Тип работы: Дипломная работа

Предмет: Информационные системы и процессы

В рамках данной работы проведен анализ законодательных и технологических аспектов использования аналогов собственноручной подписи (электронной подписи).
Основная область применения аналогов собственноручной подписи – системы электронного документооборота.
1.Нормативное регулирование работы с электронной подписью.
63-ФЗ «Об электронной подписи» определен круг субъектов правоотношений (участников электронного взаимодействия), который включает 4 категории [1]:
1) государственные органы;
2) органы местного самоуправления;
3) организации;
4) граждане.
Федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи является Министерство связи и массовых коммуникаций Российской Федерации. Минкомсвязь России осуществляет аккредитацию удостоверяющих центров, ведет Перечень аккредитованных удостоверяющих центров.
Контроль за соблюдением правил пользования СКЗИ и условий их использования, указанных в правилах пользования на них, осуществляется:
 обладателем, пользователем (потребителем) защищаемой информации, установившим режим защиты информации с применением СКЗИ;
 собственником (владельцем) информационных ресурсов (информационных систем), в составе которых применяются СКЗИ;
 ФСБ России в рамках контроля за организацией и функционированием криптографической и инженерно-технической безопасности информационно-телекоммуникационных систем, систем шифрованной,

засекреченной и иных видов специальной связи.
Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005) утверждено приказом ФСБ России от 09.02.2005 г. №66.
В соответствии с Федеральным законом «О лицензировании отдельных видов деятельности» от 4 мая 2011 г. N 99-ФЗ
Лицензированию подлежат следующие виды деятельности:
- разработка, производство, распространение шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств;
- выполнение работ, оказание услуг в области шифрования информации;
- техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя.
Как было показано выше, использование электронной подписи производится в документах различного типа, юридическая значимость и её роль в организационном документообороте которых различна.
Так, некоторые документы, подписанные электронной подписью, связаны с проведением платежных операций и компрометация электронной подписи в данном случае может привести к прямым финансовым потерям. Электронные подписи, используемые для сдачи отчетности в государственные органы, при их компрометации потенциально могут привести к утечке информации, соответствующей учетным данным организации, что может составлять коммерческую тайну или персональные данные сотрудников. Утечка информации данного типа является наказуемой согласно федеральному законодательству в области работы с персональными данными. Компрометация электронной подписи, предназначенной для работы с электронными площадками, может привести к срыву контрактов и прямым финансовым убыткам фирмы.
Документы другого типа используются лишь для внутриорганизационного документооборота, а зачастую дублируются бумажными носителями и последствия компрометации электронной подписи в данном случае не приводят к ощутимым последствиям для организации.
Таким образом, для классификации по степеням значимости и состава электронных подписей проведена их классификация по составу и квалификации. Каждому из классов электронной подписи согласно принятым стандартам сопоставлены меры организационного и технологического характера в области защиты от компрометации, правил учета и обращения ключевых носителей.
Согласно действующему законодательству, принята следующая классификация электронных подписей (рис.1). Как показано на рисунке 1, в настоящее время электронные подписи подразделяются на виды:
- простая электронная подпись;
- усиленная электронная подпись, имеющая квалифицированные и неквалифицированные виды.
Простая электронная подпись – это вид электронной подписи, использующий для подтверждения факта подписи определенного лица набор кодов, паролей или иных средств.
Основными характеристиками простой электронной подписи являются:
− наличие подтвержденного факта формирования простой подписи определенного лица;
− включение электронной подписи в документы;
− ключ простой ЭП используется в рамках правил, установленных оператором информационной системы;
− использование простой ЭП производится в соответствии с регламентами, которые устанавливаются операторами информационной системы.
Простая электронная пропись может указывать на лицо, которое подписало документ, но при этом невозможно установить факт неизменности подписи и подписанных файлов после простановки ЭП.
Область применения простой электронной подписи: внутриорганизационные системы документооборота.
Для неквалифицированной электронной подписи характерно:
− содержание в самом электронном документе, либо наличие связи с документом;
− возможность подтверждения факта формирования ЭП определенным специалистом;
− возможность проверки с использованием СКЗИ при наличии соответствующего ключа;
− формирование с использованием СКЗИ и ключей электронной подписи;
− использование в рамках правил, установленных операторами информационной системы.
Неквалифицированная ЭП может работать как с сертификатами ключа проверки электронной подписи, созданными удостоверяющим центром, так и без них.
Неквалифицированная ЭП позволяет обнаруживать факты внесения изменений в электронные документы

после момента его заверения ЭП абонентом системы.
Область использования усиленной неквалифицированной электронной подписи: электронные торги, заверение отчетности в государственные органы.
Квалифицированная электронная подпись − это электронная подпись, соответствующая всем параметрам неквалифицированной электронной подписи и имеющая дополнительные признаки:
− обязательность совместного использования сертификатом ключа проверки ЭП, который выпущен в аккредитованным удостоверяющем центре;
− для подписи документа и проверки ЭП используется комплекс средств ЭП, прошедших сертификацию в рамках действующего законодательства.
Область использования усиленной квалифицированной электронной подписи: системы документооборота в нотариате, банковские информационные системы, системы госзакупок.
Получение сертификата электронной подписи производится в специализированных удостоверяющих центрах.
Цифровой сертификат предоставляет информацию об объекте, объектом может быть пользователь, компьютер, служба, сетевое устройство и т.д. Выдается он центром сертификации и ассоциирован с парой ключей (секретным и публичным).
Цифровой сертификат – это структура данных (например, файл) состоящая из раздела данных и раздела подписи. Раздел данных содержит открытые данные, включающие как минимум открытый ключ. Раздел подписи состоит из подписи центра сертификации [3].
Перечень и структура данных сертификата определяется его стандартом, в настоящее время используется стандарт X509 версии 3.
Рассмотрим сферу действия 149-ФЗ.
1. Данным законодательным актом регулируются правоотношения в области:
1) осуществления прав, связанных с поиском, получением, передачей, производством и распространением информации;
2) использованием информационных технологий (включая системы электронного документооборота);
3) обеспечением защиты информации при использовании информационных систем.
Правовое регулирование отношений, которые возникают в области работы с информационными ресурсами, информационными технологиями и системами защиты информации, основываются на принципах:
1) свободы поиска, получения, обмена, производства и распространения информации с использованием любых законных способов;
2) возможности управления доступом к информационным ресурсам в соответствии с требованиями федерального законодательства;
3) обеспечения открытости информации, связанной с деятельностью государственных органов и органов местного самоуправления и свободного доступа к информационным ресурсам;
4) принципов равноправия представления и получения информации на языках народов Российской Федерации в рамках функционирования информационных систем, включая системы ЭДО;
5) принципы обеспечения безопасности государства в процессе реализации информационных систем, работы с ними и обеспечении защиты содержащихся в них данных;
6) принципы достоверности информации и своевременности ее предоставления;
7) неприкосновенности частной жизни, недопустимости сбора, хранения, в также использования, распространения данных о частной жизни граждан без получения их согласия;
8) недопустимости установки в нормативных правовых актах какого-либо приоритета при использовании одних информационных систем перед другими, при условии когда необходимость использования определенных информационных систем для создания и эксплуатации государственных информационных систем не установлена в федеральных законах.
В статье 11 данного федерального закона определены требования к системам электронного документооборота.
В законе закреплена обязанность органов государственной власти, органов местного самоуправления, организаций, осуществляющих в рамках федеральных законов определённые публичные полномочия по предоставлению в соответствии с выбором граждан и организаций информации в электронных форматах, подписанной усиленной квалифицированной электронной подписью, и (или) документов на бумажном носителе, кроме случаев, когда порядок предоставления данной информации устанавливается в федеральных законах или иных нормативных правовых актах Российской Федерации, в которых регулируются правоотношения в соответствующей области деятельности.

2. Данные, необходимые для осуществления государственных полномочий, осуществляемых в рамках требований федеральных законов отдельные публичные полномочия, могут представляться гражданами и организациями в электронных форматах при наличия электронной подписи, если другие требования не установлены в федеральных законах, регламентирующих комплекс правоотношений в данной области деятельности.
3. Комплекс требований к осуществлению электронного взаимодействия установлен в постановлениях Правительства Российской Федерации в рамках требований Федерального закона от 6 апреля 2011 года N 63-ФЗ "Об электронной подписи".
Также в данном законе определяются требования к заключению соглашений для осуществления электронного документооборота, в которых прописываются форматы файлов, порядок их предоставления, технология работы с электронной подписью.
Системы документооборота, используемые в условиях российских компаний, как правило, связаны с [9]:
- оборотом документации на бумажных носителях;
- работой с электронными документами;
- использованием криптографических систем.
В качестве объектов защиты информации в системах электронного документооборота могут выступать:
- персональные данные сотрудников и клиентов;
- коммерчески значимая информация, включая коммерческую тайну;
- финансовые документы;
- копии документов на бумажных и электронных носителях;
- закрытые ключи электронной подписи.
Таким образом, к обеспечению защиты информации в системах документооборота необходимо использовать комплексный подход.
Особенность криптографической защиты информации, алгоритмы которой используются в системах электронной подписи, в том, что ее реализация предполагает выполнение ряда серьезных организационных мероприятий в области защиты информации, по сути представляя собой технологические решения. особенность технологии криптографической защиты информации состоит в том, что данная методика представляет собой как возможность шифрования данных, что делает возможным получение информации только лицами, располагающими ключами шифрования данной криптографической системы, так и ряд методов, позволяющих аутентифицировать автора электронного документа, а также методы подтверждения целостности документов.
Защита данных в информационных системах с использованием средств шифрования является одним из наиболее надежных методов решения проблемы безопасности.
Современные алгоритмы, используемые в криптосистемах, являются стойкими к внешним атакам, и их подделка представляет собой достаточно сложную задачу. Однако, в ряде случаев, когда поставлена задача для группы профессионалов по подделке четко определенного ключа шифрования, возможна реализация успешной атаки на криптографические ключи атакуемой системы. Как правило, атаки производятся на объекты, имеющие достаточно высокую стоимость.
Технология по взлому криптографических ключей носит название криптоанализа. Попытка фальсификации подписи или подписанного документа криптоаналитиками называетя "атакой". Вид атаки выбирается криптоаналитиками исходя из начальных условий (набора известных данных об атакуемом объекте и используемых алгоритмах шифрования)
Актуальными в настоящее время видами атак являются [12]:
1. Атаки на основе адаптивно подобранных открытых текстов.
Указанный тип атаки возможен, когда криптоаналитик имеет возможность получения доступа к устройству, являющемуся хранилищем сертификатов, например, к смарт-картам, работающим с использованием определенных алгоритмов шифрования по ключу, защищенному от чтения пользователями.
Также указанный вид атаки возможно использовать при проведении атак на криптографические системы на основе открытых ключей. В силу того, что в криптосистемах сервисы шифрования доступны всем пользователям, то при проведении любого варианта атаки, не использующего блоки, в качестве атаки можно рассматривать любую попытку генерации подписи на основе адаптивно подобранных открытых текстов. Таким образом, для защиты криптосистем, использующих открытые ключи, необходимо соблюдать требования к устойчивости сертификатов электронной подписи к подобного рода атакам.
К шифрам, которые используются для криптографической защиты информации, предъявляются следующие требования:

- достаточный уровень криптостойкости (надежности закрытия данных);
- простота алгоритмов шифрования и расшифровки;
- незначительный уровень избыточности данных, обусловленный шифрованием;
- отсутствие чувствительности к наличию ошибок шифрования и др.

Таким образом, особенности криптографической защиты информации в отличие от остальных методов состоят в следующем [12]:
- возможность шифрования документов;
- подтверждение аутентичности электронного документа;
- подтверждение целостности электронного документа.

1. ООО «Рарус». О компании. [Электронный ресурс]. Режим доступа: https://rarus.ru/company/about/
2. Сервис электронного документооборота «ДиаДок». [Электронный ресурс]. Режим доступа: https://www.diadoc.ru/about
3. Никифоров С. Н., Ромаданова М. М. Защита информации. Пароли, скрытие, удаление данных: учебное пособие / С. Н. Никифоров, М. М. Ромаданова. - Санкт-Петербург: СПбГАСУ, 2017. - 107 с.
4. Овчинникова Т. А. Ответственность за нарушение требований законодательства РФ о персональных данных: монография / Т. А. Овчинникова . - Хабаровск : Изд-во ТОГУ, 2018. – 81с.
5. Смычёк М.А. Информационная безопасность и защита информации: учебное / М.А. Смычёк. - Нижний Новгород : Нижегородский государственный технический университет, 2016. – 125с.
6. Такатлы Д. А. Защита персональных данных / Д. А. Такатлы. - Петропавловск-Камчатский: Дальневосточный филиал Федерального государственного бюджетного образовательного учреждения высшего образования "Всероссийская академия внешней торговли Министерства экономического развития Российской Федерации", 2016. - 92 с.
7. Васильев В. П. Автоматизация формирования отчетных данных: учебное пособие / В. П. Васильев. - Краснодар: КубГАУ, 2019. - 119 с.
8. Султанова Э.Р. Электронный документооборот в системе "Электронное правительство»: курс лекций/ Э.Р. Султанова. - Казань: Медицина, 2015. – 94с.
9. Завозкин С. Ю. Информационное обеспечение интеграции информационных систем на основе системы электронного документооборота : монография / С. Ю. Завозкин. - Кемерово: Кемеровский государственный университет, 2015. - 149 с.
10. Задорожнева Ю.В. Автоматизированные базы данных: учебно-методическое пособие / Задорожнева Юлия Владимировна. - Волгоград: Сфера, 2016. - 49 с.
11. Бобылева М. П. Управленческий документооборот: от бумажного к электронному: вопросы теории и практики / М.П. Бобылева. - Москва: Термика, 2016. - 359 с.
12. Зиновьева Н. Б. Электронный документ и электронная подпись в организации: учебно-методическое пособие / Н. Б. Зиновьева. - Краснодар: КГИК, 2019. - 123 с.
13. Талипов Н. Г., Катасёв А. С. Математическое и программное обеспечение для распределения заданий в автоматизированных системах электронного документооборота: монография / Н.Г. Талипов, А.С. Катасёв. - Казань: Школа, 2017. - 159 с.
14. Медведев М.А. Разработка информационных систем. Учебное пособие. - М.: Флинта, Изд-во Урал. ун-та, 2017. - 64 с.
15. Пьянкова Н.Г. Системы электронного документооборота: учебное пособие / Н.Г. Пьянкова. - Краснодар: Краснодарский ЦНТИ, 2017. - 102 с.
16. Анохина О. В. Юридическое делопроизводство [Электронный ресурс]: учебно-методическое пособие / О.В. Анохина. - Омск : Изд-во ОмГТУ, 2018. – 147с.
17. Польшакова Н.В., Коломейченко А.С., Яковлев А.С. Информационные системы в экономике: [учебник]. - Москва : Буки Веди, 2016. - 480 с.
18. Дрыгина Ю. А., Бабаян А. Р. Делопроизводство в управлении: учебное пособие / Ю. А. Дрыгина, А. Р. Бабаян. - Ростов-на-Дону: Изд-во ЮРИУ РАНХиГС, 2018. - 257 с.
19. Кузьмина, В.И. Делопроизводство: учебное пособие / И. В. Кузьмина. - Москва : Изд-во Московского гуманитарного университета, 2017. - 127 с.
20. Белобородова Н. А. Документирование управленческой деятельности на платформе 1С: учебное пособие / Н. А.Белобородова. - Ухта: УГТУ, 2016. - 51 с.