ISSN 1992-6502 (Print) Вестник УГАТУ ISSN 2225-2789 (Online)
2017. Т. 21, № 3 (73). С. 105–112 http://journal.ugatu.ac.ru

УДК 004.65

ПРИМЕНЕНИЕ МЕТОДА ЭКСПЕРТНЫХ ОЦЕНОК ДЛЯ АВТОМАТИЗАЦИИ АУДИТА ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

В. В. САГИТОВА[1], В. И. ВАСИЛЬЕВ[2]

[1] sagitovavv@mail.ru, [2] vasilyev@ugatu.ac.ru

ФГБОУ ВО «Уфимский государственный авиационный технический университет» (УГАТУ)

Поступила в редакцию 20.06.2017

Аннотация. Рассматривается проблема аудита информационных систем персональных данных с учетом специфики персональных данных как объекта защиты. Приводится обзор основных требований к безопасности персональных данных, установленных законодательством и нормативными документами Федеральной службы по техническому и экспортному контролю (ФСТЭК) и Федеральной службы безопасности (ФСБ). Предложен подход к решению задачи автоматизации аудита информационных систем персональных данных с использованием метода экспертных оценок. Привлечение экспертов для принятия решений позволяет снизить уровень неопределенности и повысить достоверность решений, позволяющий учесть специфику персональных данных и наглядно показать руководству организации состояние защищенности персональных данных, выделяя наиболее слабые места (уязвимости) в системе защиты персональных данных.

Ключевые слова: Персональные данные; аудит информационных систем; метод экспертных оценок; уровень защищенности.

ВВЕДЕНИЕ

Защита персональных данных (ПДн) регламентируется федеральным законом ФЗ-152 «О персональных данных», в соответствии с которым оператор обязан выполнить ряд организационных и технических мер, касающихся процессов обработки ПДн [1]. ПДн как объект защиты имеют свою специфику. Такие данные являются разнородными, переходящими из одной категории в другую, привязанными к конкретному субъекту ПДн, которому в случае нарушения конфиденциальности, целостности или доступности ПДн может быть нанесен значительный ущерб. Кроме того, ущерб от неправомерных действий над ПДн трудноооценим и утеря ПДн может быть выявлена не сразу, а спустя некоторое время. Вместе с тем нормативно-методическая база по защите ПДн недостаточно проработана и зачастую противоречива. Существуют и такие препятствия, как бюджетные ограничения на обеспечение безопасности ПДн и нехватка квалифицированного персонала.

Важнейшим этапом создания эффективной системы защиты персональных данных (СЗПДн) является аудит информационных систем персональных данных (ИСПДн) – процесс получения объективных качественных и количественных оценок о текущем состоянии информационной безопасности (ИБ) в соответствии с определенным критериями и показателями безопасности [2]. Причем аудит ИСПДн проводится не только на этапе проектирования СЗПДн, но и в процессе эксплуатации – для поддержания ее в актуальном состоянии.

Процедура аудита ИСПДн требует специализированных знаний и профессионализма в принятии решений. Операторы ПДн

сталкиваются с трудностями в процессе приведения ИСПДн в соответствие требованиям законодательства вследствие отсутствия эффективной методики по проведению аудита ИСПДн, которая позволила бы наглядно показать руководству организации состояние защищенности ПДн. В связи со спецификой ПДн при аудите ИСПДн часто возникает неопределенность, неоднозначность принимаемых решений, связанная с оценкой защищенности ИСПДн и необходимостью учета нормативной базы. Одним из эффективных путей решения данной проблемы является применение метода экспертных оценок на этапе проведения аудита ИСПДн. Данный метод успешно применяется в сфере информационной безопасности банковских систем, позволяя принимать обоснованные решения в условиях неопределенности (отсутствие достоверной информации, использование качественных и количественных факторов, возникновение новых факторов).

В данной статье предлагается подход к автоматизации аудита ИСПДн с использованием метода экспертных оценок, позволяющий наглядно показать руководству организации состояние защищенности ПДн, выделяя наиболее слабые места (уязвимости) в СЗПДн и указывая эффективные способы преодоления имеющихся противоречий.

МЕТОД ЭКСПЕРТНЫХ ОЦЕНОК

Метод экспертных оценок – это метод организации работы с высококвалифицированными специалистами-экспертами и обработки мнений экспертов. Основное преимущество методов экспертных оценок – возможность их применения в условиях повышенного риска и неопределенности. Привлечение экспертов для принятия решений позволяет снизить уровень неопределенности и повысить достоверность решений. Для широкого круга трудно формализуемых проблем экспертные процедуры наиболее эффективны, а в ряде случаев могут оказаться единственным средством их решения [3, 4]. К таким трудно формализуемым задачам относится проблема защиты ПДн. Экспертные исследования в области аудита ИСПДн осуществляются для оценки текущего уровня безопасности ПДн, подготовки информации для принятия решений по совершенствованию СЗПДн.

Выделяют индивидуальные и коллективные экспертные оценки. Индивидуальные методы основаны на использовании мнений экспертов, независимых друг от друга. Коллективные методы предполагают использование широкого круга специалистов, поэтому являются наиболее эффективными с точки зрения максимальной объективности экспертной оценки. Аудит ИСПДн проводится для всестороннего изучения функционирования ИСПДн и оценки защищенности ПДн. Поэтому для задачи аудита ИСПДн целесообразно использовать коллективные экспертные оценки.

Основные требования к проведению экспертной оценки в области аудита ИСПДн:

- тщательность подбора экспертов;
- оценка надежности представленной экспертами информации;
- создание условий для продуктивного использования экспертов в ходе исследования;
- учет факторов, влияющих на суждения экспертов;
- сохранение информации экспертов без искажения на всех этапах исследования.

Одним из самых важных этапов экспертных исследований является этап подбора экспертов. Критерии подбора экспертов:

- степень компетентности эксперта (наличие ученой степени, ученого звания, стаж работы по специальности, служебное положение, число опубликованных работ);
- способность ориентироваться в областях, которые являются предметом экспертизы;
- сочетание узкой специализации и общего кругозора эксперта;
- способность к анализу и синтезу изучаемых проблем;
- умение перерабатывать и усваивать качественно новую информацию;
- сочетание психологически приемлемых друг для друга в группе экспертов раз-

личного возраста, различных научных школ и т.д.

Объективность оценки определяется согласованностью мнения экспертов. Степень согласованности экспертов оценивается по величине коэффициента конкордации (согласия). Для расчета коэффициента конкордации производится ранжирование экспертных оценок важности параметров и расчет суммы рангов по каждому направлению. Коэффициент конкордации (W) рассчитывается по формуле

$$W = \frac{12 * C}{m^2\left(n^2 - n\right)},$$

где C – сумма квадратов отклонений сумм рангов по каждому параметру от средней суммы рангов; m – количество экспертов; n – количество параметров.

Значение $W = 1$ говорит о полной согласованности мнений экспертов, значение $W = 0$ – о полной несогласованности мнений экспертов. Коэффициент конкордации менее 0,5 свидетельствует о недостаточной согласованности мнений экспертной группы, чтобы по результатам опроса экспертом можно было построить достоверный прогноз [5].

ТРЕБОВАНИЯ К АУДИТУ ИСПДН

Аудит ИСПДн позволяет руководству организации определить состояние информационных активов, оценить их защищенность, провести анализ информационных рисков, корректно и обоснованно подойти к вопросу обеспечения безопасности ПДн. Грамотно проведенный аудит позволяет повысить эффективность управления ИБ компании.

Целями проведения аудита безопасности ИСПДн являются:

- анализ угроз и уязвимостей ИСПДн;
- оценка эффективности применяемых мер по защите ПДн;
- оценка соответствия защищенности ИСПДн базовым требованиям нормативных документов;
- анализ рисков безопасности ИСПДн;
- выработка рекомендаций по улучшению системы защиты ПДн.

Постановлением Правительства №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» [6] устанавливаются четыре уровня защищенности ИСПДн и соответствующие требования для каждого из них. Относить системы к тому или иному уровню защищенности, согласно этому документу, предлагается в зависимости от следующих критериев:

1. Категории обрабатываемых ПДн:
   - специальные категории ПДн, к которым относятся ПДн, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов ПДн;
   - биометрические ПДн, к которым относятся сведения, характеризующие физиологические и биологические особенности субъекта, на основании которых можно установить его личность;
   - общедоступные ПДн, к которым относятся ПДн, полученные только из общедоступных источников ПДн;
   - иные категории ПДн, не представленные в трех предыдущих группах.
2. Форма отношений между организацией и субъектами:
   - обработка ПДн сотрудников оператора;
   - обработка ПДн субъектов, не являющихся сотрудниками оператора.
3. Количество обрабатываемых ПДн:
   - менее 100 000 субъектов;
   - более 100 000 субъектов;
4. Тип актуальных угроз:
   - угрозы 1-го типа связаны с наличием недекларированных возможностей в системном программном обеспечении (ПО), используемом в ИСПДн;
   - угрозы 2-го типа связаны с наличием недекларированных возможностей в прикладном ПО, используемом в ИСПДн;
   - угрозы 3-го типа не связаны с наличием недекларированных возможностей в ПО, используемом в ИСПДн.

Класс ИСПДн по уровням защищенности определяется в соответствии с табл. 1.

Таблица 1

Критерии классификации ИСПДн

Категория ПДн	Угрозы 1 типа	Угрозы 2 типа	Угрозы 3 типа
Специальные ПДн	1 УЗ	1 УЗ* 2 УЗ**	2 УЗ* 3 УЗ**
Биометрические ПДн	1УЗ	2 УЗ	3 УЗ
Общедоступные ПДн	2 УЗ	2 УЗ* 3 УЗ**	4 УЗ
Иные ПДн	1 УЗ	2 УЗ* 3 УЗ**	3 УЗ* 4 УЗ**
Специальные ПДн сотрудников оператора	–	2 УЗ	3 УЗ
Общедоступные ПДн сотрудников оператора	–	3 УЗ	–
Иные ПДн сотрудников оператора	–	3 УЗ	4 УЗ

Примечание. УЗ – уровень защищенности; *если больше 100000 субъектов ПДн; ** если меньше 100000 субъектов ПДн.

Приказ ФСТЭК № 21 от 18.02.2013 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн» устанавливает требования к обеспечению безопасности ПДн, к исполнителям работ по защите ПДн, к проведению оценки эффективности мер, определяет состав и содержание мер по обеспечению безопасности ПДн и требования к применению средств вычислительной техники (СВТ) и средств защиты информации (СЗИ) определенных классов в ИСПДн разных уровней защищенности [7].

Предлагаемая ниже методика разработана с применением подхода, предложенного в отраслевом Стандарте Банка России СТО БР ИББС-1.0-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации» [8]. Целью методики является оценка соответствия защищенности ИСПДн требованиям нормативных документов.

ПОКАЗАТЕЛИ БЕЗОПАСНОСТИ ИСПДН

Для проведения оценки соответствия защищенности ИСПДн требованиям нормативно-правовой базы согласно предлагаемой методике необходимо выделить групповые и частные показатели безопасности ИСПДн.

Групповые показатели безопасности ИСПДн M_i отражают состав и содержание мер по обеспечению безопасности ПДн в соответствии с Приказом ФСТЭК № 21. Поскольку в Приказе выделено 15 критериев обеспечения безопасности, то число групповых показателей M_i равно 15 (табл. 2). Оценки групповых показателей EV_{Mi} используются для получения итоговой оценки EV, отражающей степень выполнения требований нормативно-правовой базы по защите ПДн. Частные показатели безопасности ИСПДн M_{ij} входят в состав групповых показателей, и их оценки EV_{Mij} формируют оценки групповых показателей EV_{Mi}.

Таблица 2

Групповые показатели обеспечения безопасности ИСПДн

M_i	Наименование групповых показателей безопасности ИСПДн
M_1	Обеспечение безопасности ПДн средствами идентификации и аутентификации субъектов и объектов доступа (ИАФ)
M_2	Обеспечение безопасности ПДн средствами управления доступом субъектов доступа к объектам доступа (УПД)
M_3	Обеспечение безопасности ПДн средствами ограничения программной среды (ОПС)
M_4	Обеспечение защиты машинных носителей ПДн (ЗНИ)
M_5	Обеспечение регистрации событий безопасности (РСБ)
M_6	Обеспечение безопасности ПДн средствами антивирусной защиты (АВЗ)
M_7	Обеспечение безопасности ПДн средствами обнаружения вторжений (СОВ)
M_8	Обеспечение контроля (анализа) защищенности ПДн (АНЗ)
M_9	Обеспечение целостности ИСПДн (ОЦЛ)
M_{10}	Обеспечение доступности ПДн (ОДТ)
M_{11}	Обеспечение защиты среды виртуализации (ЗСВ)
M_{12}	Обеспечение защиты технических средств (ЗТС)
M_{13}	Обеспечение защиты ИСПДн, ее средств, систем связи и передачи данных (ЗИС)
M_{14}	Выявление инцидентов и реагирование на них (ИНЦ)
M_{15}	Управление конфигурацией ИСПДн и системы защиты ПДн (УКФ)

Оценивание частных показателей безопасности ИСПДн M_{ij} производится с использованием опросных анкет, учитывающих требования для каждого уровня защищенности ПДн. Фрагмент опросной анкеты представлен в табл. 3. Оценка частных показателей основывается на:

- внутренних документах организации;
- информации, полученной от сотрудников в процессе опроса;
- результатах наблюдений эксперта за деятельностью сотрудников проверяемой организации.

Для каждого из уровней защищенности ПДн частные показатели разделены на два типа:

- частные показатели, отражающие базовые требования по обеспечению безопасности ПДн, выполнение которых обязательно;
- частные показатели, отражающие требования, носящие рекомендательный характер для определенного уровня защищенности ПДн.

Если в результате оценивания частных показателей, выполнение которых обязательно, получен ответ «нет», то оценка EV_{Mij} = 0; если ответ «частично», то EV_{Mij} = 0,5; если ответ «да», то EV_{Mij} = 1.

Если в результате оценивания частных показателей, выполнение которых необязательно, получен ответ «да», то оценка EV_{Mij} = 1; если ответ «нет», то частный показатель определяется как неоцениваемый (н/о) и не учитывается в формировании дальнейших результатов оценки.

МЕТОДИКА РАСЧЕТА ПОКАЗАТЕЛЕЙ БЕЗОПАСНОСТИ ИСПДН

Для каждого группового показателя безопасности ИСПДн определяется оценка EV_{Mi}, соответствующая совокупности оценок, полученных в результате оценивания составляющих частных показателей:

$$EV_{M_i} = \sum EV_{M_{ij}}, i = 1 \div 15, j = 1 \div N_i,$$

где N_i – количество частных показателей безопасности ИСПДн, представляющих групповой показатель M_i.

Оценка EV_{Mi} далее нормируется:

Таблица 3

Фрагмент опросной анкеты

Обозначение частного показателя безопасности ИСПДн	Частный показатель безопасности ИСПДн	Обязательность выполнения для уровней защищенности ПДн				Оценка частного показателя $EV_{M_{ij}}$			
		4	3	2	1	0	0,5	1	н/о
$M_{1.1}$	Выполняется ли идентификация и аутентификация пользователей, являющихся работниками организации?	+	+	+	+				
$M_{1.2}$	Выполняется ли идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных?			+	+				
$M_{1.3}$	Осуществляется ли управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов?	+	+	+	+				
…	…								
Итоговая оценка группового показателя EV_{M_i}									
…	…								
$M_{6.1}$	Реализована ли антивирусная защита?	+	+	+	+				
$M_{6.2}$	Обновляются ли базы данных признаков вредоносных компьютерных программ (вирусов)?	+	+	+	+				
…	…								

$$\overline{EV}_{M_i} = \frac{EV_{M_i}}{EV_{M_i\max}}, i = 1 \div 15,$$

где $\overline{EV}_{M_i}$ – нормированная оценка группового показателя EV_{Mi}; $EV_{Mi\max}$ – максимально возможное значение количественной оценки EV_{Mi}.

Поскольку требования нормативных документов по защите ПДн позволяют операторам ПДн адаптировать систему защиты ПДн к условиям обработки ПДн и используемым техническим средствам, то каждый из групповых показателей EV_{Mi} характеризуется коэффициентом значимости ω_i, значение которого определяется экспертом для каждой конкретной ИСПДн ($0 \le \omega_i \le 1$). Итоговая нормированная оценка группового показателя $EV_{Mi\text{итог}}$ вычисляется по формуле

$$EV_{M_i\text{итог}} = \omega_i * \overline{EV}_{M_i}, i = 1 \div 15.$$

На основании итоговых оценок групповых показателей $EV_{Mi\text{итог}}$ вычисляется оценка EV, отражающая степень выполнения требований нормативно-правовой базы по защите ПДн:

$$EV = \sum EV_{M_i\text{итог}}, i = 1 \div 15.$$

Нормированная оценка $\overline{EV}$ определяется по формуле

$$\overline{EV} = \frac{EV}{EV_{\max}},$$

где $EV_{\max}$ – максимально возможное значение количественной оценки EV. Поскольку максимальное значение каждого из 15-ти групповых показателей равно 1, то $EV_{\max} = 15$.

Значение итоговой оценки соответствия защищенности ИСПДн требованиям нормативно-правовой базы в процентах $EV_{\%}$ вычисляется по формуле:

$$EV_{\%} = \overline{EV} * 100\%.$$

С помощью метода экспертных оценок можно не только оценить степень выполнения отдельных требований по защите ПДн, но и сравнить между собой различные варианты построения СЗПДн. Результаты оценивания $EV_{Mi\text{итог}}$ и $\overline{EV}$ отображаются на графиках, представленных на рис. 1. По оси абсцисс расположены групповые показатели обеспечения безопасности ИСПДн $M_1 \div M_{15}$. Линии 1 и 2 отражают два разных случая построения СЗПДн. Точки на этих линиях соответствуют значениям оценок $EV_{Mi\text{итог}}$. Итоговые оценки $\overline{EV}_1$ и $\overline{EV}_2$ изображены в виде прямых, параллельных оси абсцисс, уровни которых соответствуют итоговым оценкам $\overline{EV}_1$ и $\overline{EV}_2$.

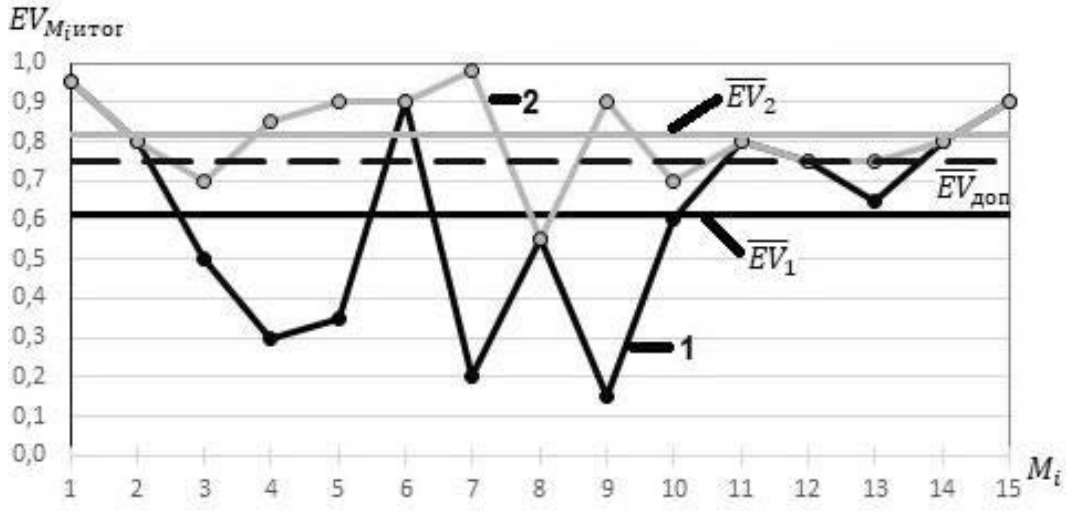

Рис. 1. Графики результатов оценки соответствия защищенности ИСПДн требованиям нормативно-правовой базы

По аналогии со Стандартом Банка России СТО БР ИББС-1.0-2014 можно ввести уровни соответствия защищенности ИСПДн требованиям нормативно-правовой базы:

- оценка $0 \le EV_{\text{норм}} \le 0{,}3$ – нулевой уровень;
- оценка $0{,}3 < EV_{\text{норм}} \le 0{,}5$ – первый уровень;
- оценка $0{,}5 < EV_{\text{норм}} \le 0{,}75$ – второй уровень;
- оценка $0{,}75 < EV_{\text{норм}} < 1$ – трений уровень;
- оценка $EV_{\text{норм}} = 1$ – четвертый уровень.

Рекомендуемыми уровнями соответствия защищенности ИСПДн требованиям нормативно-правовой базы являются уровни не ниже третьего. На рис. 1 в виде пунктирной линии, параллельной оси абсцисс изображено минимально допустимое значение уровня соответствия $\overline{EV}_{\text{доп}} = 0{,}75$.

Представление результатов оценки соответствия защищенности ИСПДн требованиям нормативных документов в виде графиков позволяет наглядно показать состояние защищенности ПДн. Из графиков видно, в какой степени выполняются те или иные меры по обеспечению безопасности ПДн. Данная информация используется, в свою очередь, для формирования рекомендаций по повышению уровня защищенности ИСПДн.

Рассмотрим пример оценки уровня соответствия защищенности ИСПДн требованиям нормативных документов. Пусть в результате оценивая эксперты получили данные представленные графиками 1 и $\overline{EV}_1$ (рис. 1). В данном случае значение $\overline{EV} = 0{,}61$ выходит за рамки допустимого, т.е. необходимо увеличить уровень некоторых наиболее низких показателей M_i и тем самым повысить показатель $\overline{EV}_1$. После внедрения рекомендуемых контрмер получаем графики 2 и $\overline{EV}_2$ (рис. 1). В данном случае $\overline{EV_2} = 0{,}82$, т.е. защищенность ИСПДн соответствует требованиям нормативно-правовой базы.

В качестве дополнительного критерия при оценке эффективности СЗПДн можно использовать критерий (показатель) стоимости реализации (внедрения) мер защиты информации:

$$S = \sum S_{M_i}, i = 1 \div 15,$$

где S_{Mi} – стоимость реализации мер по обеспечению определенного значения группового показателя безопасности M_i.

Возможны оптимальные постановки задачи проектирования СЗПДн:

а) $\overline{EV} \to \max$ при $S \le S_{\text{зад}}$ (заданный бюджет);

б) $S \to \min$ при $\overline{EV} \ge \overline{EV}_{\text{зад}}$ (заданный уровень защищенности ПДн).

Такой подход позволяет наиболее рационально построить СЗПДн, учитывая соотношение стоимости контрмер и допустимого уровня защищенности ИСПДн.

В дальнейшем планируется создание программного обеспечения с использованием предложенного подхода, что позволит автоматизировать основные этапы проведения аудита ИСПДн.

ЗАКЛЮЧЕНИЕ

В статье рассмотрен подход к решению задачи автоматизации аудита ИСПДн с использованием метода экспертных оценок. В ходе исследования решены следующие задачи:

- определена специфика ПДн как объекта защиты;
- рассмотрены существующие требования к аудиту ИСПДн;
- предложена методика оценки уровня соответствия защищенности ИСПДн требованиям нормативных документов: выделены частные и групповые показатели безопасности ИСПДн, предложена методика расчета показателей безопасности ИСПДн и их графическое представление.

Предложенная методика оценки уровня соответствия защищенности ИСПДн требованиям нормативных документов позволяет наглядно показать руководству организации состояние защищенности ПДн, выделяя наиболее слабые места (уязвимости) в системе защиты ПДн.

СПИСОК ЛИТЕРАТУРЫ

1. **О персональных данных**: Федеральный Закон от 27 июля 2006 №152-ФЗ (с изменениями и дополнениями от 29.07.2017) [Электронный ресурс]. URL: http://ivo.garant.ru/#/document/12148567:0 (дата обращения 20.06.2017). **[** *On Personal Data*, (in Russian), Federal law № 152 (with changes from 29.07.2017) [Online]. Available: http://ivo.garant.ru/#/document/12148567:0 **]**

2. **Об аудиторской деятельности**: Федеральный закон от 30 декабря 2008 № 307-ФЗ // Российская газета. 2008. **[** *On audit activity № 307*, (in Russian), Federal law, Russian Gazette, 2008. **]**

3. **Орлов А. И.** Организационно-экономическое моделирование. Экспертные оценки: учебник. М.: Изд-во МГТУ им. Н. Э. Баумана, 2011. 486 с. **[** A. I. Orlov, *Organizational-economic modeling. Expert assessments* (in Russian). M. : BMSTU, 2011. **]**

4. **Гуцыкова С. В.** Метод экспертных оценок. Теория и практика. М.: Институт психологии РАН, 2015. 170 с. **[** S. V. Gutsykova, *Method of expert assessments. Theory and practice* (in Russian). M. : Institute of Psychology of RSA, 2015. **]**

5. Шихалев А. М. Корреляционный анализ. Непараметрические методы: учебно-методическое пособие. Казань.: Казан. ун-т, 2015. 58 с. **[** A. M. Shihalev, *Correlation analysis. Non-parameter methods* (in Russian), Kazan: Kazan University, 2015. **]**

6. **Об утверждении** требований к защите персональных данных при их обработке в информационных системах персональных данных.: Постановление Правительства РФ: [утверждено Постановлением Правительства РФ 2012 г.] // Российская газета. 2012. **[** *On approval of the requirements for personal data protection during their processing in personal data information systems*, (in Russian), Government Regulation, Russian Gazette, 2012. **]**

7. **Об утверждении** состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных. : Приказ : [утвержден ФСТЭК России 2013 г.] // Российская газета. 2013. **[** *On approval of the composition and content of organizational and technical measures to ensure the security of personal data during their processing in the information system of personal data*, (in Russian), Order, Russian Gazette, 2013. **]**

8. **СТО БР ИББС-1.2-2014**. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы российской федерации требованиям СТО БР ИББС-1.2-2014. Москва: 2014. 44 с. **[** *Information security ensure of Banking System Organizations of the Russian Federation. Method for assessing the compliance of organizations information security of the banking system of the Russian Federation with requirements of STO BR IBBS-1.2-2014*, (in Russian), Moscow, 2014. **]**

ОБ АВТОРАХ

САГИТОВА Валентина Владимировна, асп. каф. выч. техники и защ. информации. Дипл. спец. по защ. информации (УГАТУ, 2012). Готовит дис. в обл. аудита информационных систем персональных данных.

ВАСИЛЬЕВ Владимир Иванович, зав. каф. выч. техники и защ. информации. Дипл. инж. по пром. электронике (УАИ, 1970). Д-р техн. наук по сист. анализу и автоматич. управлению (ЦИАМ, 1990). Иссл. в обл. интеллектуальных систем управления и защиты информации.

METADATA

Title: Application of expert estimates method for automation of privacy data information systems audit.

Authors: V. V. Sagitova[1], V. I. Vasilyev[2]

Affiliation: Ufa State Aviation Technical University (UGATU), Russia.

Email:

[1]sagitovavv@mail.ru, [2] vasilyev@ugatu.ac.ru

Language: Russian.

Source: Vestnik UGATU (scientific journal of Ufa State Aviation Technical University), vol. 21, no. 3 (77), pp. 105-112, 2017. ISSN 2225-2789 (Online), ISSN 1992-6502 (Print).

Abstract: The problem of personal data information system audit taking into account the particularity of personal data as a protection object is considered. The overview of basic requirements to personal data security established by laws and regulations of the Federal Service for Technical and Export Control and the Federal Security Service is considered. The approach to solving the problem of audit automatization for personal data information system using the method of expert estimates is offered. A way to solve a problem of audit for personal data information system based on decision making support system with intelligent data analysis technology being involved is considered.

Key words: personal data; audit of information system; method of expert estimates; security level.

About authors:

SAGITOVA, Valentina Vladimirovna, Postgrad. student, Dept. of Computer Engineering and Information Security. Information Security Specialist (USATU, 2012). Prepares diss. on personal data information systems audit.

VASILYEV, Vladimir Ivanovich, Prof., Dept. of Computer Engineering and Information Security. Dipl. Engineer in Industrial Electronics. (USATU, 1970), Dr. of Tech. Sci. (CIAM, 1990). Invest. in intelligent systems of control and information security.