Главный редактор - д.э.н., профессор К.А. Кирсанов
тел. для справок: +7 (925) 853-04-57 (с 11^{00} – до 18^{00})
Опубликовать статью в журнале - http://naukoznanie.ru

Бойков Александр Игоревич
Boikov A.I.
Прохоров Д.А.
Prohorov D.A.
НОУ ВПО ИГУПИТ

Методы защиты электронного документооборота

Protection methodsof electronic documents

Аннотация: Статья посвящена вопросам защиты электронного документооборота (ЭДО), который является системообразующим компонентом практически любого процесса управления административного типа. Построение комплексной системы защиты информации ЭДО требует точного описания объектов и целей защиты. Наиболее важной задачей в электронном докуметообороте является защита подписи.

Ключевые слова: Электронный документооборот, защита электронного документооборота, цифровая подпись.

The Abstract: The article is devotedto the protection ofelectronic document management(EDM), which is a backbonecomponent in almost everytypeof administrativecontrol process. Buildingan integrated systemof information protectionEDM requiresan accurate descriptionof objects andprotection purposes. The mostimportant taskis to protectelectronic documentssignature.

Keywords: Electronic document management,electronic documentprotection, digital signature.

***

Электронный документооборот (ЭДО) является системообразующим компонентом практически любого процесса управления административного типа. Построение комплексной системы защиты информации ЭДО требует точного описания объектов и целей защиты. Наиболее важной задачей в электронном докуметообороте является защита подписи.

Электронная цифровая подпись (ЭЦП) играет ключевую роль в общей совокупности систем криптографической защиты информации (СКЗИ). Основными составляющими информационной безопасности являются конфиденциальность, аутентификация и контроль целостности.

Конфиденциальность обеспечивается шифрованием, а аутентификация и контроль целостности — применением ЭЦП. Как правило, все элементы используются комплексно. «Но есть приложения, где основная роль отводится ЭЦП, например, в системах электронного документооборота. И, наоборот, для организации VPN[i], защиты телефонных переговоров и т.п. приоритет имеет шифрование.

Если говорить о темпах развития, то, безусловно, сегмент ЭЦП является бурно растущим. Это иллюстрируется следующими данными: еще в декабре 2004 года удостоверяющих центров насчитывалось около 150, а валидных сертификатов ключей ЭЦП около 50 тысяч. По данным на ноябрь 2005 года эти цифры уже вдвое превышены. То есть можно будет констатировать более чем стопроцентный рост по итогам года. Естественно, приведенные данные касаются публичных УЦ, привести точные цифры по закрытым, корпоративным удостоверяющим центрам невозможно по причине отсутствия какой-либо системы учета.

Главный редактор - д.э.н., профессор К.А. Кирсанов
тел. для справок: +7 (925) 853-04-57 (с 11^{00} – до 18^{00})
Опубликовать статью в журнале - http://naukoznanie.ru

Емкость рынка всегда будет определяться количеством пользователей прикладных систем с ЭЦП. Потенциальная цифра, скорее всего, имеет порядок десятка или полутора десятков миллионов, но когда такое количество валидных электронных подписей будет реально работать, наверное, сегодня не сможет спрогнозировать никто.

Необходимо обратить внимание и на национальную специфику развития ЭЦП. В России превалирует использование национальных криптоалгоритмов. Скажем, если организация относится к госсектору или сотрудничает с госструктурами, то она обязана использовать национальную криптографию, что закреплено на законодательном уровне. «Самым удивительным и отрадным фактом является то, что многие коммерческие организации используют российские криптоалгоритмы, в то время как закон «О техническом регулировании» предоставляет им свободу выбора. Действующее законодательство в части разработки и использования СКЗИ защищает интересы России и российских разработчиков. Возможно, это объясняется тем, что позиции России в криптографии традиционно сильны — во многом благодаря стратегии российских спецслужб, располагающих одним из мощнейших в мире научно-образовательных центров — ИКСИ (Институт криптографии, связи и информатики).

Второй уровень развития ЭЦП может быть назван организационным. Отсутствует единая федеральная программа координации деятельности между ведомствами в области электронного документооборота и ЭЦП. Отсюда, собственно, и проистекают все обозначенные выше проблемы правового характера, а также проблемы стандартизации.

Это же обстоятельство объясняет то, что корпоративный сектор растет гораздо быстрее, причем не только с точки зрения ЭЦП, а с точки зрения построения защищенной информационной инфраструктуры в целом. Поскольку мы говорим об информационной безопасности, по понятным причинам компании не распространяются о том, как именно организована защита информации и каким образом функционирует удостоверяющий центр каждой из них.

Однако, если речь идет о провайдерах услуг в области электронной цифровой подписи, то такие компании стремятся к публичности. Первое место среди подобных сервисов занимает организация сдачи налоговой отчетности. На сегодняшний день 300 публичных удостоверяющих центров поддерживают более 100 тыс. валидных сертификатов ключей ЭЦП. На втором месте — банковские операции. Наиболее прогрессивные игроки банковского рынка уже осознали необходимость и преимущества использования решений на базе инфраструктуры открытых ключей и развернули собственные удостоверяющие центры. К таким «пионерам» можно отнести Альфа-Банк, «Возрождение», «Петрокоммерц-банк», ВИП-банк и многие другие

Почему задача защиты документооборота становится актуальной только сейчас?

Если ответить на этот вопроспредельно коротко, то просто пришло время. Можно выделить несколько основных причин, по которым именно сейчас вопросы развития ЗЭД становятся объектом внимания:

– при непосредственном участии первых лиц государства интенсивно развиваются государственные услуги, оказываемые в электронном виде, обмен электронными документами быстро достигает критического объема, при котором неизбежно встают вопросы защиты конфиденциальной информации, в частности, персональных данных;

– услуги, предоставляемые в электронном виде, должны базироваться на ЗЭД, поскольку формированию электронного документа в ответ на запрос от физического или юридического лица, как правило, предшествует огромная работа по обмену документами между многими ведомствами, который далеко не всегда надо делать общедоступным;

Главный редактор - д.э.н., профессор К.А. Кирсанов
тел. для справок: +7 (925) 853-04-57 (с 11^{00} – до 18^{00})
Опубликовать статью в журнале - http://naukoznanie.ru

– наконец приходит массовое понимание необходимости внедрения СЭД в государственных организациях, работающих с гражданами и юридическими лицами, и применения средств защиты для обеспечения целостности и конфиденциальности информации, содержащейся в электронных документах, а также подтверждения авторства электронных документов;

– появился Закон «Об электронной подписи», который дает возможность более широко подойти к защите электронных документов, в частности, использовать различные технологии для защиты СЭД в зависимости от их принадлежности и других условий;

– появляются реальная необходимость обеспечения и понимание механизмов придания электронным документам юридической силы наравне с бумажными документами.

Что же такое защищенный электронный документооборот?

Основная идея в том, что к задаче защиты системы электронного документооборота надо подходить с точки зрения классической защиты информационной системы. А именно, кроме известных уже среди разработчиков СЭД задач по защите электронных документов, таких как:

– аутентификация пользователей и разделение доступа;

– подтверждение авторства электронного документа;

– контроль целостности электронного документа;

– конфиденциальность электронного документа;

– обеспечение юридической значимости электронного документа

Для организации ЗЭД необходимо использовать механизмы, обеспечивающие:

– контроль целостности используемого программного обеспечения;

– регистрацию событий в информационных системах;

– криптографическую защиту;

– межсетевое экранирование;

– виртуальные частные сети;

– антивирусную защиту;

– аудит информационной безопасности, которые хорошо известны специалистам по защите информации.

Безусловно, строительство «электронного правительства» должно дать мощный толчок развитию систем защиты электронного документооборота (ЗЭД). Например, развитие таких массовых систем, как система госзакупок, невозможно без ЗЭД, По сути, сами торги должны являться своего рода вершиной пирамиды, основу которой должен составлять защищенный обмен документами (сбор заявок от потребителей, бюджетирование, обоснование стоимостии т. д.). Не менее важна роль ЗЭД и при оказании государственных услуг с применением электронных документов. Здесь в полной мере возникнут и вопросы межведомственного обмена защищенными документами, который ляжет в основу подготовки по заявке гражданина или организации электронного документа, имеющего правовые последствия.

Главный редактор - д.э.н., профессор К.А. Кирсанов
тел. для справок: +7 (925) 853-04-57 (с 11^{00} – до 18^{00})
Опубликовать статью в журнале - http://naukoznanie.ru

ЛИТЕРАТУРА

1. Баканова Н. Б. Проектирование подсистем сбора и анализ информации для территориально распределенных информационных систем // Научно-техническая информация. Серия 1. Организация и методика информационной работы / Нижегородский госуниверситет. – Нижний - Новгород, 2006. с. 26-38.

2. Келдыш Н. В. Направления развития и безопасности современных систем органов управления. // Материалы Научно-практ. конференции / ВА МО. М., 2007, с. 31-39.

3. Соколов А. В., Шаньгин В. Ф. Защита информации в распределенных корпоративных сетях и системах. – М. : ДМК Пресс, 2002, с. 16-28.