РЕКОМЕНДАЦИИ В ОБЛАСТИ
СТАНДАРТИЗАЦИИ
БАНКА РОССИИ

РС БР ИББС-2.4-2010

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

ОТРАСЛЕВАЯ ЧАСТНАЯ МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

Дата введения: 2010-06-21

Издание официальное

Москва
2010

Предисловие

1. ПРИНЯТЫ И ВВЕДЕНЫ в действие Распоряжением Банка России от 21 июня 2010 года № Р-705.

2. ВВЕДЕНЫ ВПЕРВЫЕ.

Содержание

Введение

В соответствии с действующим стандартом Банка России “Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения” (далее — СТО БР ИББС-1.0) модели угроз и нарушителей должны быть основным инструментом организации банковской системы Российской Федерации (БС РФ) при развертывании, поддержании и совершенствовании системы обеспечения информационной безопасности.

Настоящая Отраслевая частная модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных организаций БС РФ (далее — Отраслевая модель угроз) содержит актуальные для большинства организаций БС РФ угрозы безопасности персональных данных при их обработке в информационных системах персональных данных (ИСПДн). Актуальные угрозы определены в результате проведения оценки рисков в соответствии с рекомендациями в области стандартизации Банка России РС БР ИББС-2.2-2009 “Обеспечение информационной безопасности организаций БС РФ. Методика оценки рисков нарушения информационной безопасности”.

РЕКОМЕНДАЦИИ В ОБЛАСТИ СТАНДАРТИЗАЦИИ БАНКА РОССИИ

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

ОТРАСЛЕВАЯ ЧАСТНАЯ МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

Дата введения: 2010-06-21

1. Область применения

Настоящий документ распространяется на организации БС РФ и содержит актуальные для большинства организаций БС РФ угрозы безопасности персональных данных при их обработке в ИСПДн.

Настоящий документ рекомендован для применения путем включения ссылок и (или) прямого использования устанавливаемых в нем положений во внутренних документах организаций БС РФ.

В случае необходимости в организации БС РФ может быть составлена частная модель актуальных угроз безопасности персональных данных при их обработке в ИСПДн организации БС РФ (далее — частная модель угроз), учитывающая особенности обработки персональных данных в конкретной организации БС РФ. При этом:

— в случае сокращения набора угроз частной модели угроз (по сравнению с Отраслевой моделью угроз) рекомендуется проводить согласование частной модели угроз с Банком России и Федеральной службой по техническому и экспортному контролю (далее — ФСТЭК России);

— в случае расширения набора угроз частной модели угроз (по сравнению с Отраслевой моделью угроз) дополнительное согласование с Банком России и ФСТЭК России не требуется.

Положения настоящего руководства применяются на добровольной основе, если только в отношении конкретных положений обязательность не установлена действующим законодательством Российской Федерации, нормативным актом Банка России или условиями договора.

В качестве методики выбора актуальных для организации БС РФ угроз и последующего составления частной модели угроз рекомендуется использовать рекомендации в области стандартизации Банка России РС БР ИББС-2.2-2009 “Обеспечение информационной безопасности организаций БС РФ. Методика оценки рисков нарушения информационной безопасности”.

2. Нормативные ссылки

В настоящем документе использованы нормативные ссылки на СТО БР ИББС-1.0.

3. Термины и определения

В настоящем документе применены термины в соответствии с СТО БР ИББС-1.0, а также следующие термины с соответствующими определениями:

3.1. **Источник угрозы безопасности персональных данных:** Объект или субъект, реализующий угрозы безопасности персональных данных путем воздействия на объекты среды обработки персональных данных организации БС РФ.

3.2. **Объект среды обработки персональных данных:** Материальный объект среды хранения, передачи, обработки, уничтожения и т.д. персональных данных.

3.3. **Оценка риска нарушения безопасности персональных данных:** Систематический и документированный процесс выявления, сбора, использования и анализа информации, позволяющей провести оценивание рисков нарушения безопасности персональных данных, обрабатываемых в организации БС РФ.

3.4. **Риск нарушения безопасности персональных данных[1]:** Риск, связанный с угрозой безопасности персональных данных.

3.5. **Угроза безопасности персональных данных:** Угроза нарушения свойств безопасности персональных данных — доступности, целостности или конфиденциальности персональных данных организации БС РФ.

4. Обозначения и сокращения

БС — банковская система;
ИСПДн — информационная система персональных данных;
НСД — несанкционированный доступ;
ПДн — персональные данные;
РФ — Российская Федерация.

5. Общий подход к составлению Отраслевой модели угроз

5.1. Угрозы безопасности персональных данных (ПДн) при их обработке в информационных системах персональных данных (ИСПДн) организаций БС РФ — это:

- угроза нарушения доступности ПДн;
- угроза нарушения целостности ПДн;
- угроза нарушения конфиденциальности[2] (неправомерное использование) ПДн, в том числе за счет хищения отчуждаемых машинных носителей с несанкционированно копированной информацией.

5.2. Отраслевая модель угроз содержит систематизированный перечень актуальных угроз безопасности ПДн при их обработке в ИСПДн, источников актуальных угроз безопасности ПДн, уровней реализации угроз безопасности ПДн, типов материальных объектов среды обработки ПДн (далее — актуальные угрозы безопасности ПДн).

Актуальная угроза безопасности ПДн — угроза безопасности ПДн, риск реализации которой не является допустимым для организации БС РФ по результатам проведения оценки рисков нарушения безопасности персональных данных, обрабатываемых в ИСПДн.

5.3. Отраслевая модель угроз содержит единые исходные данные по актуальным для организации БС РФ угрозам безопасности ПДн, связанным с несанкционированным, в том числе случайным, доступом в ИСПДн с целью ознакомления, изменения, копирования, неправомерного распространения ПДн или деструктивных воздействий на элементы ИСПДн и обрабатываемых в них ПДн с целью уничтожения или блокирования ПДн.

В рамках настоящей Отраслевой модели угроз под доступом к ПДн понимаются ознакомление с ПДн, их обработка, в частности, копирование, модификация или уничтожение ПДн (в со-

---

[1] Риски нарушения безопасности персональных данных заключаются в возможности утраты свойств безопасности персональных данных в результате реализации угроз безопасности персональных данных, вследствие чего субъекту персональных данных и (или) организации БС РФ может быть нанесен ущерб.

[2] Конфиденциальность ПДн – обязательное для соблюдения оператором или иным получившим доступ к ПДн лицом требование не допускать их распространения без согласия субъекта ПДн или иного законного основания (пункт 10 статьи 3 Федерального закона “О персональных данных”). Обеспечение конфиденциальности ПДн не требуется в случае обезличивания ПДн и в отношении общедоступных ПДн (пункт 2 статьи 7 Федерального закона “О персональных данных”).

ответствии с Руководящим документом “Защита от несанкционированного доступа к информации. Термины и определения”, Гостехкомиссия России. М.: Воениздат, 1992).

К несанкционированному доступу (НСД) к ПДн при их обработке в ИСПДн, в частности, относятся:

доступ к ПДн или действия с ПДн, нарушающие установленные права и (или) правила разграничения доступа с использованием штатных средств, предоставляемых ИСПДн;

несанкционированное воздействие на ресурсы ИСПДн, осуществляемое с использованием вредоносных программ (вредоносного кода).

6. Исходные данные Отраслевой модели угроз

6.1. Категории ПДн:

категория 1 — персональные данные, отнесенные в соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ “О персональных данных” (далее — Федеральный закон “О персональных данных”) [3] к специальным категориям персональных данных;

категория 2 — персональные данные, отнесенные в соответствии с Федеральным законом “О персональных данных” к биометрическим персональным данным;

категория 3 — персональные данные, которые не могут быть отнесены к категории 1, категории 2 или категории 4;

категория 4 — персональные данные, отнесенные в соответствии с Федеральным законом “О персональных данных” к общедоступным или обезличенным персональным данным.

6.2. Перечень основных источников угроз безопасности ПДн:

- неблагоприятные события природного и техногенного характера;
- террористы, криминальные элементы;
- компьютерные злоумышленники, осуществляющие целенаправленные деструктивные воздействия, в том числе использование компьютерных вирусов и других типов вредоносных кодов и атак;
- поставщики программно-технических средств, расходных материалов, услуг и т.п.;
- подрядчики, осуществляющие монтаж, пусконаладочные работы оборудования и его ремонт;
- сотрудники организации БС РФ, являющиеся легальными участниками процессов в ИСПДн и действующие вне рамок предоставленных полномочий;
- сотрудники организации БС РФ, являющиеся легальными участниками процессов в ИСПДн и действующие в рамках предоставленных полномочий.

6.3. Уровни информационной инфраструктуры, на которых возможна реализация угроз безопасности ПДн:

- физический уровень;
- сетевой уровень;
- уровень сетевых приложений и сервисов;
- уровень операционных систем;
- уровень систем управления базами данных;
- уровень банковских технологических процессов и приложений.

7. Отраслевая модель угроз

Отраслевая модель угроз безопасности ПДн (Таблица) содержит обобщенное описание угроз безопасности ПДн для каждой категории ПДн, включающее:

- источник угрозы безопасности ПДн;
- угроза безопасности ПДн;
- уровень реализации угрозы безопасности ПДн;
- типы материальных объектов среды обработки ПДн (далее — типы объектов среды).

Таблица. Отраслевая модель угроз безопасности ПДн

№ п/п	Источник угрозы безопасности ПДн	Уровень реализации угрозы безопасности ПДн	Типы объектов среды	Угроза безопасности ПД
1	2	3	4	5
	ПДн категории 1, ПДн категории 2			
1	Компьютерные злоумышленники, осуществляющие целенаправленное деструктивное воздействие	Сетевой уровень	Маршрутизаторы, коммутаторы, концентраторы	Нарушение целостности
2				Нарушение доступности
3		Уровень сетевых приложений и сервисов	Программные компоненты передачи данных по компьютерным сетям (сетевые сервисы)	Нарушение целостности
4				Нарушение доступности
5		Уровень операционных систем	Файлы данных с ПДн	Нарушение конфиденциальности
6				Нарушение целостности
7				Нарушение доступности
8		Уровень систем управления базами данных	Базы данных с ПДн	Нарушение конфиденциальности
9				Нарушение целостности
10				Нарушение доступности
11		Уровень банковских технологических приложений и сервисов	Прикладные программы доступа и обработки ПДн, автоматизированные рабочие места ИСПДн	Нарушение конфиденциальности
12				Нарушение целостности
13	Поставщики программно-технических средств, расходных материалов, услуг и т.п. и подрядчики, осуществляющие монтаж, пусконаладочные работы оборудования и его ремонт	Уровень операционных систем	Файлы данных с ПДн	Нарушение конфиденциальности
14				Нарушение целостности
15		Уровень систем управления базами данных	Базы данных с ПДн	Нарушение конфиденциальности
16				Нарушение целостности
17		Уровень банковских технологических приложений и сервисов	Прикладные программы доступа и обработки ПДн, автоматизированные рабочие места ИСПДн	Нарушение конфиденциальности
18				Нарушение целостности
19	Сотрудники, действующие в рамках предоставленных полномочий	Физический уровень	Линии связи, аппаратные и технические средства, серверы, физические носители информации	Нарушение конфиденциальности
20				Нарушение целостности
21		Сетевой уровень	Маршрутизаторы, коммутаторы, концентраторы	Нарушение конфиденциальности
22				Нарушение целостности
23				Нарушение доступности
24		Уровень сетевых приложений и сервисов	Программные компоненты передачи данных по компьютерным сетям (сетевые сервисы)	Нарушение конфиденциальности
25				Нарушение целостности
26				Нарушение доступности
27		Уровень операционных систем	Файлы данных с ПДн	Нарушение конфиденциальности
28				Нарушение целостности
29				Нарушение доступности
30		Уровень систем управления базами данных	Базы данных с ПДн	Нарушение конфиденциальности
31				Нарушение целостности
32				Нарушение доступности
33		Уровень банковских технологических приложений и сервисов	Прикладные программы доступа и обработки ПДн, автоматизированные рабочие места ИСПДн	Нарушение конфиденциальности
34				Нарушение целостности
35				Нарушение доступности

№ п/п	Источник угрозы безопасности ПДн	Уровень реализации угрозы безопасности ПДн	Типы объектов среды	Угроза безопасности ПД
1	2	3	4	5
36	Сотрудники, действующие вне рамок предоставленных полномочий	Уровень операционных систем	Файлы данных с ПДн	Нарушение конфиденциальности
37				Нарушение целостности
38		Уровень систем управления базами данных	Базы данных с ПДн	Нарушение конфиденциальности
39				Нарушение целостности
40		Уровень банковских технологических приложений и сервисов	Прикладные программы доступа и обработки ПДн, автоматизированные рабочие места ИСПДн	Нарушение конфиденциальности
41				Нарушение целостности
	ПДн категории 3			
42	Компьютерные злоумышленники, осуществляющие целенаправленное деструктивное воздействие	Сетевой уровень	Маршрутизаторы, коммутаторы, концентраторы	Нарушение целостности
43				Нарушение доступности
44		Уровень сетевых приложений и сервисов	Программные компоненты передачи данных по компьютерным сетям (сетевые сервисы)	Нарушение целостности
45				Нарушение доступности
46		Уровень операционных систем	Файлы данных с ПДн	Нарушение конфиденциальности
47				Нарушение целостности
48				Нарушение доступности
49		Уровень систем управления базами данных	Базы данных с ПДн	Нарушение конфиденциальности
50				Нарушение целостности
51				Нарушение доступности
52	Сотрудники, действующие в рамках предоставленных полномочий	Физический уровень	Линии связи, аппаратные и технические средства, серверы, физические носители информации	Нарушение конфиденциальности
53				Нарушение целостности
54		Сетевой уровень	Маршрутизаторы, коммутаторы, концентраторы	Нарушение конфиденциальности
55				Нарушение целостности
56				Нарушение доступности
57		Уровень сетевых приложений и сервисов	Программные компоненты передачи данных по компьютерным сетям (сетевые сервисы)	Нарушение конфиденциальности
58				Нарушение целостности
59				Нарушение доступности
60		Уровень операционных систем	Файлы данных с ПДн	Нарушение конфиденциальности
61				Нарушение целостности
62				Нарушение доступности
63		Уровень систем управления базами данных	Базы данных с ПДн	Нарушение конфиденциальности
64				Нарушение целостности
65				Нарушение доступности
66		Уровень банковских технологических приложений и сервисов		Нарушение конфиденциальности
67				Нарушение целостности
68				Нарушение доступности

№ п/п	Источник угрозы безопасности ПДн	Уровень реализации угрозы безопасности ПДн	Типы объектов среды	Угроза безопасности ПД
1	2	3	4	5
69	Сотрудники, действующие вне рамок предоставленных полномочий	Уровень операционных систем	Файлы данных с ПДн	Нарушение конфиденциальности
70				Нарушение целостности
71				Нарушение доступности
72		Уровень систем управления базами данных	Базы данных с ПДн	Нарушение конфиденциальности
73				Нарушение целостности
74		Уровень банковских технологических приложений и сервисов	Прикладные программы доступа и обработки ПДн, автоматизированные рабочие места ИСПДн	Нарушение конфиденциальности
75				Нарушение целостности
	ПДн категории 4			
76	Компьютерные злоумышленники, осуществляющие целенаправленное деструктивное воздействие	Уровень операционных систем	Файлы данных с ПДн	Нарушение целостности
77				Нарушение доступности
78		Уровень систем управления базами данных	Базы данных с ПДн	Нарушение целостности
79				Нарушение доступности
80	Сотрудники, действующие в рамках предоставленных полномочий	Уровень операционных систем	Файлы данных с ПДн	Нарушение целостности
81				Нарушение доступности
82		Уровень систем управления базами данных	Базы данных с ПДн	Нарушение целостности
83				Нарушение доступности
84		Уровень банковских технологических приложений и сервисов	Прикладные программы доступа и обработки ПДн, автоматизированные рабочие места ИСПДн	Нарушение целостности
85				Нарушение доступности
86	Сотрудники, действующие вне рамок предоставленных полномочий	Уровень операционных систем	Файлы данных с ПДн	Нарушение целостности
87		Уровень систем управления базами данных	Базы данных с ПДн	Нарушение целостности
88		Уровень банковских технологических приложений и сервисов	Прикладные программы доступа и обработки ПДн, автоматизированные рабочие места ИСПДн	Нарушение целостности

Библиография

[1] Постановление Правительства РФ от 17 ноября 2007 г. № 781 “Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных”.

[2] Приказ Федеральной службы по техническому и экспортному контролю, Федеральной службы безопасности Российской Федерации и Министерства информационных технологий и связи Российской Федерации от 13 февраля 2008 г. № 55/86/20 “Об утверждении Порядка проведения классификации информационных систем персональных данных”.

[3] Федеральный закон “О персональных данных” от 27 июля 2006 г. № 152-ФЗ.

Ключевые слова: банковская система Российской Федерации, персональные данные, модель угроз, информационная система персональных данных.