Практический опыт оценки соответствия стандарту БАНКА РОССИИ СТО БР ИББС–1.0–2010

(CNews FORUM 2010, 10 ноября)

Лысенко Юрий

Начальник Управления информационной безопасности

HomeCredit & Finance Bank

Цели внедрения Стандарта для Банка

- Тренд развития угроз безопасности
- Совершенствование СУИБ
- Соответствие бизнес-целям Банка
- Прозрачность процессов управления
- Обнаружение «слабых мест» в защите
- Требования законодательства и регулирующих органов, особенно 152-ФЗ

Какие трудности встретятся!

1. Взаимодействие между подразделениями.
2. Согласование документов, работ.
3. Отсутствие заинтересованности.
4. Отсутствие документированности информационно-технологических процессов. (Для платежных технологических процессов документация есть).
5. Отсутствие схемы потоков персональных данных.
6. Сложность восприятия некоторых вопросов Стандарта, возможность различного толкования вопроса.
7. «Латание дыр» как в части документации, так и программно-техническом обеспечении.
8. Отсутствие четкого алгоритма оценивания частных показателей с учетом оценок уточняющих вопросов по Персональным данным (п. 10.4 Методики оценки, Таблица 7)
9. Отсутствие ПО для автоматизации расчета показателей.

Методические рекомендации АРБ
по выполнению законодательных требований при обработке персональных данных в организациях банковской системы Российской Федерации

- Если организация БС РФ не вводит Стандарты Банка России приказом, то ее деятельность при обработке персональных данных подлежит оценке при осуществлении надзора и контроля уполномоченными государственными органами на соответствие требованиям нормативных документов Регуляторов в области персональных данных, без учета отраслевых особенностей банковской сферы деятельности, отраженных в Комплексе БР ИББС.

ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ
«ХОУМ КРЕДИТ энд ФИНАНС БАНК»

ПРИКАЗ № 869

г. Москва «21» 11.09 2010 г.

О принятии к исполнению комплекса документов БР ИББС и проведении самооценки на соответствие текущего уровня информационной безопасности Банка стандарту Банка России

В целях:

- обеспечения информационной безопасности Банка;
- исполнения требований Федерального закона "О персональных данных" и требований (рекомендаций) Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, Федеральной службы безопасности Российской Федерации и Федеральной службы по техническому и экспортному контролю,

ПРИКАЗЫВАЮ:

1. Директору Департамента защиты бизнеса принять к исполнению и руководствоваться в работе по обеспечению информационной безопасности Банка комплексом документов в области

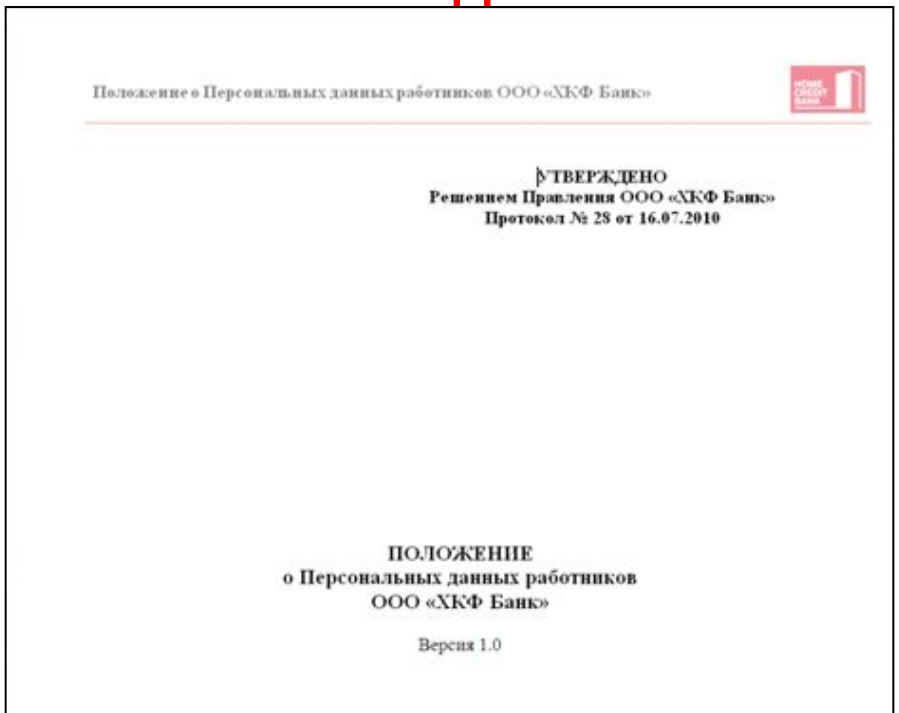
Общий подход к определению требований по обеспечению безопасности персональных данных в ИСПДн

- Выбор требований по обеспечению безопасности персональных данных в информационных системах персональных данных (ИСПДн) осуществляется в зависимости от результатов классификации ИСПДн.
- В соответствии с действующим стандартом СТО БР ИББС-1.0 все ИСПДн организаций БС РФ относятся **к специальным**. ИСПДн организации БС РФ классифицируются на основе категорий обрабатываемых в ИСПДн персональных данных.

- Типовые информационные системы - информационные системы, в которых требуется обеспечение только конфиденциальности персональных данных.
- **Специальные информационные системы** - информационные системы, в которых вне зависимости от необходимости обеспечения конфиденциальности персональных данных требуется обеспечить хотя бы одну из характеристик безопасности персональных данных, отличную от конфиденциальности (защищенность от уничтожения, изменения, блокирования, а также иных несанкционированных действий).
- К специальным информационным системам должны быть отнесены: информационные системы, в которых обрабатываются персональные данные, касающиеся состояния здоровья субъектов персональных данных; информационные системы, в которых предусмотрено принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы.

Общие требования по обработке персональных данных в организации БС РФ

- В организации БС РФ должен быть определен и документально зафиксирован перечень ИСПДн. В перечень ИСПДн должны быть включены как минимум АБС, целью создания и исполь зования которых является обработка персональных данных.
- **АБС, реализующие банковские платежные технологические процессы, не относятся к ИСПДн.**



Положение о Персональных данных работников ООО «ХКФ Банк»

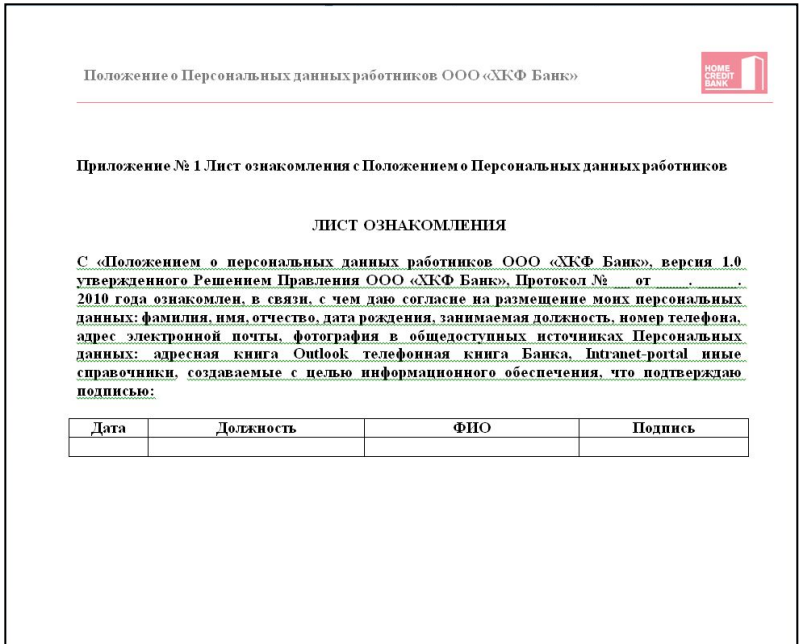
УТВЕРЖДЕНО
Решением Правления ООО «ХКФ Банк»
Протокол № 28 от 16.07.2010

ПОЛОЖЕНИЕ
о Персональных данных работников
ООО «ХКФ Банк»

Версия 1.0

Общие требования по обработке персональных данных в организации БС РФ

- Работники организации БС РФ, осуществляющие обработку персональных данных в ИСПДн, должны быть проинформированы о факте обработки ими персональных дан ных, категориях обрабатываемых персональных данных, а также должны быть ознакомлены под роспись со всей совокупностью требований по обработке и обеспечению безопасности персональных данных в части, касающейся их должностных



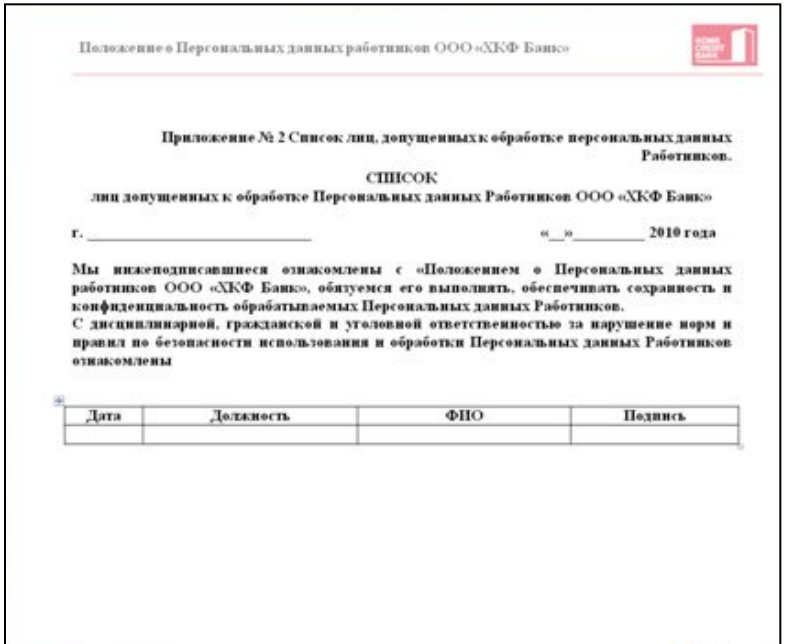
Положение о Персональных данных работников ООО «ХКФ Банк»

Приложение № 1 Лист ознакомления с Положением о Персональных данных работников

ЛИСТ ОЗНАКОМЛЕНИЯ

С «Положением о персональных данных работников ООО «ХКФ Банк», версия 1.0 утвержденного Решением Правления ООО «ХКФ Банк», Протокол № от . . 2010 года ознакомлен, в связи, с чем даю согласие на размещение моих персональных данных: фамилия, имя, отчество, дата рождения, занимаемая должность, номер телефона, адрес электроиной почты, фотография в общедоступных источниках Персональных данных: адресная книга Outlook телефоиная книга Банка, Intranet-portal иные справочники, создаваемые с целью информационного обеспечения, что подтверждаю подписью:

Дата	Должность	ФИО	Подпись



Положение о Персональных данных работников ООО «ХКФ Банк»

Приложение № 2 Список лиц, допущенных к обработке персональных данных Работников.

СПИСОК
лиц допущенных к обработке Персональных данных Работников ООО «ХКФ Банк»

г. _____ «__»_____ 2010 года

Мы нижеподписавшиеся ознакомлены с «Положением о Персональных данных работников ООО «ХКФ Банк», обязуемся его выполнять, обеспечивать сохранность и конфиденциальность обрабатываемых Персональных данных Работников.
С дисциплинарной, гражданской и уголовной ответственностью за нарушение норм и правил по безопасности использования и обработки Персональных данных Работников ознакомлены

Дата	Должность	ФИО	Подпись

Автоматизированные системы, в которых обрабатываются персональные данные, но целью работы которых не является обработка персональных данных, включаются в перечень систем, обрабатывающих персональные данные, но не классифицируются как ИСПДн.

Схема потоков персональных данных

Схема потоков персональных данных в ООО «ХКФ Банк»

1. Потоки персональных данных работников

Потоки персональных данных работников ООО «ХКФ Банк» представлены на рисунке 1.

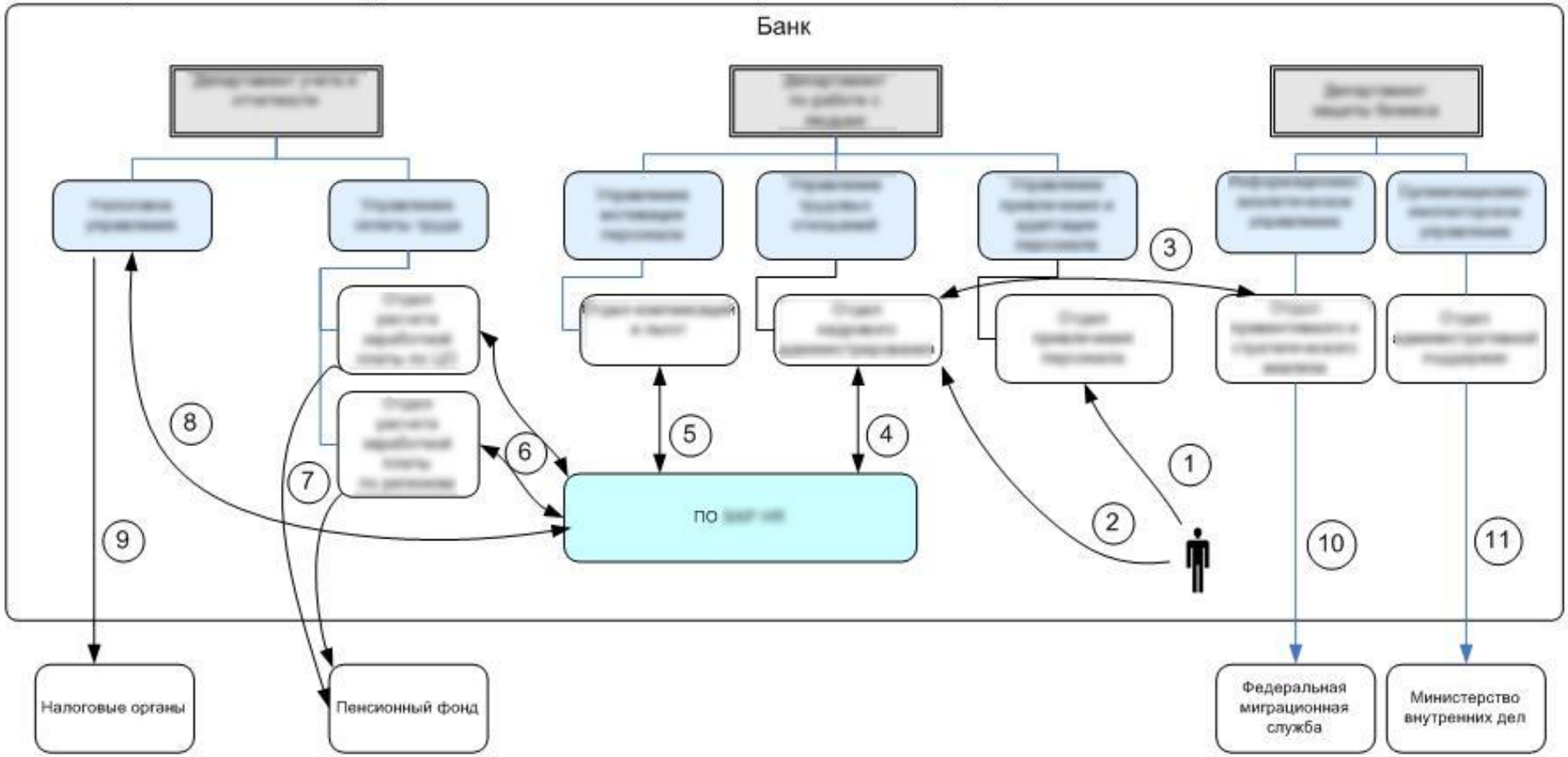


Рисунок 1 – Потоки персональных данных работников Банка

На рисунке 1 обозначены следующие информационные потоки:

1) Получение резюме
2) Передача документов для оформления, заполнение анкет

STOAuditor

Файл Отчет

M1 0,69	M2 0,33	M3 0,62	M4 0,55	M5 0,75	M6 1	M7 0,81	M8 0,48	M9 0	M10 1	M11 0,77	M12 0,89	M13 0,12	M14 0,27	M15 0,87	M16 0,4	M17 0,51	M18 0,32	M19 0,67	M20 0,38	M21 0,47	M22 0,89	M23 0,81
M24 0,63	M25 0,49	M26 0,67	M27 0,74	M28 0,94	M29 0,4	M30 0,49	M31 0,52	M32 0,87	M33 0,49	M34 1	ПДн	Результаты										

☐ Учитывать ПДн

Групповой показатель M1 «Обеспечение информационной безопасности при назначении и распределении ролей и обеспечении доверия к персоналу»

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	0	0,25	0,5	0,75	1	н/о	Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
M1.1	Определены ли в документах организации роли ее работников?	Обязательный					X		0,0678	0,0678
M1.2	Формируются ли роли, связанные с выполнением деятельности по обеспечению ИБ, на основании требований разделов 7 и 8 стандарта СТО БР ИББС-1.0?	Обязательный		X					0,034	0,0085
M1.3	Персонифицированы ли роли в организации с установлением ответственности за их выполнение?	Обязательный					X		0,0586	0,0586
M1.4	Зафиксирована ли документально в должностных инструкциях ответственность за выполнение ролей?	Обязательный					X		0,0538	0,0538
M1.5	Отсутствуют ли в организации роли, совмещающие функции разработки и сопровождения системы/ПО?	Рекомендуемый					X		0,0609	0,0609
M1.6	Отсутствуют ли в организации роли, совмещающие функции разработки и эксплуатации системы/ПО?	Рекомендуемый						X	0	н/о
M1.7	Отсутствуют ли в организации роли, совмещающие функции сопровождения и эксплуатации?	Рекомендуемый					X		0,0609	0,0609
M1.8	Отсутствуют ли в организации роли, совмещающие функции администратора системы и администратора информационной безопасности?	Рекомендуемый					X		0,0772	0,0772
M1.9	Отсутствуют ли в организации роли, совмещающие функции по выполнению операций в системе и контроля их выполнения?	Рекомендуемый					X		0,0772	0,0772
M1.10	Определены ли документально в организации и выполняются ли процедуры контроля деятельности работников, обладающих совокупностью полномочий (ролями), позволяющих получить контроль над защищаемым информационным активом организации?	Обязательный	X						0,1169	0
M1.11	Определены ли в документах организации процедуры приема на работу, влияющую на обеспечение ИБ, включающие: - проверку подлинности предоставленных документов, заявляемой квалификации, точности и полноты биографических навыков; - проверку в части профессиональных навыков и оценку профессиональной пригодности?	Обязательный					X		0,0599	0,0599
M1.12	Предусматривают ли указанные в частном показателе M1.11 процедуры документальную фиксацию результатов проводимых проверок?	Обязательный		X					0,0433	0,010825
M1.13	Определены ли в документах организации процедуры регулярной проверки в части профессиональных навыков и оценки профессиональной пригодности работников?	Рекомендуемый					X		0,0353	0,0353
M1.14	Предусматривают ли указанные в частном показателе M1.13 процедуры документальную фиксацию результатов проводимых проверок?	Рекомендуемый					X		0,0353	0,0353
M1.15	Определены ли в документах организации процедуры внеплановой проверки работников при выявлении фактов их нештатного поведения, участия в инцидентах ИБ или подозрений в таком поведении или участии?	Рекомендуемый						X	0	н/о
M1.16	Предусматривают ли указанные в частном показателе M1.15 процедуры документальную фиксацию результатов проводимых проверок?	Рекомендуемый						X	0	н/о
M1.17	Обязаны ли все работники организации давать письменные обязательства о соблюдении конфиденциальности, приверженности правилам корпоративной этики, включая требования по недопущению конфликта интересов?	Обязательный					X		0,0447	0,0447
M1.18	Регламентируются ли положениями, включенными в договора (соглашения) с внешними организациями и клиентами, требования по ИБ?	Обязательный		X					0,0524	0,0131
M1.19	Определены ли в трудовых контрактах (соглашениях, договорах) и(или) должностных инструкциях обязанности персонала по выполнению требований ИБ?	Обязательный		X					0,0679	0,016975
M1.20	Приравнивается ли невыполнение работниками организации требований ИБ к невыполнению должностных обязанностей и приводит ли, как минимум, к дисциплинарной ответственности?	Обязательный		X					0,0539	0,013475

$EV_{M1} = 0,69$

$EV1 = 0$

$EV2 = 0,5824$

$EV3 = 0,6729$

$R = 0$

$EV_{БИТП} = 0,7$

$EV_{БПТП} = 0,6786$

$EV_{ООПД} = 0$

$EV^{1}_{ОЗПД} = 0,7367$

$EV^{2}_{ОЗПД} = 0,7743$

STOAuditor

Файл Отчет

M1 0,69	M2 0,33	M3 0,62	M4 0,55	M5 0,75	M6 1	M7 0,81	M8 0,48	**M9 0**	M10 1	M11 0,77	M12 0,89	M13 0,12	M14 0,27	M15 0,87	M16 0,4	M17 0,51	M18 0,32	M19 0,67	M20 0,38	M21 0,47	M22 0,89	M23 0,81
M24 0,63	M25 0,49	M26 0,67	M27 0,74	M28 0,94	M29 0,4	M30 0,49	M31 0,52	M32 0,87	M33 0,49	M34 1	ПДн	Результаты										

☐ Учитывать ПДн

Групповой показатель M9 «Общие требования по обработке персональных данных в организации БС РФ»

$EV_{M9} = 0$
$EV1 = 0$
$EV2 = 0,5824$
$EV3 = 0,6729$
$R = 0$
$EV_{БИТП} = 0,7$
$EV_{БПТП} = 0,6786$
$EV_{ООПД} = 0$
$EV^{1}_{ОЗПД} = 0,7367$
$EV^{2}_{ОЗПД} = 0,7743$

Обозначение частного показателя ИБ	Частный показатель ИБ	Обязательность выполнения	0	0,25	0,5	0,75	1	н/о	Коэффициент значимости частного показателя ИБ	Вычисленное значение показателя ИБ
M9.1	Определены ли в организации, зафиксированы ли документально и утверждены ли руководством организации цели обработки персональных данных?	Обязательный					X		н/о	1
M9.2	Определена ли в организации необходимость уведомления Уполномоченного органа по защите прав субъектов персональных данных об обработке персональных данных?	Обязательный					X		н/о	1
M9.3	Определены ли в организации для каждой цели обработки персональных данных, зафиксированы ли документально и утверждены ли руководством организации: - объем и содержание персональных данных; - сроки обработки, в том числе сроки хранения персональных данных; - необходимость получения согласия субъектов персональных данных?	Обязательный					X		н/о	1
M9.4	Проводится ли в организации классификация персональных данных в соответствии со степенью тяжести последствий потери свойств безопасности персональных данных для субъекта персональных данных?	Рекомендуемый					X		н/о	1
M9.5	Выделяются ли при проведении классификации персональных данных следующие категории: - персональные данные, отнесенные в соответствии с Федеральным законом «О персональных данных» к специальным категориям персональных данных; - персональные данные, отнесенные в соответствии с Федеральным законом «О персональных данных» к биометрическим персональным данным; - персональные данные, которые не могут быть отнесены к специальным категориям персональных данных, к биометрическим персональным данным, к общедоступным или обезличенным персональным данным - персональные данные, отнесенные в соответствии с Федеральным законом «О персональных данных» к общедоступным или обезличенным персональным данным?	Рекомендуемый					X		н/о	1
M9.6	Осуществляется ли организацией передача персональных данных третьему лицу только на основании договора, существенным условием которого является обязанность обеспечения третьим лицом безопасности персональных данных при их обработке? Примечание: если иное установлено законодательством Российской Федерации, показателю присваивается оценка «н/о».	Обязательный					X		н/о	1
M9.7	Прекращается ли в организации обработка персональных данных и уничтожаются ли собранные персональные данные в следующих случаях и в сроки, установленные законодательством РФ: - по достижении целей обработки или при утрате необходимости в их достижении; - по требованию субъекта персональных данных или Уполномоченного органа по защите прав субъектов персональных данных - если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки; - при отзыве субъектом персональных данных согласия на обработку своих персональных данных, если такое согласие требуется в соответствии с законодательством РФ? Примечание: если иное установлено законодательством РФ, показателю присваивается оценка «н/о».	Обязательный					X		н/о	1
M9.8	Определен ли в организации и зафиксирован ли документально порядок уничтожения персональных данных (в том числе и материальных носителей персональных данных)?	Обязательный	X						н/о	0
M9.9	Определен ли в организации и зафиксирован ли документально порядок обработки обращений субъектов (или их законных представителей) по вопросам обработки их персональных данных?	Обязательный					X		н/о	1
M9.10	Определен ли в организации и зафиксирован ли документально порядок действий в случае запросов Уполномоченного органа по защите прав субъектов персональных данных или иных надзорных органов, осуществляющих контроль и надзор в области персональных данных?	Обязательный					X		н/о	1
M9.11	Определен ли в организации и зафиксирован ли документально подход к отнесению АБС к информационным системам персональных данных (ИСПДн)?	Обязательный					X		н/о	1
M9.12	Определен ли в организации и зафиксирован ли документально перечень ИСПДн, в который включены, как минимум, АБС, целью создания и использования которых является обработка персональных данных и не включены АБС, реализующие банковские платежные	Обязательный					X		н/о	1

STOAuditor

Файл Отчет

М1 0,69	М2 0,33	М3 0,62	М4 0,55	М5 0,75	М6 1	М7 0,81	М8 0,48	М9 0	М10 1	М11 0,77	М12 0,89	М13 0,12	М14 0,27	М15 0,87	М16 0,4	М17 0,51	М18 0,32	М19 0,67	М20 0,38	М21 0,47	М22 0,89	М23 0,81
М24 0,63	М25 0,49	М26 0,67	М27 0,74	М28 0,94	М29 0,4	М30 0,49	М31 0,52	М32 0,87	М33 0,49	М34 1	ПДн	Результаты										

Учитывать ПДн

Оценка степени выполнения требований СТО БР ИББС-1.0, регламентирующих защиту персональных данных в ИСПДн

$EV_{М9} = 0$
$EV1 = 0$
$EV2 = 0,5824$
$EV3 = 0,6729$
$R = 0$
$EV_{БИТП} = 0,7$
$EV_{БПТП} = 0,6786$
$EV_{ООПД} = 0$
$EV^{1}_{ОЗПД} = 0,7367$
$EV^{2}_{ОЗПД} = 0,7743$

Тип ИСПДн: ИСПДн-И

- ИСПДн-С
- ИСПДн-Б
- ИСПДн-И
- ИСПДн-Д

Номер	Пу... ИБ	...ИББС-1.2	Уточняющий вопрос	Не выполняется	Выполняется не в полном объеме	Выполняется в полном объеме
1	5.2	М10.2, М10.3,М12.2, М12.3, М12.4	Отнесена ли каждая информационная система персональных данных (ИСПДн) организации к одному из следующих классов - ИСПДн-С, ИСПДн-Б, ИСПДн-И, ИСПДн-Д[1]?			X
2	6.1.1	М2.1, М2.2, М2.3, М2.4	Реализуются ли требования (организуется ли выполнение требований) по обеспечению безопасности персональных данных в ИСПДн комплексом организационных, технологических, технических и программных мер, средств и механизмов защиты информации? Осуществляется ли реализация требований по обеспечению безопасности персональных данных структурным подразделением или должностным лицом (работником) организации, ответственным за обеспечение безопасности персональных данных, либо на договорной основе организацией - контрагентом организации, имеющей лицензию на деятельность по технической защите конфиденциальной информации? Допускается возложение ответственности за обеспечение безопасности персональных данных на существующее в организации подразделение (например, на службу ИБ). Осуществляется ли реализация требований по обеспечению безопасности ПДн по согласованию и под контролем службы ИБ организации?			X
3	6.1.2	М2.1, М2.2, М2.3, М2.5, М2.6, М8.3, М8.5, М15.6, М15.7	Включает ли создание ИСПДн организации разработку и согласование (утверждение) предусмотренной техническим заданием организационно-распорядительной, проектной и эксплуатационной документации на создаваемую систему (в документации должны быть отражены вопросы обеспечения безопасности обрабатываемых персональных данных)? Осуществляется ли разработка концепций, технических заданий, проектирование, создание и тестирование, приемка и ввод в действие ИСПДн по согласованию и под контролем структурного подразделения или должностного лица (работника) организации, ответственным за обеспечение безопасности персональных данных, и службы ИБ организации?	X		
4	6.1.3	М4.1, М4.5	Защищены ли от воздействий вредоносного кода все информационные активы, принадлежащие ИСПДн организации? Определены ли в организации и зафиксированы ли документально требования по обеспечению безопасности персональных данных средствами антивирусной защиты и порядок проведения контроля реализации этих требований в соответствии с требованиями пункта 7.5 СТО БР ИББС-1.0?		X	
5	6.1.4	М3.5, М3.6, М3.7, М3.8	Определена ли в организации система контроля доступа, позволяющая осуществлять контроль доступа к коммуникационным портам, устройствам ввода-вывода информации, съемным машинным носителям и внешним накопителям информации ИСПДн?	X		
6	6.1.5	М1.1, М1.3, М1.4, М1.19, М16.1, М29.1	Действуют ли работники, осуществляющие обработку персональных данных в ИСПДн, в соответствии с инструкцией (руководством, регламентом и т.п.), входящей в состав эксплуатационной документации на ИСПДн, и соблюдают ли работники требования документов организации по обеспечению ИБ?			X
7	6.1.6	М1.1, М1.3, М1.4, М8.4, М8.5, М15.6, М15.7, М15.8	Возложены ли приказами (распоряжениями) обязанности по администрированию средств защиты и механизмов защиты, реализующих требования по обеспечению ИБ ИСПДн организации, на администраторов информационной безопасности ИСПДн?	X		
8	6.1.7	М1.1, М1.3, М1.4, М1.13, М1.14, М2.5, М2.6, М2.11, М2.12, М3.2, М3.11, М3.12, М3.14, М3.15, М3.16, М3.17, М3.2, М3.11, М3.12, М3.14, М3.15, М3.16, М3.17, М8.5, М8.12, М15.6,	Определен ли порядок действий администратора информационной безопасности ИСПДн и персонала, занятых в процессе обработки персональных данных, инструкциями (руководствами), которые готовятся разработчиком ИСПДн в составе эксплуатационной документации на ИСПДн? Выполняются ли следующие требования к таким инструкциям (руководствам): - устанавливают требования к квалификации администратора информационной безопасности и персонала в области защиты информации, а также актуальный перечень защищаемых объектов и правила его обновления; - содержат в полном объеме актуальные (по времени) данные о полномочиях пользователей; - содержат данные о технологии обработки информации в объеме, необходимом для администратора информационной безопасности; - содержат параметры конфигурации средств защиты и механизмов защиты информации от НСД, используемых в зоне ответственности администратора информационной безопасности, а также определяют порядок и			X

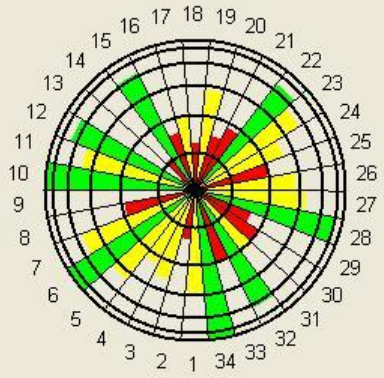
STOAuditor

Файл Отчет

M1 0,69	M2 0,33	M3 0,62	M4 0,55	M5 0,75	M6 1	M7 0,81	M8 0,48	M9 0	M10 1	M11 0,77	M12 0,89	M13 0,12	M14 0,27	M15 0,87	M16 0,4	M17 0,51	M18 0,32	M19 0,67	M20 0,38	M21 0,47	M22 0,89	M23 0,81
M24 0,63	M25 0,49	M26 0,67	M27 0,74	M28 0,94	M29 0,4	M30 0,49	M31 0,52	M32 0,87	M33 0,49	M34 1	ПДн	Результаты										

☐ Учитывать ПДн

Результаты самооценки



Оценка степени выполнения требований СТО БР ИББС-1.0 по направлению "текущий уровень ИБ организации": 0

Оценка степени выполнения требований СТО БР ИББС-1.0 по направлению "менеджмент ИБ организации": 0,5824

Оценка степени выполнения требований СТО БР ИББС-1.0 по направлению "уровень осознания ИБ организации": 0,6729

Оценка степени выполнения требований СТО БР ИББС-1.0, регламентирующих обработку персональных данных: 0

Оценка степени выполнения требований СТО БР ИББС-1.0, регламентирующих защиту персональных данных в информационных системах персональных данных, без учета оценки степени выполнения требований СТО БР ИББС-1.0 по обеспечению информационной безопасности при использовании средств криптографической защиты информации: 0,7367

Оценка степени выполнения требований СТО БР ИББС-1.0, регламентирующих защиту персональных данных в информационных системах персональных данных, с учетом оценки степени выполнения требований СТО БР ИББС-1.0 по обеспечению информационной безопасности при использовании средств криптографической защиты информации: 0,7743

Оценка степени выполнения требований СТО БР ИББС-1.0, регламентирующих банковский информационный технологический процесс: 0,7

Оценка степени выполнения требований СТО БР ИББС-1.0, регламентирующих банковский платежный технологический процесс: 0,6786

Итоговый уровень соответствия ИБ организации БС РФ требованиям СТО БР ИББС-1.0: 0

$EV_{M9} = 0$

$EV1 = 0$

$EV2 = 0,5824$

$EV3 = 0,6729$

$R = 0$

$EV_{БИТП} = 0,7$

$EV_{БПТП} = 0,6786$

$EV_{ООПД} = 0$

$EV^{1}_{ОЗПД} = 0,7367$

$EV^{2}_{ОЗПД} = 0,7743$

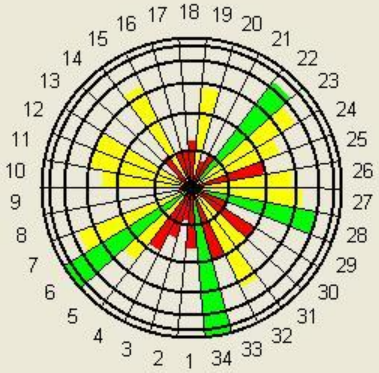
STOAuditor

Файл Отчет

M1 0,41	M2 0,22	M3 0,35	M4 0,47	M5 0,61	M6 1	M7 0,81	M8 0,1	M9 0	M10 0,6	M11 0,7	M12 0,71	M13 0,12	M14 0,27	M15 0,76	M16 0,26	M17 0,24	M18 0,32	M19 0,67	M20 0,19	M21 0,26	M22 0,89	M23 0,81
M24 0,63	M25 0,49	M26 0,67	M27 0,74	M28 0,85	M29 0,25	M30 0,49	M31 0,52	M32 0,74	M33 0,49	M34 1	ПДн	Результаты										

☑ Учитывать ПДн

Результаты самооценки



Оценка степени выполнения требований СТО БР ИББС-1.0 по направлению "текущий уровень ИБ организации": 0

Оценка степени выполнения требований СТО БР ИББС-1.0 по направлению "менеджмент ИБ организации": 0,5135

Оценка степени выполнения требований СТО БР ИББС-1.0 по направлению "уровень осознания ИБ организации": 0,6214

Оценка степени выполнения требований СТО БР ИББС-1.0, регламентирующих обработку персональных данных: 0

Оценка степени выполнения требований СТО БР ИББС-1.0, регламентирующих защиту персональных данных в информационных системах персональных данных, без учета оценки степени выполнения требований СТО БР ИББС-1.0 по обеспечению информационной безопасности при использовании средств криптографической защиты информации: 0,46

Оценка степени выполнения требований СТО БР ИББС-1.0, регламентирующих защиту персональных данных в информационных системах персональных данных, с учетом оцен□ки степени выполнения требований СТО БР ИББС-1.0 по обеспечению информационной безо□пасности при использовании средств криптографической защиты информации: 0,5371

Оценка степени выполнения требований СТО БР ИББС-1.0, регламентирующих банковский информационный технологический процесс: 0,4657

Оценка степени выполнения требований СТО БР ИББС-1.0, регламентирующих банковский платежный технологический процесс: 0,5529

Итоговый уровень соответствия ИБ организации БС РФ требованиям СТО БР ИББС-1.0: 0

$EV_{M9} = 0$

EV1 = 0

EV2 = 0,5135

EV3 = 0,6214

R = 0

$EV_{битп} = 0,4657$

$EV_{бптп} = 0,5529$

$EV_{оопд} = 0$

$EV^{1}_{озпд} = 0,46$

$EV^{2}_{озпд} = 0,5371$

Какие трудности встретятся!

1. Взаимодействие между подразделениями.
2. Согласование документов, работ.
3. Отсутствие заинтересованности.
4. Отсутствие документированности информационно-технологических процессов. (Для платежных технологических процессов документация есть).
5. Отсутствие схемы потоков персональных данных.
6. Сложность восприятия некоторых вопросов Стандарта, возможность различного толкования вопроса.
7. «Латание дыр» как в части документации, так и программно-техническом обеспечении.
8. Отсутствие четкого алгоритма оценивания частных показателей с учетом оценок уточняющих вопросов по Персональным данным (п. 10.4 Методики оценки, Таблица 7)
9. Отсутствие ПО для автоматизации расчета показателей.