УДК 004.62

Н.И. Елисеев

МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ПРИ ЕЕ ОБРАБОТКЕ В СИСТЕМЕ ЗАЩИЩЕННОГО ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

В электронной среде процесс обработки документированной информации представляет собой сложный организационно-технический процесс, сопряженный с рядом угроз безопасности информации, реализация которых может привести к утрате документом своей юридической значимости и как следствие к определенному ущербу. В работе определены основные виды деструктивных воздействий на элементы системы защищенного электронного документооборота, приводящие к утрате электронным документом свойства юридической значимости.

Система защищенного электронного документооборота; угрозы безопасности информации; электронный документ; электронная подпись; юридическая значимость электронного документа.

N.I. Eliseev

MODEL OF INFORMATION SECURITY RISKS IN PROTECTED ELECTRONIC RECORDS MANAGEMENT SYSTEM

The Electronic Record processing is organizational and technical difficult. This process connected with information security risks which can lead to the losing the Electronic Records legal status and the damage of the system as a result. In this paper are defined the main types of attacks on the Electronic Records Management Systems elements which can lead to the losing the Electronic Records legal status.

The protected electronic records management systems; information security risks; electronic records; digital signature; electronic records legal status.

Введение. Основной функцией современных систем защищенного электронного документооборота (СЗЭД) является обеспечение защищенного обмена юридически значимыми электронными документами (ЭлД). Защищенность системы электронного документооборота (СЭД) обеспечивается совокупностью программных и технических средств защиты информации и процессов ее обработки от доступа не легитимных пользователей (процессов). Юридическая значимость ЭлД определяется установленными правилами документирования и результатом проверки соответствия ЭлД следующим требованиям [1-3]:

1) *конфиденциальности ЭлД* – доступность ЭлД только полномочным пользователям (процессам);

2) *целостности ЭлД* – неизменностью определенных элементов ЭлД на всех этапах его жизненного цикла, независимо от способов и средств обработки ЭлД;

3) *доступности ЭлД* – возможностью доступа к определенным элементам ЭлД и представления их в требуемой форме за определенное время;

4) *легитимности ЭлД* – правомерностью использованных на протяжении жизненного цикла ЭлД технологий его обработки;

5) *достоверности ЭлД* – полного и точного отражения в ЭлД подтверждаемых операций, деятельности или фактов;

6*) аутентичности (подлинности) ЭлД* – соответствием заявленной сущности ЭлД, а также времени, месту и автору, заявленному в ЭлД.

В процессе обработки ЭлД может подвергаться различным деструктивным воздействиям, приводящим к потере его юридической значимости. Последствия потери юридической значимости ЭлД будут определяться ролью ЭлД в решении конкретной задачи. На рис. 1 в общем виде отражена причинно-следственная связь деструктивных воздействий на ЭлД и возможного ущерба.

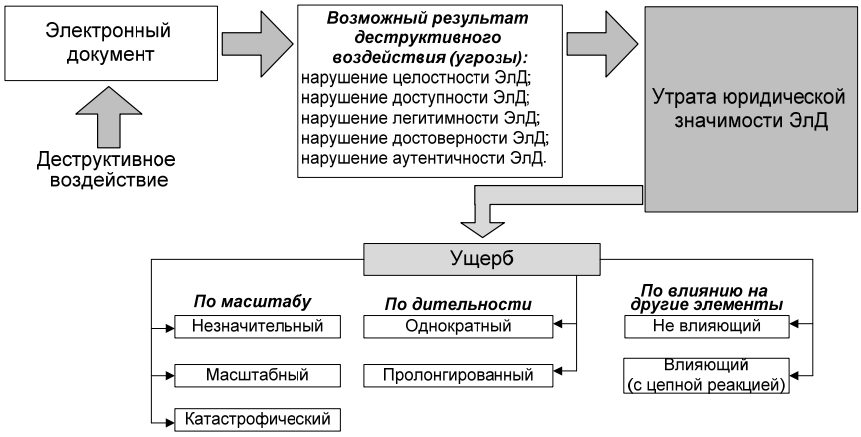

Рис. 1. Возможный ущерб от деструктивного воздействия на ЭлД

Таким образом, угрозы безопасности информации в СЭД необходимо рассматривать с позиций системной угрозы утраты юридической значимости ЭлД.

Целью статьи является анализ возможных деструктивных воздействий на элементы СЭД, приводящих к утрате юридической значимости ЭлД.

1. Системный анализ структуры и функций современной СЭД. Современная СЭД представляет собой автоматизированную информационную систему обработки ЭлД обеспеченную комплексом программных и технических средств защиты информации. Таким образом, декомпозицию СЭД можно условно выполнить на четыре ключевых подсистемы: подсистема обработки ЭлД, подсистема обеспечения безопасности информации, пользователи СЭД и подсистему электропитания. Обобщенная структура СЭД представлена на рис. 2.

Введем обозначения для каждой из подсистем СЭД:

S_1 – система электропитания;

S_2 – система ввода/вывода (в т.ч. отображения ЭлД);

S_3 – система хранения ЭлД;

S_4 – система обработки ЭлД (модификация, преобразование, копирование и т.д.);

S_5 – система приема/передачи информации;

S_6 – система разграничения доступа;

S_7 – система проверки подлинности;

S_8 – пользователь СЭД.

В зависимости от запрашиваемой функции СЭД происходит активация определенных связей элементов системы. На рис. 3 представлен функциональный граф активируемых связей между элементами СЭД при выполнении следующих функций:

F_1 – чтение (в т. ч. удаленно) ЭлД;

F_2 – модификация ЭлД (формирование, редактирование, копирование, удаление, согласование);

F_3 – передача ЭлД, вывод на носители;

F_4 – обработка бумажных экземпляров документов.

Возможными состояниями ЭлД относительно свойства юридической значимости могут быть:

Z = «1» – юридически значимый ЭлД;

Z = «0» – ЭлД, не имеющий юридической значимости.

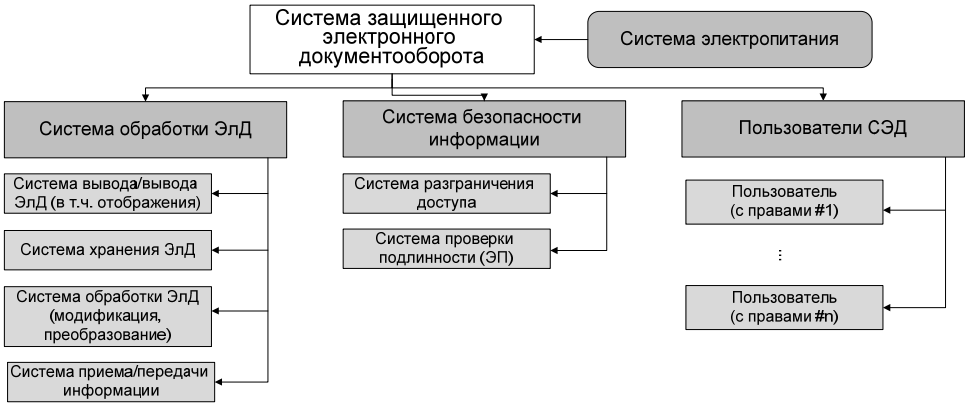

Рис. 2. Структура современной СЗЭД

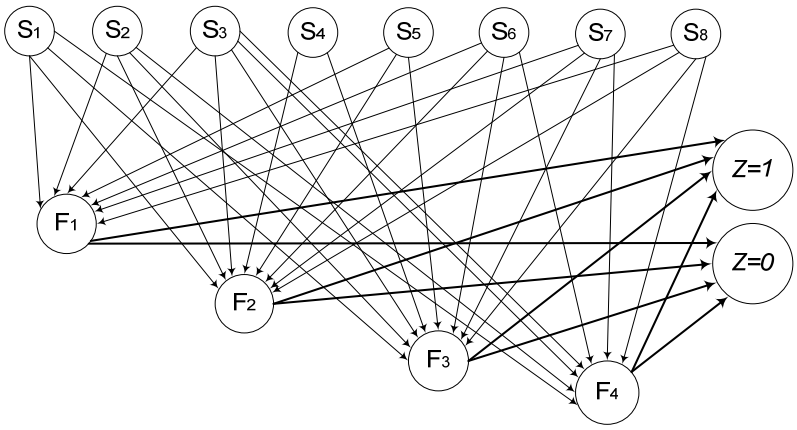

Рис. 3. Функциональный граф связей элементов СЗЭД

Вершинам $S_1 - S_8$ соответствуют подсистемы СЗЭД, вершинам $F_1 - F_4$ соответствуют результаты функционирования СЗЭД при активации определенных связей, соответствующих ребрам графа. Условимся присваивать ребру графа значение «1» в случае выполнения системами $S_1 - S_8$ своих функций и «0» в случае отказа. Представим возможные значения результатов выполнения СЗЭД своих функций в виде следующих логических зависимостей:

$$F_1 = S_1 \wedge S_2 \wedge S_3 \wedge S_5 \wedge S_6 \wedge S_7 \wedge S_8;$$

$$F_2 = S_1 \wedge S_2 \wedge S_3 \wedge S_4 \wedge S_5 \wedge S_6 \wedge S_7 \wedge S_8;$$

$$F_3 = S_1 \wedge S_2 \wedge S_3 \wedge S_4 \wedge S_5 \wedge S_6 \wedge S_7 \wedge S_8;$$

$$F_4 = S_1 \wedge S_2 \wedge S_3 \wedge S_6 \wedge S_7 \wedge S_8.$$

Тогда юридическая значимость ЭлД на каждом этапе его жизненного цикла будет определяться функционалом: $Z = \prod_{i=1}^{n} F_{ij}$, $j = \overline{1, d}$, где n – общее количество этапов обработки ЭлД; d – общее количество функций СЗЭД.

Анализ связей элементов СЗЭД отраженных на рис. 3 позволяет сделать вывод, что отказ практически любого элемента СЗЭД приводит к утрате ЭлД своей юридической значимости. В следствии чего угрозы безопасности информации в СЗЭД необходимо рассматривать как виды возможных воздействий на элементы СЗЭД, приводящие к их отказу.

2. Модель угроз безопасности информации в СЗЭД. В табл. 1 представлены возможные воздействия на элементы СЗЭД, приводящие к нарушению их нормального функционирования и как следствие к утрате ЭлД своей юридической значимости.

Таблица 1

Угрозы безопасности информации в СЗЭД

Элемент СЗЭД	Вид деструктивного воздействия	Результат воздействия, приводящий к утрате ЭлД юридической значимости
Система энергоснабжения	1. Перегрузка системы. 2. Отказ комплектующих элементов системы. 3. Вывод из строя системы внешним воздействием.	Нарушение нормального функционирования всех элементов СЗЭД.
Система ввода/вывода (в т.ч. отображения)	Несоответствие формата ЭлД средствам ввода/вывода (в т.ч. отображения).	Нарушение доступности требуемой формы представления ЭлД.
	Искажения при распознавании бумажной копии ЭлД (OCR преобразование) [4].	Нарушение целостности ЭлД.
	Ошибки обработки бумажных копий ЭлД при отложенном сканировании (подмена РККД).	Нарушение аутентичности ЭлД.
Система хранения	Воздействия на носитель информации.	Нарушение целостности ЭлД. Нарушение доступности ЭлД.

Продолжение табл. 1

Система обработки ЭлД	Внесение искажений в ЭлД (программными средствами или пользователями) после подписания ЭП.	Нарушение целостности ЭлД.
	Внесение искажений в ЭлД программными средствами в момент подписания ЭП.	Нарушение достоверности ЭлД.
	Изменение формата ЭлД.	Нарушение целостности ЭлД.
	Изменение содержания ЭлД самим автором.	Нарушение достоверности ЭлД.
	Создание не легитимных копий ЭлД.	Нарушение легитимности ЭлД. Нарушение конфиденциальности ЭлД.
Система приема/передачи информации	Перегрузка системы (преднамеренная (DDoS атака), непреднамеренная). Отказ комплектующих элементов. Вывод из строя системы внешним воздействием.	Нарушение доступности удаленных ЭлД. Нарушение доступности списков отозванных сертификатов, системы штампов времени.
	Внесение системой приема/передачи искажений в ЭлД.	Нарушение целостности ЭлД.
Система разграничения доступа	Подбор пароля.	Нарушение конфиденциальности ЭлД.
	Ошибки администрирования: доступ не легитимных пользователей; отказ в доступе легитимных пользователей.	Нарушение конфиденциальности ЭлД. Нарушение доступности ЭлД.
Система проверки подлинности	Взлом ключа ЭП	Нарушение легитимности ЭлД. Нарушение достоверности ЭлД. Нарушение аутентичности ЭлД.
	Нарушение целостности ЭП.	Нарушение целостности ЭлД.
	Подмена владельца сертификата ЭП	Нарушение легитимности ЭлД. Нарушение достоверности ЭлД. Нарушение аутентичности ЭлД.

Окончание табл. 1

Система проверки подлинности	Кража, копирование, взлом пароля контейнера ЭП.	Нарушение легитимности ЭлД. Нарушение достоверности ЭлД. Нарушение аутентичности ЭлД.
	Незаконное делегирование уполномоченным лицом права подписи ЭлД.	Нарушение легитимности ЭлД. Нарушение достоверности ЭлД. Нарушение аутентичности ЭлД.
	Подписание ЭлД лицом на то неуполномоченным.	Нарушение легитимности ЭлД.
	Подмена корневых сертификатов открытых ключей ЭП.	Нарушение легитимности ЭлД.
	Подмена списков отозванных сертификатов.	Нарушение легитимности ЭлД.
	Отказ носителя ключа ЭП.	Невозможность подписания, согласования и т.д. ЭлД.
Пользователь СЭД	Установка не сертифицированного ПО.	Нарушение легитимности ЭлД.
	Модификация (в т.ч. формата) ЭлД (преднамеренная, непреднамеренная).	Нарушение целостности ЭлД.
	Удаление ЭлД (преднамеренное, непреднамеренное).	Нарушение доступности ЭлД.
	Несанкционированное копирование ЭлД (в т.ч. передача ЭлД без удаления оригинала).	Нарушение конфиденциальности ЭлД. Нарушение легитимности ЭлД.
	Незаконные манипуляции с журналом событий СЭД (изменение хронологии событий)	Нарушение достоверности «динамических» ЭлД (ЭлД дополняемых с течением времени (журналы и т.д.)

Заключение. Ключевым требованием, предъявляемым к современной СЗЭД, является предоставление легитимным пользователям доступа к юридически значимым ЭлД и средствам их обработки. Нарушение функционирования СЗЭД может привести к ущербу, определяемому значимостью СЗЭД в системе управления

определенным объектом. Модель угроз, представленная в данной работе, позволяет определить необходимые уровни функционирования подсистемы обеспечения безопасности информации в СЗЭД, а именно:

- *первый уровень (превентивный)* – уровень организационно-технических мер, направленных на локализацию и устранение возможных предпосылок к возникновению угроз безопасности информации в СЗЭД;
- *второй уровень (текущего контроля)* – контроль этапов обработки ЭлД (с определенной периодичностью) влияющих на юридическую значимость ЭлД;
- *третий уровень (устранения последствий реализованных угроз)* – обеспечение возможности восстановления юридической значимости ЭлД в минимальные сроки в случае реализации комплексной угрозы потери юридической значимости ЭлД.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *ГОСТ Р ИСО 15489-1-2007*. Система стандартов по информации, библиотечному и издательскому делу. Управление документами. Общие требования. – Введ. 2007-03-12. – М.: Стандартинформ, 2007. – 23 с.
2. *ГОСТ 2.051-2006*. Единая система конструкторской документации. Электронные документы. Общие положения. – Введ. 2006-09-01. – М.: Изд-во стандартов, 2006. – 12 с.
3. *Елисеев Н.И.. Финько О.А.* Системные основы защищенного гибридного документооборота // Тр. междунар. конф. «Управление развитием крупномасштабных систем» / ИПУ РАН. – М., 2011.
4. *Елисеев Н.И., Финько О.А.* Обеспечение подлинности аналоговых документов в системе электронного документооборота МО РФ// Инфофорум – 2012: Материалы Национального форума информационной безопасности (Москва, 7–8 февраля 2012 г.). URL : http://www.2012.infoforum.ru/2012/program (дата обращения: 11.10.2012 г.).

Статью рекомендовал к опубликованию д.т.н., профессор В.Н. Марков.

Елисеев Николай Иванович – Филиал Военной академии связи (г. Краснодар); e-mail: eliseev_81_09@mail.ru; 350063, г. Краснодар, ул. Красина, 4; тел.: +79094476289; доцент.

Eliseev Nikolay Ivanovich – Branch of the Military Academy of Communications (Krasnodar); e-mail: eliseev_81_09@mail.ru; 4, Krasina, Krasnodar, 350063, Russia; phone: +79094476289; associate professor.

УДК 631.8

И.А. Калмыков, О.И. Дагаева

НОВЫЕ ТЕХНОЛОГИИ ЗАЩИТЫ ДАННЫХ В ЭЛЕКТРОННЫХ КОММЕРЧЕСКИХ СИСТЕМАХ НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ ПСЕВДОСЛУЧАЙНОЙ ФУНКЦИИ

Целью исследований является сокращение занимаемого программным обеспечением объема, необходимого для эффективной работы носителя электронных денежных средств (смарт-карты) за счет использования разработанной псевдослучайной функции (ПСФ), многократное применение которой в различных протоколах позволит увеличить объем наличности, хранимой в «электронном кошельке».

В работе представлены задачи, решение которых возможно путем применения разработанной ПСФ повышенной эффективности в протоколе определения двойной оплаты и протоколе снятия со счета. Реализация разработанной функции использует ключ в $\log_2 \ell$ *раз меньший размером по сравнения с ПСФ Наора-Рейнголда, при этом стойкость*