Кирбенев Ю.В.
Научный руководитель: А.В.Провоторов
Муромский институт (филиал) федерального государственного образовательного учреждения высшего образования «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых»
602264, г. Муром, Владимирская обл., ул. Орловская, 23
mrblackops@Mail.ru

Система защиты информации методом присвоения персональных сертификатов пользователям

Присвоение персональных сертификатов пользователям является одной из самых сложных, иинтересных задач при работе с защитой информации.

Применение данной технологии может быть использовано в любой сфере деятельности: банковская сфера, перерабатывающие предприятия, заводы, фабрики и так далее. В данном случае, была выбрана сфера деятельности: ювелирное предприятие, которое занимается: разработкой, созданием и выпуском готовой ювелирной продукции и на котором необходимо обеспечить безопасную передачу данных по внутрисетевым каналам связи между тремя основными отделами.

Первоочередными задачами, стоящими перед разработчиком являются:

- «Простота использования системы защиты»;
- «Использование новейшего алгоритма шифрования, для обеспечения максимальной степени защищенности данных»;
- «Стоимость разработки системы защиты».

Особое внимание следует уделить процессу автоматизации при работе с системой защиты. Данный процесс имеет особые перспективы в области защиты информации.

- Формирование уникального ключа пользователя, на основании технических данных оборудования, установленного на персональном компьютере происходит в автоматическом режиме;
- Формирование нового персонального сертификата администратором сети, а так же шифрование данных внутри сертификата – происходит в автоматическом режиме.

Выполнение вышеуказанных действий в автоматическом режиме будут являться новым шагом в сфере защиты информации.

Так же, важным критерием при разработке системы защиты является правильность построения алгоритма шифрования.

За основу взята технология X509.Crypto – которая определяет стандартные форматы данных и процедуры распределения открытых ключей с помощью соответствующих сертификатов с цифровыми подписями.

Использование данной технологии позволит решить поставленную задачу в полной форме, а так же предоставит возможность совершить существенный прорыв в области применения программно-технических методов защиты информации.

При формировании нового персонального сертификата происходит привязка данного сертификата к уникальному ключу пользователя, что на 100% исключает факт утечки конфиденциальных данных методами: копирования, подмены либо разбора программного кода злоумышленником.

Стоимость разработки системы защиты является минимальной, так как алгоритм шифрования частично-бесплатен и основная часть функций данного алгоритма, для выполнения всех необходимых методов шифрования данных – входит в открытый для разработчиков особый контент.