Нормативные акты по информационной безопасности в банковской сфере

Блок 2. Международные обязательства

Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных

Блок 1. Базовые документы

Конституция РФ
Ст.23
1. Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени.
2. Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения.
Ст.24
1. Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются.
Ст.29
4. Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Перечень сведений, составляющих государственную тайну, определяется федеральным законом.
Ст.17 ч.3
Осуществление прав и свобод человека и гражданина не должно нарушать права и свободы других лиц.

Доктрина информационной безопасности РФ

Стратегия развития информационного общества в РФ от 7 февраля 2008 г. N Пр-212

Блок 3. Кодексы

Гражданский кодекс РФ
Ст. 857 Банковская тайна
Ст.160 Письменная форма сделки
4 Часть (в части прав на результаты интеллектуальной деятельности и средства индивидуализации)
Главы 9, 10, 23, 24, 49, 50, 77

Таможенный кодекс РФ
Статья 10 Отношение к информации, полученной таможенными органами

Трудовой кодекс РФ
Статья 81. Расторжение трудового договора по инициативе работодателя
Глава 14 Защита персональных данных работника

Семейный кодекс РФ
Статья 139 Тайна усыновления ребенка

Налоговый кодекс РФ
Статья 102. Налоговая тайна

Уголовный кодекс РФ
Статья 137. Нарушение неприкосновенности частной жизни
Статья 138. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений
Статья 140. Отказ в предоставлении гражданину информации
Статья 146. Нарушение авторских и смежных прав
Статья 171. Незаконное предпринимательство
Статья 183. Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну
Статья 272. Неправомерный доступ к компьютерной информации
Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ
Статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети

КоАП РФ
Статья 5.27 Нарушение законодательства о труде и об охране труда
Статья 13.11 Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных)
Статья 13.12 Нарушение правил защиты информации
Статья 19.5 Невыполнение в срок законного предписания (постановления, представления, решения) органа (должностного лица), осуществляющего государственный надзор (контроль)
Статья 19.20 Осуществление деятельности, не связанной с извлечением прибыли, без специального разрешения (лицензии)

Блок 4. Федеральные законы

Блок 4.1. Законы регулирующие отдельные аспекты нескольких видов деятельности

Федеральный закон «О лицензировании отдельных видов деятельности»
Федеральный закон «О техническом регулировании»
Закон РСФСР «О конкуренции и ограничении монополистической деятельности на товарных рынках»
Федеральный закон «Об обязательном экземпляре документов» (в части определения документа, ст.1)

Блок 4.2. Законы регулирующие отдельные виды деятельности

Федеральный закон "О Центральном банке Российской Федерации (Банке России)"
Федеральный закон "О банках и банковской деятельности"
Федеральный закон "О страховании вкладов физических лиц в банках Российской Федерации"
Федеральный закон «Об архивном деле в Российской Федерации»
Федеральный закон «Об адвокатской деятельности и адвокатуре в Российской Федерации»
Закон Российской Федерации «Об организации страхового дела в Российской Федерации»
Федеральный закон «О бухгалтерском учете»
Федеральный закон «Об акционерных обществах»
Федеральный закон «О рынке ценных бумаг»
Федеральный закон «Об инвестиционных фондах»
Федеральный закон «Об аудиторской деятельности»
Закон Российской Федерации «О средствах массовой информации»
Федеральный закон "О несостоятельности (банкротстве) кредитных организаций"
Федеральный закон"О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма"
Федеральный закон "О выплатах Банка России по вкладам физических лиц в признанных банкротами банках, не участвующих в системе обязательного страхования вкладов физических лиц в банках Российской Федерации"
Федеральный закон "О валютном регулировании и валютном контроле"
Федеральный закон "О кредитных историях"

Блок 4.3. Законы о деятельности органов государственной власти

Закон Российской Федерации «О безопасности»
Федеральный закон «О системе государственной службы Российской Федерации»
Федеральный закон «О государственной гражданской службе Российской Федерации»
Федеральный закон «О судебных приставах»
Федеральный закон «Об органах федеральной службы безопасности в Российской Федерации»
Федеральный закон «О внешней разведке»
Федеральный закон «О государственной охране»
Федеральный закон «Об оперативно-розыскной деятельности»
Федеральный закон «О порядке освещения деятельности органов государственной власти в государственных средствах массовой информации»
Федеральный закон «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера»
Федеральный закон «Об экспортном контроле»
Федеральный закон «О военно-техническом сотрудничестве Российской Федерации с иностранными государствами»
Федеральный закон «О порядке выезда из Российской Федерации и въезда в Российскую Федерацию»

Блок 4.4. Законы непосредственно касающиеся ИБ

149-ФЗ Об информации, информационных технологиях и о защите информации

1-ФЗ Об электронной цифровой подписи (Об электронной подписи)

152-ФЗ О персональных данных

160-ФЗ О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных

98-ФЗ О коммерческой тайне

Блок 5. Постановления Правительства и Указы Президента

Указ Президента РФ № 188 «Об утверждении Перечня сведений конфиденциального характера»

Постановление правительства № 781 «Об утверждении Положения об обеспечении безопасности ПДн при их обработке в ИСПДн»

Постановление Правительства № 687 «Об утверждении Положения об особенностях обработки ПДн, осуществляемой без использования средств автоматизации»

Постановление Правительства N 512 «Об утверждении требований к материальным носителям биометрических ПДн и технологиям хранения таких данных вне ИСПДн»

Постановление Правительства № 608 «О сертификации средств защиты информации»

Блок 6. Другие Указы Президента

Указ Президента РФ № 537 «О стратегии национальной безопасности Российской Федерации до 2020 года»
Указ Президента РФ № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»
Указ Президента РФ № 320 «О Федеральной службе по надзору в сфере массовых коммуникаций, связи и охраны культурного наследия»
Указ Президента РФ № 468 «О Комиссии по экспортному контролю Российской Федерации»
Указ Президента РФ № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю»
Указ Президента РФ № 1013 «Вопросы Федеральной службы охраны Российской Федерации»
Указ Президента РФ № 580 «Об утверждении списка товаров и технологий двойного назначения, которые могут быть использованы при создании вооружений и военной техники и в отношении которых осуществляется экспортный контроль»
Указ Президента РФ № 314 «О системе и структуре федеральных органов исполнительной власти»
Указ Президента РФ № 960 «Вопросы Федеральной службы безопасности Российской Федерации»
Указ Президента РФ № 96 «О Комиссии по экспортному контролю Российской Федерации»
Указ Президента РФ № 188 «Об утверждении Перечня сведений конфиденциального характера»
Указ Президента РФ № 334 «О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации»
Указ Президента РФ № 170 «Об основах государственной политики в сфере информатизации»
Указ Президента РФ № 2334 «О дополнительных гарантиях прав граждан на информацию»

Блок 7. Другие Постановления Правительства

Постановление Правительства № 228 «О федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций»
Постановление Правительства № 691 «Об утверждении Положения о лицензировании внешнеэкономических операций с товарами, информацией, работами, услугами, результатами интеллектуальной деятельности (правами на них), в отношении которых установлен экспортный контроль»
Постановление Правительства № 418 «О Министерстве связи и массовых коммуникаций Российской Федерации»
Постановление Правительства № 957 «Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами»
Постановление Правительства № 931 «О некоторых мерах по обеспечению информационного взаимодействия государственных органов и органов местного самоуправления при оказании государственных услуг гражданам и организациям»
Постановление Правительства № 758 «О государственной аккредитации организаций, осуществляющих деятельность в области информационных технологий»
Постановление Правительства № 354 «Об утверждении Положения о Федеральной службе по надзору в сфере массовых коммуникаций, связи и охраны культурного наследия»
Постановление Правительства № 353 «Вопросы Федеральной службе по надзору в сфере массовых коммуникаций, связи и охраны культурного наследия»
Постановление Правительства № 532 «О лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации»
Постановление Правительства № 504 «О лицензировании деятельности по технической защите конфиденциальной информации»
Постановление Правительства № 45 «Об организации лицензирования отдельных видов деятельности»
Постановление Правительства № 766 «Об утверждении перечня продукции, подлежащей декларированию соответствия, порядка принятия декларации о соответствии и ее регистрации»
Постановление Правительства № 770 «Об утверждении Положения о лицензировании деятельности физических и юридических лиц, не уполномоченных на осуществление оперативно-розыскной деятельности, связанной с разработкой, производством, реализацией, приобретением в целях продажи, ввоза в Российскую Федерацию и вывоза за ее пределы специальных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации и Перечня видов специальных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации в процессе осуществления оперативно-розыскной деятельности»
Постановление Правительства № 163 «Об аккредитации органов по сертификации и испытательных лабораторий (центров), выполняющих работы по подтверждению соответствия»
Постановление Правительства РФ N 455 «О внесении изменений в Положение об аккредитации органов по сертификации и испытательных лабораторий (центров), выполняющих работы по подтверждению соответствия»
Постановление Правительства № 330 утверждено «Положение об особенностях оценки соответствия продукции (работ, услуг), используемой в целях защиты сведений, отнесенных к охраняемой в соответствии с законодательством РФ информации ограниченного доступа, не содержащей сведения, составляющие гостайну»
Постановление Правительства № 532 «Об утверждении перечня средств связи, подлежащих обязательной сертификации»

Блок 8. Документы регуляторов по ПДн

Документы ФСТЭК | Документы ФСБ | Документы Роскомнадзора

Приказ 55/86/20
Порядок проведения классификации ИСПДн

Методика определения актуальных угроз безопасности (ПДн)

Базовая модель угроз безопасности ПДн при их обработке в ИСПДн

Приказ №58 О методах и способах защиты информации в ИСПДн

Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих ГТ в случае их использования для обеспечения безопасности ПДн при их обработке в ИСПДн

Методические рекомендации по обеспечению с помощью криптосредств безопасности ПДн при их обработке в ИСПДн с использованием средств автоматизации.

Типовой регламент №149/7/2/6-1173 проведения в пределах полномочий мероприятий по контролю (надзору) за выполнением требований, установленных Правительством РФ, к обеспечению безопасности ПДн при их обработке в ИСПДн

Приказ № 630 «Административный регламент проведения проверок Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций при осуществлении федерального государственного контроля (надзора) за соответствием обработки персональных данных требованиям законодательства РФ в области персональных данных»

Приказ № 08 «Об утверждении образца формы уведомления об обработке персональных данных»

Блок 9. Другие ведомственные документы

Приказ Минкомсвязи России №104 «Об утверждении Требований по обеспечению целостности, устойчивости функционирования и безопасности информационных систем общего пользования»
Приказ ФСБ России №286 «Об утверждении Административного регламента Федеральной службы безопасности Российской федерации по исполнению государственной функции по лицензированию разработки, производства шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем»
Приказ ФСБ России №123 «Об утверждении Административного регламента Федеральной службы безопасности Российской Федерации по исполнению государственной функции по лицензированию деятельности по разработке и (или) производству средств защиты конфиденциальной информации»
Приказ ФСБ России №106 «Об утверждении Административного регламента Федеральной службы безопасности Российской Федерации по исполнению государственной функции по лицензированию деятельности по распространению шифровальных (криптографических) средств»
Приказ ФСБ России №105 «Об утверждении Административного регламента Федеральной службы безопасности Российской Федерации по исполнению государственной функции по лицензированию деятельности по техническому обслуживанию шифровальных (криптографических) средств»
Приказ ФСБ России №104 «Об утверждении Административного регламента Федеральной службы безопасности Российской Федерации по исполнению государственной функции по лицензированию деятельности по предоставлению услуг в области шифрования информации»
Приказ Минкомсвязи России г. №32 «Об утверждении Положения об общероссийском государственном информационном центре»
Положение ПКЗ-2005 «Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации»
Приложение к Приказу ФАПСИ № 152 «Инструкция об организации и обеспечении хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»

Блок 10. Документы ЦБ

Блок 10.1. Положения ЦБ

Положение № 2-П «О безналичных расчетах в РФ»

Положение № 302-П «О правилах ведения бухгалтерского учета в кредитных организациях, расположенных на территории РФ»

Положение № 36-П «О межрегиональных электронных расчетах, осуществляемых через расчетную сеть Банка России»

Положение № 242-П «Об организации внутреннего контроля в кредитных организациях и банковских группах»

Временное положение № 17-П «О порядке приема к исполнению поручений владельцев счетов, подписанных аналогами собственноручной подписи, при проведении безналичных расчетов кредитными организациями»

Положение № 20-П «О правилах обмена электронными документами между Банком России, кредитными организациями (филиалами) и другими клиентами Банка России при осуществлении расчетов через расчетную сеть Банка России»

Положение № 318-П «О порядке ведения кассовых операций в кредитных организациях на территории РФ»
п. 2.8 «Организация работы с денежной наличностью при использовании банкоматов, электронных кассиров, автоматических сейфов и других программно-технических комплексов»

Блок 10.2. Указания ЦБ

Указание № 1176-У «О бизнес-планах кредитных организаций» (п.п. 3.3 и п.п. 3.3.11)

Указание № 2194-У «О внесении изменений в Положение Банка России от 16 декабря 2003 года N 242-П "Об организации внутреннего контроля в кредитных организациях и банковских группах»

Указание №1390-У «О порядке информирования кредитными организациями Центрального банка Российской Федерации об использовании в своей деятельности интернет-технологий»

Блок 10.3. Письма ЦБ

Письмо № 115-Т «Об идентификации физического лица при выдаче ему предоплаченной карты»

Письмо № 47-Т «О Методических рекомендациях по проведению проверки и оценки организации внутреннего контроля в кредитных организациях» (п.п. 1.5.1 и п.п. 3.4)

Письмо № 11-Т «О рекомендациях для кредитных организаций по дополнительным мерам информационной безопасности при использовании систем интернет-банкинга»

Письмо № 128-Т О Рекомендациях по информационному содержанию и организации Web-сайтов кредитных организаций в сети Интернет

Письмо № 44-Т «О проверке осуществления кредитными организациями идентификации клиентов, обслуживаемых с использованием технологий дистанционного банковского обслуживания (включая интернет-банкинг)»

Письмо № 141-Т «О Рекомендациях по подходам кредитных организаций к выбору провайдеров и взаимодействию с ними при осуществлении дистанционного банковского обслуживания»

Письмо № 197-Т «О рисках при дистанционном банковском обслуживании»

Письмо № 36-Т «О рекомендациях по организации управления рисками, возникающими при осуществлении кредитными организациями операций с применением систем интернет-банкинга»

Письмо № 60-Т «Об особенностях обслуживания кредитными организациями клиентов с использованием технологии дистанционного доступа к банковскому счету клиента (включая интернет-банкинг)»

Письмо № 115-Т «Об исполнении Федерального закона "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма в части идентификации клиентов, обслуживаемых с использованием технологий дистанционного банковского обслуживания (включая интернет-банкинг)»

Письмо № 01-23/3148 О введении в действие Стандартов и Рекомендаций в области стандартизации Банка России по вопросам информационной безопасности банковской организации Российской Федерации

ПИСЬМО ШЕСТЕРЫХ (Банк России, Ассоциация российских банков, ФСТЭК России, Роскомнадзор, ФСБ и АРБР)

Блок 10.4. Инструкции ЦБ

Инструкция N 28-И Об открытии и закрытии банковских счетов, счетов по вкладам (депозитам)

Блок 11. СТО БР ИББС

Комплекс БР ИББС

Общие положения СТО БР ИББС – 1.0

Аудит информационной безопасности СТО БР ИББС - 1.1

Методика оценки соответствия СТО БР ИББС - 1.2

Документы по обеспечению информационной безопасности РС БР ИББС – 2.0

Руководство по самооценке РС БР ИББС – 2.1

Методика оценки рисков нарушения информационной безопасности РС БР ИББС – 2.2

Отраслевая частная модель угроз безопасности ПДн при их обработке в ИСПДн организаций БС РФ РС БР ИББС – 2.4

Отраслевая частная модель угроз РС БР ИББС – 2.4

Методические рекомендации по выполнению законодательных требований при обработке ПДн

Блок 12. Другие стандарты по ИБ

Блок 12.1. Некоторые российские стандарты

ГОСТ 34.601-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания

ГОСТ Р ИСО/МЭК 18044-2007 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности

ГОСТ Р ИСО/МЭК 15408-2008 Методы и средства обеспечения информационной безопасности Критерии оценки безопасности информационных технологий

ГОСТ Р ИСО 9001-2008 Система менеджмента качества. Требования

Блок 12.2. Некоторые зарубежные стандарты

ISO 27000 - Международные стандарты управления информационной безопасностью
ISO 15408 - Общие критерии оценки безопасности информационных технологий
PCI DSS - стандарт защиты информации в индустрии платежных карт
BS 25999, BS 25777 - Британские стандарты по управлению непрерывностью бизнеса и информационно-коммуникационных технологий
ISO 20000 и ITIL - библиотека лучших практик в области управления ИТ
ISO 18028 - Международные стандарты сетевой безопасности серии
ISO 13335 - Международные стандарты безопасности информационных технологий
BSI\IT Baseline Protection Manual
Basel II - Международная конвергенция измерения капитала и стандартов капитала: новые подходы
Международные стандарты, открытые для публичного доступа
The BCI Good Practice Guidelines
Стандарты Федерального Агентства по Информационной Безопасности (BSI) Германии
Система предварительного ознакомления с проектами Британских стандартов
NIST SP 800 Series - Специальные публикации Национального Института Стандартов и Технологий США

Евгений Царев
http://www.tsarev.biz/