§5 ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

Костин А.О., Жигулин Г.П., Володина А.А.

АНАЛИЗ УГРОЗЫ УТРАТЫ ЮРИДИЧЕСКОЙ СИЛЫ ЭЛЕКТРОННОГО ДОКУМЕНТА В СИСТЕМЕ УДАЛЕННОГО ФИНАНСОВОГО ДОКУМЕНТООБОРОТА

Аннотация. *Автор подробно рассматривает такие аспекты темы, как угроза безопасности информации для органов власти города Санкт-Петербурга, в системе удаленного финансового документооборота (СУФД). Рассказаны преимущества СУФД, новой системы, введенной в июле 2013 года, перед системой электронного документооборота (СЭД). Представлена информация для получения квалифицированного сертификата ключа проверки в федеральном казначействе города Санкт-Петербурга. Рассмотрены частные свойства электронного документа с помощью, которых он сохраняет юридическую силу с технической точки зрения. Методологией исследования угрозы утраты юридической силы электронного документа, является отрицательный результат проверки электронной подписи при передаче информации. Основной вывод данной статьи является в построении обобщенной модели, описывающей условия реализации угрозы «утраты юридической силы электронного документа». Научная новизна заключается в рассмотрении угрозы, которая затрагивает вопросы информационной безопасности при передаче данных между органами власти города Санкт-Петербурга с федеральным казначейством.*

Ключевые слова: *СУФД, электронный документ, угроза безопасности информации, электронная подпись, утрата юридической силы, система электронного документооборота, Федеральное казначейство, квалифицированный сертификат, источник угроз, муниципальный округ.*

Abstract. *The authors carefully examine such aspects of the topic as the threat to information security for the St. Petersburg municipal authorities within the system of remote financial document management. The authors underline the advantages of the system of remote financial document management, new system introduced*

DOI: 10.7256/2073-8560.2016.2.14865

in July of 2013 before the system of electronic document management. The article presents information for receiving the qualified certificate of verification key in the federal treasury of St. Petersburg. The individual properties of electronic document management, with the help of which it retains its legal power from the technical point of view, are being reviewed. The main conclusion consists in building a generalized model that describes the conditions under which emerges the threat of "loss of legal power of an electronic document". The scientific novelty consists in examination of threat with regards to the questions of information security during the transfer of data between the St. Petersburg municipal authorities and the federal treasury.

Key words: *electronic document management system, loss of legal force, electronic signature, threat to information security, electronic document, Remote financial document, federal treasury, qualified certificate, source of threats, municipality.*

В современном мире важна скорость передачи информации, принятие решений. Во многом из-за этого произошел переход к безбумажной технологии управления. Эта технология основывается на использовании трех основных концепций:

– переход к электронным документам;
– создание системы управления документами;
– система электронного документооборота.

В результате этого произошел процесс, в котором с точки зрения юриспруденции бумажный документооборот равен электронному документообороту. Создалась новая система электронного документооборота (СЭД).

Применение систем электронного документооборота позволяет сотрудникам контролировать прохождение документов и доступ к ним, а также управлять хранением и публикациями документов, снизить избыточность данных и бумажные процессы. Поэтому с помощью СЭД повышается эффективность деятельности коммерческих компаний и промышленных предприятий. В государственных учреждениях на базе технологий электронного документооборота решаются задачи внутреннего управления, межведомственного взаимодействия и взаимодействия с населением, что является необходимым условием для перехода к «электронному» правительству.

До недавнего времени в муниципальных учреждениях Санкт-Петербурга для этих целей использовалось прикладное программное обеспечение системы электронного документооборота (ППО СЭД). В июле 2013 года произошел переход на систему удаленного финансового документооборота (СУФД). В дальнейшем произошел переход на СУФД всех муниципальных учреждений страны и в конце 2013 года он был завершен. Рассмотрим в чем заключается принципиальная разница между СЭД и СУФД.

СУФД онлайн – это принципиально новый канал обслуживания, с помощью которого каждый клиент в любое удобное для него время и из любой точки, подключенной к Интернету, имеет возможность:

– удобно и безопасно управлять своими платежами и финансовыми документами;
– иметь доступ к актуальной отчетности, сформированной в автоматизированной системе Федерального казначейства (АСФК).

Основные его преимущества перед СЭД:

- Отсутствие специализированного ППО СЭД на устройстве клиента.
- Не требуется стационарное автоматизированного рабочего места.
- Нет необходимости в поддержании актуальных версий ППО СЭД и справочников.
- Также отпадает необходимость в вызове специалистов по настройке ПП СЭД и(или) отправки системного блока для настройки.
- Более широкий набор услуг.
- Отсутствие базы данных у клиента. Вся база хранится в управлении федерального казначейства (УФК).
- Справочники всегда актуальны (так как они находятся непосредственно в автоматизированной системе Федерального казначейства (АСФК)).
- Безопасность. СУФД-онлайн гарантируется безопасность данных. Шифрование данных через защищённое VPN -соединение. ППО Континент АП.
- Минимальные затраты на информационно-технологическую инфраструктуру.
- Нет необходимости в дополнительном промежуточном серверном оборудовании, что повышает надёжность системы.
- Работа в режиме реального времени.
- Возможность доступа в любом месте, в любое время, при подключении к Интернету.

DOI: 10.7256/2073-8560.2016.2.14865

Рис. 1. Схема работы СУФД портала

- Всегда актуальная версия.
- Наличие в интернете документации, инструкций, форумов, видеоуроков, в дополнение к специалистам УФК.

Пользователи федерального казначейства обладают автоматизированным рабочим место, с настроенным доступом к порталу и уникальным идентифицируемым номером. Самое важное преимущество заключается в скорости осуществляемых процессов во время работы: документы клиентов попадают почти мгновенно в прикладное программное обеспечение автоматической системы федерального казначейства (ППО АСФК). Данные поступают на сервер приложений, который обеспечивает постоянство работы портала. Сервер приложений связан с базой данных. Такая система имеет трехуровневую архитектуру. С сервером приложений непосредственно работают операторы федерального казначейства.

Таким образом пользователь СУФД имеет возможность отслеживать зачисления средств по своим счетам и проведение платежей.

Проанализируем СУФД на наличие угроз информационной безопасности. Для защиты СУФД используются электронно-цифровые подписи (ЭЦП). ЭЦП представляет собой реквизит документа, позволяющий установить отсутствие искажения содержащейся в документе информации, а также однозначно определить отправителя документа. В основном разработчики не дают четких требований, какие защищенные сервисы необходимо развернуть на ее основе. В общем случае к задаче создания защищенного электронного документооборота необходимо подходить с точки зрения классической защиты информационной системы, несмотря на изменения правового поля и недостатка стандартов. Главная цель информационной безопасности это обеспечении выполнения таких задач, как:

– аутентификация пользователей и разделение доступа;
– подтверждение авторства электронного документа;
– контроль целостности электронного документа;
– конфиденциальность электронного документа;
– обеспечение юридической значимости электронного документа.

Современные реалии изменили направление в защите. Раньше обеспечивалась защита непосредственно самих электронных документов или информационных ресурсов, содержащих документы. Теперь в условиях изменения направления атак, соответственно меняется и объект защиты. Таким образом, защищать надо не столько сами документы, сколько системы передачи, обработки и хранения электронных документов при доступе пользователей к работе с электронными документами.

Рассмотрим общую модель защищенного СУФД рисунок 2. Она состоит из внешнего и внутреннего сектора.

Во внешний сектор входят удаленные рабочие места и рабочие места в учреждениях, которые основаны на локально-вычислительных сетях, защищенной Wi-Fi-сети, VPN-каналах и т.д. Во внутренний сектор входят аппаратный межсетевой экран (МСЭ) «Континент-АП», предназначенный для фильтрации IP-пакетов сетевого трафика компьютера, на котором установлен абонентский пункт и сервер операционной системы (ОС) с поддержкой домена, который может быть организован на следующих платформах: Windows Server. Сервер приложения может иметь две реализации: прикладная программа для ОС и Web-интерфейс. Сервер базы данных (БД) реализован на основе клиент-серверных системах управления базами данных (СУБД,) к которым относятся MS SQL Server и Oracle. Все эти компоненты составляют единый механизм доступа к электронным документам. Сервер ОС является одновременно и центром сертификации защищенного протокола.

После обновления ядра портала появилась меню «последние действия пользователя. Зайдя в неё можно отследить все последние действия пользователя, отправление платежей, создание новый документов, выгрузка данных

DOI: 10.7256/2073-8560.2016.2.14865

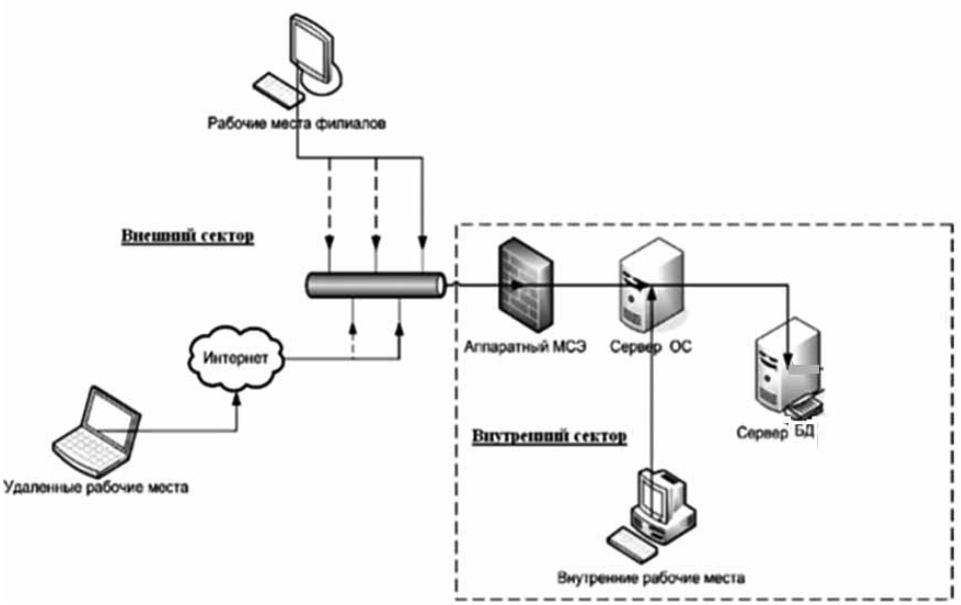

Рис. 2. Общая модель защищенного СУФД

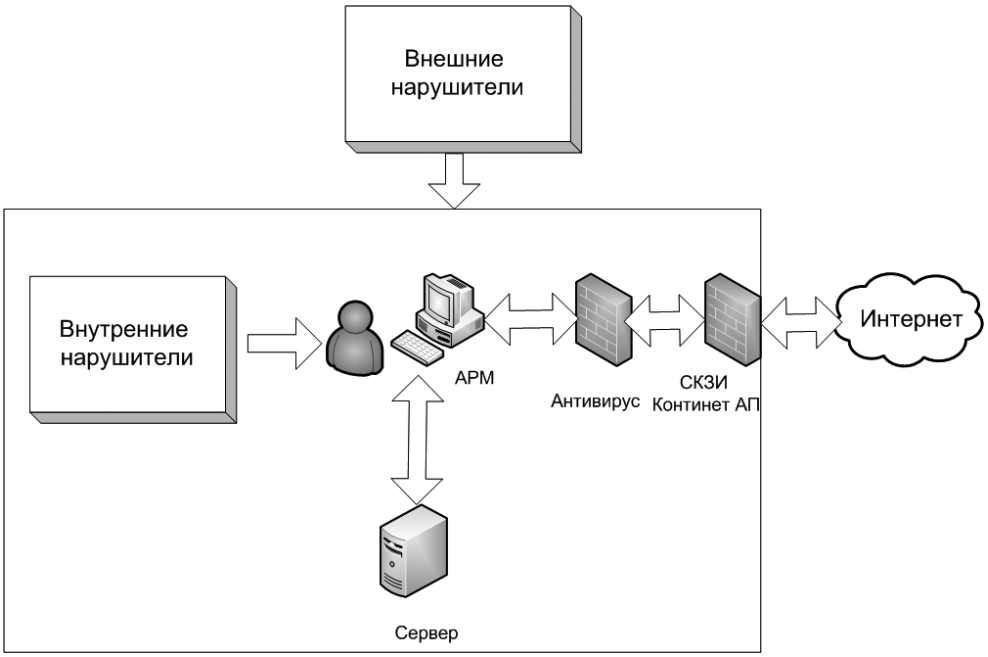

Рис. 3. Модель угроз АРМ

и т.д. Сама система не дает доступ к порталу с двух компьютеров от имени одного пользователя, срабатывает защита и пользователь выводится из системы. С точки зрения угрозы безопасности, есть всего четыре действия производимые с информацией, которые могут содержать в себе угрозу: сбор, модификация, утечка и уничтожение. Проникновение к порталу через конкретного пользователя через настроенное рабочее место возможен только при проникновении нарушетеля на территорию учреждения, при удаленном подключении к компьютеру пользователя (teamviemer, ammyy admin) или непосредственно сотрудником организации. Нарушители системы делятся на внешних и внутренних. Построим модель угроз АРМ рисунок 3.

Важнейшей задачей является защита персональных данных от посторонних лиц. Дадим определение угрозам безопасности.

Угрозы безопасности персональных данных – это некая совокупность условий или воздействующих факторов, которые создают опасность в отношении персональных данных, заключающуюся в ознакомлении посторонних лиц с защищаемыми персональными данными, несанкционированном изменении, уничтожении, рас-

DOI: 10.7256/2073-8560.2016.2.14865

	Угрозы безопасности информации	Актуальность угрозы
Внешние нарушители	угроза «Анализа сетевого трафика» с перехватом передаваемой во внешние сети информации	-
	угроза внедрения по сети вредоносных программ	+
	угроза выявления паролей	-
	угроза получения НСД путем подмены доверенного объекта	-
	угроза типа «Отказ в обслуживании	-
Внутренние нарушители	угроза удаленного запуска приложений;	+
	Угроза НСД к ПДн, обрабатываемым на автоматизированном рабочем месте	-
	угрозы утечки информации по техническим каналам	-

Рис. 4. Угрозы безопасности персональных данных

пространении, а также других неправомерных действий с персональными данными.

Рассмотрим с какими угрозами представленная схема защиты СУФД справляется.

Для непосредственного доступа к СУФД необходимо получить в федеральном казначействе квалифицированный сертификат ключа проверки (КСКП). На рисунке 5 представлен порядок выдачи КСКП. После получения сертификата его необходимо установить на рабочее место с помощью программы Crypto pro, используя полученный при создании ключа контейнер. После необходимо осуществить его привязку через федеральное казначейство. Только после этого пользователь получит не только доступ к порталу, а также права электронной подписи документов и отправки их сразу в ППО АСФК.

Ключевым объектом приложения является электронный документ (ЭД). С технической точки зрения, юридическая сила ЭД – это комплексное свойство, сообщаемое ЭД действующим законодательством при одновременном наличии у ЭД следующих частных свойств:

– доступность ЭД – возможность физического доступа к требуемым элементам ЭД, а также возможность преобразования файла ЭД в требуемую для восприятия человека форму за конечное время;
– целостность ЭД – неизменность определенных параметров ЭД на всех этапах его жизненного цикла, независимо от способов и средств обработки ЭД;
– подлинность (аутентичность) ЭД – соответствие заявленной сущности ЭД, а также времени, месту и автору, заявленному в ЭД;
– легитимность – правомерность использованных на протяжении жизненного цикла ЭД технологий его обработки.
– конфиденциальность – доступности элементов ЭД только полномочным пользователям (процессам).

В случае нарушение одного из этих требований приводит к утрате ЭД свойство юридической силы.

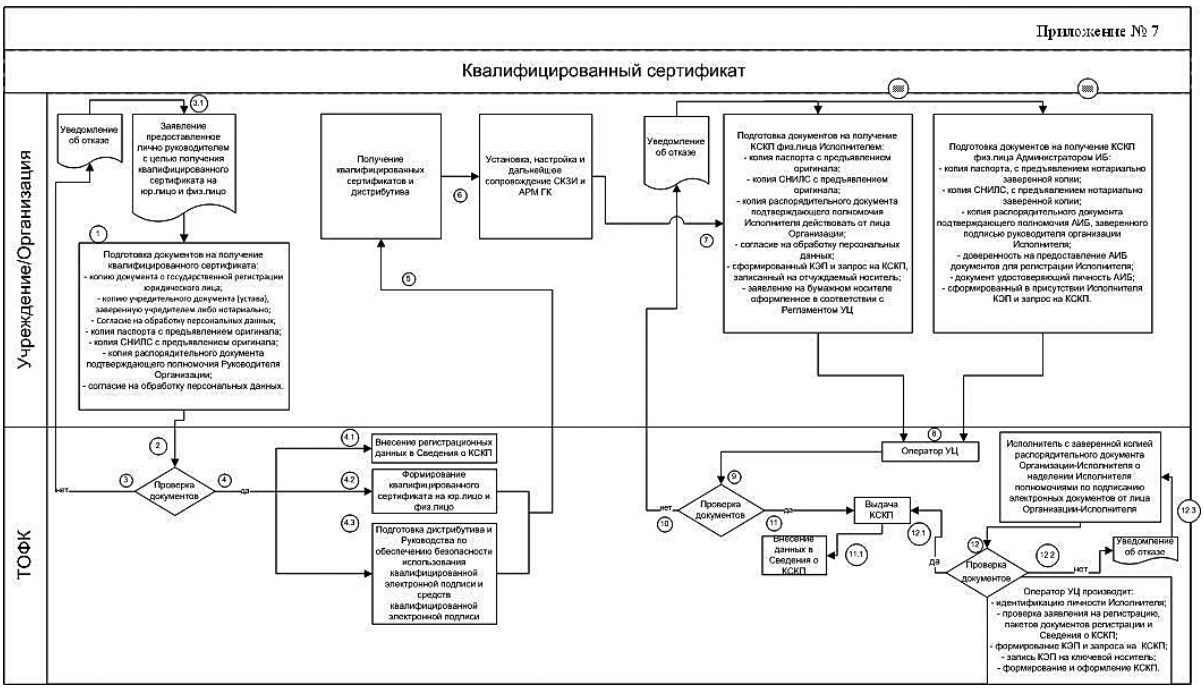

Рис. 5. Порядок выдачи КСКП

DOI: 10.7256/2073-8560.2016.2.14865

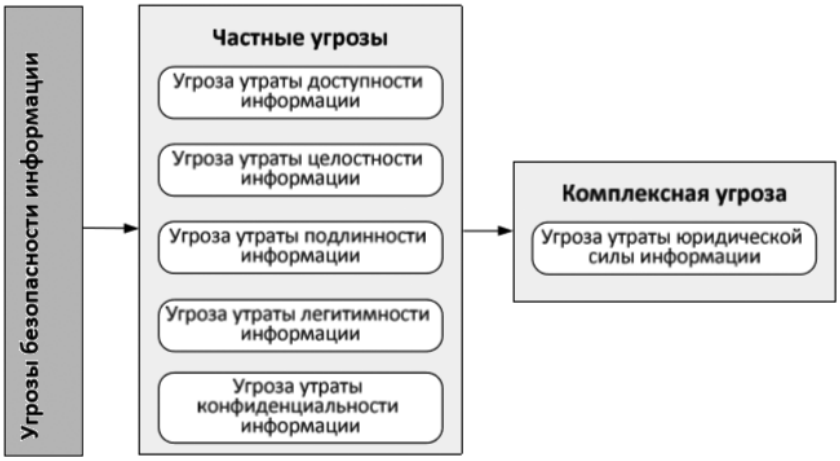

Рис. 6. Классификация угроз безопасности информации в СУФД

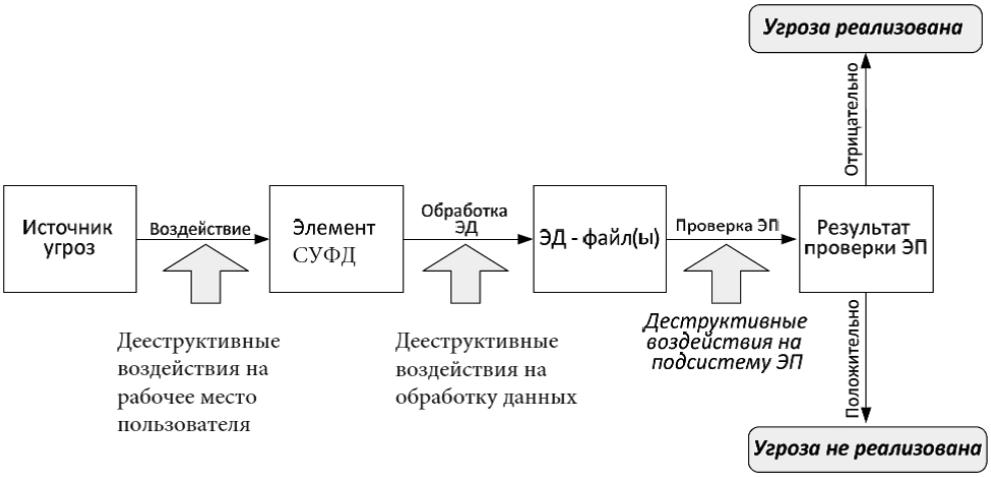

Рис. 7. Обобщенная модель реализации угрозы утраты юридической силы ЭД

Юридическую значимость электронному документу придаёт электронная цифровая подпись, которая на территории Российской Федерации равнозначна собственноручной подписи в документе на бумажном носителе при одновременном соблюдении следующих условий:

– сертификат ключа подписи, относящийся к этой ЭЦП, не утратил силу (действует) на момент проверки или на момент подписания электронного документа;
– при наличии доказательств, определяющих момент подписания;
– подтверждена подлинность электронной цифровой подписи в электронном документе;
– электронная цифровая подпись используется в соответствии со сведениями, указанными в сертификате ключа подписи.

Основными параметрами информации являются параметры, характеризующие свойства доступности, целостности, подлинности, легитимности и конфиденциальности. Обозначим их через $x_{дост}$, $x_{цел}$, $x_{подл}$, $x_{легит}$, $x_{конф}$. Эти величины характеризуют частные свойства доступности, целостности, подлинности, легитимности и конфиденциальности соответственно. Элементы $x_{дост}$, $x_{цел}$, $x_{подл}$, $x_{легит}$, $x_{конф}$ принадлежат множеству, принимающему только два значения или «1» или «0». Определим для этих элементов значение «1» в случае соответствия параметров ЭД наличию одного из указанных частных свойств и значение «0» в случае несоответствия параметров ЭД. Тогда величина, характеризующая наличие («1») или отсутствие («0») свойства юридической силы, может быть выражена следующей зависимостью:

$$X_{юрид.сила} = x_{дост} \wedge x_{цел} \wedge x_{подл} \wedge x_{легит} \wedge x_{конф}. \quad (1)$$

Свойство юридической силы является целостным свойством ЭД, возникающим при одновременном наличии частных свойств доступности, целостности, подлинности, легитимности

DOI: 10.7256/2073-8560.2016.2.14865

и конфиденциальности. Согласно (1) утрата любого из частных свойств неизбежно приведет к потере свойства юридической силы и как следствие к неспособности ЭД в полном объеме выполнять свои функции. Поэтому основной системной угрозой, свойственной для СУФД, является комплексная угроза «утраты юридической силы ЭД». Обобщенная классификация угроз безопасности информации в СУФД представлена на рисунке 6.

Основным показателем, отражающим факт реализации угрозы утраты юридической силы ЭД, является отрицательный результат проверки электронной подписи (ЭП). С учетом технических особенностей обработки информации в СУФД обобщенная модель реализации угрозы утраты юридической силы ЭД будет иметь вид, представленный на рисунке 7.

Выводы:

Переход муниципальных учреждений города Санкт-Петербург с СЭД на СУФД потребовал выявления вероятных угроз потери информации. Системный анализ свойств информации в СУФД позволил классифицировать частные угрозы характерные для ЭД, а также выявить угрозу «утраты юридической силы ЭД». Рассмотрен способ получения КСКП в федеральном казначействе. Построена модель угроз автоматизированного рабочего места, составлена таблица, позволяющая проанализировать защищенность системы от внешних и внутренних нарушителей.

На основе результатов анализа функциональных связей элементов СУФД была построена обобщенная модель, отражающая условия реализации комплексной угрозы «утраты юридической силы ЭД».

БИБЛИОГРАФИЯ

1. А.А. Малюк, В.С. Горбатов, В.И. Королев и др.-Введение в информационную безопасность – М.: Горячая линия – Телеком, 2013. – 288 с.
2. Булдакова Т.И., Глазунов Б.В., Ляпина Н.С. Оценка эффективности защиты систем электронного документооборота. Доклады ТУСУРа, № 1 (25), часть 2, июнь 2012.
3. С.А. Петренко, В.А.Курбатов.-Политики информационной безопасности-ДМК Пресс, 2010.-118 с.
4. http://www.sufdonline.ru/
5. http://rcto.otr.ru/MO/page/252/
6. http://piter.roskazna.ru
7. А.В. Куракин, М.В. Костенников.-Государственная служба и информационная безопасность // Журнал «Вопросы безопасности» – 2014. – № 6.
8. А.И. Халиуллин.-Внедрение электронного документооборота в деятельность правоохранительных органов государств Содружества Независимых Государств // Журнал «Кибернетика и программирование» – 2013. – № 6
9. В.Л. Шульц.-Сценарный анализ в управлении социальной безопасностью // Национальная безопасность / nota bene.-2012.-6.-С. 4-21.
10. И.Г. Дровникова, А.А.Никитин.-Оценка эффективности программных средств защиты информации сертифицированного общего программного обеспечения. Воронежский институт МВД России, В/Ч 28683.. Интернет-журнал «Технологии техносферной безопасности» Выпуск № 1 (47), 2013 г.
11. А.Н. Люльченко.-Описание проблемных ситуаций функционирования систем защиты информации // Научно-технический сборник. СПб-Петродворец: ВТИ ЖДВ и ВОСО. – 2013.-№ 27.
12. В.Л. Шульц, В.В. Кульба, А.Б. Шелков, И.В. Чернов Методы сценарного анализа угроз эффективному функционированию систем организационного управления // Тренды и управление.-2013.-1.-С. 6-30. DOI: 10.7256/2307-9118.2013.01.2.
13. Усманова И.В., Коровина Л.В. К вопросу о разработке автоматизированной информационной системы анализа документооборота // Программные системы и вычислительные методы.-2014.-1.-С. 63-69. DOI: 10.7256/2305-6061.2014.1.11398.

REFERENCES

1. A.A. Malyuk, V.S. Gorbatov, V.I. Korolev i dr.-Vvedenie v informatsionnuyu bezopasnost' – M.: Goryachaya liniya – Telekom, 2013. – 288 s.
2. Buldakova T.I., Glazunov B.V., Lyapina N.S. Otsenka effektivnosti zashchity sistem elektronnogo dokumentooborota. Doklady TUSURa, № 1 (25), chast' 2, iyun' 2012.

DOI: 10.7256/2073-8560.2016.2.14865

3. S.A. Petrenko, V.A.Kurbatov.-Politiki informatsionnoi bezopasnosti-DMK Press, 2010.-118 s.
4. http://www.sufdonline.ru/
5. http://rcto.otr.ru/MO/page/252/
6. http://piter.roskazna.ru
7. A.V. Kurakin, M.V. Kostennikov.-Gosudarstvennaya sluzhba i informatsionnaya bezopasnost' // Zhurnal «Voprosy bezopasnosti» – 2014. – № 6.
8. A.I. Khaliullin.-Vnedrenie elektronnogo dokumentooborota v deyatel'nost' pravookhranitel'nykh organov gosudarstv Sodruzhestva Nezavisimykh Gosudarstv // Zhurnal «Kibernetika i programmirovanie» – 2013. – № 6
9. V.L. Shul'ts.-Stsenarnyi analiz v upravlenii sotsial'noi bezopasnost'yu // Natsional'naya bezopasnost' / nota bene.-2012.-6.-C. 4-21.
10. I.G. Drovnikova, A.A.Nikitin.-Otsenka effektivnosti programmnykh sredstv zashchity informatsii sertifitsirovannogo obshchego programmnogo obespecheniya. Voronezhskii institut MVD Rossii, V/Ch 28683.. Internet-zhurnal «Tekhnologii tekhnosfernoi bezopasnosti» Vypusk № 1 (47), 2013 g.
11. A.N. Lyul'chenko.-Opisanie problemnykh situatsii funktsionirovaniya sistem zashchity informatsii // Nauchno-tekhnicheskii sbornik. SPb-Petrodvorets: VTI ZhDV i VOSO. – 2013.-№ 27.
12. V.L. Shul'ts, V.V. Kul'ba, A.B. Shelkov, I.V. Chernov Metody stsenarnogo analiza ugroz effektivnomu funktsionirovaniyu sistem organizatsionnogo upravleniya // Trendy i upravlenie.-2013.-1.-C. 6-30. DOI: 10.7256/2307-9118.2013.01.2.
13. Usmanova I.V., Korovina L.V. K voprosu o razrabotke avtomatizirovannoi informatsionnoi sistemy analiza dokumentooborota // Programmnye sistemy i vychislitel'nye metody.-2014.-1.-C. 63-69. DOI: 10.7256/2305-6061.2014.1.11398.

DOI: 10.7256/2073-8560.2016.2.14865