УДК 004.056.53

П.С. Ложников, С.С. Жумажанова

Об угрозах безопасности сведений ограниченного доступа в системах смешанного документооборота и правовом регулировании в области применения цифровых подписей с биометрической активацией

Рассматривается вопрос внедрения технологии гибридного документооборота и необходимость внесения соответствующих изменений в нормативно-правовую базу Российской Федерации. Приведена предварительная оценка масштаба таких изменений. Построена модель нарушителя и актуальных угроз безопасности информации в системах смешанного документооборота, обозначены пути нейтрализации выявленных угроз механизмами гибридного документооборота.

Ключевые слова: смешанный документооборот, биометрическая идентификация, электронная подпись, гибридный документооборот, модель угроз.

doi: 10.21293/1818-0442-2018-21-4-35-43

Последние данные о развитии рынка систем электронного документооборота (СЭД) показывают положительную динамику роста спроса на такие системы. Ежегодный прирост объема рынка СЭД в России составляет от 10% [1]. Нормативно-правовое регулирование в сфере электронного документооборота (ЭДО) также совершенствуется, но внедрение новых технологий требует внесения разного рода корректировок в законодательную сферу. Масштаб вносимых изменений зависит от внедряемой в СЭД технологии. Правительство РФ, приняв во внимание происходящие трансформации в сфере информационных технологий, их повсеместное распространение во все области производства и услуг, разработало программу «Цифровая экономика Российской Федерации» (далее – программа). Программа устанавливает данные в цифровой форме в качестве ключевого элемента взаимодействия сферы производства и социально-экономической деятельности, нацелена на устранение препятствий и ограничений для создания высокотехнологических бизнесов и повышение конкурентоспособности РФ на глобальном рынке. Ограничения и препятствия, описанные в программе, включают наличие правовых пробелов для перехода к полностью безбумажному документообороту, а также значимости цифровых данных, в том числе применительно к документам на бумажном носителе.

Документ – ключевой элемент системы электронного и бумажного документооборота, так как на обеспечение его безопасности и аутентичности направлено совершенствование информационных технологий и нормативно-правовой базы. Электронный документ, как правило, защищен электронной подписью (ЭП), позволяющей идентифицировать лицо, подписавшее документ, подделать такую подпись в отличие от обычной рукописной практически невозможно, но можно ее потерять. ЭП с биометрической активацией позволяет устранить эту проблему – закрытый ключ ЭП генерируется заранее заданным криптографическим алгоритмом после предъявле-

ния пользователем своего биометрического образа при каждом подписании документа. Так как на сегодняшний день перейти к полностью безбумажному документообороту невозможно, а именно наблюдается практика внедрения смешанного документооборота, то необходимо решить вопрос применения ЭП к бумажному документу. Техническая сторона этого вопроса находится на стадии его решения [2], в то же время нормативно-правовая база нуждается в корректировке: требуется провести анализ того, как предложенный механизм защиты документа решит проблемы нейтрализации актуальных угроз безопасности информации, а также будет ли такой документ иметь юридическую силу, и оценить масштабы изменения нормативно-правовой базы РФ для решения этого вопроса.

Актуальные угрозы информационной безопасности сведений ограниченного доступа и способы борьбы с ними в системах смешанного документооборота

Документ в любой форме его представления на любом этапе его жизненного цикла (ЖЦ) подвержен угрозам информационной безопасности, поэтому необходимо своевременно идентифицировать их источники. В РФ полномочия по своевременному выявлению новых угроз и их источников, а также разработке соответствующих методических документов возлагаются на федеральный орган исполнительной власти в области обеспечения безопасности (ФСБ России) и федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации (ФСТЭК России). Источниками угроз, как правило, выступают антропогенные факторы – нарушители, злоумышленники. Успех нарушителя при реализации угрозы определяется следующими факторами: его потенциалом (возможностями, квалификацией), мотивами и положением относительно среды обращения документа (внешний, внутренний), методами реализации угроз(ы), уязвимостями объекта нападения, которые могут быть различны для

отдельных стадий ЖЦ документа. Приведенные факторы отражены в методических документах ФСТЭК [3] и ФСБ [4] России, используемых для создания моделей угроз и нарушителей в информационных системах (ИС), обрабатывающих сведения конфиденциального характера.

Как правило, первоначальным базисом классификации нарушителей в документах ФСТЭК и ФСБ России является их положение относительно среды обращения документа, т.е. наличие у них прав доступа и возможностей по доступу к информации и (или) к компонентам информационной системы, что дает возможность разделить нарушителей на два типа:

– внешние нарушители – это лица, которые не имеют права доступа к ИС и ее компонентам, но имеют возможность реализовать угрозу за пределами границ ИС;

– внутренние нарушители – это лица, которые имеют право постоянного (разового) доступа к ИС и ее компонентам.

При этом важно учитывать, что, как правило, последние обладают наибольшими возможностями при реализации угроз, внешний нарушитель может действовать совместно с внутренним нарушителем, а также в составе группы, реализация угрозы возможна в любой точке ИС, в качестве точки атаки на всю ИС или ее часть нарушитель выберет самое слабое звено ИС, при наличии подключения к сети Интернет высока вероятность воздействия со стороны внешнего нарушителя. Данные два вида нарушителей с учетом указанных выше факторов делятся на категории. Описание каждой категории нарушите-

лей информационной безопасности, а также способов доступа и наличие полномочий при реализации угрозы приведены в табл. 1.

В практике разработки моделей актуальных угроз и нарушителей безопасности сведений конфиденциального характера указанная категоризация охватывает весь спектр нарушителей, являющихся источником потенциальных угроз. Состав и содержание самих угроз определяются в том числе совокупностью условий и факторов, создающих опасность несанкционированного (в том числе случайного) доступа к защищаемым сведениям. Обоснование актуальности / неактуальности угроз сопровождается описанием организационно-технических мер, позволяющих нейтрализовать такие угрозы. Типовая модель угроз для ИС, имеющих подключение к сетям общего пользования, включает в себя следующие классы угроз [3]:

– угрозы утечки информации по техническим каналам;

– угрозы несанкционированного доступа (НСД) к данным, обрабатываемым на автоматизированном рабочем месте, в том числе угрозы из внешних сетей.

Описание подклассов угроз применительно к системам смешанного документооборота представлено на рис. 1.

В табл. 2 представлена модель угроз применительно к системам смешанного документооборота, в которых производится обработка сведений исключительно конфиденциального характера. Данная модель является абстрактной без привязки к конкретной ИС, поэтому значения вероятностей реализации угроз в данном случае отсутствуют.

Таблица 1

Категории нарушителей информационной безопасности

№ п/п	Тип нарушителя	Категория ФСБ – Нi, ФСТЭК – Nj (условное обозначение)	Способ доступа и полномочия доступа к персональным данным
1	Внешний	Н1, Н2, N0	Лица без доступа к ИС и защищаемым данным, но с возможностью самостоятельно планировать и осуществлять атаки только за пределами контролируемой зоны (КЗ), а также в пределах КЗ без физического доступа к аппаратным элементам ИС
2	Внутренний	Н3, N1	Зарегистрированные пользователи ИС, имеющие санкционированный доступ к аппаратным компонентам ИС, на которых в том числе реализованы средства криптографической защиты информации (СКЗИ), но не имеющие доступа к защищаемым данным. Лица, осуществляющие разработку, поставку, сопровождение и ремонт технических средств ИС
3		Н4, Н5, N2, N3	Зарегистрированные пользователи ИС, осуществляющие доступ к ресурсам ИС с рабочего места. Зарегистрированные пользователи ИС, имеющие удаленный доступ к защищаемым данным. Имеют возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ
4		Н4, Н5, N4, N5, N6	Зарегистрированные пользователи ИС с полномочиями системного администратора, администратора безопасности сети (сегмента сети) ИС. Имеют возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ
5		Н6, N7	Программисты-разработчики прикладного программного обеспечения (ПО) и лица, обеспечивающие поставку и сопровождение ПО в ИС. Имеют возможность привлекать специалистов в области разработки и анализа СКЗИ

Рис. 1. Классы угроз смешанного документооборота

Таблица 2

Обобщенная модель угроз смешанного документооборота

Угроза	Реализация угрозы	Меры защиты	Нарушители
1	2	3	4
1.1	– Удаленный просмотр со средств отображения информации; – просмотр помощью скрытых устройств видеонаблюдения	– Установка жалюзи, штор. – Расположение средств отображения информации с учётом предотвращения возможного просмотра на них такой информации	H1, H2, N0
2.1.1	– Вынос пользователями учтенных машинных носителей информации (МНИ);	– Круглосуточная охрана помещений ИС. – Физическая охрана средств вычислительной техники. – Утверждение организационно-распорядительных документов (ОРД), регламентирующих порядок доступа в помещения сотрудников и посторонних лиц	H3-H5, N1-N6
2.1.2	– несанкционированное копирование информации на неучтенные МНИ;		
2.1.3	– отправка защищаемой информации (в том числе изображений) по сети Интернет посредством персональных компьютеров и смартфонов		
2.1.4	– НСД нарушителями в помещения, где расположены элементы сетевой инфраструктуры и проходят каналы связи организации, с последующим деструктивным воздействием на них		H3-H5, N1-N6

Продолжение табл. 2

1	2	3	4
2.1.5	– НСД нарушителями в помещения, где расположены элементы сетевой инфраструктуры и проходят каналы связи организации, с последующим деструктивным воздействием на них; – за пределами КЗ при техническом обслуживании (ремонте) элементов ИС; – при бесконтрольном выполнении работ сторонних организаций внутри КЗ	Утверждение ОРД, регламентирующих порядок доступа в помещения сотрудников и посторонних лиц, а также правила проведения технического обслуживания элементов ИС, в том числе при выносе за пределы КЗ	H1-H5, N0, N4-N6
2.1.6	– НСД нарушителями в помещения, где расположены средства защиты ИС, при получении указанными; – пользователями прав администратора в результате непреднамеренных действий администраторов; – намеренное отключение, изменение настроек средств защиты информации системными администраторами, направленные на НСД к информации	– Утверждение ОРД по работе с установленными средствами защиты. – Назначение ответственных лиц в ИС организации (администратора безопасности)	H3-H5, N1-N6
2.2.1	– Деструктивное программное воздействие нарушителем на некоторые программы или систему в целом путём изменения компонентов программной среды; – внедрение программных компонентов, в том числе вредоносного ПО; – перехват данных, поступающих от периферийных устройств; – искажение исходного кода прикладного и системного ПО; – внедрение вредоносного кода в прикладное и системное ПО при использовании уязвимостей исходного кода ПО; – восстановление некорректно удаленных данных с внешних/внутренних носителей информации	– Установка лицензионного ПО. – Утверждение ОРД в части организации мер антивирусной защиты. – Назначение ответственных лиц в ИС организации (администратора безопасности)	H1-H3, N0, N1
2.2.2	– При непосредственном доступе к ресурсам ИС путем внедрения аппаратных закладок; – при техническом обслуживании элементов ИС	Утверждение ОРД, регламентирующих порядок доступа в помещения сотрудников и посторонних лиц, а также правила проведения технического обслуживания элементов ИС, в том числе при выносе элементов за пределы КЗ	H1, H2, N0
2.2.3	В процессе разработки программного обеспечения	– Установка лицензионного ПО. – Периодическое обновление ПО. – Назначение ответственных лиц в ИС организации (администратора безопасности)	H6, N7
2.3.1	– Предоставление пользователем/администратором своими непреднамеренными действиями (бездействием) возможности внешнему нарушителю получения НСД к информации в ИС	– Утверждение ОРД о необходимости соблюдения конфиденциальности в отношении обрабатываемых данных и содержащие правила и порядок обработки/уничтожения защищаемых сведений; ознакомление пользователей и ответственных лиц с указанными ОРД	H1-H5, N0-N6
2.3.2	– Действия человеческого фактора пользователей ИС при нарушении ими парольной политики, передаче ключей доступа третьим лицам; – НСД к участкам оперативного или постоянного запоминающих устройств, в которых хранится информация для аутентификации	– Утверждение требований к выбору паролей и периодичности смены паролей (парольной политики). – Проведение инструктажей о действиях в случаях утраты или компрометации паролей	H3-H5, N1-N6
2.3.3	– Действия человеческого фактора пользователей ИС при невыполнении ими положений по работе с защищаемыми сведениями	– Утверждение ОРД, содержащих правила и порядок обработки сведений конфиденциального характера, а также порядок резервного копирования и восстановления защищаемой информации	H3-H5, N2-N6

Продолжение табл. 2

1	2	3	4
2.3.4	– Сбои в работе аппаратно-программных средств, входящих в состав ИС	– Утверждение ОРД в части реализации мер по резервному копированию баз данных, содержащих сведения конфиденциального характера. – Назначение ответственных лиц (администратора безопасности)	H3-H5, N1-N6
2.4.1	– НСД пользователями, не допущенными к обработке защищаемой информации, но способным теми или иными способами ее получить	– Утверждение ОРД, регламентирующих порядок доступа в помещения сотрудников и посторонних лиц. – Круглосуточная охрана помещений ИС. – Физическая охрана средств вычислительной техники со стороны сотрудников охраны и сотрудников организации. – Установка на окна жалюзи либо штор. – Расположение средств отображения защищаемой информации (экраны дисплеев, бумажные носители и пр.) с учётом предотвращения возможного просмотра на них такой информации, в том числе с помощью оптических средств	H1-H3, N0, N1
2.4.2	– НСД Допущенными пользователями, преследующими корыстные цели вследствие своих противоправных действий	– Утверждение ОРД, содержащих правила и порядок обработки сведений конфиденциального характера. – Получение письменного обязательства о неразглашении защищаемой информации	H3-H5, N2-N6
2.5.1	– При получении доступа в операционную среду путем использования стандартных функций ОС либо прикладной программы для выполнения НСД	– Установка на ПЭВМ средства доверенной загрузки. – Утверждение ОРД, регламентирующих порядок доступа в помещения сотрудников и посторонних лиц.	H1-H5, N0-N6
2.5.2	– С помощью внешнего носителя для загрузки сторонней операционной системы или вредоносного программного обеспечения	– Круглосуточная охрана помещений ИС. – Физическая охрана средств вычислительной техники со стороны сотрудников охраны и сотрудников организации	H1-H5, N0-N6
2.6.1	– При использовании внутренних/внешних сервисов в защищаемой сети, с возможностями ограничения доступности сервисов, внешним нарушителем путём доступа/перехвата/изменения HTTP cookies, заражения DNS-кеша, искажения XML-схемы, использование альтернативных путей доступа к ресурсам	– Установка межсетевого экрана, позволяющего фильтровать входящий и исходящий трафик. – Криптографическое преобразование информации, передаваемой за пределы КЗ по каналам связи	H1, H2, N0
2.6.2	– С применением специального программного обеспечения – сетевой сканер		H1, H2, N0
2.6.3	– Путём подмены доверенного объекта сети с целью дальнейшего получения доступа к защищаемой информации, получения доступа к гипервизору, к механизмам администрирования среды виртуализации и др.		H1, H2, N0
2.6.4	– Путём внедрения по сети вредоносного программного обеспечения с целью дальнейшего получения НСД к ресурсам информационной системы, идентификационной/аутентификационной информации, ограничения доступа к ресурсам и сервисам и др.	– Установка лицензионного ПО. – Утверждение ОРД в части организации мер антивирусной защиты, в том числе своевременного обновления антивирусных баз, а также о правилах хранения и удаления данных с внешних/внутренних носителей информации. – Назначение ответственных лиц в ИС организации (администратора безопасности)	H1, H2, N0
2.6.5	– Путём перехвата информации, передаваемой по каналам связи, с целью дальнейшего анализа этой информации и получения НСД к сервисам ИС	– Установка межсетевого экрана, позволяющего фильтровать входящий и исходящий трафики. – Криптографическое преобразование информации, передаваемой за пределы КЗ по каналам связи	H1, H2, N0
2.6.6	– При отказе дискредитированной системой в доступе легальным пользователям при лавинообразном увеличении числа сетевых соединений с данной системой		H1, H2, N0

Из приведенной модели можно сделать вывод, что большая часть угроз нейтрализуется на практике внедрением организационно-распорядительных документов (ОРД), ознакомлением с ними сотрудников организации, распределением обязанностей по организационно-техническому обеспечению системы защиты информации, а также установкой специальных программно-технических средств, прошедших оценку соответствия требованиям по защите информации. Внедрение ОРД и проведение инструктажей направлено в значительной части на нейтрализацию человеческого фактора, однако даже если пользователь, следуя указаниям парольной политики, верно сгенерирует пароль, то избежать такого свойства пароля, как его отчуждаемость от пользователя, практически невозможно – он может быть утерян, забыт, украден, передан третьему лицу и т.д., что является сильнейшим недостатком данного типа аутентификации.

Гибридный документооборот представляет собой модификацию схемы смешанного документа, в котором:

- присутствует надежная привязка всех аутентификаторов субъекта (паролей, ключей, кодов доступа и т.д.) к его биометрическим характеристикам;

- обеспечивается равная защита документа как в электронном, так и в бумажном представлении; под равной защитой подразумевается использование одних тех же механизмов защиты для обоих форматов документа [5].

К тому же реализация такой модели документооборота обеспечивает соблюдение принципа экономической целесообразности, т.к. нет необходимости закупать дорогостоящее аппаратное обеспечение – имеется возможность реализации средств биометрической защиты на стандартном оборудовании компьютерных систем [6].

Правовое регулирование в сфере применения цифровых подписей

Техническая сторона вопроса по нейтрализации актуальных угроз безопасности информации в части передачи или утери персональных идентификаторов решена таким образом, чтобы не нарушить ставший привычным механизм документооборота – пользователи также используют веб-камеру и недорогой графический планшет, однако получаемые биометрические параметры используются для получения заранее сгенерированного закрытого ключа и формирования ЭП, которую, соответственно, невозможно кому-либо передать или потерять, а также подделать или украсть. Биометрический эталон и данные для генерации ключа хранятся в нейросетевом преобразователе «биометрия-код» (ПБК) в виде таблицы нейросетевых функционалов таким образом, что извлечь одну составляющую вычислительно сложно без знания другой [7]. Использование ПБК снимает вопрос о месте хранения закрытого ключа пользователя.

Гибридный документ имеет ряд отличий от привычных бумажной и электронной форматов документа: он также снабжен обязательными реквизитами юридически значимого документа, в том числе графическим изображением рукописной подписи (печати при необходимости), в дополнение к ним идут QR-коды, содержащие сгенерированную ЭП, ссылку на облако на оригинальный документ, а также синдромы исправления ошибок. Последние необходимы при переводе документа из бумажной формы в электронную и чтении его посредством специального OCR-приложения, выдающего минимальные ошибки при повторном печатании и сканировании документа (рис. 2) [8].

Рис. 2. Внешний вид гибридного документа

По приведенному описанию предложенной модели документооборота можно сделать вывод, что обеспечивается равная защита документов как в цифровой, так и аналоговой форме, и достигнутый таким образом уровень на порядок выше традиционных методов обеспечения защиты и подтверждения аутентичности документа.

В повседневной практике подтверждение юридической значимости документов, подписанных ЭП, после истечения срока действия сертификата проверки ЭП, выданных аккредитованным удостоверяющим центром (УЦ), ложатся на плечи УЦ. Согласно ФЗ «Об электронной подписи» [9] УЦ должен вести реестр выданных сертификатов проверки ЭП, а также хранить информацию о владельцах выданных, в том числе аннулированных сертификатах проверки ЭП и т.д. При прекращении деятельности УЦ вся указанная информация передается для хранения в уполномоченный федеральный орган (ныне Минкомсвязь России).

Важный вопрос, который может возникнуть при анализе модели гибридного документооборота, заключается в следующем: будет ли графическое изо-

бражение подписи – одного из обязательных реквизитов документа – придавать ему юридическую силу? Прежде чем ответить на этот вопрос, важно отметить, что, проставив подпись в документе, должностное лицо берет на себя ответственность за целостность и аутентичность документа и возможные последствия, следующие за его исполнением. В российском законодательстве есть некоторые допущения использования факсимильной подписи в документе, если такое предусмотрено соглашением сторон (п. 2 ст. 160 ГК РФ) [10]. В описанной модели гибридного документооборота пользователь каждый раз воспроизводит автограф на графическом планшете или ином устройстве сенсорного ввода при доступе в свой аккаунт, т.е. размещенное в документе графическое изображение подписи никак нельзя назвать факсимиле – оно является личной цифровой рукописной подписью владельца документа, к тому же подделать такую подпись невозможно, так как при аутентификации в личном кабинете учитываются динамические признаки воспроизведения подписи [11]. Принадлежность обычной рукописной подписи, также называемой физической, к конкретному лицу доверенная сторона, как правило, устанавливает по ее внешнему виду, которое злоумышленник может повторить после некоторого времени тренировок (в отличие от динамических характеристик) – мало кто при обычной проверке документа прибегает к помощи графологов.

Технология цифровой рукописной подписи еще не закреплена в российском законодательстве, но подобного можно ожидать в ближайшее время. Правительственной комиссией по использованию информационных технологий были утверждены планы мероприятий, нацеленных на реализацию всех мер, зафиксированных в программе. По итогам Парламентских слушаний в Государственной думе Федерального собрания Российской Федерации на тему «Формирование правовых условий финансирования и развития цифровой экономики» от 20 февраля 2018 г., одной из ключевых задач является унификация требований по идентификации, расширение возможностей и способов идентификации, в том числе урегулирование работы, а также статуса электронных документов, подписанных аналогом собственноручной подписи клиента на электронном планшете или ином устройстве.

С учетом нацеленности законодателей на принятие ЭП с биометрической активацией равноценной усиленной ЭП, остается открытым вопрос о внедрении этой технологии в организациях. Ограничится такой переход одним законодательным актом или рядом дополняющих друг друга нормативных документов, судить сложно. Рассмотрим один обязательный критерий принятия этой технологии как обязательного компонента системы защиты информации. Как известно, к системам защиты государственных муниципальных информационных систем предъявляется требование о наличии сертификата соответствия применяемых средств защиты, выдан-

ных уполномоченными органами (ФСТЭК и ФСБ России). Сертификация предлагаемой технологии генерации ЭП с биометрической активацией (ЭП, создаваемая только после аутентификации пользователя по биометрическим параметрам), имеет свои особенности. Принцип их работы основан на том, что каждый человек уникален, что, с другой стороны, создает проблемы при построении таких систем – нельзя создать единый биометрический портрет среднестатистического пользователя на основании данных одного или нескольких субъектов [12]. Для этого необходима большая база биометрических образов «Свой» и «Чужой», доступная любому пользователю СЗИ при его приобретении. Требования по формированию баз естественных биометрических образов изложены в ГОСТ Р 52633.1-2009 [13]. Практика сбора таких баз уже наблюдается в банковской сфере в рамках единой биометрической системы (ЕБС) [14], которая в дальнейшем может применяться и в других отраслях: например, в здравоохранении, образовании, ритейле, электронной коммерции, для получения государственных услуг [15].

С учетом того, что достижения в области биометрической идентификации практически находятся на пике своего развития и могут всецело удовлетворить требования современного общества, можно утверждать, что современные технологии и процесс нормативно-правового регулирования в данной сфере идут нога в ногу.

Заключение

Технология гибридного документооборота является перспективным решением проблем существующего смешанного документооборота. Во-первых, обеспечивается достаточный уровень безопасности и аутентичности документа за счет применения биометрических образов для формирования ЭП, исключающих угрозы антропогенного характера при несоблюдении парольной политики; во-вторых, предусмотрена возможность использования одних и тех же реквизитов (ЭП) документа в цифровой и аналоговой форме его представления. Последнее вызывает ряд вопросов об юридической значимости такого документа. Одним из вариантов решения является приравнивание цифровой рукописной подписи, введенной на планшете и перенесенной на документ, равнозначной обычной физической рукописной подписи.

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 16-07-01204.

Литература

1. Российский рынок СЭД/ЕСМ-систем вырос до 41,6 млрд руб. [Электронный ресурс]. – Режим доступа: [http://www.tadviser.ru/Статья:СЭД_\(рынок_России\)](http://www.tadviser.ru/Статья:СЭД_(рынок_России)) (дата обращения: 16.10.2018).
2. Ivanov A.I. A hybrid document formation technology / A.I. Ivanov, P.S. Lozhnikov, A.E. Samotuga // *Cybernetics and Systems Analysis*. – 2014. – Vol. 50, No. 6. – P. 956–959.
3. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах

персональных данных (Выписка): утв. ФСТЭК РФ 15.02.2008 [Электронный ресурс]. – Режим доступа: <https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/379-bazovaya-model-ugroz-bezopasnosti-personalnykh-dannykh-pri-ikh-obrabotke-v-informatsionnykh-sistemakh-personalnykh-dannykh-vypiska-fstek-rossii-2008-god> (дата обращения: 18.10.2018).

4. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных: утв. ФСТЭК 14.02.2008 [Электронный ресурс]. – Режим доступа: <https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/380-metodika-opredeleniya-aktualnykh-ugroz-bezopasnosti-personalnykh-dannykh-pri-ikh-obrabotke-v-informatsionnykh-sistemakh-personalnykh-dannykh-fstek-rossii-2008-god> (дата обращения: 18.10.2018).

5. Ложников П.С. Биометрическая защита гибридного документооборота. – Новосибирск: Изд-во СО РАН, 2017. – 148 с.

6. Оценка идентификационных возможностей биометрических признаков от стандартного периферийного оборудования / В.И. Васильев, С.С. Жумажанова, П.С. Ложников, А.Е. Сулаво // Вопросы защиты информации. – 2016. – № 1 (112). – С. 12–20.

7. Иванов А.И. Нейросетевая защита конфиденциальных биометрических образов гражданина и его личных криптографических ключей. – Пенза: ПНИЭИ, 2014. – 57 с.

8. Ложников П.С. О возможности обеспечения равной защиты документов на бумажном и электронном носителе биометрическими и криптографическими методами (обзор) // Вопросы защиты информации. – 2018. – № 4. – С. 10–19 (В печати).

9. Об электронной подписи: Федер. закон от 06.04.2011 г. № 63-ФЗ, последняя редакция [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_112701/ (дата обращения: 20.10.2018).

10. Гражданский кодекс Российской Федерации. – Ч. 1: Федер. закон от 30 нояб. 1994 г. № 51-ФЗ (в ред. от 30 дек. 2012 г.; с изм. и доп. от 22 июня 2017 г.) [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_5142/ (дата обращения: 20.10.2018).

11. Method of protecting paper and electronic text documents through a hidden biometric identifier based on a signature / P.S. Lozhnikov, A.E. Sulavko, A.V. Eremenko, D.A. Volkov // X International IEEE Scientific and Technical Conference «Dynamics of Systems, Mechanisms and Machines» (Dynamics), 15–17 November, 2016, Omsk, Russia. P. 1–5. doi: 10.1109/Dynamics.2016.7819037.

12. Фунтиков В.А. Проблемы, возникающие при тестировании и сертификации высоконадежных биометрических средств / В.А. Фунтиков, А.Ю. Малыгин, Ю.И. Олейник // Тр. Междунар. симпозиума «Надежность и качество». – 2006. – Т. 1. – С. 15–17.

13. ГОСТ Р 52633.1–2009. Защита информации. Техника защиты информации. Требования к формированию баз естественных биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации. – Введ. 2010–01–01. – М.: Стандартинформ, 2010. – 25 с.

14. Российские банки начали сбор биометрических данных клиентов // Новости. Известия [Электронный ресурс]. – Режим доступа: <https://iz.ru/761824/2018-07-01/rossiiskie-banki-nachali-sbor-biometricheskikh-dannykh-klientov> (дата обращения: 20.10.2018).

15. Об утверждении порядка обработки, включая сбор и хранение, параметров биометрических персональных данных в целях идентификации, порядка размещения и обновления биометрических персональных данных в единой биометрической системе, а также требований к информационным технологиям и техническим средствам, предназначенным для обработки биометрических персональных данных в целях проведения идентификации: приказ Минкомсвязи России от 25.06.2018 № 321 [Электронный ресурс]. – Режим доступа: <http://base.garant.ru/71985302/> (дата обращения: 20.10.2018).

Ложников Павел Сергеевич

Канд. техн. наук, доцент, зав. каф. комплексной защиты информации» (КЗИ) Омского государственного технического ун-та (ОмГТУ)
Мира пр-т, д. 11, г. Омск, Россия, 644050
ORCID 0000-0001-7878-1976
Тел.: +7 (381-2) 62-87-07
Эл. почта: lozhnikov@mail.ru

Жумажанова Самал Сагидуллоевна

Аспирант, ассистент каф. КЗИ ОмГТУ
Мира пр-т, д. 11, г. Омск, Россия, 644050
ORCID 0000-0002-6785-5201
Тел.: +7-950-216-89-79
Эл. почта: samal_shumashanova@mail.ru

Lozhnikov P.S., Zhumazhanova S.S.

On threats to the security of restricted information in mixed document flow and legal regulation in the application of digital signatures with biometric activation

The article describes the issue of introducing hybrid document management technology and the need to make appropriate changes to the regulatory base of the Russian Federation. A preliminary estimate of the scale of such changes is given. A model of the intruder and actual threats to the security of information in mixed document management systems has been built, and ways of neutralizing the identified threats by hybrid workflow mechanisms are indicated.

Keywords: mixed document flow, biometric identification, electronic signature, hybrid document flow, threat model.

doi: 10.21293/1818-0442-2018-21-4-35-43

References

1. The Russian market for EDS/ECM-systems has grown to 41.6 billion rubles // TAdviser.ru [Electronic resource]. Available at: <http://www.tadviser.ru/Article:CED> (Russian) (accessed: October 16, 2018) (in Russ.).
2. Ivanov A.I., Lozhnikov P.S., Samotuga A.E. A hybrid document formation technology. *Cybernetics and Systems Analysis*, 2014, vol. 50, no. 6, pp. 956–959.
3. The basic model of threats to the security of personal data processed in the information systems of personal data (Extract): FSTEC of the Russian Federation 15.02.2008 [Electronic resource]. Available at: <https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/379-bazovaya-model-ugroz-bezopasnosti-personalnykh-dannykh-pri-ikh-obrabotke-v-informatsionnykh-sistemakh-personalnykh-dannykh-vypis-ka-fstek-rossii-2008-god> (accessed: October 18, 2018) (in Russ.).

4. Methods for determining the actual threats to the security of personal data processed in the information systems of personal data: FSTEC of the Russian Federation 14.02.2008 [Electronic resource]. Available at: <https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/380-metodika-opredeleniya-aktualnykh-ugroz-bezopasnosti-personalnykh-dannykh-pri-ikh-obrabotke-v-informatsionnykh-sistemakh-personal-nykh-dannykh-fstek-rossii-2008-god> (accessed: October 18, 2018) (in Russ.).
5. Lozhnikov P.S. Biometricheskaya zashchita gibridnogo dokumentooborota [Biometric protection of hybrid workflow]. SB RAS Publ., 2017. 130 p.
6. Vasilyev V.I., Zhumazhanova S.S., Lozhnikov P.S., Sulavko A.E. Identification possibilities assessment of biometric features from standard peripheral equipment. *Information protection issues*, 2016, no. 1 (112), pp. 12–20 (in Russ.).
7. Ivanov A.I. Neyrosetevaya zashchita konfidentsial'nykh biometricheskikh obrazov grazhdanina i yego lichnykh kriptograficheskikh klyuchey. Monografiya [Neural network protection of confidential biometric images of a user and his personal cryptographic keys. Monograph]. Penza: PNIEI, 2014. 57 p.
8. Lozhnikov P.S. On the possibility of equal protection providing for documents in paper and electronic form using biometric and cryptographic methods (Review). *Information security question*, 2018, no. 4, pp. 10–19 (in Press.).
9. On electronic signature: federal law from 06.04.2011 No. 63–FZ (last revised) [Electronic resource]. Available at: http://www.consultant.ru/document/cons_doc_LAW_112701/ (accessed: October 20, 2018) (in Russ.).
10. Civil Code of the Russian Federation. Part 1: federal law from 21.10.94 No. 51-FZ (last edition) [Electronic resource]. Available at: http://www.consultant.ru/document/cons_doc_LAW_5142/ (accessed: October 20, 2018) (in Russ.).
11. Lozhnikov P.S., Sulavko A.E., Eremenko A.V., Volkov D.A. Method of protecting paper and electronic text documents through a hidden biometric identifier based on a signature. X International IEEE Scientific and Technical Conference «Dynamics of Systems, Mechanisms and Machines» (Dynamics), 15–17 November, 2016, Omsk, Russia. pp. 1–5. doi: 10.1109/Dynamics.2016.7819037.
12. Funtikov V.A., Malygin A.Yu., Oleinik Yu.I. Problems arising from testing and certification of highly reliable biometrics. Proceedings of the International Symposium «Reliability and Quality», 2006, vol. 1, pp. 15–17 (in Russ.).
13. GOST R 52633.1–2009 Information protection. Information protection technology. Requirements for creation procedures for bases of natural biometric images, intended for high-reliability biometric authentication means testing. Intr. 2010-01-01. M.: Standartinform. 2010, 25 p. (in Russ.).
14. Russian banks began collecting customers' biometric data // News. Izvestia [Electronic resource]. Available at: <https://iz.ru/761824/2018-07-01/rossiiskie-banki-nachali-sbor-biometricheskikh-dannykh-klientov> (accessed October 20, 2018).
15. On the approval of the processing procedure, including the collection and storage, parameters of biometric personal data for identification purposes, the order of placement and updating of biometric personal data in a single biometric system, as well as the requirements for information technologies and technical means processing of biometric personal data for identification purposes: the order of the Ministry of Communications and Mass Media of Russia from 25.06.2017 No. 321 [Electronic resource]. Available at: <http://base.garant.ru/71985302/> (accessed: October 20, 2018) (in Russ.).

Pavel S. Lozhnikov

PhD, Associate Professor, Head of Department «Complex Information Protection» (CIP) of Omsk State Technical University (OmSTU) 11, Mira pr., Omsk, Russia, 644050
ORCID 0000-0001-7878-1976
Phone: +7 (381-2) 62-87-07
Email: lozhnikov@mail.ru

Samal S. Zhumazhanova

Postgraduate student, Assistant at Department «Complex Information Protection» (CIP) of Omsk State Technical University (OmSTU) 11, Mira pr., Omsk, Russia, 644050
ORCID 0000-0002-6785-5201
Phone: +7-950-216-89-79
Email: samal_shumashanova@mail.ru