руемого района являются возможные гипотетические зоны взрыва (выброса) и зоны возможного поражения в случае аварий на объекте.

В докладе рассматриваются алгоритмические подходы к многоступенчатому экологическому мониторингу и приборное оснащение позволяющее обеспечить контроль территорий на предприятиях с химическим воздействием на окружающую среду.

Сохраняется сложная экологическая обстановка на территории России и высокий уровень опасностей природного характера. Промышленный рост металлургической, химической и др. опасных отраслей экономики России в условиях значительного износа основных производственных фондов, снижение технологической дисциплины и квалификации обслуживающего персонала может привести к увеличению числа техногенных катастроф. Особую опасность может представлять технологический терроризм экстремистского и религиозного толка на радиационно и химически опасных предприятиях.

Усложняющийся характер опасностей и угроз различного характера требует изменения приоритетов в государственной политике по обеспечению безопасности населения и территории от опасностей и угроз различного характера, в конечном итоге позволит вместо «культуры реагирования на ЧС» перейти на «культуру предупреждения».

1. Габричидзе, Т.Г. Система многоступенчатого экологического мониторинга и ее сопряжение с АИУС РСЧС. Аварии и катастрофы. Предупреждение и ликвидация последствий. Учебное пособие в 6 книгах. Книга 6 /Т.Г. Габричидзе, В.А. Алексеев, П.М. Фомин. – Под ред. В.А. Котляровского. – М.: Изд-во АСВ, 2003. – С.140 –158.

УДК 681.3

ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ В СИСТЕМЕ ОРГАНИЗАЦИИ КОНКУРСНЫХ ТОРГОВ

Артамонов В.А., Короткевич О.С.

Белорусский национальный технический университет, Минск, Беларусь

Создание системы электронных конкурсных торгов предполагает адекватную техническую реализацию правовых отношений между заказчиками и поставщиками товаров и услуг. При традиционном документообороте принимаемые сторонами обязательства и предоставляемые ими сведения подтверждаются завизированными бумажными документами. Однако ряд необходимых условий, например, конфиденциальность поданной в запечатанном конверте заявки, либо неотказуемость от неё к моменту подведения итогов конкурса, технически обеспечиваются исключительно добросовестностью организатора конкурса.

При переходе к электронному документообороту техническая реализация этих специфических моментов правовых отношений, помимо прочих, должна гарантировать выполнение (или по крайней мере существенно затруднить нарушение) сторонами предусмотренных условий.

Техническая реализация этих специфичных условий основана на использовании инфраструктуры открытого ключа (PKI).

Архитектура PKI

Защита информации в PKI (public key infrastructure) основана на методе асимметричного шифрования с использованием пары ключей: открытого и закрытого.

В асимметричном шифровании криптоалгоритмы составляют асимметричные пары. Если один из алгоритмов использует закрытый ключ, тогда парный ему алгоритм – соответствующий открытый ключ. Такие пары составляют алгоритмы собственно асимметричного шифрования (зашифровки и расшифровки), а также выработки и проверки электронной цифровой подписи (ЭЦП). Владелец закрытого ключа всегда применяет один алгоритм из пары, а все остальные, знающие только открытый ключ, – парный ему алгоритм.

ЭЦП – это реквизит электронного документа, вырабатываемый с помощью закрытого ключа и проверяемый с помощью соответствующего открытого ключа. Практически невозможно получить ЭЦП, не зная закрытого ключа, или изменить документ так, чтобы правильно выработанная ЭЦП осталась неизменной. Поэтому ЭЦП с высокой степенью достоверности свидетельствует, во-первых, о неизменности подписанного ей документа и, во-вторых, что выработавший ее субъект знает закрытый ключ. Неотказуемость от подписи основывается на том, что правильно подписать документ можно, только владея закрытым ключом.

Каждая криптосистема с открытым, ключом имеет собственный способ генерации ключевой пары и включает свой набор криптоалгоритмов. Не все асимметричные криптосистемы универсальны, т.е. реализуют как технологию ЭЦП, так и конфиденциальную передачу информации, но каждая из них обеспечивает аутентификацию (проверку подлинности) субъекта, которая сводится к доказательству владения им соответствующим закрытым ключом.

Приемы защиты на базе асимметричного шифрования

Рассмотрим принципиальную схему выработки и проверки ЭЦП с применением алгоритмов асимметричного шифрования. Для выработки ЭЦП подписываемый документ подвергается хэшированию (см. рисунок 1), а полученный хэш зашифровывается закрытым ключом.

Рисунок 1 – Схема выработки ЭЦП при ассиметричном шифровании

Хэширование применяется для сокращения объема шифруемой информации и повышения тем самым производительности. Хэш-функция, не будучи взаимно однозначным отображением, вырабатывается таким образом, чтобы было практически невозможно изменить документ, сохранив результат хэширования. По хэшу невозможно восстановить исходный документ, но это и не нужно, поскольку проверка ЭЦП заключается в сравнении расшифрованной открытым ключом ЭЦП с хэшем документа.

Совпадение с высокой степенью достоверности гарантирует, во-первых, неизменность документа (защиту от подделки), и, во-вторых, что его подписал владелец закрытого ключа. Схема проверки ЭЦП при ассиметричном шифровании изображена на рисунке 2.

Аутентификация субъекта сводится к доказательству того, что он владеет закрытым ключом, соответствующим опубликованному открытому. В криптосистемах, поддерживающих технологию ЭЦП, доказательство владения заключается в том, что субъект подписывает своим закрытым ключом присланный ему запрос и посылает его обратно. Если при проверке оказалось, что запрос подписан правильно, то субъект действительно обладает соответствующим закрытым ключом.

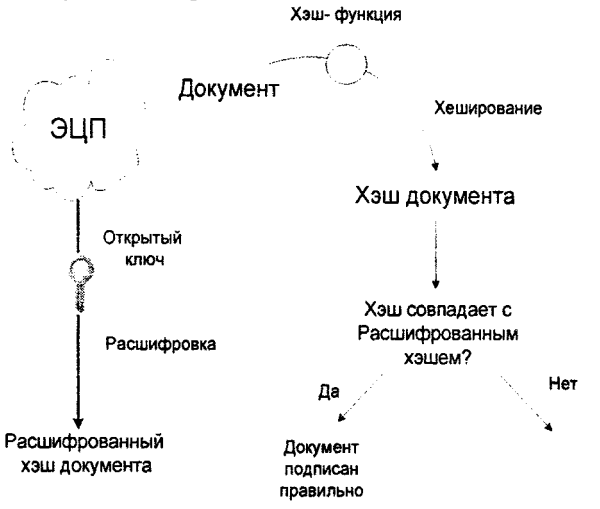

Рисунок 2 – Схема проверки ЭЦП при ассиметричном шифровании

Асимметричные алгоритмы шифрования позволяют обеспечить конфиденциальность при передаче сообщения от одного субъекта другому. Для этого отправителю достаточно зашифровывать сообщение открытым ключом получателя. Поскольку расшифровать сообщение можно только зная соответствующий закрытый ключ, это гарантирует, что прочитать его не сможет никто, кроме получателя.

Далее в докладе рассматриваются практические аспекты организации электронной системы проведения конкурсных торгов с использованием технологии ASP.NET.

УДК 681.3

ТЕХНОЛОГИЯ МОДЕЛИРОВАНИЯ СЕТЕВЫХ КОНФИГУРАЦИЙ

Артамонов В.А., Красинский Д.Н.

Белорусский национальный технический университет, Минск, Беларусь

Эталонная модель OSI описывает, каким образом информация проделывает путь через среду сети (например, провода) от одной прикладной программы (например, программы обработки крупноформатных таблиц) до другой прикладной программы, находящейся в другом компьютере. Эталонная модель OSI не является реализацией сети. Она только определяет функции каждого уровня. В этом отношении она напоминает план для постройки корабля. Точно также как для выполнения фактической работы по плану могут быть заключены контракты с любым количеством кораблестроительных компаний, любое число поставщиков сети могут построить протокол реализации по спецификации протокола. И если этот план не будет предельно понятным, корабли, построенные различными компаниями, пользующимися одним и тем же планом, пусть незначительно, но будут отличаться друг от друга. Примером самого незначительного отличия могут быть гвозди, забитые в разных местах.

Кроме того, разные люди, реализующие один и тот же проект, всегда интерпретируют его немного по-разному. И наконец, неизбежные ошибки реализации приводят к тому, что изделия разных реализаций отличаются исполнением. Этим объясняется то, что реализация протокола одной компании не всегда взаимодействует с реализацией этого протокола, осуществленной другой компанией.

Как правильно спроектировать сеть и проверить её работоспособность наглядно? Для этого необходимо смоделировать предполагаемую сетевую конфигурацию, настроить параметры всех элементов сети и проверить функционирование как всей