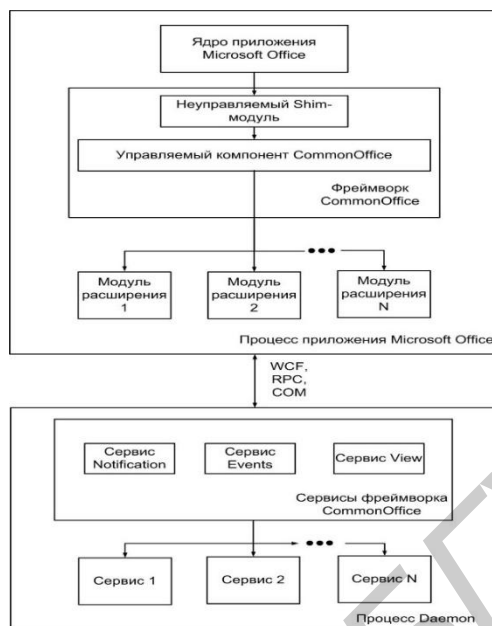


обслуживания модулей (модель Microsoft Office) на модель, при которой модули обслуживаются параллельно (параллельное обслуживание модулей берет на себя фреймворк CommonOffice).



Список использованных источников:

1. Слепцова, Л. Программирование на VBA в Microsoft Office 2010 / Л. Слепцова. – М. : Вильямс, 2010. – 432 с.
2. Thangaswamy, V. VSTO 3.0 for Office 2007 Programming / V. Thangaswamy – Packt Publishing, – 2009 – 260 p.

ПЕРСПЕКТИВЫ АВТОМАТИЗИРОВАНИЯ ИНЖЕНЕРНЫХ РАСЧЕТОВ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ ПОЖАРНОЙ БЕЗОПАСНОСТИ

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

Корначева Т.А., старший инспектор НИИ ПБ и ЧС МЧС Беларуси

Ю.С.Иванов, к.т.н., НИИ ПБ и ЧС МЧС Беларуси

Технические нормативно-правовые акты (далее – ТНПА) в области пожарной безопасности направлены на предотвращение возникновения пожара, а также воздействия на людей его опасных факторов. В то же время ТНПА не должны противоречить экономическим критериям эффективности на всех стадиях жизненного цикла объекта (научная разработка, проектирование, строительство, эксплуатация) [1]. Одним из важных этапов при проектировании и строительстве объектов является обеспечение пожарной безопасности, в рамках которого необходимо осуществить организационно-технические и инженерные мероприятия. В зависимости от назначения объекта требования по пожарной безопасности аккумулируются из различных ТНПА.

В области противопожарного нормирования и стандартизации распространены два основных метода нормирования: нормативный – установление минимально-допустимых критериев согласно правилам и требованиям нормативов и функционально-ориентированный (расчетный) метод, который позволяет максимально уточнить требования пожарной безопасности для конкретного объекта, учитывая его экономическую эффективность и целесообразность [2].

Услуги по осуществлению экспертной деятельности, такие как разработка паспортов пожарной безопасности, проведение расчетов по обеспечению (оценке) пожарной безопасности (либо выборка из указанного перечня работ), относятся к лицензируемым видам деятельности согласно п. 10.7 [3]. Большое значение имеет наличие инженерно-технической квалификации и знаний в области предотвращения пожаров у специалистов, выполняющих данные расчеты, т.к. любые ошибки могут привести к неверным интерпретациям расчетных результатов и, как следствие, – к снижению уровня противопожарной защиты.

В настоящее время в Республике Беларусь автоматизировано несколько расчетных методик в области противопожарного нормирования и стандартизации, которые размещены на web-сайте МЧС [4]. Однако, эти программные средства (далее – ПС) имеют ряд недостатков: 1. разработаны для локального использования и исключают возможность работы с ними через web-доступ, что не гарантирует использование пользователем актуальной версии программы; 2. не являются кроссплатформенными и работают только на операционной системе (далее – ОС) MicrosoftWindows, пользователи других ОС (в том числе мобильных) не могут воспользоваться этими программами; 3. для решения комплексных задач потребуется использование сразу нескольких приложений, в то же время функционал некоторых из них может быть объединен в одном ПС; 4. отсутствует возможность сохранения истории выполненных расчетов или создания шаблонов расчетов для их применения при формировании отчета.

В целях создания более совершенного программного обеспечения ведется разработка информационно-вычислительного комплекса (далее – ИВК) на базе web-технологий с доступом через сеть Интернет. ИВК позволит централизовать и унифицировать проведение инженерных расчетов и существенно сократить трудозатраты на экспертизу проектной документации. Использование ИВК работниками инспекции государственного пожарного надзора предоставит возможность осуществить достоверную экспресс-проверку инженерных расчетов в области противопожарного нормирования и стандартизации в сжатые сроки при осуществлении надзорной деятельности.

Список использованных источников:

1. Система стандартов безопасности труда. Пожарная безопасность. Общие требования: ГОСТ 12.1.004-91. – Введ. с 01.07.92 / Государственный стандарт союза ССР. – М.: Издательство стандартов, 1992. – 91 с.
2. Татарников С. Расчетные методы обеспечения пожарной безопасности при проектировании зданий и сооружений / С. Татарников // Служба спасения 101. – 2010. – №7(151). – С.27-29
3. О лицензировании отдельных видов деятельности: Указ Президента Республики Беларусь 1 сентября 2010 г. № 450. – М.: Зар-но в Нац. реестре правовых актов Республики Беларусь 03.09.2010 г. № 1/11914
4. Расчетные программы для проектировщиков [Электронный ресурс] / Официальный сайт Министерства по чрезвычайным ситуациям Республики Беларусь – Режим доступа: <http://mchs.gov.by/rus/main/business/programs>. – Дата доступа: 21.03.2016.

ЭЛЛИПТИЧЕСКИЕ КРИВЫЕ И ИХ ПРИМЕНЕНИЕ В КРИПТОГРАФИИ

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

Короткевич А. В.

Ярмолик В. Н. – д-р. техн. наук, профессор

Обеспечение безопасности информации является одной из важнейших проблем современного общества. Такая безопасность может быть достигнута с использованием различных криптографических методов, одними из самых передовых и перспективных среди которых являются криптосистемы, основанные на свойствах эллиптических кривых.

В общем случае уравнение эллиптической кривой имеет вид:

$$y^2 + axy + by = x^3 + cx^2 + dx + e,$$

где x, y – переменные; a, b, c, d, e – действительные числа.

Для определения операции сложения для точек на эллиптической кривой сделаем следующие предположения:

1. На плоскости существует бесконечно удаленная точка $0 \in E$, в которой сходятся все вертикальные прямые.

2. Будем считать, что касательная к кривой пересекает точку касания два раза.

3. Если три точки эллиптической кривой лежат на прямой линии, то их сумма есть 0.

Введем следующие правила сложения точек на эллиптической кривой [1]:

1. Точка 0 выступает в роли нулевого элемента. Так $0 = -0$ и для любой точки P на эллиптической кривой $P + 0 = P$.

2. Вертикальная линия пересекает кривую в двух точках с одной и той же координатой x – скажем, $S = (x, y)$ и $T = (x, -y)$. Эта прямая пересекает кривую и в бесконечно удаленной точке. Поэтому $S + T + 0 = 0$ и $S = -T$.

3. Чтобы сложить две точки P и Q с разными координатами x , следует провести через эти точки прямую и найти точку пересечения ее с эллиптической кривой (рисунок 1). Если прямая не является касательной к кривой в точках P или Q , то существует только одна такая точка, обозначим ее S . Согласно нашему предположению $P + Q + S = 0$. Следовательно, $P + Q = -S$ или $P + Q = T$.

Чтобы удвоить точку Q следует провести касательную в точке Q и найти другую точку пересечения S с эллиптической кривой. Тогда $Q + Q = 2Q = -S$.