираются случайно из того же изображения так, что их значения лежат между 0 и $p-1$.

Безопасность полученного алгоритма

Расширенный алгоритм Диффи-Хеллмана, предложенный в работе, имеет преимущества перед оригинальным алгоритмом в защите от атак неавторизо-

ванных субъектов. Переменные, использующиеся в математических вычислениях, получены из небольших изображений, что дает дополнительную защиту.

Главным недостатком алгоритма Диффи-Хеллмана является уязвимость к атаке "человек-по-середине", при которой злоумышленник находится между отправителем и получателем и способен перехватывать все сообщения. Он может сгенерировать свои ключи и иметь доступ к зашифрованной информации. Но, передавая значения p и g через изображения, взлом значительно усложняется. Более того, второй шаг шифрования - использование разных математических уравнений - также является дополнительной защитой.

Приложение полученного алгоритма

В качестве практического приложения описанного в работе алгоритма был реализован программный продукт (рис. 1), позволяющий генерировать ключи для сторон A и B из произвольного изображения.

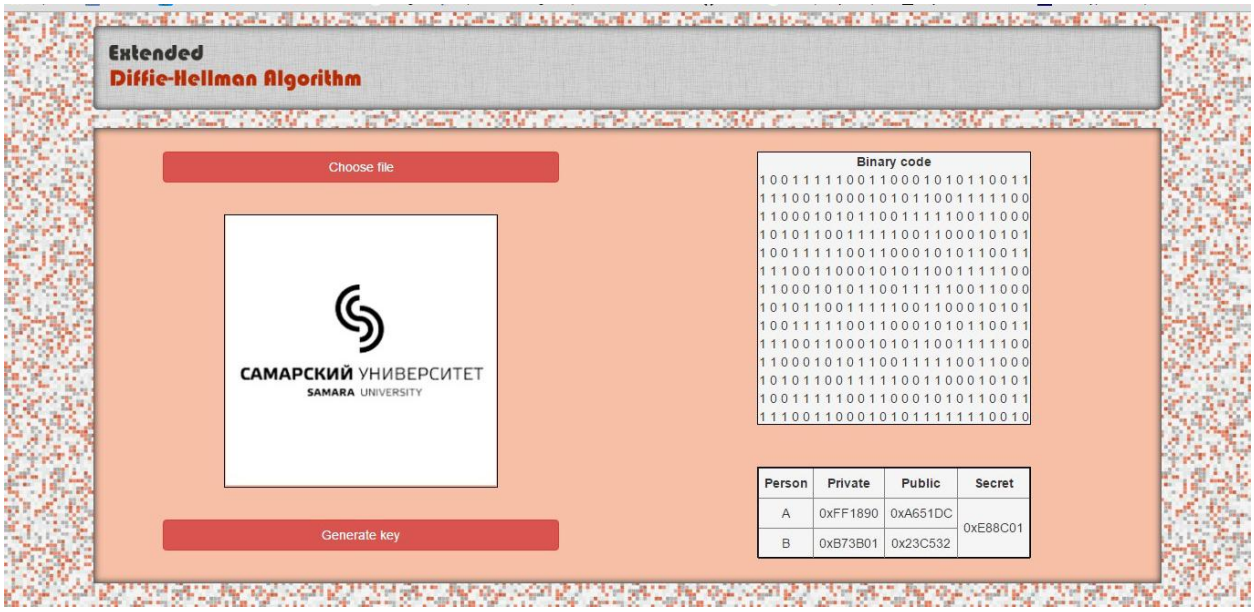

Рисунок 1. Пример работы программы

Список литературы:

1. Ишмухаметов Ш.Т, Рубцова Р.Г. Математические основы защиты информации: учеб. пособие. Казань, 2012. — 138 с.
2. Diffie W., Hellman M. E., «New directions in cryptography» IEEE Trans. Inform. Theory, vol. IT-22, pp. 644–654, Nov. 1976.

ПРИМЕНЕНИЕ ЭЛЛИПТИЧЕСКИХ КРИВЫХ В КРИПТОГРАФИИ

Швейкин Владислав Витальевич
студент, факультет информатики СНИУ им. Королёва,
РФ, г. Самара
E-mail: xelle163@gmail.com

Танаев Иван Владимирович
студент, факультет информатики СНИУ им. Королёва,
РФ, г. Самара
E-mail: killabeeez@mail.ru

Дмитриев Егор Андреевич
студент, факультет информатики СНИУ им. Королёва,
РФ, г. Самара
E-mail: pritstant@yandex.ru

Завгородний Станислав Дмитриевич
студент, факультет информатики СНИУ им. Королёва,
РФ, г. Самара
E-mail: stas1885@mail.ru

Введение

Эллиптической кривой является множество точек, которые удовлетворяют уравнению $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$.

Если положить, что характеристика поля не равна 2 и 3, тогда эллиптическая кривая будет плоской кривой, которая определена уравнением вида

$y^2 = x^3 + ax + b$, где a и b — действительные числа. Этот вид уравнений называется уравнениями Вейерштрасса.

Эллиптические кривые бывают гладкими и сингулярными. Для гладких эллиптических кривых всегда выполняется неравенство: $4a^3 + 27b^2 \neq 0$.

В отличии от гладких эллиптических кривых для сингулярных кривых данное условие выполняться не будет.

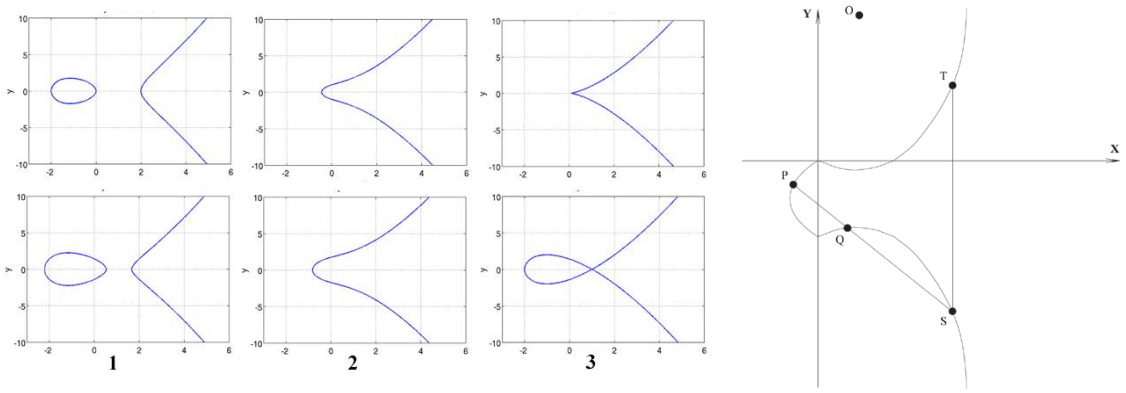

Рисунок 1. Слева в 1 и 2 столбце приведены примеры гладких эллиптических кривых, в 3 столбце - сингулярных, справа эллиптическая кривая в общем виде

Эллиптические кривые в криптографии

Важным моментом является то, что все рассмотренные до этого кривые являются эллиптическими кривыми над вещественными числами. Отсюда возникает проблема округления. Т.е., пользуясь кривыми над вещественными числами, невозможно получить биекцию между исходным текстом и зашифрованными данными. Чтобы не возникала проблема округления, в криптографии используются только эллиптические кривые над конечными полями. Таким образом, эллиптической кривой будет являться набор точек, координаты которых принадлежат конечному полю. На сегодняшний день в криптографии используются два вида эллиптических кривых: над конечным полем Z_P, которое является кольцом вычетов по модулю простого числа. А также над полем $GF(2^m)$, являющимся бинарным конечным полем. Эллиптических кривые над полем $GF(2^m)$ обладают важным свойством. Элементы поля $GF(2^m)$ можно легко представить в виде n-битных кодовых слов, что позволяет ускорить аппаратную реализацию эллиптических алгоритмов.

Все математические операции на эллиптических кривых над конечным полем производятся, опираясь на законы конечного поля, над которым эллиптическая кривая построена. Таким образом, при вычислении, например, суммы двух точек эллиптической кривой E над кольцом вычетов Z_P операции

производятся по модулю числа p. Однако если сложить два одинаковых элемента из бинарного конечного поля, то в результате получается 0, поскольку сложение происходит по модулю 2. Получается, что характеристика этого поля равна 2. Но эллиптическая кривая вида $y^2 = x^3 + ax + b$, описанная над полем характеристики 2 или 3, становится сингулярной, что является нежелательным для использования в криптографии. Поэтому над бинарным конечным полем применяются кривые вида:

$y^2 + xy = x^3 + ax^2 + b$, *где* $b \neq 0$.

Другим важным понятием эллиптической криптографии является **порядок эллиптической кривой**, показывающий количество точек кривой над конечным полем. По теорема Хассе утверждается, что при количество точек N кривой, которая определена над полем Z_q с q элементами, справедливо равенство: $|N - (q + 1)| \leq 2\sqrt{q}$.Учитывая, что бинарное конечное поле $GF(2^n)$ состоит из 2^n элементов, можно утверждать, что порядок кривой $E_{2^n}(a,b)$ равен 2^n+1-t, где $|t| \leq \sqrt{(2^n)}$.Если t делится на характеристику поля без остатка, эллиптическая кривая над бинарным конечным полем в таком случае называется **суперсингулярной**.

Криптография на эллиптических кривых

Все точки эллиптической кривой над конечным полем образуют группу. И для такой группы определены операция сложения и умножения точки G на число k, представляя умножение как сумма G+G+..+G из k слагаемых. Пусть имеется сообщение M, которое представлено в виде целого числа. Сообщение можно зашифровать пользуясь выражением: C=M*G. Возникает задача определения сложности восстановления сообщения M, при известных параметрах кривой E(a,b), зашифрованного текста C и точки G. Данная задача является не чем иным, как дискретным логарифмом на эллиптической кривой, и быстрого решения она не имеет. Кроме того, принято считать, что задача дискретного логарифма на эллиптической кривой значительно труднее для решения, чем задача дискретного логарифмирования в конечных полях. Наиболее быстрые методы, которые разработаны для конечных полей,

становятся бесполезными в случае эллиптических кривых. Для решения дискретного логарифма на конечном поле существуют сравнительно быстрые алгоритмы, которые имеют сложность

$O(\exp(c(\log p \log \log p)^d))$, где p является размером поля, а c и d некоторыми константами. Данные алгоритмы носят название "субэкспоненциальные" и позволяют достаточно легко раскрывать дискретный логарифм в конечном поле, при условии, что размер поля очень большой, порядка 2^{1024}.

Наряду с дискретными логарифмами на конечных полях наиболее быстрые методы решения дискретного логарифма на эллиптической кривой имеют сложность $O(\sqrt{q})$, где q — количество точек эллиптической кривой. Следовательно, для обеспечения уровня стойкости в 2^{80} операций нужно, чтобы значение $q=2^{160}$. При вычислении дискретного логарифма в конечном поле необходимо поле порядка $q=2^{1024}$, чтобы получить аналогичный уровень сложности.

Следует иметь ввиду, что мощность вычислительной техники постоянно повышается, а значит значение q будет также постоянно увеличиваться.

Но так как графики функций $O(\exp(c(\log p \log \log p)^d))$ и $O(\sqrt{q})$ кординально отличаются друг от друга, в группе точек эллиптической кривой значение q будет расти в разы медленнее, чем в произвольном конечном поле.

Варианты атак

1. **Алгоритм Шенкса.** Алгоритм также известен как алгоритм больших и малых шагов (как Baby-step/giant-step). Для группы размером n происходит вычисление таблицы, размер которой будет $n^{1/2}$. После этого по данной таблице осуществляется поиск искомого элемента. Алгоритм обладает сложностью $O(\sqrt{q})$.

2. **Уязвимость сингулярных и суперсингулярных кривых.** Не существует общих методов решения задачи дискретного логарифма на эллиптических кривых. Однако такие методы на самом деле существуют только для определенного рода кривых: сингулярных и суперсингулярных.

Благодаря специфичным свойствам этих кривых задача дискретного логарифма на эллиптической кривой сводится к задаче дискретного логарифма в конечном поле. Поэтому для такого рода кривых стандартные 160-320 битные ключи будут сильно уязвимы. Злоумышленники смогут вскрыть секретный ключ, за относительно короткое время.

3. **Алгоритм Полига-Хеллмана**. Он является алгоритмом решения дискретного логарифма. Пусть n это количество точек эллиптической кривой, а также само число n раскладывается на простые числа p_1, p_2,.., p_n. Весь метод приводится к тому, что необходимо найти дискретные логарифмы по модулю простого числа p_i. После этого общее решение находится с помощью китайской теоремы об остатках. Атака сводит проблему дискретного логарифма в большом поле n к задаче с намного меньшим полем p. Для противостояния данной атаке необходимо выбирать кривые, количество точек которых делится на весьма большое простое число $q \approx n$.

4. **Уязвимость аномальных кривых.** Количество точек n эллиптической кривой вычисляется по формуле **n=q+1-t**, где q — размер исходного поля. Если t делится на 2, кривая называется суперсингулярной, поэтому может показаться отличной идеей использовать кривые, количество точек которых равно q, т.е. t=1. Данные кривые называются **аномальными.** Решение дискретного логарифма на аномальных эллиптических кривых оказывается намного более простой задачей, чем для сингулярных и суперсингулярных кривых.

Список литературы:

1. Болотов А., Гашков С., Фролов А., Часовских А. Элементарное введение в эллиптическую криптографию.

ПРИМЕНЕНИЕ ТЕОРИИ ЧИСЕЛ В АЛГОРИТМЕ ШИФРОВАНИЯ RSA

Швейкин Владислав Витальевич
студент, факультет информатики СНИУ им. Королёва,
РФ, г. Самара
E-mail: xelle163@gmail.com

Завгородний Станислав Дмитриевич
студент, факультет информатики СНИУ им. Королёва,
РФ, г. Самара
E-mail: stas1885@mail.ru

Танаев Иван Владимирович
студент, факультет информатики СНИУ им. Королёва,
РФ, г. Самара
E-mail: killabeeez@mail.ru

Дмитриев Егор Андреевич
студент, факультет информатики СНИУ им. Королёва,
РФ, г. Самара
E-mail: pritstant@yandex.ru

В данной статье рассматривается практическое применение теории чисел на примере алгоритма шифрования RSA. Мы разберем некоторые понятия из теории чисел, необходимые для изучения алгоритма RSA, а также проанализируем основные этапы работы алгоритма на примере.

Основные определения и теоремы

Введем некоторые определения, которые будут использованы в работе.

1. Криптография – наука о методах обеспечения конфиденциальности, целостности данных, аутентификации, а также невозможности отказа от авторства.

2. Простое число – натуральное (целое положительное) число ℕ, которое имеет ровно два различных натуральных делителя – единицу и самого себя.

3. Функция Эйлера $\varphi(n)$ – функция, определенная на положительных числах, значение которой равно количеству натуральных чисел, меньших n и взаимно-простых с n.

Некоторые свойства функции Эйлера:

$\varphi(p) = p - 1$

$\varphi(p^k) = p^k - p^{k-1}$

$\varphi(n \cdot m) = \varphi(n) \cdot \varphi(m)$

4. *НОД(a, b) = d, d* - наибольший общий делитель, если

1) $a \vdots d \wedge b \vdots d$

2) $a \vdots d_1 \wedge b \vdots d_1 \Rightarrow d \vdots d_1$

5. Расширенный алгоритм Евклида – алгоритм, результатом работы которого является представление *НОД(a, b)* в виде соотношения Безу: *НОД(a,b)=* $a \cdot s + b \cdot t$, где числа *s,t* – коэффициенты Безу.

Пусть a,b – целые числа и не равные одновременно нулю, и последовательность чисел $a > b > r_1 > r_2 > ... > r_n$ определена тем, что r_1 - остаток от деления $\frac{a}{b}$, r_2 - остаток от деления $\frac{b}{r_1}$, … , r_k - остаток от деления $\frac{r_{k-2}}{r_{k-1}}$, а r_{n-1} делится на r_n нацело.

$a = b \cdot q_0 + r_1$

$b = r_1 \cdot q_1 + r_2$

$r_1 = r_2 \cdot q_2 + r_3 = a + b \cdot (-q_0)$

$r_2 = r_3 \cdot q_3 + r_4 = b - r_1 \cdot q_1 = a \cdot (-q_1) + b \cdot (1 + q_1 \cdot q_0)$

$r_{k-2} = r_{k-1} \cdot q_{k-1} + r_k$

$r_{n-1} = r_n \cdot q_n$

$НОД(a,b) = r_n = r_{n-2} - r_{n-1} \cdot q_{n-1} = ... = a \cdot s + b \cdot t$

<u>Теорема Эйлера.</u> Если числа a и n взаимно простые, то $a^{\varphi(n)} \equiv 1 (\mathrm{mod}\, n)$, *φ(n)*- функция Эйлера.

Введение

Теория чисел – раздел математики, который находит широкое практическое применение в современном мире. Одним из таких примеров является криптографический алгоритм RSA с открытым ключом, безопасность

которого основана на трудности задачи факторизации, то есть разложении числа на простые множители.

Генерация ключей

1. Выберем два случайных простых числа p и q, такие что $p \neq q$. Для обеспечения максимальной безопасности следует выбирать p и q равной длины.

2. Вычислим произведение $n = p \cdot q$ и функцию Эйлера $\varphi(n) = (p-1)\cdot(q-1)$.

3. Выберем случайное целое число e $(1 < e < \varphi(n))$ взаимно простое со значением функции Эйлера $\varphi(n)$, т.е. *НОД(e,* $\varphi(n)$*)*=1. Пара {e,n} является открытым ключом алгоритма RSA.

4. Вычислим число d $(1 < d < n)$, обратное к числу e по модулю $\varphi(n)$. То есть $d \cdot e \equiv 1(\bmod \varphi(n))$. Пара {d,n} является закрытым ключом алгоритма RSA.

Шифрование

1. Для шифрования сообщения m необходимо разбить его на цифровые блоки длиной меньшей n.

2. Используя открытый ключ {e,n}, зашифруем каждый блок сообщения по формуле $c_i = enc(m_i) = m_i^e \bmod n$

3. Зашифрованное сообщение c будет состоять из блоков c_i той же самой длины.

Дешифрование

1. Возьмем зашифрованный блок c_i и используя закрытый ключ {d,n} вычислим $m_i = c_i^d \bmod n$. Операция восстановления исходного сообщения основана на теореме Эйлера: $c_i^d = (m_i^e)^d = m_i^{k\cdot\varphi(n)+1} = m_i \cdot m_i^{k\cdot\varphi(n)} = m_i \cdot 1^k = m_i$

2. Преобразуем цифровые блоки в исходное сообщение.

Пример работы алгоритма

Генерация ключей:

1. Выберем два случайных простых числа p = 47, q = 53

2. Вычислим произведение $n = 47 \cdot 53 = 2491$, функция Эйлера $\varphi(n) = (47-1)\cdot(53-1) = 46 \cdot 52 = 2392$

3. Выберем случайное целое число e = 71 (1<71<2392), *НОД*(71,2392) =1. Пара {71,2491} будет являться открытым ключом шифрования алгоритма RSA.

Используя расширенный алгоритм Евклида, вычислим число d, обратное к числу 71 по модулю 2392. В первых двух столбцах таблицы запишем числа, для которых необходимо найти наибольший общий делитель, для нашей задачи это A=2392 и B = 71. Третий столбец содержит остаток от деления A на B. Четвертый - целая часть от деления A на B. После заполнения первых четырех столбцов, наибольшим общим делителем будет являться последний остаток отличный от нуля, то есть *НОД*(2392,71) = 1. Начнем заполнять последние два столбца, содержащие X и Y с конца. В последнюю строчку запишем X=0 и Y=1. Затем, зная значения x_{i+1} и y_{i+1}, последовательно найдем x_i и y_i по формулам: $x_i = y_{i+1}$, $y_i = x_{i+1} - y_{i+1} \cdot (AdivB)$, где $A\ div\ B$ = *[A/B]* – целая часть от деления А на В.

Таблица 1.

Расширенный алгоритм Евклида

A	***B***	***A mod B***	***[A/B]***	***X***	***Y***
2392	71	49	33	29	-977
71	49	22	1	-20	29
49	22	5	2	9	-20
22	5	2	4	-2	9
5	2	1	2	1	-2
2	1	0	2	0	1

Искомым значение обратного элемента будет являться y = -977, $d = y \bmod \varphi(n) = -977 \bmod 2392 = 1415$. Пара {1415,2491} будет закрытым ключом алгоритма RSA.

Шифрование:

Закодируем с помощью алгоритма RSA сообщение: “**самарский университет**”.

1. Заменим каждую букву её порядковым номером в алфавите.

Таблица 2.

Замена букв алфавита на порядковый номер

m_1 = ’с’ = 19	m_2 = ’а’ = 1	m_3 = ’м’ = 14
m_4 = ’а’ = 1	m_5 = ’р’ = 18	m_6 = ’с’ = 19
m_7 = ’к’ = 12	m_8 = ’и’ = 10	m_9 = ’й’ = 11
m_{10} = ‘ ‘ = 34	m_{11} = ’у’ = 21	m_{12} = ’н’ = 15
m_{13} = ’и’ = 10	m_{14} = ’в’ = 3	m_{15} = ’е’ = 6
m_{16} = ’р’ = 18	m_{17} = ’с’ = 19	m_{18} = ’и’ = 10
m_{19} = ’т’ = 20	m_{20} = ’е’ = 6	m_{21} = ’т’ = 20

2. Используя открытый ключ {71,2491}, зашифруем каждый блок сообщения

Таблица 3.

Шифрование

$c_1 = 19^{71} \bmod 2491 = 2224$	$c_2 = 1^{71} \bmod 2491 = 1$	$c_3 = 14^{71} \bmod 2491 = 2358$
$c_4 = 1^{71} \bmod 2491 = 1$	$c_5 = 18^{71} \bmod 2491 = 1311$	$c_6 = 19^{71} \bmod 2491 = 2224$
$c_7 = 12^{71} \bmod 2491 = 285$	$c_8 = 10^{71} \bmod 2491 = 1639$	$c_9 = 11^{71} \bmod 2491 = 1289$
$c_{10} = 34^{71} \bmod 2491 = 1062$	$c_{11} = 21^{71} \bmod 2491 = 1381$	$c_{12} = 15^{71} \bmod 2491 = 1561$
$c_{13} = 10^{71} \bmod 2491 = 1639$	$c_{14} = 3^{71} \bmod 2491 = 1889$	$c_{15} = 6^{71} \bmod 2491 = 2104$
$c_{16} = 18^{71} \bmod 2491 = 1311$	$c_{17} = 19^{71} \bmod 2491 = 2224$	$c_{18} = 10^{71} \bmod 2491 = 1639$
$c_{19} = 20^{71} \bmod 2491 = 164$	$c_{20} = 6^{71} \bmod 2491 = 2104$	$c_{21} = 20^{71} \bmod 2491 = 164$

3. Таким образом зашифрованное сообщение можно представить в виде последовательности блоков с = {2224, 1, 2358, 1, 1311, 2224, 285, 1639, 1289, 1062, 1381, 1561, 1639, 1889, 2104, 1311, 2224, 1639, 164, 2104, 164}.

Дешифрование:

1. Используя закрытый ключ {1415, 2491}, расшифруем последовательно каждый блок сообщения с = {2224, 1, 2358, 1, 1311, 2224, 285, 1639, 1289, 1062, 1381, 1561, 1639, 1889, 2104, 1311, 2224, 1639, 164, 2104, 164}.

Таблица 4.

Дешифрование

$m_1 = 2224^{1415} \bmod 2491 = 19$	$m_2 = 1^{1415} \bmod 2491 = 1$	$m_3 = 2358^{1415} \bmod 2491 = 14$
$m_4 = 1^{1415} \bmod 2491 = 1$	$m_5 = 1311^{1415} \bmod 2491 = 18$	$m_6 = 2224^{1415} \bmod 2491 = 19$
$m_7 = 285^{1415} \bmod 2491 = 12$	$m_8 = 1639^{1415} \bmod 2491 = 10$	$m_9 = 1289^{1415} \bmod 2491 = 11$
$m_{10} = 1062^{1415} \bmod 2491 = 34$	$m_{11} = 1381^{1415} \bmod 2491 = 21$	$m_{12} = 1561^{1415} \bmod 2491 = 15$
$m_{13} = 1639^{1415} \bmod 2491 = 10$	$m_{14} = 1889^{1415} \bmod 2491 = 3$	$m_{15} = 2104^{1415} \bmod 2491 = 6$
$m_{16} = 1311^{1415} \bmod 2491 = 18$	$m_{17} = 2224^{1415} \bmod 2491 = 19$	$m_{18} = 1639^{1415} \bmod 2491 = 10$
$m_{19} = 164^{1415} \bmod 2491 = 20$	$m_{20} = 2104^{1415} \bmod 2491 = 6$	$m_{21} = 164^{1415} \bmod 2491 = 20$

2. Преобразовав порядковые номера букв алфавита в текст, получим исходное сообщение: “**самарский университет**”.

Заключение

В настоящей работе были изучены некоторые определения и теоремы из теории чисел необходимые для понимания алгоритма RSA. Продемонстрировано практическое применение теории чисел, а также рассмотрены основные этапы работы алгоритма RSA.

Список литературы:

1. Додонова Н.Л. Конспект лекций по дисциплине алгебраические структуры и теория чисел. Самара, 2016
2. Шнайер, Б.М. Прикладная криптография/ Б.М. Шнайер - ТРИУМФ 2002. – 816 с.

СЕКЦИЯ

«МОДЕЛИРОВАНИЕ»

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ДВИЖЕНИЯ КОСМИЧЕСКОЙ ТРОСОВОЙ СИСТЕМЫ В НЕЦЕНТРАЛЬНОМ ГРАВИТАЦИОННОМ ПОЛЕ ЗЕМЛИ

Сахибназарова Виктория Бахтиёровна
студент магистратуры, факультет информатики СНИУ им. академика С.П. Королева, РФ, г. Самара
E-mail: vik-tori-s@yandex.ru

В настоящее время одной из активно развиваемых и востребованных областей деятельности человека является космическая отрасль. Изучение состояния Земли, посредством съемок с орбиты, мониторинг верхних слоев атмосферы, обеспечение спутниковой связи и телевидения – все это осуществимо благодаря космическим летательным аппаратам, вращающимся вокруг Земли. А математическое моделирование – удобнейший инструмент, позволяющий без значительных затрат средств и времени предсказать поведение летательного аппарата, и продемонстрировать его реакцию на изменение исходных условий движения.

В данной работе происходит моделирование движения космической тросовой системы (КТС) — комплекса искусственных космических объектов (спутников, кораблей, грузов), соединенных длинными тонкими гибкими элементами (тросами, кабелями, шлангами), совершающий орбитальный полет. В наиболее простом виде КТС — это связка двух космических аппаратов (в данной работе – космический аппарат (КА) и спускаемая капсула (СК)), соединенных тросом длиной в десятки или даже сотни километров [3].

Уравнения движения КТС представляют собой совокупность уравнений движения центров масс КА и СК, движения относительно центра масс, а также уравнения, описывающие работу механизма управления развёртыванием троса.

Для вывода уравнений движения требуется определить возмущающие силы. При движении космической тросовой системы в гравитационном поле Земли возмущающими силами являются: аэродинамические силы, действующие как на трос, так и на концевые тела, а также силы связанные с нецентральностью гравитационного поля Земли.

Для составления уравнений движения центров масс концевых тел используется второй закон Ньютона, где в правой части уравнения добавляются слагаемые, связанные с действием внешних сил (1).

$$m \cdot \frac{d^2 r}{dt^2} = -\frac{K}{r^2} \cdot \frac{\vec{r}}{r} + \vec{F} \tag{1}$$

где K – гравитационный параметр Земли, r – радиус-вектор центра массы тела, а F – сумма внешних сил (силы упругости троса и гравитационной силы).

Уравнения вращательного движения описываются динамическими (2) и кинематическими (3) уравнениями Эйлера [2]:

$$\begin{aligned} I_X \cdot \frac{d\omega_X}{dt} + \omega_Y \cdot \omega_Z \cdot (I_Z - I_Y) &= \sum M_X, \\ I_Y \cdot \frac{d\omega_Y}{dt} + \omega_X \cdot \omega_Z \cdot (I_X - I_Z) &= \sum M_Y, \\ I_Z \cdot \frac{d\omega_Z}{dt} + \omega_X \cdot \omega_Z \cdot (I_Y - I_X) &= \sum M_Z, \end{aligned} \tag{2}$$

$$\begin{aligned} \frac{d\psi}{dt} &= \frac{\omega_X \cdot \sin\varphi + \omega_Y \cdot \cos\varphi}{\sin\theta}, \\ \frac{d\varphi}{dt} &= \omega_Z - \frac{(\omega_X \cdot \sin\varphi + \omega_Y \cdot \cos\varphi) \cdot \cos\theta}{\sin\theta}, \\ \frac{d\theta}{dt} &= \omega_X \cdot \cos\varphi - \omega_Y \cdot \sin\varphi, \end{aligned} \tag{3}$$

где I_X, I_Y, I_Z – моменты инерции груза в главных связанных осях; ω_i и $\sum M_i$ ($i = x,y,z$) – проекции угловых скоростей вращения груза и действующих на него моментов на оси главной связанной системы координат; ψ, φ, θ - углы Эйлера, определенные относительно связанной системы координат; $M_i = M_{elast_i}$, где $\vec{M}_{elast_i}$ - момент от силы упругости троса.

Момент от силы упругости троса ($\vec{M}_{elast_i}$) определяется из выражения $\vec{M}_{elast_i} = \overrightarrow{\Delta R}_e \times \vec{F}_{elast_i}$ (4), где $\overrightarrow{\Delta R}_e$ - радиус-вектор точки крепления троса относительно центра масс концевого тела; $\vec{F}_{elast_i}$ - сила упругости.

Для определения модуля силы упругости применяется односторонний закон Гука

$$F_{elast} = \begin{cases} \frac{c\cdot(L_{AB}-L)}{L}, \text{при } L_{AB} - L > 0, \\ 0, \text{при } L_{AB} - L \leq 0 \end{cases} \quad (5)$$

где L_{AB} - расстояние между точками крепления троса на КА и на грузе, L - длина выпущенного из механизма троса, $c = ES$ - жесткость троса, E и S - модуль Юнга и площадь поперечного сечения троса.

Уравнения, описывающие работу механизма управления, записываются в виде

$$m_{in} \cdot \frac{dV_T}{dt} = F_{elast} - F_c$$

$$\frac{dL}{dt} = V_T \quad (6)$$

где $F_c = K_L \cdot \left(L - L_{progr}\right) + K_V \cdot \left(V_T - V_{progr}\right)$ - управляющая сила в механизме развертывания, m_{in} - коэффициент, характеризующий инерционность механизма; K_L и K_V - коэффициенты обратной связи системы управления; V_T - скорость троса.

В работе рассматривается нецентральное гравитационное поле, гравитационный потенциал которого, определяется следующим образом:

$$U = U_0 + U_1 + U_2 + ... \quad (7)$$

Для практических исследований гравитационный потенциал Земли, часто записывают с учётом только трёх составляющих гравитационного потенциала (7), в следующей форме [1]:

$$U = \frac{\mu}{r} + \frac{\varepsilon}{r^3}\left(\frac{1}{2} - \sin^2\varphi\right) + \frac{\chi}{r^5}\left(\sin^4\varphi - \frac{6}{7}\sin^2\varphi + \frac{3}{35}\right), \quad (8)$$

где $\varepsilon = 2.634\cdot10^5$ км$^5\cdot$с$^{-2}$, χ=6.773$\cdot10^5$ км$^5\cdot$с$^{-2}$

В ортогональной геоцентрической системе координат, гравитационные силы имеют вид:

$$G_x = m\frac{\partial U}{\partial x},$$
$$G_y = m\frac{\partial U}{\partial y}, \qquad (9)$$
$$G_z = m\frac{\partial U}{\partial z}.$$

Здесь m - масса тела, движение которого исследуется.

Описанная выше математическая модель реализована в программном продукте, позволяющем проводить моделирование с учетом и без учета вращательного движения концевых тел, а также с учетом и без учета нецентральности гравитационного поля Земли. Результаты моделирования программа позволяет сохранять в виде таблицы (таблица 1).

Таблица 1.

Фрагмент таблицы результатов моделирования

Время	**0**	**500**	**1000**
Координата X положения КА	-3312621,323	337577,7029	3885985,043
Координата Y положения КА	6588,72	7626,188954	6172,26759
Координата Z положения КА	2723982,713	3678798,662	3430296,003
Проекция скорости КА на ось X	2975,22	746,1308207	-1706,287791
Проекция скорости КА на ось Y	5016618,199	5488526,885	4162855,732
Проекция скорости КА на ось Z	2750,05	-907,7134617	-4237,966049
Координата X положения СК	-3312621,328	337071,9846	3885723,079
Координата Y положения СК	6587,727	7625,228867	6173,591237
Координата Z положения СК	2723982,717	3679266,055	3431014,126
Проекция скорости СК на ось X	2976,04	747,3111662	-1705,871776
Проекция скорости СК на ось Y	5016618,206	5489368,527	4164013,162
Проекция скорости СК на ось Z	2751,554	-905,6709843	-4237,685482
Угол отклонения троса от местной вертикали	0	-0,556332251	-0,804822095

На рисунке 1 приведен график изменения длины выпущенного троса и график изменения расстояния между КА и СК, в зависимости от времени.

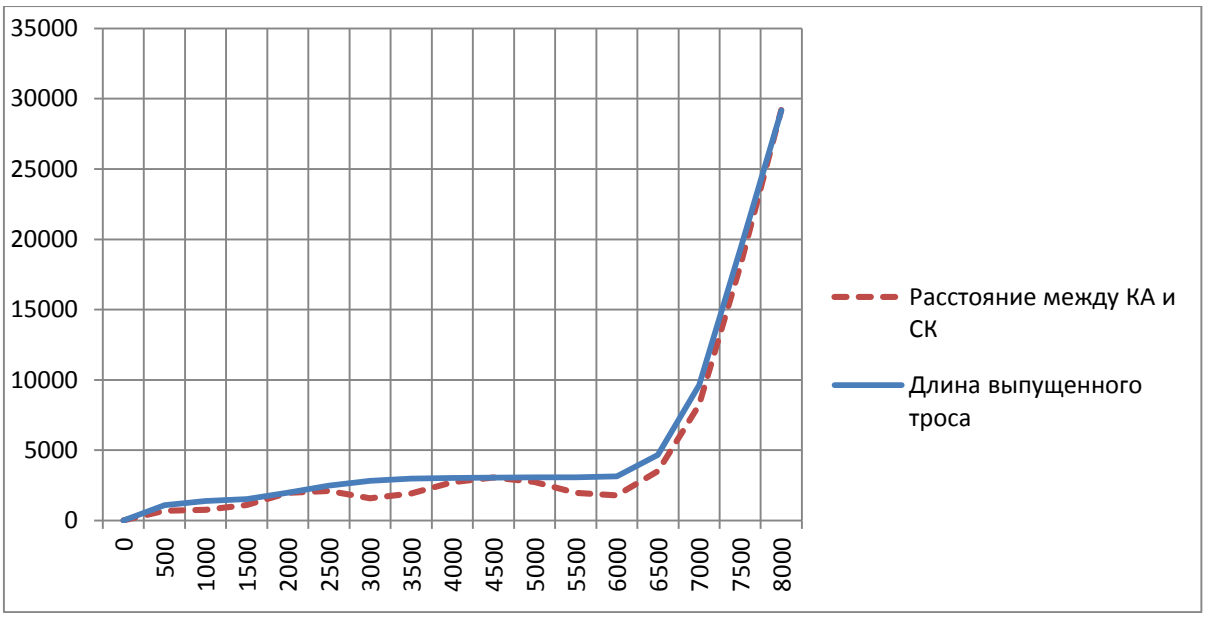

Рисунок 1. График зависимости от времени длины выпущенного троса и расстояния между КА и СК

Полученная математическая модель движения космической тросовой системы в нецентральном поле Земли, можем быть использована для расчёта траектории развёртывания КТС, и определения начальных условий дальнейшего спуска СК в плотных слоях атмосферы.

Список литературы:

1. Анучин О. Н., Комарова И. Э., Порфирьев Л. Ф. Бортовые системы навигации и ориентации искусственных спутников Земли. – СПб.: ГНЦ РФ ЦНИИ “Электроприбор”, 2004. – 326 с.
2. Заболотнов Ю.М., Наумов О.Н. Анализ пространственного вращательного движения концевого тела при развертывании орбитальной тросовой системы [Текст]/Ю.М. Заболотнов, О.Н. Наумов // Управление и навигация летательных аппаратов. – Самара. СГАУ, 2012 г. – С. 104-107
3. Осипов В.Г., Шошунов Н.Л. Космические тросовые системы: история и перспективы // Земля и Вселенная – 1998. - №4. [электронный ресурс] — Режим доступа. — URL: http://epizodsspace.airbase.ru/bibl/ziv/1998/4/kos-tros-sis.html (дата обращения 17.05.2016)

СЕКЦИЯ

«РЕСУРСОСБЕРЕЖЕНИЕ»

ВЛИЯНИЕ ЧЕЛОВЕЧЕСКОЙ ДЕЯТЕЛЬНОСТИ НА ЖИЗНЕННО ВАЖНЫЕ РЕСУРСЫ И СТАБИЛЬНОСТЬ ЭКОСИСТЕМ

Дубленных Филипп Дмитриевич
студент, кафедра «Безопасность жизнедеятельности и защита окружающей среды» ДГТУ, РФ, г. Ростов-на-Дону

Кобзева Ирина Олеговна
студент, кафедра «Безопасность жизнедеятельности и защита окружающей среды» ДГТУ, РФ, г. Ростов-на-Дону
E-mail: irinakobzeva1996@mail.ru

Атмосферный воздух является одним из основных элементов живой природы. Он представляет собой смесь газов атмосферы, находящихся за пределами жилых, производственных и иных помещений.

Высокая концентрация производства и несовершенство используемых традиционных технологий привели к заметному ухудшению экологической обстановки во многих индустриальных регионах страны, где разрушение окружающей среды достигло больших масштабов и характеризуется недопустимым загрязнением территорий, водных источников и воздушного бассейна.

На процессы жизнедеятельности на земле в наибольшей степени влияют изменение кислородного баланса в атмосфере и повышение концентрации CO2. Дефицит кислорода в атмосфере, определяется сокращением его поступления из природных источников и увеличением его потребления. На техногенную деятельность человечество расходует кислорода до 40 млрд. т./год. При ежегодном 5%-ном приросте потребления свободного кислорода на технологические нужды содержание кислорода в окружающей среде может снизиться до критического для человека предела, до 17% по массе.

В сумме на сжигание нефти, угля, газа и дров за всю историю человечества было израсходовано 275*109 тонн кислорода, из которых 88% приходится на последние 50 лет. Каждый год в мире на сжигание топлива расходуется около 10 млрд. тонн свободного кислорода. За последние 500 млн. лет ежегодное продуцирование кислорода в процессе фотосинтеза составило около 200 млрд. тонн. За прошедшие годы, из-за сплошной вырубки лесов, годовая продукция кислорода уменьшилась до 190 млрд. тонн. Если принимать в расчет ежегодное мировое промышленное потребление кислорода, то эта цифра упадет до 185 млрд. тонн в год, т.е. почти на 8%. Последствия подобного бесконтрольного расходования кислорода атмосферы, человечество еще не в состоянии оценить.

Кислород на нашей планете словно создан самой жизнь. Около 2 млрд лет назад содержание свободного кислорода в земной атмосфере начало возрастать. По прошествии времени содержание кислорода в атмосфере значительно изменялось, поскольку менялись уровни его образования и использования.

Основными источниками кислорода на Земле является планктон океана (60%) и леса (30%).

Из части атмосферного кислорода сформировался защитный озоновый слой, что послужило развитию наземных растений и животных. Озон формируется в верхних слоях стратосферы и в нижних слоях мезосферы.

Озон и атомарный кислород реагируют в кислородной атмосфере соответственно реакциям:

$O_3 + hv$ (380 нм) $= O_2 + O$,

$O_3 + O = 2O_2$,

$O + O + M = O_2 + M$.

Серия этих реакций образует «цикл Чепмена».

В 1974 году американскими учеными, специалистами в области химии стратосферы, Ш. Роулендом и М. Молина было доказано разрушительное действие хлорфторуглеродных соединений на стратосферный озон (за это открытие они удостоились нобелевской премии).

ХФУ (хлорфторуглероды) соединения, которые можно встретить как в быту, так и в промышленном производстве, – это пропелленты в аэрозольных упаковках, хладоагенты (фреоны) в холодильниках и кондиционерах.

Постепенно ХФУ поднимаются в верхний слой атмосферы и разрушают озонный слой – щит атмосферы, спасающий от УФ-излучения. Время жизни двух наиболее опасных веществ – Фреон-11 и Фреон-12 – от 70 до 100 лет. Сохранение таких темпов выброса ХФУ в атмосферу, грозит в течение 70 лет сократить количество стратосферного озона на 90%. И, по всей вероятности, произойдет следующее:

- исчезновение многих видов животных;
- рак кожи примет эпидемический характер;
- УФ-излучение неблагоприятно скажется на сельскохозяйственных культурах.

ХФУ под воздействием солнечных лучей создает каталитическую цепную реакцию в верхних слоях атмосферы, в результате которой один атом хлора способен разрушить до 100 000 молекул озона. Канцерогенным является УФ-излучение с длиной волны короче 320 нм. Предвидится, что каждый процент сокращения озонного слоя повлечет за собой увеличение числа случаев заболевания раком кожи на 5–6%. Технический прогресс и экономический рост в природопользовании вызывают увеличение потребления природных ресурсов. Многие виды природных ресурсов с позиции экономической эффективности их разработки близки к исчерпанию. Разработка новых ресурсов и усиление эксплуатации уже имеющихся, требуют огромных всевозрастающих капитальных вложений. Отсюда следует вывод: необходим переход на ресурсосберегающие пути, формирование дальнейшей экономической политики.

В то же время человечество стоит перед дилеммой: все большей необходимости в использовании мировых природных ресурсов, а с другой стороны - как сохранить окружающую среду от загрязнения. Существует понятие географическая среда, которая постоянно взаимодействует с природой и обществом, и понятие окружающая среда. И та, и другая необходима

человечеству для его материальной и духовной жизни. Немаловажный фактор - как географическая среда влияет на здоровье людей и это в последнее время очень волнует человечество.

Круговороты химических элементов и их сложных соединений осуществляются за счёт саморегулирующих процессов, в которых участвуют практически все составные части экосистем. Эти процессы в отличии от антропогенных превращений веществ, являются безотходными. В природе нет ничего бесполезного или вредного, даже от вулканических извержений есть польза, т.к. с вулканическими газами в воздух поступают необходимые живым организмам полезные элементы. Кислород поступает в атмосферу в результате фотосинтеза и расходуется организмами при дыхании. По мере развития цивилизации всё возрастающую роль на биогеохимический круговорот оказывает человек, но его влияние осуществляется в противоположной природе направлении. Человек нарушает сложившиеся круговороты веществ, и в этом проявляется его разрушительная по отношению к биосфере роль.

В результате химической обработки сырья выделяются большое количество вредных веществ (соединения фосфора, фтора, мышьяка, оксиды азота, серы, углерода, попутные отходящие продукты биологического синтеза и т. д.), выброс которых в окружающую среду приводит к ухудшению качества воздуха, водных ресурсов, почвы. Твердые отходы химических предприятий (золы, адсорбенты, шламы, осадки после химических реакций) занимают обширные площади, изымаемые из сельскохозяйственного и иного использования для захоронения и хранения. В среднем из 100 % перерабатываемого химического сырья в готовую продукцию превращается только 30-40 %. Остальное идет в отвалы, отходы, хвосто- и шламохранилища, выбрасывается в атмосферу.

Загрязнение окружающей среды ведет к ее химической деформации и не благоприятным геоклиматическим изменениям, создает угрозу здоровья людей, вызывает деградацию экологических систем.

Вместе с тем усилия по обеспечению устойчивого развития сталкиваются с такими общими препятствиями, как ограниченность природных ресурсов, хрупкость экосистем и подверженность стихийным бедствиям. Препятствия на пути развития и уязвимость могут быть обусловлены сочетанием таких факторов, как удаленность, географическая разбросанность, стихийные бедствия, высокая степень экономической открытости, узость внутренних рынков, ограниченность природных ресурсов и незащищенность экосистем.

Человеческое общество приобрело черты цивилизации потребления, экономика которой поддерживается преимущественно за счёт удовлетворения большого числа второстепенных, не жизненно важных потребностей, граничащие с абсурдом и безмерной роскошью потребности, что приводит, к избыточной техногенной нагрузке на природу и на окружающую человека среду.

Природопользование – влияние человеческой деятельности на окружающую среду, в результате прямого или косвенного воздействия.

Изучение процессов, происходящих в биосфере и влияние их на хозяйственную деятельность человека показывает, что предотвратить истощение природных ресурсов и деградацию природной среды может только создание экологически безотходных и малоотходных производств.

Рационального природопользования – это система взаимодействия человеческого общества и окружающей среды, построенная на основе научных законов природы и в наибольшей степени отвечающая задачам как развития производства, так и сохранения биосферы.

Список литературы:

1. Кривошеин Д.А., Муравей Л.А. Экология и безопасность жизнедеятельности: Учеб. пособие для вузов, М.: ЮНИТИ-ДАНА, 2000. - 447с.
2. Романов В., Романова Р. Выбросы вредных веществ и их опасности для живых организмов. Учеб. пособие, изд. «Физматкнига», 2009 – 390с.
3. Тетельмин В.В., Язев В.А. Основы рационального природопользования. Учеб. пособие, изд. «Интеллект», 2012 – 288с.

ВОЗМОЖНОСТЬ И ПЕРСПЕКТИВА ИСПОЛЬЗОВАНИЯ ОТХОДОВ ТЕПЛОЭНЕРГЕТИКИ В ПРОИЗВОДСТВЕ ЗАПОЛНИТЕЛЯ ДЛЯ КОНСТРУКЦИОННЫХ БЕТОНОВ

Сумарокова Любовь Сергеевна
студент, кафедра материаловедения в строительстве,
Уральский Федеральный университет,
РФ, г. Екатеринбург
E-mail: Sumarokova-94@mail.ru

Фомина Ирина Викторовна
научный руководитель, старший преподаватель, кафедра материаловедения в строительстве, Уральский Федеральный университет,
РФ, г. Екатеринбург

Приводятся результаты исследований золоцементных композиций с добавлением отходов теплоэнергетики и отходов производства нерудных строительных материалов. Установлено влияние дополнительного помола золы-уноса и влияния отходов дробления горной породы горнблендита на прочность золоцементного камня. Рассмотрены вопросы использования золоцементных композиций с добавлением отходов в производстве заполнителя для конструкционных бетонов.

В настоящее время в условиях нарастающей экологической напряженности в мире проблема рационального использования и эффективного сбережения природных ресурсов становится важнейшей задачей жизнедеятельности любого государства.

На территории Свердловской области, занимающей значительную часть Среднего Урала, эксплуатируется более десятка ТЭС, некоторые из них, такие как Рефтинская ГРЭС, являются крупнейшими в стране. На Рефтинской ГРЭС, сжигающей каменный уголь Экибастузского бассейна, образуется наибольшее количество золошлаков (до 5 млн. т), а уровень их утилизации составляет только 5 %. Использование отходов от сжигания твердого топлива – это не только проблема возрастающего загрязнения окружающей среды, но и вопрос экономии материальных и природных ресурсов [3].

По данным Агентства по прогнозированию балансов в электроэнергетике и по использованию золошлаков в России составляет только 10-13 %. В то время как уровень использования золошлакоотвалов в странах Европы: в Германии и в Дании достигло практически 100 %, в США, Великобритании, Польше и в Китае - 50-70 %. Это связано с тем, что зола-уноса в развитых странах является таким же товаром, причем дефицитным, как тепло и электроэнергия [6].

Увеличение объема производства и расширение номенклатуры специальных видов заполнителей для конструкционных бетонов можно осуществить, например, путем организации их производства из золы-уноса Рефтинской ГРЭС (Филиал ОАО «ЭнелОГК-5»).

Разработка комплексных технологических приемов, позволит модифицировать структуру золоцементного камня по средствам помола и добавок, что улучшит основные свойства золоцементного камня [4]. В связи с этим актуальной проблемой является научно-техническое обоснование методов совершенствования технологии получения золоцементного камня на основе промышленных отходов.

В работе были использованы следующие материалы: зола-уноса (ЗУ) Рефтинской ГРЭС (Свердловская область, п. Рефтинский) от сжигания каменного угля Экибастузского бассейна (Казахстан); пыль при дроблении горной породы горнблендита ($П_{гб}$) ОАО «Первоуральское рудоуправление» (Свердловская область, г. Первоуральск), портландцемент (ПЦ) в ЦЕМ I 42,5Н производства ОАО «Сухоложскцемент» (Свердловская область, г. Сухой Лог), химическая добавка Na_2SO_4.

Методика испытаний золоцементного камня была составлена таким образом, чтобы выявить влияние дополнительного помола золы-уноса и влияние отходов дробления горной породы горнблендита на прочность золоцементного камня, а также возможность использования золоцементной композиции для получения безобжигового зольного гравия.

Безобжиговый зольный гравий (БЗГ) – искусственный пористый заполнитель, получаемый в виде гранул из предварительно увлажненной смеси золы и портландцемент с последующим твердением.

Технология производства БЗГ состоит из следующих операций: подготовка сырьевых материалов, дозирование, смешивание компонентов, увлажнение смеси и формирование гранул требуемой крупности, их твердения при тепловлажностной обработке (ТВО (3+6+3 режим)). Для получения заполнителя подбирали составы смесей с постоянным количеством портландцемента, минеральной добавки и разным содержанием золы. Портландцемент и часть золы подвергались совместному помолу, вследствие чего было получено золоцементное вяжущее. В табл.1 приведены результаты испытаний образцов после тепловлажностной обработки, полученных из зольного теста содержащего минеральную и химическую добавку: пыль при дроблении горной породы горнблендита и Na_2SO_4.

Таблица 1.

Физико-механические свойства БЗГ после ТВО

Свойства	**Значения**		
	1 состав	**2 состав**	**3 состав**
Истинная плотность, кг/м^3	2318	2258	2327
Средняя плотность, кг/м^3	1412	1554	1620
Насыпная плотность, кг/м^3	890	960	1010
Водопоглощение, мас. %	4,0	5,7	6,3
Пористость, %	39	31	32
Прочность при сжатии в цилиндре, МПа	8	12	11
Примечание: 1 состав - 20 % ПЦ + 65 % ЗУ + 15 % $П_{гб}$ + 2 % Na_2SO_4; 2 состав - 40 % ЗЦВ + 45 % ЗУ + 15 % $П_{гб}$ + 2 % Na_2SO_4; 3 состав - 60 % ЗЦВ + 25 % ЗУ + 15 % $П_{гб}$ + 2 % Na_2SO_4. ЗЦВ – золоцементное вяжущее, полученное совместным помолом золы-уноса и портландцемента.			

По физико-механическим свойствам полученные заполнители удовлетворяют требованиям ГОСТ 9757-90 [1]. Установлено, что наибольшую плотность имеет состав № 3, немного ниже плотность у состава № 2, самая низкая плотность у состава № 1. Что касается значений предела прочности при сжатии, то наилучшие результаты получены у составов № 2 и № 3. Именно эти составы рекомендуется для производства заполнителя для бетона.

При помоле части золы с вяжущим происходит обнажение активной поверхности стекловидной фазы, что способствует повышению активности зол в цементных системах, и это приводит к увеличению прочностных характеристик золоцементного камня [5]. Введение пыли уплотняет структуру золоцементного камня, улучшая физико-механические свойства заполнителя. По ГОСТ 32496-2013 [2] полученный БЗГ имеет марки по прочности П350 и П400, по насыпной плотности, соответственно, марки М900, М1000 и М1100.

Применение легких пористых заполнителей позволяет получать эффективные легкие бетоны для теплоизоляции, стеновых панелей, разнообразных несущих конструкций. Замена обычных тяжелых заполнителей пористыми позволяет существенно изменить свойства бетона в желаемом направлении: уменьшить плотность, улучшить теплоизоляционные свойства. В то же время достаточная прочность ряда пористых заполнителей обеспечивает возможность получения на их основе конструкционных легких бетонов высокой прочности.

Список литературы:

1. ГОСТ 9757-90. Гравий, щебень и песок искусственные пористые. Технические условия. Введ. 01.01.91. М.: Издательство стандартов, 2007. – 9с.;
2. ГОСТ 32496-2013. Заполнители пористые для легких бетонов. Технические условия. Введ. 01.01.15. М.: Издательство стандартов, 2014. – 17 с;
3. Капустин Ф.Л., Фомина И.В. Получение легкого заполнителя на основе золы-уноса Рефтинского ГРЭС для конструкционных бетонов // Экология и промышленность России. – 2014. – № 8. – 32-34 с.;
4. Капустин Ф.Л., Фомина И.В. Малоцементные композиции для получения безобжигового зольного гравия // IV Международный семинар-конкурс молодых ученых и аспирантов, работающих в области вяжущих веществ, бетонов и сухих смесей. – 2013. [электронный ресурс] – Режим доступа. – URL:http://elar.urfu.ru/bitstream/10995/27614/1/ ivmim_2012_14.pdf (дата обращения: 2015);
5. Каримов И. Влияние тонкодисперсных минеральных наполнителей на прочность бетона: Автореф. дис… канд. техн. наук – Уфа, 2005. – 13 с.;
6. Колбина Л. Модернизация на Рефтинской ГРЭС делает актуальным расширение применения золошлаковых отходов в регионе // Эксперт-Урал. – 2015. – № 43. – 18 с.

ДЛЯ ЗАМЕТОК

«НАУЧНОЕ СООБЩЕСТВО СТУДЕНТОВ XXI СТОЛЕТИЯ. ТЕХНИЧЕСКИЕ НАУКИ»

Электронный сборник статей по материалам XLV студенческой международной заочной научно-практической конференции

№ 8 (44)
Сентябрь 2016 г.

В авторской редакции

Издательство АНС «СибАК»
630049, г. Новосибирск, Красный проспект, 165, офис 4.
E-mail: mail@sibac.info

СибАК

www.sibac.info