УДК 004.942

# ИМИТАЦИОННАЯ МОДЕЛЬ РЕАЛИЗАЦИИ ВНУТРЕННИХ И ВНЕШНИХ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ НА СЕГМЕНТЕ «МАРШРУТИЗАТОР – МАРШРУТИЗАТОР»

**[1]Шувалов И.А., [2]Семенчин Е.А.**

*[1]Управление ГИБДД ГУ МВД России по Краснодарскому краю, Краснодар, e-mail: ilya_kizlyar@mail.ru;*

*[2]ФГБОУ ВПО «Кубанский государственный университет», Краснодар, e-mail: es14@mail.ru*

В работе предложена имитационная модель реализации угроз безопасности одного из сегментов информационной системы обработки персональных данных «Информационные ресурсы Управления ГИБДД», используемой в служебной деятельности сотрудниками Управления государственной инспекцией безопасности дорожного движения Главного управления Министерства внутренних дел России по Краснодарскому краю. Поэтапно описан процесс создания имитационной модели. В результате проведенных экспериментов с предложенной имитационной моделью выделены угрозы, которые имеют высокую вероятность реализации при прохождении запроса на рассмотренном сегменте. Используя данные, также полученные в результате проведенных экспериментов с моделью, проведена оценка качества имеющейся системы защиты от реализации угроз безопасности информационной системы обработки персональных данных и выделены угрозы, отсутствие защиты от которых наиболее значимо влияет на конечный результат.

**Ключевые слова: имитационное моделирование, угрозы безопасности, безопасность персональных данных**

# SIMULATION MODELING OF IMPLEMENTATION OF INTERNAL AND EXTERNAL SECURITY RISKS OF THE INFORMATION SYSTEM ON THE SEGMENT «ROUTER- ROUTER»

**[1]Shuvalov I.A., [2]Semenchin E.A.**

*[1]Control of traffic police of Head department of the Ministry of Internal Affairs of Krasnodar Krai, Krasnodar, e-mail: ilya_kizlyar@mail.ru;*

*[2]Kuban State University Krasnodar, e-mail: es14@mail.ru*

In article the simulation model of implementation of security risks of one of segments of an information system of processing of personal data «Information resources of Management of traffic police» is offered. The system is used in the official activities by employees of Management by State Inspection for Road Traffic Safety of Head department of the Ministry of Internal Affairs of Russia for Krasnodar Krai. Process of creation of a simulation model is described step by step. As a result of the carried-out experiments with the offered simulation model threats which have high probability of implementation when passing request on the considered segment. Using data retrieveds, the assessment of quality of available system of protection against implementation of security risks of an information system of processing of personal data is carried out and threats absence of protection from which most significantly influences the end result.

**Keywords: simulation modeling, security risks, safety of personal data**

В связи со вступлением в силу с 1 июля 2011 года требований Федерального закона от 23 декабря 2010 года № 359-ФЗ «О внесении изменения в статью 25 федерального закона «О персональных данных» [2], проблема приведения информационных систем обработки персональных данных в соответствие с требованиями с Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»[3] является актуальной для многих организаций, как для государственных, так и для частных. Одной из первостепенных проблем, которую необходимо решить для выполнения требований Федерального закона, является выявление актуальных угроз безопасности информационной системы.

Целью настоящей статьи является выявление актуальных угроз безопасности информационной системы путем построения имитационной модели данной системы. В качестве объекта исследования предложена имитационная модель функционирования информационной системы обработки персональных данных «Информационные ресурсы Управления ГИБДД ГУ МВД России по Краснодарскому краю». В качестве среды моделирования использовано программное обеспечение «Anylogic», разработанное российской компанией «Экс Джей Технолоджис».

Рассматриваемая система содержит множество узлов и ответвлений, в связи с чем для детального ее изучения отдельно рассматривается каждый сегмент. В данной работе рассматривается сегмент, в котором запрос поступает к маршрутизатору Управления ГИБДД от маршрутизатора подразделения по арендуемым (при использовании технологий VSAT или xDSL) или ведомственным (волоконно-оптические линии связи) каналам связи. Экспертной

комиссией, созданной из специалистов, отвечающих за информационные подсистемы системы «Информационные ресурсы УГИБДД», выделены угрозы, которые могут быть реализованы на рассмотренном сегменте (табл. 1).

Опишем общую схему функционирования имитационной модели. Запрос движется между двумя маршрутизаторами по соединительной линии (каналу связи), на которой расположены точки наступления угроз. Запрос, проходя точку наступления угрозы, либо продолжает движение к маршрутизатору Управления и фиксируется факт нереализации угрозы, либо с вероятностью наступления угрозы попадает на альтернативный путь движения и фиксируется факт наступления угрозы. Если наступившая угроза препятствует дальнейшему продвижению запроса, например, угроза типа «Отказ в обслуживании», то цикл заканчивается и в счетчик наступивших угроз прибавляется одно значение. Если угроза не препятствует дальнейшему продвижению, например, угроза выявления паролей по сети, то в счетчик наступивших угроз также прибавляется одно значение, но запрос продолжает движение.

Для определения вероятности наступления угроз при построении модели использованы экспериментальные данные (см. табл. 1):

**Таблица 1**

Вероятности наступления угроз

| Наименование угрозы | Вероятность наступления угрозы |
|---|---|
| Вывод из строя узлов ПЭВМ, каналов связи | 0,1 |
| Выход из строя аппаратно-программных средств | 0,1 |
| Сбой системы электроснабжения | 0,1 |
| Стихийное бедствие | 0,1 |
| Угроза подмены довер. объекта | 0,1 |
| Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации в пределах контролируемой зоны внешними нарушителями | 0,1 |
| Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации в пределах контролируемой зоны внутренними нарушителями | 0,1 |
| Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб и др. | 0,1 |
| Угрозы выявления паролей по сети | 0,25 |
| Угрозы навязывания ложного маршрута сети | 0,1 |
| Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации за переделами с контролируемой зоны | 0,25 |
| Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях | 0,1 |
| Угрозы типа «Отказ в обслуживании» | 0,1 |

Общая схема наступления угроз представлена на рис. 1.

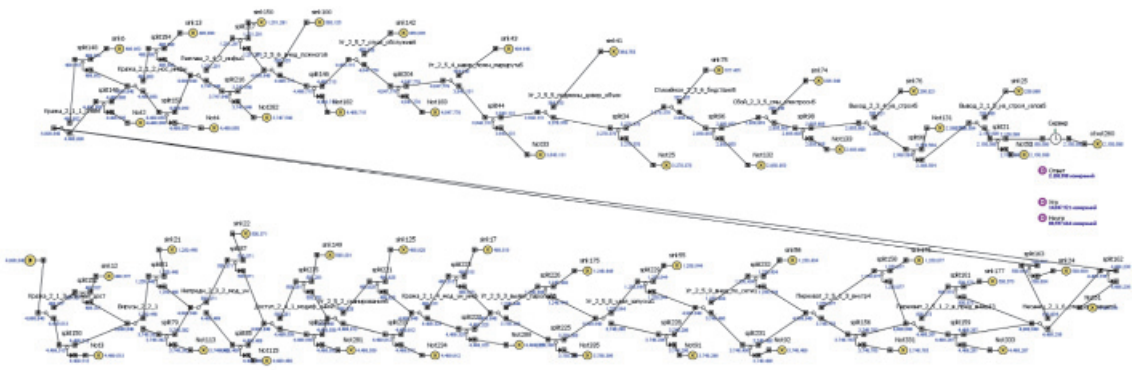

*Рис. 1. Общая схема наступления угроз*

Для получения наиболее достоверных результатов было принято решение использовать 1 000 000 единиц модельного времени, что, в среднем, позволяет сгенерировать 5 000 000 запросов.

В результате многократно проведенных опытов выявлено, что количество завершенных запросов составляет 43,09 % от количества сгенерированных.

На следующем этапе в построенную модель добавлены вероятности реализации угроз (табл. 2), определенные экспертной комиссией. Данные вероятности добавлены в виде точки реализации угрозы, расположенной на альтернативном пути продвижения запроса.

После добавления вероятностей реализации угроз модель приняла следующий вид (рис. 2). Результатом добавления вероятностей реализации угроз стало увеличение до 88,92 % сгенерированных запросов, завершивших движение до сервера, от количества поступивших.

**Таблица 2**

Вероятность реализации угроз

| Наименование угрозы | Вероятность реализации угрозы |
|---|---|
| Вывод из строя узлов ПЭВМ, каналов связи | 0,1 |
| Выход из строя аппаратно-программных средств | 0,1 |
| Сбой системы электроснабжения | 0,25 |
| Стихийное бедствие | 0,25 |
| Угроза подмены довер. объекта | 0,1 |
| Угроза «Анализ сетевого трафика» с перехватом в пределах КЗ внешними нарушителями | 0,25 |
| Угроза «Анализ сетевого трафика» с перехватом в пределах КЗ внутренними нарушителями | 0,25 |
| Угрозы сканирования, направленные на выявление топологии сети, открытых портов и др. | 0,25 |
| Угрозы выявления паролей по сети | 0,5 |
| Угрозы навязывания ложного маршрута сети | 0,1 |
| Угроза «Анализ сетевого трафика» с перехватом за переделами КЗ | 0,5 |
| Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях | 0,1 |
| Угрозы типа «Отказ в обслуживании» | 0,25 |

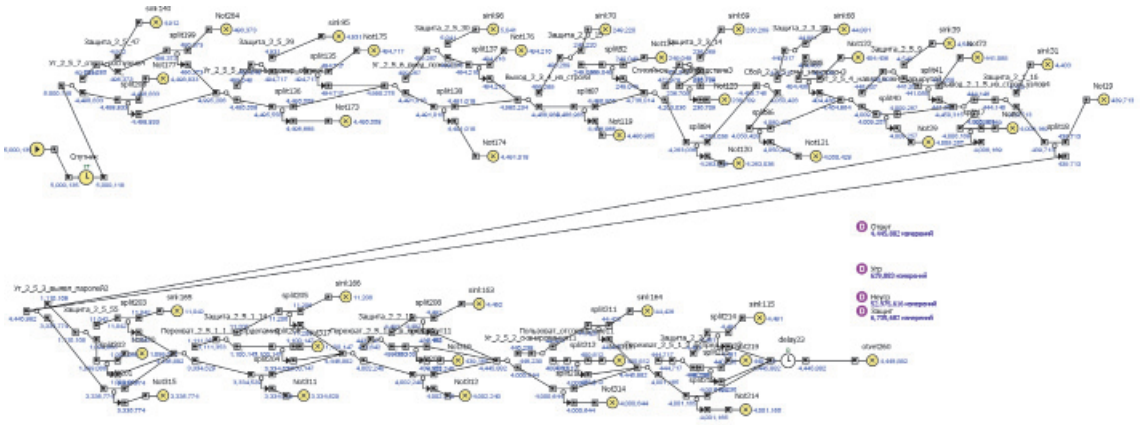

*Рис. 2. Схема реализации угроз*

Следующим этапом стало добавление в систему вероятностей реализации угроз при наличии дополнительной системы защиты. Система защиты добавлена также в виде точки, расположенной на пути реализации угрозы. Вероятности реализации угроз при наличии защиты также предложены экспертами (табл. 3). В итоге схема реализации угроз приняла вид, представленный на рис. 3.

**Таблица 3**

Вероятность реализации угрозы при наличии защиты

| Наименование угрозы | Вероятность реализации угрозы с защитой |
|---|---|
| Вывод из строя узлов ПЭВМ, каналов связи | 0,01 |
| Выход из строя аппаратно-программных средств | 0,5 |
| Сбой системы электроснабжения | 0,1 |
| Стихийное бедствие | 0,5 |
| Угроза подмены довер. объекта | 0,01 |
| Угроза «Анализ сетевого трафика» с перехватом в пределах КЗ внешними нарушителями | 0,01 |
| Угроза «Анализ сетевого трафика» с перехватом в пределах КЗ внутренними нарушителями | 0,01 |
| Угрозы сканирования, направленные на выявление топологии сети, открытых портов и др. | 0,1 |
| Угрозы выявления паролей по сети | 0,5 |
| Угрозы навязывания ложного маршрута сети | 0,01 |
| Угроза «Анализ сетевого трафика» с перехватом за переделами КЗ | 0,01 |
| Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях | 0,01 |
| Угрозы типа «Отказ в обслуживании» | 0,01 |

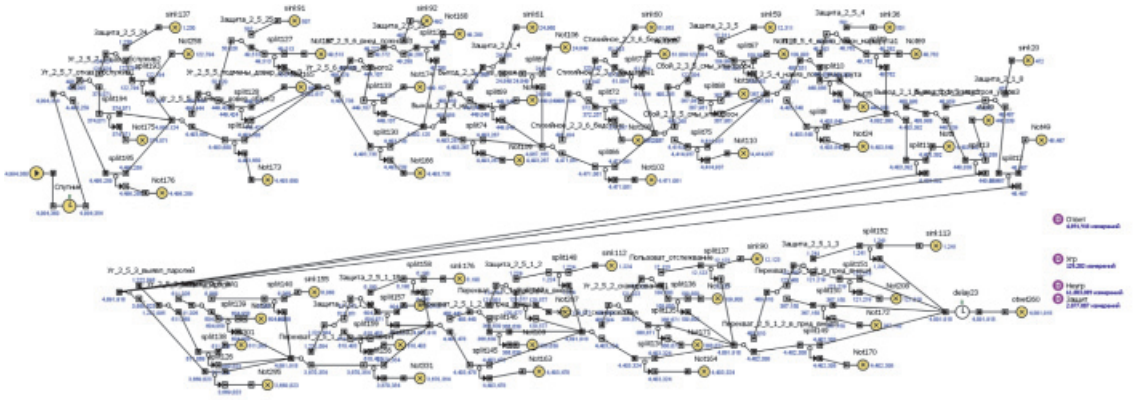

*Рис. 3. Схема реализации угроз при наличии системы защиты*

В результате проведенных экспериментов установлено, что до маршрутизатора Управления поступает 97,95 % сгенерированных запросов, при среднем количестве реализовавшихся угроз на один запрос 0,026, что равносильно одной реализованной угрозе на 39 поступивших запросов. Процент реализованных угроз от количества реализованных, нереализованных и не наступивших угроз составил 0,2.

В целях выявления угроз, которые наиболее значимо влияют на конечный результат, результаты реализации угроз рассмотрены отдельно от остальных результатов измерений (табл. 4).

Проведенные эксперименты с имитационной моделью показали, что к наиболее вероятным угрозам относятся:

- стихийное бедствие – 47,93 % от общего количества реализовавшихся угроз;
- выход из строя аппаратно-программных средств – 19,31 %;
- сбой системы электроснабжения – 9,52 %.
- угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, открытых портов и служб, открытых соединений и др. – 9,38 %.

В целях оценки качества и значимости защиты от каждой угрозы, которая, по мнению экспертной комиссии, может наступить на данном сегменте имитационной модели, из модели поочередно убиралась дополнительная защита от каждой угрозы и проводились измерения. Полученные результаты измерений представлены в табл. 5.

**Таблица 4**

Процент количества реализованных угроз

| Наименование угрозы | Кол-во угроз с защитой | Процент от кол-ва угроз с от общего кол-ва |
|---|---|---|
| Вывод из строя узлов ПЭВМ, каналов связи | 472 | 0,365 |
| Выход из строя аппаратно-программных средств | 24960 | 19,307 |
| Сбой системы электроснабжения | 12311 | 9,523 |
| Стихийное бедствие | 61963 | 47,929 |
| Угроза подмены довер. объекта | 507 | 0,392 |
| Угроза «Анализ сетевого трафика» с перехватом в пределах КЗ внеш. нарушителями | 1224 | 0,947 |
| Угроза «Анализ сетевого трафика» с перехватом в пределах КЗ внутр. нарушителями | 1241 | 0,960 |
| Угрозы сканирования сети | 12123 | 9,377 |
| Угрозы выявления паролей по сети | 6068 | 4,694 |
| Угрозы навязывания ложного маршрута сети | 501 | 0,388 |
| Угроза «Анализ сетевого трафика» с перехватом за переделами КЗ | 6190 | 4,788 |
| Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях | 492 | 0,392 |
| Угрозы типа «Отказ в обслуживании» | 1230 | 0,951 |

**Таблица 5**

Результаты измерений

| Наименование угрозы | Кол-во запросов | Кол-во завершенных запросов | Кол-во реализованных угроз | Кол-во нереализованных угроз | Кол-во нереализованных угроз вследствие защиты | Кол-во угроз, реализованных при отсутствии защиты |
|---|---|---|---|---|---|---|
| Вывод из строя узлов ПЭВМ, каналов связи | 4997275 | 4846486 | 177394 | 61690498 | 2018342 | 48880 |
| Выход из строя аппаратно-программных средств | 5004910 | 4877560 | 154190 | 61799198 | 2048685 | 49943 |
| Сбой системы электроснабжения | 5003060 | 4789537 | 239928 | 61248833 | 1935840 | 123117 |
| Стихийное бедствие | 4999970 | 4835475 | 191280 | 61476302 | 1997640 | 124135 |
| Угроза подмены довер. объекта | 5007475 | 4856558 | 177781 | 61529762 | 2016343 | 49854 |
| Угроза «Анализ сетевого трафика» с перехватом в пределах КЗ внешними нарушителями | 4997500 | 4894671 | 251281 | 61916330 | 1959505 | 122881 |
| Угроза «Анализ сетевого трафика» с перехватом в пределах КЗ внутр. нарушителями | 4993975 | 4890926 | 251022 | 61871221 | 1957135 | 122124 |
| Угрозы сканирования сети | 4996915 | 4894668 | 237608 | 61913327 | 1971119 | 122717 |
| Угрозы выявления паролей по сети | 4995535 | 4894067 | 735484 | 61908465 | 1473383 | 612318 |
| Угрозы навязывания ложного маршрута сети | 5004440 | 4852972 | 178139 | 61730070 | 2017331 | 49250 |
| Угроза «Анализ сетевого трафика» с перехватом информации за переделами КЗ | 4994540 | 4891885 | 735148 | 61879219 | 1475212 | 611745 |
| Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях | 5004825 | 4853402 | 178383 | 61540698 | 2015855 | 48793 |
| Угрозы типа «Отказ в обслуживании» | 4992680 | 4768869 | 249957 | 60443111 | 1908623 | 125026 |

На основе полученных результатов были найдены (табл. 6): процент количества завершенных запросов от количества поступивших в систему; процент количества реализовавшихся угроз от общего количества реализованных и нереализованных угроз; процент количества угроз, реализация которых предотвращена системой защиты, от общего количества реализованных и нереализованных угроз; процент количества реализованных угроз, защита от которых не учитывалась во время проведения эксперимента, от общего количества реализованных угроз.

**Таблица 6**

Результаты численных расчетов

| Наименование угрозы | Процент пройденных запросов | Процент кол-ва реализованных угроз | Процент кол-ва угроз, реализация которых предотвращена системой защиты, от общего кол-ва угроз | Процент кол-ва реализованных угроз при отсутствии защиты от угрозы, от кол-ва реализованных угроз |
|---|---|---|---|---|
| Вывод из строя узлов ПЭВМ, каналов связи | 96,983 | 0,278 | 3,159 | 27,554 |
| Выход из строя аппаратно-программных средств | 97,455 | 0,241 | 3,201 | 32,391 |
| Сбой системы электроснабжения | 95,732 | 0,378 | 3,052 | 51,314 |
| Стихийное бедствие | 96,710 | 0,300 | 3,138 | 64,897 |
| Угроза подмены довер. объекта | 96,986 | 0,279 | 3,164 | 28,042 |
| Перехват в пределах КЗ внешними нарушит. | 97,942 | 0,392 | 3,056 | 48,902 |
| Перехват в пределах КЗ внутренними нарушит. | 97,937 | 0,392 | 3,054 | 48,651 |
| Угрозы сканирования сети | 97,954 | 0,371 | 3,074 | 51,647 |
| Угрозы выявления паролей по сети | 97,969 | 1,147 | 2,298 | 83,254 |
| Угрозы навязывания ложного маршрута сети | 96,973 | 0,279 | 3,156 | 27,647 |
| Угроза «Анализ сетевого трафика» с перехватом за переделами КЗ | 97,945 | 1,147 | 2,302 | 83,214 |
| Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях | 96,974 | 0,280 | 3,163 | 27,353 |
| Угрозы типа «Отказ в обслуживании» | 95,517 | 0,399 | 3,049 | 50,019 |

Проанализировав результаты, представленные в табл. 6, можно выделить угрозы, отсутствие защиты от которых наиболее очевидно влияет на конечный результат. Среди угроз наибольшее влияние оказывает отсутствие зашиты от угрозы типа «Отказ в обслуживании» (количество запросов, дошедших до окончания модели, сократилось с 97,95 до 95,52%). Также снижение завершенных запросов до 95,73% приводит отсутствие защиты от угрозы сбоя системы электроснабжения соответственно. Отсутствие защиты от остальных угроз влияет на конечный результат в менее значимой мере (не более 1,5%). Помимо указанных угроз можно отметить угрозу выявления паролей по сети и угрозу «Анализ сетевого трафика» с перехватом информации за переделами контролируемой зоны, отсутствие защиты от которых приводит к увеличению процента реализованных угроз от количества всех учтенных угроз до 1,15.

Эффективность средств защиты также можно оценить, сравнив процент реализации конкретной угрозы от общего количества реализованных угроз с процентом количества реализованных угроз, защита от которых не учитывалась во время проведения эксперимента, от общего количества реализованных угроз (табл. 7).

Проанализировав результаты, представленные в табл. 7, можно сделать вывод, что в целом система защиты ИСПДн от реализации угроз является эффективной. Вероятность реализации таких угроз, как угрозы выхода из строя аппаратно-программных средств и наступления стихийных бедствий, достаточно большая и, в то же время, наличие защиты кардинальным образом не влияет на общий результат. Отсутствие эффективной защиты обусловлено тем, что вероятность реализации данных угроз носит спонтанный характер и в очень малой степени зависит от регулируемых факторов (например, от человеческого фактора).

**Таблица 7**

Сравнение процентов реализации угроз

| Наименование угрозы | Процент реализации угрозы при наличии защиты | Процент реализации угрозы при отсутствии защиты |
|---|---|---|
| Вывод из строя узлов ПЭВМ, каналов связи | 0,365 | 27,554 |
| Выход из строя аппаратно-программных средств | 19,307 | 32,391 |
| Сбой системы электроснабжения | 9,523 | 51,314 |
| Стихийное бедствие | 47,929 | 64,897 |
| Угроза подмены довер. объекта | 0,392 | 28,042 |
| «Анализ сетевого трафика с перехватом в пределах КЗ внешн. нарушит. | 0,947 | 48,902 |
| Анализ сетевого трафика с перехватом в пределах КЗ внутр. нарушителями | 0,960 | 48,651 |
| Угрозы сканирования сети | 9,377 | 51,647 |
| Угрозы выявления паролей по сети | 4,694 | 83,254 |
| Угрозы навязывания ложного маршрута сети | 0,388 | 27,647 |
| Анализ сетевого трафика с перехватом информации за переделами КЗ | 4,788 | 83,214 |
| Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях | 0,392 | 27,353 |
| Угрозы типа «Отказ в обслуживании» | 0,951 | 50,019 |

Однако, рассматривая полученные результаты, нельзя судить о всей модели в общем, так как угрозы, актуальные на данном сегменте модели, могут не оказывать заметного влияния на модель в целом.

### Список литературы

1. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных: утверждена заместителем директора ФСТЭК России 15 февраля 2008 г. // Федеральная служба по техническому и экспортному контролю. – URL: http://www.fstec.ru/_spravs/ (дата обращения 17.02.2011 г.).

2. О внесении изменения в статью 25 Федерального закона «О персональных данных»: Федеральный закон от 23 декабря 2010 г. № 359-ФЗ: принят Государственной Думой 10 декабря 2010 г.: одобрен Советом Федерации 15 декабря 2010 г. // Российская газета. – 2010. – 27 декабря.

3. О персональных данных: Федеральный закон от 27 июля 2006 г. № 152-ФЗ: принят Государственной Думой 8 июля 2006 г.: одобрен Советом Федерации 14 июля 2006 г. // Российская газета. – 2006. – 29 июля.

4. Об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных: положение Правительства Российской Федерации от 17 ноября 2007 г. № 781 г.: утверждено постановлением Правительства Российской Федерации от 17 ноября 2007 года № 781 // Российская газета. – 2007. – 21 ноября.

5. Определение актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных: методика: утверждена заместителем директора ФСТЭК России 14 февраля 2008 г. // Федеральная служба по техническому и экспортному контролю. – URL: http://www.fstec.ru/_spravs/ (дата обращения 17.02.2011 г.).

### References

1. *Bazovaja model' ugroz bezopasnosti personal'nyh dannyh pri ih obrabotke v informacionnyh sistemah personal'nyh dannyh* [Basic model of security risks of personal data in case of their processing in information systems of personal data] Available at: URL: http://www.fstec.ru/_spravs/ (accessed 17.02.2011).

2. *O vnesenii izmenenija v stat'ju 25 Federal'nogo zakona «O personal'nyh dannyh»* (About modification of article 25 of the Federal law «About personal data»): Федеральный закон от 23 декабря 2010 г. Federal low 359 (2010).

3. *O personal'nih dannih* (About personal data) Federal low 152 (2006).

4. *Ob obespechenii bezopasnosti personal'nyh dannyh pri ih obrabotke v informacionnyh sistemah personal'nyh dannyh* (About safety of personal data in case of their processing in information systems of personal data) regulations of the Government of the Russian Federation 781 (2007).

5. *Metodika opredelenija aktual'nyh ugroz bezopasnosti personal'nyh dannyh pri ih obrabotke v informacionnyh sistemah personal'nyh dannyh* (Technique of determination of actual security risks of personal data in case of their processing in information systems of personal data) Available at: URL: http://www.fstec.ru/_spravs/ (accessed 17.02.2011.).

**Рецензенты**:

Приходько А.И., д.т.н., профессор кафедры общего, стратегического, информационного менеджмента и бизнес-процессов;

Лебедев К.А., д.ф.-м.н, профессор кафедры прикладной математики ФГБОУ ВПО «Кубанский государственный университет», г. Краснодар.

Работа поступила в редакцию 20.07.2012.