С О Д Е Р Ж А Н И Е

ИНФОРМАЦИЯ
о вводе в действие рекомендаций в области стандартизации Банка России

Банк России вводит в действие с 1 сентября 2014 года рекомендации в области стандартизации Банка России "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Обеспечение информационной безопасности на стадиях жизненного цикла автоматизированных банковских систем" (РС БР ИББС-2.6-2014)* (далее — Рекомендации).

Рекомендации подготовлены и введены в действие с целью повышения уровня информационной безопасности организаций банковской системы Российской Федерации в соответствии с Федеральным законом от 27 декабря 2002 года № 184-ФЗ "О техническом регулировании" по решению Подкомитета по стандартизации "Безопасность финансовых (банковских) операций" (ПК1) Технического комитета по стандартизации "Стандарты финансовых операций" (ТК122) Федерального агентства по техническому регулированию и метрологии.

Рекомендации опубликованы на официальном сайте Банка России в сети Интернет в подразделе "Информационная безопасность организаций банковской системы Российской Федерации" раздела "Информация по кредитным организациям".

ИНФОРМАЦИЯ
о включении ценных бумаг в Ломбардный список Банка России

В соответствии с решением Совета директоров Банка России от 25 июля 2014 года в Ломбардный список Банка России включены следующие ценные бумаги:

государственные облигации Волгоградской области, имеющие государственный регистрационный номер выпуска RU35005VLO0;

государственные облигации Оренбургской области, имеющие государственный регистрационный номер выпуска RU35002AOR0;

облигации государственного займа Республики Саха (Якутия), имеющие государственный регистрационный номер выпуска RU35006RSY0;

государственные облигации Белгородской области, имеющие государственный регистрационный номер выпуска RU35008BEL0;

государственные облигации Ярославской области, имеющие государственный регистрационный номер выпуска RU35013YRS0;

государственные облигации Липецкой области, имеющие государственный регистрационный номер выпуска RU34009LIP0;

биржевые облигации Коммерческого Банка "Московское ипотечное агентство" (Открытое Акционерное Общество), имеющие идентификационный номер выпуска 4B020303344B;

биржевые облигации Банка ВТБ (открытое акционерное общество), имеющие идентификационный номер выпуска 4B022601000B;

биржевые облигации Открытого акционерного общества "Российский Сельскохозяйственный банк", имеющие идентификационные номера выпусков 4B020703349B, 4B020403349B;

биржевые облигации "Газпромбанк" (Открытое акционерное общество), имеющие идентификационный номер выпуска 4B020900354B;

биржевые облигации Закрытого акционерного общества "КРЕДИТ ЕВРОПА БАНК", имеющие идентификационный номер выпуска 4B021803311B;

биржевые облигации ОТКРЫТОГО АКЦИОНЕРНОГО ОБЩЕСТВА "АЛЬФА-БАНК", имеющие идентификационный номер выпуска 4B021101326B;

биржевые облигации Банка ЗЕНИТ (открытое акционерное общество), имеющие идентификационный номер выпуска 4B021303255B;

облигации "ИНГ БАНК (ЕВРАЗИЯ) ЗАО" (ЗАКРЫТОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО), имеющие государственный регистрационный номер выпуска 40202495B;

биржевые облигации Общества с ограниченной ответственностью Инвестиционный коммерческий банк "Совкомбанк", имеющие идентификационный номер выпуска 4B020100963B;

биржевые облигации Открытого Акционерного Общества "БИНБАНК", имеющие идентификационный номер выпуска 4B020402562B;

---

* Опубликованы в разделе "Официальные документы".

жилищные облигации с ипотечным покрытием Закрытого акционерного общества “Ипотечный агент МКБ”, имеющие государственный регистрационный номер выпуска 4-02-81652-H;

жилищные облигации с ипотечным покрытием Закрытого акционерного общества “Ипотечный агент МТСБ”, имеющие государственный регистрационный номер выпуска 4-02-81796-H;

облигации Общества с ограниченной ответственностью “Фольксваген Банк РУС”, имеющие государственный регистрационный номер выпуска 40703500B;

долговые эмиссионные ценные бумаги, выпущенные юридическими лицами — нерезидентами Российской Федерации за пределами Российской Федерации, имеющие следующие коды ISIN: XS0205828477, XS0461926569, XS0463663442, XS0554659671, XS0555493203, XS0643176448, XS0643183220, XS0889401724, XS0922296883, XS0997544860.

ИНФОРМАЦИЯ О РЕГИСТРАЦИИ И ЛИЦЕНЗИРОВАНИИ КРЕДИТНЫХ ОРГАНИЗАЦИЙ НА 1 ИЮЛЯ 2014 ГОДА*

Регистрация кредитных организаций

1.	**Зарегистрировано КО** Банком России либо на основании его решения уполномоченным регистрирующим органом, всего[1]**	**1059**
	в том числе:	
	– банков	**986**
	– небанковских КО	**73**
1.1.	Зарегистрировано КО со 100-процентным иностранным участием в капитале	**75**
1.2.	КО, зарегистрированные Банком России, но еще не оплатившие уставный капитал и не получившие лицензию (в рамках законодательно установленного срока)	**1**
	в том числе:	
	– банки	**1**
	– небанковские КО	**0**

Действующие кредитные организации

2.	**КО, имеющие право на осуществление банковских операций, всего[2]**	**884**
	в том числе:	
	– банки	**824**
	– небанковские КО	**60**
2.1.	КО, имеющие лицензии (разрешения), предоставляющие право на:	
	– привлечение вкладов населения	**723**
	– осуществление операций в иностранной валюте	**593**
	– генеральные лицензии	**263**
	– проведение операций с драгметаллами	**206**
2.2.	КО с иностранным участием в уставном капитале, всего	**238**
	в том числе:	
	– со 100-процентным	**75**
	– свыше 50 процентов	**42**
2.3.	КО, включенные в реестр банков – участников системы обязательного страхования вкладов, всего[3]	**734**
3.	**Зарегистрированный уставный капитал действующих КО (млн. руб.)**	**1 591 378**
4.	**Филиалы действующих КО на территории Российской Федерации, всего**	**1880**
	в том числе:	
	– ОАО “Сбербанк России”[4]	**95**
	– банков со 100-процентным иностранным участием в уставном капитале	**94**
5.	**Филиалы действующих КО за рубежом, всего[5]**	**6**
6.	**Филиалы банков-нерезидентов на территории Российской Федерации**	**0**
7.	**Представительства действующих российских КО, всего[6]**	**323**
	в том числе:	
	– на территории Российской Федерации	**281**
	– в дальнем зарубежье	**29**
	– в ближнем зарубежье	**13**
8.	**Дополнительные офисы КО (филиалов), всего**	**24 341**
	в том числе ОАО “Сбербанк России”	**11 868**
9.	**Операционные кассы вне кассового узла КО (филиалов), всего**	**7275**
	в том числе ОАО “Сбербанк России”	**4878**
10.	**Кредитно-кассовые офисы КО (филиалов), всего**	**2512**
	в том числе ОАО “Сбербанк России”	**0**

Материал подготовлен Департаментом лицензирования деятельности и финансового оздоровления кредитных организаций

11.	**Операционные офисы КО (филиалов), всего**	**9291**
	в том числе ОАО “Сбербанк России”	**654**
12.	**Передвижные пункты кассовых операций КО (филиалов), всего**	**163**
	в том числе ОАО “Сбербанк России”	**158**

Отзыв лицензий и ликвидация юридических лиц

13.	**КО, у которых отозвана (аннулирована) лицензия на осуществление банковских операций и которые не исключены из Книги государственной регистрации кредитных организаций[7]**	**174**
14.	**Внесена запись в Книгу государственной регистрации кредитных организаций о ликвидации КО как юридического лица, всего[8]**	**2103**
	в том числе:	
	– в связи с отзывом (аннулированием) лицензии	**1630**
	– в связи с реорганизацией	**472**
	в том числе:	
	– в форме слияния	**2**
	– в форме присоединения	**470**
	в том числе:	
	– путем преобразования в филиалы других банков	**382**
	– путем присоединения к другим банкам (без образования филиала)	**88**
	– в связи с нарушением законодательства в части оплаты уставного капитала	**1**

* Информация подготовлена в т.ч. на основании сведений, поступивших из уполномоченного регистрирующего органа на отчетную дату.

Пояснения к таблице

** КО – кредитная организация. Термин “кредитная организация” в настоящей информации включает в себя одно из следующих понятий:

- юридическое лицо, зарегистрированное Банком России (до 1.07.2002) или уполномоченным регистрирующим органом и имеющее право на осуществление банковских операций;
- юридическое лицо, зарегистрированное Банком России (до 1.07.2002) или уполномоченным регистрирующим органом, имевшее, но утратившее право на осуществление банковских операций.

[1] Указываются КО, имеющие статус юридического лица на отчетную дату, в том числе КО, утратившие право на осуществление банковских операций, но еще не ликвидированные как юридическое лицо.

[2] Указываются КО, зарегистрированные Банком России (до 1.07.2002) или уполномоченным регистрирующим органом и имеющие право на осуществление банковских операций.

[3] Данные приводятся на основании сведений, представленных в Банк России государственной корпорацией “Агентство по страхованию вкладов” на отчетную дату.

[4] Указываются филиалы ОАО “Сбербанк России”, внесенные в Книгу государственной регистрации кредитных организаций и получившие порядковые номера. До 1.01.1998 в ежемесячной информации о кредитных организациях по данной строке указывалось общее количество учреждений ОАО “Сбербанк России” – **34 426**.

[5] Указываются филиалы, открытые российскими КО за рубежом.

[6] В число представительств российских КО за рубежом включены представительства, по которым поступили в Банк России уведомления об открытии их за рубежом.

[7] Общее количество КО с отозванной (аннулированной) лицензией на осуществление банковских операций (включая КО, по которым в Книгу государственной регистрации кредитных организаций внесена запись об их ликвидации) – **1804**.

[8] После 1.07.2002 запись в Книгу государственной регистрации кредитных организаций о ликвидации кредитной организации как юридического лица вносится только после государственной регистрации кредитной организации в связи с ее ликвидацией уполномоченным регистрирующим органом.

Справка о количестве действующих кредитных организаций и их филиалов в территориальном разрезе по состоянию на 1.07.2014

Наименование региона	Количество КО в регионе	Количество филиалов в регионе		
		всего	КО, головная организация которых находится в данном регионе	КО, головная организация которых находится в другом регионе
1	2	3	4	5
Российская Федерация	**884**	**1880**	**294**	**1586**
ЦЕНТРАЛЬНЫЙ ФЕДЕРАЛЬНЫЙ ОКРУГ	525	373	65	308
Белгородская область	4	11	1	10
Брянская область	0	9	0	9
Владимирская область	3	12	0	12
Воронежская область	2	29	0	29
Ивановская область	6	11	0	11
Калужская область	4	10	0	10
Костромская область	6	6	0	6
Курская область	2	8	0	8
Липецкая область	1	11	1	10
Орловская область	1	13	0	13
Рязанская область	4	11	0	11
Смоленская область	2	11	4	7
Тамбовская область	1	4	0	4
Тверская область	4	13	1	12
Тульская область	4	12	0	12
Ярославская область	5	25	2	23
Московский регион (справочно)	*476*	*177*	*56*	*121*
г. Москва	467	137	18	119
Московская область	9	40	0	40
СЕВЕРО-ЗАПАДНЫЙ ФЕДЕРАЛЬНЫЙ ОКРУГ	70	262	8	254
Республика Карелия	1	12	2	10
Республика Коми	1	12	2	10
Архангельская область	1	19	0	19
в т.ч. Ненецкий АО	0	1	0	1
Архангельская область без данных по Ненецкому АО	1	18	0	18
Вологодская область	10	12	3	9
Калининградская область	2	23	1	22
Ленинградская область	4	12	0	12
Мурманская область	3	13	0	13
Новгородская область	2	9	0	9
Псковская область	2	6	0	6
г. Санкт-Петербург	44	144	0	144
ЮЖНЫЙ ФЕДЕРАЛЬНЫЙ ОКРУГ	45	211	14	197
Республика Адыгея (Адыгея)	4	5	1	4
Республика Калмыкия	2	3	0	3
Краснодарский край	14	68	1	67
Астраханская область	5	13	0	13
Волгоградская область	4	34	0	34
Ростовская область	16	88	12	76
СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ ОКРУГ	35	148	65	83
Республика Дагестан	17	68	56	12
Республика Ингушетия	0	6	0	6
Кабардино-Балкарская Республика	5	11	3	8
Карачаево-Черкесская Республика	5	5	0	5
Республика Северная Осетия – Алания	3	9	1	8
Чеченская Республика	0	5	0	5
Ставропольский край	5	44	5	39

Наименование региона	Количество КО в регионе	Количество филиалов в регионе		
		всего	КО, головная организация которых находится в данном регионе	КО, головная организация которых находится в другом регионе
1	2	3	4	5
ПРИВОЛЖСКИЙ ФЕДЕРАЛЬНЫЙ ОКРУГ	100	362	54	308
Республика Башкортостан	8	33	0	33
Республика Марий Эл	2	13	4	9
Республика Мордовия	4	4	0	4
Республика Татарстан (Татарстан)	22	66	45	21
Удмуртская Республика	2	10	0	10
Чувашская Республика – Чувашия	4	8	0	8
Пермский край	5	35	0	35
Кировская область	3	7	0	7
Нижегородская область	12	74	2	72
Оренбургская область	8	13	0	13
Пензенская область	1	14	0	14
Самарская область	17	49	3	46
Саратовская область	9	26	0	26
Ульяновская область	3	10	0	10
УРАЛЬСКИЙ ФЕДЕРАЛЬНЫЙ ОКРУГ	40	204	60	144
Курганская область	2	8	0	8
Свердловская область	15	66	4	62
Тюменская область	15	61	18	43
в т.ч. Ханты-Мансийский АО – Югра	8	16	3	13
Ямало-Ненецкий АО	0	9	0	9
Тюменская область без данных по Ханты-Мансийскому АО – Югре и Ямало-Ненецкому АО	7	36	15	21
Челябинская область	8	69	38	31
СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ ОКРУГ	47	209	21	188
Республика Алтай	2	6	1	5
Республика Бурятия	1	8	2	6
Республика Тыва	1	3	0	3
Республика Хакасия	2	3	0	3
Алтайский край	7	15	6	9
Забайкальский край	0	6	0	6
Красноярский край	5	33	3	30
Иркутская область	7	22	1	21
Кемеровская область	6	15	0	15
Новосибирская область	8	60	0	60
Омская область	6	20	0	20
Томская область	2	18	8	10
ДАЛЬНЕВОСТОЧНЫЙ ФЕДЕРАЛЬНЫЙ ОКРУГ	22	96	7	89
Республика Саха (Якутия)	4	14	0	14
Камчатский край	3	8	3	5
Приморский край	6	19	2	17
Хабаровский край	2	30	0	30
Амурская область	2	6	0	6
Магаданская область	0	6	0	6
Сахалинская область	5	8	2	6
Еврейская АО	0	4	0	4
Чукотский АО	0	1	0	1
КРЫМСКИЙ ФЕДЕРАЛЬНЫЙ ОКРУГ	0	15	0	15
Республика Крым	0	10	0	10
г. Севастополь	0	5	0	5

Примечание.

По строке “Московский регион” в колонках 4 и 5 указано количество филиалов, головная кредитная организация которых находится, соответственно, в данном регионе (г. Москве и Московской области) и других регионах Российской Федерации.

Количество внутренних структурных подразделений действующих кредитных организаций (филиалов) в территориальном разрезе по состоянию на 1.07.2014

Наименование региона	Дополнительные офисы	Операционные кассы вне кассового узла	Кредитно-кассовые офисы	Операционные офисы	Всего
1	2	3	4	5	6
Российская Федерация	**24 341**	**7275**	**2512**	**9291**	**43 419**
ЦЕНТРАЛЬНЫЙ ФЕДЕРАЛЬНЫЙ ОКРУГ	7331	2396	282	2070	12 079
Белгородская область	162	194	19	132	507
Брянская область	101	52	9	106	268
Владимирская область	204	101	11	151	467
Воронежская область	329	212	37	169	747
Ивановская область	174	7	9	88	278
Калужская область	133	36	9	117	295
Костромская область	117	3	5	72	197
Курская область	134	76	22	107	339
Липецкая область	156	76	23	115	370
Орловская область	103	46	9	63	221
Рязанская область	134	66	15	98	313
Смоленская область	99	43	9	89	240
Тамбовская область	127	130	11	67	335
Тверская область	141	76	11	96	324
Тульская область	167	53	11	144	375
Ярославская область	235	2	16	150	403
Московский регион (справочно)	*4815*	*1223*	*56*	*306*	*6400*
г. Москва	3256	754	40	171	4221
Московская область	1559	469	16	135	2179
СЕВЕРО-ЗАПАДНЫЙ ФЕДЕРАЛЬНЫЙ ОКРУГ	2397	213	357	1057	4024
Республика Карелия	115	7	15	48	185
Республика Коми	168	21	17	91	297
Архангельская область	200	4	27	98	329
в т.ч. Ненецкий АО	13	0	0	1	14
Архангельская область без данных по Ненецкому АО	187	4	27	97	315
Вологодская область	237	12	45	113	407
Калининградская область	129	18	31	92	270
Ленинградская область	46	18	13	350	427
Мурманская область	125	6	14	95	240
Новгородская область	120	2	16	50	188
Псковская область	113	8	12	54	187
г. Санкт-Петербург	1144	117	167	66	1494
ЮЖНЫЙ ФЕДЕРАЛЬНЫЙ ОКРУГ	2685	445	330	760	4220
Республика Адыгея (Адыгея)	76	7	12	18	113
Республика Калмыкия	37	1	3	10	51
Краснодарский край	1162	138	139	340	1779
Астраханская область	119	63	14	71	267
Волгоградская область	266	167	48	198	679
Ростовская область	1025	69	114	123	1331
СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ ОКРУГ	810	120	113	117	1160
Республика Дагестан	141	41	9	13	204
Республика Ингушетия	15	1	0	1	17
Кабардино-Балкарская Республика	82	41	5	8	136
Карачаево-Черкесская Республика	34	2	3	8	47
Республика Северная Осетия – Алания	44	12	6	13	75
Чеченская Республика	39	0	6	8	53
Ставропольский край	455	23	84	66	628

Наименование региона	Дополнительные офисы	Операционные кассы вне кассового узла	Кредитно-кассовые офисы	Операционные офисы	Всего
1	2	3	4	5	6
ПРИВОЛЖСКИЙ ФЕДЕРАЛЬНЫЙ ОКРУГ	4931	2502	588	2064	10 085
Республика Башкортостан	794	362	89	214	1459
Республика Марий Эл	66	40	13	60	179
Республика Мордовия	147	79	8	61	295
Республика Татарстан (Татарстан)	738	490	76	250	1554
Удмуртская Республика	259	12	35	141	447
Чувашская Республика – Чувашия	143	136	34	100	413
Пермский край	598	24	52	231	905
Кировская область	207	80	34	101	422
Нижегородская область	601	286	74	143	1104
Оренбургская область	295	269	52	151	767
Пензенская область	159	209	20	91	479
Самарская область	469	171	64	247	951
Саратовская область	290	263	21	191	765
Ульяновская область	165	81	16	83	345
УРАЛЬСКИЙ ФЕДЕРАЛЬНЫЙ ОКРУГ	2245	559	351	822	3977
Курганская область	92	169	15	82	358
Свердловская область	932	170	81	112	1295
Тюменская область	733	100	95	352	1280
в т.ч. Ханты-Мансийский АО – Югра	355	58	39	155	607
Ямало-Ненецкий АО	136	16	7	63	222
Тюменская область без данных по Ханты-Мансийскому АО – Югре и Ямало-Ненецкому АО	242	26	49	134	451
Челябинская область	488	120	160	276	1044
СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ ОКРУГ	2873	912	328	1531	5644
Республика Алтай	36	4	3	8	51
Республика Бурятия	171	3	15	115	304
Республика Тыва	40	0	5	10	55
Республика Хакасия	86	18	7	77	188
Алтайский край	259	443	31	177	910
Забайкальский край	170	1	13	87	271
Красноярский край	506	98	36	267	907
Иркутская область	327	48	39	218	632
Кемеровская область	298	90	53	225	666
Новосибирская область	503	124	70	83	780
Омская область	331	78	34	156	599
Томская область	146	5	22	108	281
ДАЛЬНЕВОСТОЧНЫЙ ФЕДЕРАЛЬНЫЙ ОКРУГ	1042	127	110	629	1908
Республика Саха (Якутия)	188	32	9	118	347
Камчатский край	71	5	4	38	118
Приморский край	312	24	48	170	554
Хабаровский край	221	23	29	88	361
Амурская область	126	21	10	81	238
Магаданская область	37	7	3	13	60
Сахалинская область	66	13	5	81	165
Еврейская АО	21	2	2	19	44
Чукотский АО	0	0	0	21	21
КРЫМСКИЙ ФЕДЕРАЛЬНЫЙ ОКРУГ	27	1	53	241	322
Республика Крым	25	1	42	171	239
г. Севастополь	2	0	11	70	83

Группировка действующих кредитных организаций по величине зарегистрированного уставного капитала* по состоянию на 1.07.2014

№ п/п	Величина уставного капитала	Количество кредитных организаций				Изменение (+/–)
		на 1.01.2014		на 1.07.2014		
		количество	удельный вес к итогу, %	количество	удельный вес к итогу, %	
1	до 3 млн. руб.	15	1,6	13	1,5	–2
2	от 3 до 10 млн. руб.	15	1,6	13	1,5	–2
3	от 10 до 30 млн. руб.	45	4,9	44	5,0	–1
4	от 30 до 60 млн. руб.	36	3,9	33	3,7	–3
5	от 60 до 150 млн. руб.	143	15,5	128	14,5	–15
6	от 150 до 300 млн. руб.	251	27,2	234	26,5	–17
7	от 300 до 500 млн. руб.	116	12,6	116	13,1	0
8	от 500 млн. руб. до 1 млрд. руб.	116	12,6	115	13,0	–1
9	от 1 до 10 млрд. руб.	161	17,4	161	18,2	0
10	от 10 млрд. руб. и выше	25	2,7	27	3,1	2
11	Всего по Российской Федерации	923	100	884	100	–39

* Уставный капитал, величина которого оплачена участниками, внесена в устав кредитной организации и учтена в Книге государственной регистрации кредитных организаций после регистрации устава в уполномоченном регистрирующем органе.

Группировка действующих кредитных организаций по величине зарегистрированного уставного капитала по состоянию на 1.07.2014

Наименование региона	До 3 млн. руб.	От 3 до 10 млн. руб.	От 10 до 30 млн. руб.	От 30 до 60 млн. руб.	От 60 до 150 млн. руб.	От 150 до 300 млн. руб.	От 300 до 500 млн. руб.	От 500 млн. руб. до 1 млрд. руб.	От 1 до 10 млрд. руб.	От 10 млрд. руб и выше	Всего
1	2	3	4	5	6	7	8	9	10	11	12
Российская Федерация	**13**	**13**	**44**	**33**	**128**	**234**	**116**	**115**	**161**	**27**	**884**
ЦЕНТРАЛЬНЫЙ ФЕДЕРАЛЬНЫЙ ОКРУГ	3	7	27	22	56	134	57	80	117	22	525
Белгородская область	0	0	0	0	1	0	2	1	0	0	4
Брянская область	0	0	0	0	0	0	0	0	0	0	0
Владимирская область	0	0	0	0	1	1	0	1	0	0	3
Воронежская область	0	0	0	0	1	0	1	0	0	0	2
Ивановская область	0	0	1	0	3	2	0	0	0	0	6
Калужская область	0	0	0	1	0	3	0	0	0	0	4
Костромская область	0	0	0	0	1	1	3	0	1	0	6
Курская область	0	0	1	0	1	0	0	0	0	0	2
Липецкая область	0	0	0	0	0	0	0	1	0	0	1
Орловская область	0	0	0	0	0	0	1	0	0	0	1
Рязанская область	0	0	0	3	0	1	0	0	0	0	4
Смоленская область	0	0	0	0	1	0	1	0	0	0	2
Тамбовская область	0	0	0	0	1	0	0	0	0	0	1
Тверская область	0	0	0	1	1	2	0	0	0	0	4
Тульская область	0	0	1	0	1	2	0	0	0	0	4
Ярославская область	0	0	1	2	1	0	0	1	0	0	5
Московский регион (справочно)	*3*	*7*	*23*	*15*	*43*	*122*	*49*	*76*	*116*	*22*	*476*
г. Москва	3	6	23	15	42	120	47	75	114	22	467
Московская область	0	1	0	0	1	2	2	1	2	0	9
СЕВЕРО-ЗАПАДНЫЙ ФЕДЕРАЛЬНЫЙ ОКРУГ	3	3	5	3	13	16	10	8	9	0	70
Республика Карелия	0	0	0	0	1	0	0	0	0	0	1
Республика Коми	0	0	0	0	1	0	0	0	0	0	1
Архангельская область	0	0	1	0	0	0	0	0	0	0	1
в т.ч. Ненецкий АО	0	0	0	0	0	0	0	0	0	0	0
Архангельская область без данных по Ненецкому АО	0	0	1	0	0	0	0	0	0	0	1
Вологодская область	0	0	1	0	3	3	1	1	1	0	10
Калининградская область	0	0	0	0	0	1	0	0	1	0	2
Ленинградская область	0	0	1	0	0	1	2	1	0	0	5
Мурманская область	1	0	0	0	0	1	0	1	0	0	3
Новгородская область	0	1	0	0	0	1	0	0	0	0	2
Псковская область	0	0	0	0	1	0	1	0	0	0	2
г. Санкт-Петербург	2	2	2	3	7	9	6	5	7	0	43

Наименование региона	До 3 млн. руб.	От 3 до 10 млн. руб.	От 10 до 30 млн. руб.	От 30 до 60 млн. руб.	От 60 до 150 млн. руб.	От 150 до 300 млн. руб.	От 300 до 500 млн. руб.	От 500 млн. руб. до 1 млрд. руб.	От 1 до 10 млрд. руб.	От 10 млрд. руб и выше	Всего
1	2	3	4	5	6	7	8	9	10	11	12
ЮЖНЫЙ ФЕДЕРАЛЬНЫЙ ОКРУГ	1	1	3	0	7	21	7	3	2	0	45
Республика Адыгея (Адыгея)	0	0	2	0	0	2	0	0	0	0	4
Республика Калмыкия	0	0	0	0	2	0	0	0	0	0	2
Краснодарский край	0	0	1	0	2	5	3	1	2	0	14
Астраханская область	1	1	0	0	0	2	1	0	0	0	5
Волгоградская область	0	0	0	0	0	4	0	0	0	0	4
Ростовская область	0	0	0	0	3	8	3	2	0	0	16
СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ ОКРУГ	1	0	2	0	10	13	6	3	0	0	35
Республика Дагестан	1	0	1	0	3	8	3	1	0	0	17
Республика Ингушетия	0	0	0	0	0	0	0	0	0	0	0
Кабардино-Балкарская Республика	0	0	0	0	3	2	0	0	0	0	5
Карачаево-Черкесская Республика	0	0	1	0	1	0	1	2	0	0	5
Республика Северная Осетия – Алания	0	0	0	0	1	0	2	0	0	0	3
Чеченская Республика	0	0	0	0	0	0	0	0	0	0	0
Ставропольский край	0	0	0	0	2	3	0	0	0	0	5
ПРИВОЛЖСКИЙ ФЕДЕРАЛЬНЫЙ ОКРУГ	2	1	2	2	15	23	21	12	18	4	100
Республика Башкортостан	0	0	0	0	0	2	4	1	1	0	8
Республика Марий Эл	0	0	2	0	0	0	0	0	0	0	2
Республика Мордовия	0	0	0	0	0	0	3	1	0	0	4
Республика Татарстан (Татарстан)	1	1	0	0	2	5	1	4	5	3	22
Удмуртская Республика	0	0	0	0	0	0	2	0	0	0	2
Чувашская Республика – Чувашия	0	0	0	0	1	2	1	0	0	0	4
Пермский край	1	0	0	0	1	1	0	0	2	0	5
Кировская область	0	0	0	1	0	0	0	1	1	0	3
Нижегородская область	0	0	0	0	4	2	4	0	2	0	12
Оренбургская область	0	0	0	0	3	0	1	2	2	0	8
Пензенская область	0	0	0	0	0	1	0	0	0	0	1
Самарская область	0	0	0	0	1	6	1	3	5	1	17
Саратовская область	0	0	0	1	2	2	4	0	0	0	9
Ульяновская область	0	0	0	0	1	2	0	0	0	0	3

Наименование региона	До 3 млн. руб.	От 3 до 10 млн. руб.	От 10 до 30 млн. руб.	От 30 до 60 млн. руб.	От 60 до 150 млн. руб.	От 150 до 300 млн. руб.	От 300 до 500 млн. руб.	От 500 млн. руб. до 1 млрд. руб.	От 1 до 10 млрд. руб.	От 10 млрд. руб и выше	Всего
1	2	3	4	5	6	7	8	9	10	11	12
УРАЛЬСКИЙ ФЕДЕРАЛЬНЫЙ ОКРУГ	1	0	2	2	8	10	4	3	9	1	40
Курганская область	0	0	0	0	1	1	0	0	0	0	2
Свердловская область	0	0	0	1	4	5	0	1	4	0	15
Тюменская область	1	0	1	1	3	3	1	0	4	1	15
в т.ч. Ханты-Мансийский АО – Югра	0	0	1	1	2	0	1	0	2	1	8
Ямало-Ненецкий АО	0	0	0	0	0	0	0	0	0	0	0
Тюменская область без данных по Ханты-Мансийскому АО – Югре и Ямало-Ненецкому АО	1	0	0	0	1	3	0	0	2	0	7
Челябинская область	0	0	1	0	0	1	3	2	1	0	8
СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ ОКРУГ	2	1	2	2	14	10	9	3	4	0	47
Республика Алтай	0	0	1	0	1	0	0	0	0	0	2
Республика Бурятия	0	0	0	0	0	0	0	1	0	0	1
Республика Тыва	0	0	0	0	0	1	0	0	0	0	1
Республика Хакасия	0	0	0	0	0	1	1	0	0	0	2
Алтайский край	0	0	0	1	4	1	0	0	1	0	7
Забайкальский край	0	0	0	0	0	0	0	0	0	0	0
Красноярский край	0	0	1	0	1	1	2	0	0	0	5
Иркутская область	0	0	0	0	3	3	1	0	0	0	7
Кемеровская область	0	0	0	1	2	1	2	0	0	0	6
Новосибирская область	2	0	0	0	1	0	1	2	2	0	8
Омская область	0	1	0	0	2	1	1	0	1	0	6
Томская область	0	0	0	0	0	1	1	0	0	0	2
ДАЛЬНЕВОСТОЧНЫЙ ФЕДЕРАЛЬНЫЙ ОКРУГ	0	0	1	2	5	7	2	3	2	0	22
Республика Саха (Якутия)	0	0	0	0	1	1	0	1	1	0	4
Камчатский край	0	0	1	1	0	0	0	0	1	0	3
Приморский край	0	0	0	0	2	4	0	0	0	0	6
Хабаровский край	0	0	0	0	1	1	0	0	0	0	2
Амурская область	0	0	0	0	0	0	0	2	0	0	2
Магаданская область	0	0	0	0	0	0	0	0	0	0	0
Сахалинская область	0	0	0	1	1	1	2	0	0	0	5
Еврейская АО	0	0	0	0	0	0	0	0	0	0	0
Чукотский АО	0	0	0	0	0	0	0	0	0	0	0
КРЫМСКИЙ ФЕДЕРАЛЬНЫЙ ОКРУГ	0	0	0	0	0	0	0	0	0	0	0
Республика Крым	0	0	0	0	0	0	0	0	0	0	0
г. Севастополь	0	0	0	0	0	0	0	0	0	0	0

ИНФОРМАЦИЯ О РЕГИСТРАЦИИ И ЛИЦЕНЗИРОВАНИИ КРЕДИТНЫХ ОРГАНИЗАЦИЙ ВО II КВАРТАЛЕ 2014 ГОДА

Кредитные организации, вновь зарегистрированные Банком России во II квартале 2014 г.

(информация подготовлена на основании сведений, поступивших из уполномоченного регистрирующего органа на отчетную дату)

№ п/п	Наименование КО	Рег. №	Дата регистрации
1	АГЕНТСТВО КРЕДИТНЫХ ГАРАНТИЙ	3526-Д	20.06.2014
2	КЭБ БАНК РУС	3525	6.06.2014

Кредитные организации, реорганизованные в форме присоединения во II квартале 2014 г.

(информация подготовлена на основании сведений, поступивших из уполномоченного регистрирующего органа на отчетную дату)

№ п/п	Информация о присоединившейся КО				Информация о КО, к которой осуществлено присоединение		
	Наименование	Рег. №	Дата регистрации	Дата реорганизации	Наименование	Рег. №	Дата регистрации
1	КИТ ФИНАНС ИНВЕСТИЦИОННЫЙ БАНК	1911	11.06.1992	18.04.2014	АБСОЛЮТ БАНК	2306	22.04.1993

Кредитные организации, получившие во II квартале 2014 г. впервые после регистрации лицензию на осуществление банковских операций

№ п/п	Наименование КО	Рег. №	Дата регистрации	Дата выдачи лицензии	Вид лицензии
1	АГЕНТСТВО КРЕДИТНЫХ ГАРАНТИЙ	3526-Д	20.06.2014	26.06.2014	рублевая

Кредитные организации, получившие право расширить свою деятельность на основе получения лицензии Банка России на осуществление банковских операций со средствами в иностранной валюте во II квартале 2014 г.

Нет

Кредитные организации, получившие право расширить свою деятельность за счет снятия ограничений на установление корреспондентских отношений с иностранными банками во II квартале 2014 г.

№ п/п	Наименование КО	Рег. №	Дата регистрации	Дата выдачи лицензии на осуществление операций в иностранной валюте
1	ДЕВОН-КРЕДИТ	1972	22.07.1992	22.05.2014
2	РОСИНТЕРБАНК	226	11.01.1990	4.06.2014

Кредитные организации, получившие право расширить свою деятельность на основе получения генеральной лицензии Банка России во II квартале 2014 г.

Нет

Материал подготовлен Департаментом лицензирования деятельности и финансового оздоровления кредитных организаций

Кредитные организации, получившие право расширить свою деятельность на основе получения лицензии Банка России на привлечение во вклады средств физических лиц в рублях или в рублях и иностранной валюте во II квартале 2014 г.

Нет

Кредитные организации, получившие право расширить свою деятельность на основе получения лицензии на проведение операций с драгметаллами во II квартале 2014 г.

№ п/п	Наименование КО	Рег. №	Дата регистрации	Дата выдачи лицензии
1	ББР БАНК	2929	27.06.1994	12.05.2014

Небанковские кредитные организации, получившие право расширить круг осуществляемых банковских операций путем получения лицензии, содержащей более широкий перечень банковских операций по сравнению с имеющимся в ранее выданных им лицензиях во II квартале 2014 г.

Нет

Кредитные организации, изменившие свое место нахождения и получившие в связи с этим новую лицензию во II квартале 2014 г.

№ п/п	Наименование КО	Рег. №	Дата регистрации	Прежнее место нахождения КО	Новое место нахождения КО	Дата выдачи лицензии
1	СОВРЕМЕННЫЙ КОММЕРЧЕСКИЙ БАНК	3316	15.10.1997	115035, г. Москва, ул. Садовническая, 82, стр. 2	156000, г. Кострома, пр-т Текстильщиков, 46	15.05.2014
2	ФИНАНС БИЗНЕС БАНК	520	19.10.1990	352190, Краснодарский край, Гулькевичский р-н, г. Гулькевичи, ул. Советская, 29а	109028, г. Москва, ул. Солянка, 3, стр. 2	22.05.2014

Кредитные организации, по которым внесена запись в Книгу государственной регистрации о ликвидации во II квартале 2014 г.

(информация подготовлена на основании сведений, поступивших из уполномоченного регистрирующего органа на отчетную дату)

№ п/п	Наименование КО	Рег. №	Дата регистрации	Дата отзыва лицензии	Дата ликвидации
1	ДИАЛОГ-ОПТИМ	3107	4.10.1994	10.08.2004	8.05.2014
2	ДИАМОНД-БАНК	3225	1.03.1995	25.04.2007	5.05.2014
3	ИНВЕСТКОМБАНК БЭЛКОМ	2222	6.01.1993	7.09.2006	19.05.2014
4	КИТ ФИНАНС ИНВЕСТИЦИОННЫЙ БАНК	1911	11.06.1992	–	18.04.2014
5	КРАСБАНК	1569	13.09.1991	21.05.2008	5.06.2014
6	ЛИБРА	2980	18.07.1994	8.10.2009	30.04.2014
7	СУЛАК	749	13.11.1990	1.03.2013	13.05.2014
8	ТЮМЕНЬЭНЕРГОБАНК	2419	12.07.1993	3.12.2008	27.05.2014

Список кредитных организаций, изменивших свое наименование и получивших в связи с этим новую лицензию во II квартале 2014 г.

№ п/п	Прежнее наименование КО	Новое наименование КО	Рег. №	Место нахождения	Дата регистрации	Дата выдачи лицензии
1	Общество с ограниченной ответственностью Медицинский коммерческий Банк “Аверс”	Общество с ограниченной ответственностью Банк “Аверс”	415	420111, г. Казань, ул. М.Джалиля, 3	25.09.1990	9.06.2014
2	Общество с ограниченной ответственностью “Коммерческий химический экспортно-импортный банк”	Общество с ограниченной ответственностью “Азия Банк”	3183	109012, г. Москва, ул. Ильинка, 4, пом. 7-15, 67-69	22.12.1994	28.04.2014
3	Открытое акционерное общество “Арксбанк”	Банк “Агентство расчетно-кредитная система” (открытое акционерное общество)	1868	394000, г. Воронеж, пр-т Революции, 1а	22.05.1992	3.04.2014
4	Общество с ограниченной ответственностью “ПромСервисБанк”	Общество с ограниченной ответственностью Банк Оранжевый	1659	190013, г. Санкт-Петербург, ул. Рузовская, 16, литер А	10.12.1991	7.04.2014
5	Закрытое акционерное общество коммерческий банк “КЕДР”	Открытое акционерное общество коммерческий банк “КЕДР”	1574	660049, г. Красноярск, ул. Ленина, 37, пом. 6	30.09.1991	14.04.2014
6	Открытое акционерное общество “Флексинвест Банк”	Акционерный Коммерческий Банк “МИРЪ” (Открытое Акционерное Общество)	3089	109004, г. Москва, ул. Николоямская, 40, стр. 1	6.09.1994	20.06.2014
7	Общество с ограниченной ответственностью “Промышленно-Транспортный Банк”	ПромТрансБанк (Общество с ограниченной ответственностью)	2638	450008, Республика Башкортостан, г. Уфа, ул. Ленина, 70	30.12.1993	4.04.2014
8	Закрытое акционерное общество “ДжиИ Мани Банк”	Закрытое акционерное общество “Современный Коммерческий Банк”	3316	156000, г. Кострома, пр-т Текстильщиков, 46	15.10.1997	15.05.2014
9	Открытое акционерное общество “НОМОС-БАНК”	Открытое акционерное общество Банк “Финансовая Корпорация Открытие”	2209	115114, г. Москва, ул. Летниковская, 2, стр. 4	15.12.1992	19.06.2014

Список филиалов кредитных организаций, внесенных в Книгу государственной регистрации кредитных организаций во II квартале 2014 г.

№ п/п	Наименование КО	Рег. № КО	Дата регистрации КО	Наименование филиала (место нахождения)	№ филиала	Место нахождения филиала
1	АГРОИНКОМБАНК	1946	6.07.1992	в г. Севастополе	3	299029, г. Севастополь, пр-т Генерала Острякова, 80
2	БАЙКАЛБАНК	2632	24.12.1993	Крымский	7	295034, Российская Федерация, Республика Крым, г. Симферополь, пр-т Победы, 4
3	ВЕРХНЕВОЛЖСКИЙ	1084	5.12.1990	Крымский	3	299011, г. Севастополь, ул. Суворова, 39а
4	ВЛАДИКОМБАНК	2851	17.05.1994	Севастопольский	3	299040, Республика Крым, г. Севастополь, пр-т Генерала Острякова, 69а
5	ВНЕШПРОМБАНК	3261	3.07.1995	Астраханский	24	414004, г. Астрахань, Кировский р-н, ул. Ульяновых, 3а, литер Б
6	ГЕНБАНК	2490	13.09.1993	в г. Симферополе	3	295011, Республика Крым, г. Симферополь, ул. Севастопольская, 13
7	ДОНХЛЕББАНК	2285	30.03.1993	Санкт-Петербургский	5	191024, г. Санкт-Петербург, Центральный р-н, ул. Херсонская, 12-14, литер А
8	КРАЙИНВЕСТБАНК	3360	14.02.2001	“Крым”	1	295000, Республика Крым, г. Симферополь, ул. Долгоруковская/Жуковского/А.Невского, 1/1/6
9	КРАЙИНВЕСТБАНК	3360	14.02.2001	“Севастополь”	2	299011, г. Севастополь, ул. Одесская, 27б
10	КУБАНЬ КРЕДИТ	2518	28.09.1993	“Симферопольский”	1	295000, Республика Крым, г. Симферополь, ул. Пролетарская, 1а, литер А
11	МАСТ-БАНК	3267	18.08.1995	“Симферопольский”	9	295024, Республика Крым, г. Симферополь, ул. Севастопольская, 10
12	МАСТ-БАНК	3267	18.08.1995	“Пятигорский”	8	357501, Ставропольский край, г. Пятигорск, ул. Дзержинского, 101
13	РОССИЙСКИЙ КРЕДИТ	324	26.06.1990	в Приволжском федеральном округе	83	603006, г. Нижний Новгород, Нижегородский р-н, ул. Ошарская, 52
14	РОССИЙСКИЙ КРЕДИТ	324	26.06.1990	в Южном федеральном округе	84	400066, г. Волгоград, ул. Комсомольская, 4
15	РОССИЙСКИЙ НАЦИОНАЛЬНЫЙ КОММЕРЧЕСКИЙ БАНК	1354	25.01.1991	Таврический	11	Республика Крым, г. Симферополь, ул. Киевская, 55а
16	РОССИЯ	328	27.06.1990	Симферопольский	21	295000, Республика Крым, г. Симферополь, пр-т Кирова, 36
17	РОСТОВСКИЙ УНИВЕРСАЛЬНЫЙ	2813	29.04.1994	Филиал № 1	1	344082, г. Ростов-на-Дону, ул. М.Горького, 28/41
18	РУССКИЙ ФИНАНСОВЫЙ АЛЬЯНС	2035	26.08.1992	в г. Грозном	3	364051, Чеченская Республика, г. Грозный, пр-т Путина, 18а/87
19	СЕВЕРНЫЙ КРЕДИТ	2398	25.06.1993	Симферопольский	8	Республика Крым, г. Симферополь, ул. Карла Маркса, 47 / Галерейный пер., 4, пом. 16
20	ТЕМПБАНК	55	24.01.1989	“Петербургский”	11	191028, г. Санкт-Петербург, Литейный пр-т, 32, пом. 2Н, литер А
21	ТЕМПБАНК	55	24.01.1989	“Астраханский”	10	414040, г. Астрахань, Кировский р-н, ул. Марфинская / ул. Раскольникова, 7а/12, литер Жж
22	ФИА-БАНК	2542	25.10.1993	“Крымский”	5	295005, Республика Крым, г. Симферополь, ул. Севастопольская / ул. Сергеева-Ценского, 8/1
23	ФИНАНСОВЫЙ СТАНДАРТ	1053	3.12.1990	Севастополь	4	299011, г. Севастополь, пр-т Нахимова, 1
24	ФИНАНСОВЫЙ СТАНДАРТ	1053	3.12.1990	Новосибирский	3	630091, г. Новосибирск, Центральный р-н, ул. Ядринцевская, 23
25	ФОРБАНК	2063	9.09.1992	Сибирский	4	656056, г. Барнаул, ул. Гоголя, 36 / ул. М.Горького, 29

Список филиалов кредитных организаций, исключенных из Книги государственной регистрации кредитных организаций во II квартале 2014 г.

№ п/п	Наименование банка	Рег. № банка	Дата регистрации банка	Наименование филиала (место нахождения)	№ филиала	Место нахождения филиала**
1	АБСОЛЮТ БАНК	2306	22.04.1993	в г. Нижнем Новгороде	15	603115, г. Нижний Новгород, ул. Студеная, 68а
2	АБСОЛЮТ БАНК	2306	22.04.1993	в г. Казани	7	420111, Республика Татарстан, г. Казань, ул. Островского, 14
3	АБСОЛЮТ БАНК	2306	22.04.1993	в г. Ростове-на-Дону	11	344006, г. Ростов-на-Дону, Кировский р-н, ул. Максима Горького, 140/56
4	АВТОВАЗБАНК	23	16.11.1988	в г. Оренбурге	21	460000, г. Оренбург, ул. Челюскинцев, 16
5	АВТОГРАДБАНК	1455	26.04.1991	Челябинский	7	454007, Челябинская область, г. Челябинск, пр-т Ленина, 11б
6	АНТАЛБАНК	3115	10.10.1994	в г. Назрани	1	386102, Республика Ингушетия, г. Назрань, ул. Московская, 13а
7	АРТ-БАНК	2779	6.04.1994	в г. Москве	1	121165, г. Москва, ул. Киевская, 24
8	БАНК МОСКВЫ	2748	15.03.1994	Сочинский	33	354000, Краснодарский край, г. Сочи, ул. М.Горького, 15
9	ВКАБАНК	1027	29.11.1990	Советский	1	414057, г. Астрахань, пр-д Воробьева, 12
10	ВКАБАНК	1027	29.11.1990	Трусовский	3	414015, г. Астрахань, ул. Дзержинского, 56а
11	ВТБ 24	1623	18.11.1991	№ 7111	108	340041, г. Тула, ул. Демонстрации, 2г
12	ГАЗБАНК	2316	28.04.1993	в г. Ейске	2	353660, Краснодарский край, г. Ейск, ул. Ленина, 71
13	ГАЗПРОМБАНК	354	31.07.1990	в г. Ухте	18	169400, Республика Коми, г. Ухта, ул. 30 лет Октября, 25
14	ГАЗПРОМБАНК	354	31.07.1990	в г. Мурманске	43	183025, г. Мурманск, ул. Карла Маркса, 15
15	ГЕОБАНК	2027	27.08.1992	Нижегородский	1	603093, г. Нижний Новгород, ул. Родионова, 165, к. 9, пом. П5
16	ГЕОБАНК	2027	27.08.1992	Санкт-Петербургский	2	197374, г. Санкт-Петербург, ул. Беговая, 3, литер А
17	ГЛОБЭКС	1942	7.07.1992	“Северо-Западный”	15	191028, г. Санкт-Петербург, ул. Моховая, 18, литер Ж, пом. 2Н
18	ГУТА-БАНК	256	12.03.1990	в г. Воронеже	19	394030, г. Воронеж, ул. Кольцовская, 40
19	ДИАЛОГ-ОПТИМ*	3107	4.10.1994	“Тольяттинский”	13	445042, Самарская обл., г. Тольятти, ул. Свердлова, 22
20	ДИАЛОГ-ОПТИМ*	3107	4.10.1994	Липецкий	2	398600, г. Липецк, ул. Неделина, 1а
21	ДИАЛОГ-ОПТИМ*	3107	4.10.1994	Ижевский	4	426076, Удмуртская Республика, г. Ижевск, ул. Коммунаров, 202
22	ДИАЛОГ-ОПТИМ*	3107	4.10.1994	Ростовский	5	344006, г. Ростов-на-Дону, ул. Большая Садовая, 124д
23	ДИАЛОГ-ОПТИМ*	3107	4.10.1994	Ставропольский	6	355003, г. Ставрополь, ул. Ленина, 351
24	ДИАЛОГ-ОПТИМ*	3107	4.10.1994	Московский областной	1	143966, Московская обл., г. Реутов, ул. Новая, 14, корп. 2
25	ДИАЛОГ-ОПТИМ*	3107	4.10.1994	в г. Иркутске	7	664000, г. Иркутск, ул. Степана Разина, 27
26	ДИАЛОГ-ОПТИМ*	3107	4.10.1994	Омский	11	644010, г. Омск, ул. Ленина, 48
27	ДИАЛОГ-ОПТИМ*	3107	4.10.1994	“Оренбургский”	14	460021, Оренбургская обл., г. Оренбург, ул. 60 лет Октября, 26а
28	ДИАЛОГ-ОПТИМ*	3107	4.10.1994	“Воронежский”	15	394026, г. Воронеж, ул. Донбасская, 2
29	ДИАЛОГ-ОПТИМ*	3107	4.10.1994	“Волгоградский”	16	400026, г. Волгоград, пр-т Героев Сталинграда, 40
30	ДИАЛОГ-ОПТИМ*	3107	4.10.1994	“Нижегородский”	18	603016, г. Нижний Новгород, ул. Веденяпина, 1б

№ п/п	Наименование банка	Рег. № банка	Дата регистрации банка	Наименование филиала (место нахождения)	№ филиала	Место нахождения филиала**
31	ДИАЛОГ-ОПТИМ*	3107	4.10.1994	Мурманский	12	183039, г. Мурманск, ул. Книповича, 23
32	ДИАЛОГ-ОПТИМ*	3107	4.10.1994	Владимирский	10	600000, г. Владимир, ул. Кремлевская, 5а
33	ДИАЛОГ-ОПТИМ*	3107	4.10.1994	Уральский	9	620014, г. Екатеринбург, ул. Малышева, 29
34	ДИАЛОГ-ОПТИМ*	3107	4.10.1994	Калининградский	8	236039, г. Калининград, ул. Ореховая, 7-19
35	ДИАЛОГ-ОПТИМ*	3107	4.10.1994	Саратовский	17	410600, Саратовская обл., г. Саратов, ул. Советская, 20/28
36	ЗАУБЕР БАНК	1614	22.01.1992	в г. Санкт-Петербурге	3	197198, Санкт-Петербург, Большой пр-т П.С., 25/2, литер А, пом. 9Н
37	КБЦ	914	22.11.1990	МОСКОВСКИЙ	1	123557, г. Москва, Большой Тишинский пер., 8, стр. 1
38	КИТ ФИНАНС ИНВЕСТИЦИОННЫЙ БАНК*	1911	11.06.1992	в г. Москве	1	125009, г. Москва, ул. Большая Никитская, 17, стр. 2
39	ЛЕГИОН	3117	10.10.1994	в г. Невинномысске	10	357108, Ставропольский край, г. Невинномысск, б-р Мира, 16
40	ЛИПЕЦКИЙ ОБЛАСТНОЙ БАНК	1794	18.05.1992	в г. Москве	1	123317, г. Москва, Стрельбищенский пер., 5, стр. 1
41	МАХАЧКАЛИНСКИЙ ГОРОДСКОЙ БАНК	2866	1.06.1994	г. Махачкала	1	367002, Республика Дагестан, г. Махачкала, пр-т Гамидова, 35а
42	МОЙ БАНК. ИПОТЕКА	2436	26.07.1993	Новосибирский	5	630102, г. Новосибирск, ул. Обская, 2
43	МОСКОВСКИЙ ИНДУСТРИАЛЬНЫЙ БАНК	912	22.11.1990	“Московское областное региональное управление”	5	124460, г. Москва, Зеленоград, Панфиловский пр-т, 22
44	МОСУРАЛБАНК	2468	24.08.1993	Краснозаводский	2	141300, Московская обл., г. Сергиев Посад, ул. Шлякова, 2а
45	НАРОДНЫЙ БАНК	2249	18.01.1993	Краснодарский	4	350001, г. Краснодар, ул. Ставропольская, 62
46	НАЦИОНАЛЬНЫЙ РЕЗЕРВНЫЙ БАНК	2170	26.11.1992	“Воронеж”	2	394018, г. Воронеж, ул. Орджоникидзе, 36б
47	НОВОЕ ВРЕМЯ	3492	27.11.2008	в г. Санкт-Петербурге	2	196105, г. Санкт-Петербург, пр-т Юрия Гагарина, 1, литер А, пом. 19Н
48	РОСТ БАНК	2888	10.06.1994	в г. Архангельске	37	163000, г. Архангельск, ул. Поморская, 45
49	РУБЛЕВСКИЙ	2192	16.12.1992	Гостиный Двор	1	117846, г. Москва, ул. Вавилова, 69
50	РУССЛАВБАНК	1073	5.12.1990	Калужский	4	248000, г. Калуга, ул. Дзержинского, 43
51	РУССЛАВБАНК	1073	5.12.1990	Петрозаводский	6	185035, Республика Карелия, г. Петрозаводск, ул. Горького, 25
52	САММИТ БАНК	85	26.04.1989	в г. Москве	3	107076, г. Москва, Колодезный пер., 2а, стр. 1, пом. II
53	СКА-БАНК	1957	10.07.1992	Сафоновский	3	215500, Смоленская обл., г. Сафоново, ул. Кирова, 3
54	СКА-БАНК	1957	10.07.1992	Рославльский	6	216500, Смоленская обл., г. Рославль, ул. Карла Маркса, 3
55	СКБ-БАНК	705	2.11.1990	“Челябинский”	37	454091, Челябинская обл., г. Челябинск, ул. Свободы, 72
56	СОБИНБАНК	1317	29.12.1990	Калининградский	5	236029, г. Калининград, ул. Генерал-лейтенанта Озерова, 49
57	СОБИНБАНК	1317	29.12.1990	Королевский	13	141080, Московская обл., г. Королев, ул. Горького, 12а, пом. № XIII, XIV
58	СОВЕТСКИЙ	558	24.10.1990	“Судоходный”	7	163000, г. Архангельск, ул. Поморская, 49
59	СПИРИТБАНК	2053	8.09.1992	Донской	1	301770, Тульская обл., г. Донской, ул. Заводская, 17
60	СТРОЙКОМБАНК	3050	10.08.1994	Санкт-Петербургский	1	196191, г. Санкт-Петербург, пл. Конституции, 7, литер А
61	ТВЕРЬУНИВЕРСАЛБАНК	777	14.11.1990	в г. Москве	13	109390, г. Москва, ул. Люблинская, 14
62	ТРАНСПОРТНЫЙ ИНВЕСТИЦИОННЫЙ БАНК	3238	22.03.1995	“Развитие” в г. Махачкале	3	367002, Республика Дагестан, г. Махачкала, пр-т Петра I, 32

№ п/п	Наименование банка	Рег. № банка	Дата регистрации банка	Наименование филиала (место нахождения)	№ филиала	Место нахождения филиала**
63	ТЮМЕНЬАГРОПРОМБАНК	917	23.11.1990	в с. Ярково	24	626050, Тюменская обл., Ярковский р-н, с. Ярково, ул. Пионерская, 102а/1
64	ТЮМЕНЬАГРОПРОМБАНК	917	23.11.1990	в с. Мужи	21	629640, Тюменская обл., Ямало-Ненецкий автономный округ, Шурышкарский р-н, с. Мужи, ул. Комсомольская, 7
65	ТЮМЕНЬАГРОПРОМБАНК	917	23.11.1990	в с. Аксарка	20	629620, Тюменская обл., Ямало-Ненецкий автономный округ, Приуральский р-н, с. Аксарка, ул. Первомайская, 26
66	ТЮМЕНЬАГРОПРОМБАНК	917	23.11.1990	в с. Казанское	9	627420, Тюменская обл., Казанский р-н, с. Казанское, ул. Луначарского, 24а
67	ТЮМЕНЬАГРОПРОМБАНК	917	23.11.1990	в г. Ишиме	8	627750, Тюменская обл., г. Ишим, ул. Карякина, 25
68	ТЮМЕНЬАГРОПРОМБАНК	917	23.11.1990	в г. Заводоуковске	6	627144, Тюменская обл., г. Заводоуковск, ул. Шоссейная, 3/4
69	ТЮМЕНЬАГРОПРОМБАНК	917	23.11.1990	в р.п. Голышманово	5	627300, Тюменская обл., Голышмановский р-н, р.п. Голышманово, ул. Садовая, 74
70	ТЮМЕНЬАГРОПРОМБАНК	917	23.11.1990	в с. Абатское	1	627540, Тюменская обл., Абатский р-н, с. Абатское, ул. Зеленая, 35/1
71	ТЮМЕНЬАГРОПРОМБАНК	917	23.11.1990	в с. Бердюжье	3	627440, Тюменская обл., Бердюжский р-н, с. Бердюжье, ул. Кирова, 15
72	УРАЛСИБ	2275	28.01.1993	в г. Астрахани	53	414056, г. Астрахань, ул. Савушкина, № 25, литер А
73	УРАЛСИБ	2275	28.01.1993	в г. Нижневартовске	12	628606, Тюменская обл., Ханты-Мансийский автономный округ – Югра, г. Нижневартовск, ул. 60 лет Октября, 10б
74	ХАНТЫ-МАНСИЙСКИЙ БАНК	1971	27.07.1992	в г. Нефтеюганске	7	628309, Тюменская обл., Ханты-Мансийский автономный округ – Югра, г. Нефтеюганск, ул. Набережная, 1
75	ЭКОНОМБАНК	1319	29.12.1990	в г. Ртищево Саратовской обл.	12	412031, Саратовская обл., г. Ртищево, ул. Советская, 18/1
76	ЭКОНОМБАНК	1319	29.12.1990	в г. Энгельсе Саратовской обл.	4	413100, Саратовская обл., г. Энгельс, пл. Свободы, 22
77	ЭКОНОМБАНК	1319	29.12.1990	в г. Вольске Саратовской обл.	5	412900, Саратовская обл., г. Вольск, ул. Ленина, № 84
78	ЭКОНОМБАНК	1319	29.12.1990	в г. Балашове Саратовской обл.	6	412300, Саратовская обл., г. Балашов, ул. Гагарина, 144
79	ЭКОНОМБАНК	1319	29.12.1990	в р.п. Степное Саратовской обл.	7	413210, Саратовская обл., Советский р-н, р.п. Степное, ул. Карла Маркса, 21, пом. 1
80	ЭКОНОМБАНК	1319	29.12.1990	в г. Марксе Саратовской обл.	10	413090, Саратовская обл., г. Маркс, пр. Ленина, 51а
81	ЭКОНОМБАНК	1319	29.12.1990	в г. Балаково Саратовской обл.	11	413853, Саратовская обл., г. Балаково, ул. Титова, 2а
82	ЭКСПРЕСС-ВОЛГА	3085	6.09.1994	в г. Ульяновске	5	432011, г. Ульяновск, ул. Гончарова, 31/1
83	ЭЛЛИПС БАНК	1950	7.07.1992	“Золотое кольцо”	1	601483, Владимирская обл., г. Гороховец, ул. Ленина, 143
84	ЭЛЛИПС БАНК	1950	7.07.1992	“Северо-Западный региональный центр”	2	190000, г. Санкт-Петербург, Вознесенский пр-т, 21, литер А, пом. 2Н
85	ЭЛЛИПС БАНК	1950	7.07.1992	“Восток-Капитал”	4	603024, г. Нижний Новгород, ул. Ванеева, 4/45, пом. П7
86	ЭЛЬБИН	2267	29.01.1993	в с. Ботлих	16	368970, Республика Дагестан, Ботлихский р-н, с. Ботлих

* Банки, по которым внесена запись в Книгу государственной регистрации кредитных организаций о ликвидации.

** Из Устава кредитной организации.

Кредитные организации, открывшие представительства на территории Российской Федерации и за рубежом во II квартале 2014 г.

№ п/п	Наименование КО	Рег. № КО	Дата регистрации КО	Наименование представительства	Место нахождения представительства
1	ФИНАНСОВЫЙ СТАНДАРТ	1053	3.12.1990	Крымское	295017, Республика Крым, г. Симферополь, ул. Фрунзе, 8
2	ЗАРЕЧЬЕ	817	16.11.1990	в г. Ялте	298600, Республика Крым, г. Ялта, ул. Свердлова, 3
3	РОССИЯ	328	27.06.1990	в Республике Крым	Республика Крым, г. Симферополь, ул. Турецкая, 12
4	ТРАСТОВЫЙ РЕСПУБЛИКАНСКИЙ БАНК	3404	11.04.2002	в г. Севастополе	299011, г. Севастополь, ул. Большая Морская, 35 / ул. Суворова, 39, комплекс встроенных нежилых помещений № 2, состоящий из помещений первого этажа с I-1 по I-5

Кредитные организации, реорганизованные в форме преобразования во II квартале 2014 г.

(информация подготовлена на основании сведений, поступивших из уполномоченного регистрирующего органа на отчетную дату)

Нет

Кредитные организации, имеющие лицензию на привлечение во вклады денежных средств физических лиц в рублях и получившие право расширить свою деятельность на основе получения лицензии Банка России на привлечение во вклады денежных средств физических лиц в иностранной валюте во II квартале 2014 г.

Нет

28 июля 2014 года № ОД-1922

ПРИКАЗ
Об уточнении персонального состава временной администрации по управлению кредитной организацией общество с ограниченной ответственностью "БАНК ФИНИНВЕСТ" ООО "БАНК ФИНИНВЕСТ" (г. Санкт-Петербург)

В связи с производственной необходимостью и в дополнение к приказу Банка России от 07.07.2014 № ОД-1658 "О назначении временной администрации по управлению кредитной организацией общество с ограниченной ответственностью "БАНК ФИНИНВЕСТ" ООО "БАНК ФИНИНВЕСТ" (г. Санкт-Петербург) в связи с отзывом лицензии на осуществление банковских операций"

ПРИКАЗЫВАЮ:

1. Вывести с 29 июля 2014 года из состава временной администрации по управлению кредитной организацией общество с ограниченной ответственностью "БАНК ФИНИНВЕСТ" Мишина Антона Владимировича — эксперта 1 категории сектора технической защиты информации отдела безопасности и защиты информации Отделения 1 Москва.

2. Руководителям территориальных учреждений Банка России довести в установленном порядке содержание настоящего приказа до сведения всех кредитных организаций, расположенных на подведомственной территории, в срок не позднее рабочего дня, следующего за днем его получения.

3. Пресс-службе Банка России (Граник А.В.) опубликовать настоящий приказ в "Вестнике Банка России" в десятидневный срок с момента принятия и дать для средств массовой информации соответствующее сообщение.

И.О. ПРЕДСЕДАТЕЛЯ ЦЕНТРАЛЬНОГО БАНКА
РОССИЙСКОЙ ФЕДЕРАЦИИ Г.И. ЛУНТОВСКИЙ

28 июля 2014 года № ОД-1923

ПРИКАЗ
Об уточнении персонального состава временной администрации по управлению кредитной организацией Банк "Навигатор" (открытое акционерное общество) Банк "Навигатор" (ОАО) (г. Москва)

В связи с производственной необходимостью и в дополнение к приказу Банка России от 13.05.2014 № ОД-998 "О назначении временной администрации по управлению кредитной организацией Банк "Навигатор" (открытое акционерное общество) Банк "Навигатор" (ОАО) (г. Москва) в связи с отзывом лицензии на осуществление банковских операций"

ПРИКАЗЫВАЮ:

1. Вывести с 29 июля 2014 года из состава временной администрации по управлению кредитной организацией Банк "Навигатор" (открытое акционерное общество) Скибко Людмилу Глебовну — главного экономиста отдела отчетности кредитных организаций Управления надзора за деятельностью кредитных организаций ГУ Банка России по Оренбургской области и Богданову Ларису Евгеньевну — ведущего юрисконсульта Юридического отдела ГУ Банка России по Иркутской области.

2. Руководителям территориальных учреждений Банка России довести в установленном порядке содержание настоящего приказа до сведения всех кредитных организаций, расположенных на подведомственной территории, в срок не позднее рабочего дня, следующего за днем его получения.

3. Пресс-службе Банка России (Граник А.В.) опубликовать настоящий приказ в "Вестнике Банка России" в десятидневный срок с момента принятия и дать для средств массовой информации соответствующее сообщение.

И.О. ПРЕДСЕДАТЕЛЯ ЦЕНТРАЛЬНОГО БАНКА
РОССИЙСКОЙ ФЕДЕРАЦИИ Г.И. ЛУНТОВСКИЙ

28 июля 2014 года № ОД-1924

ПРИКАЗ
Об уточнении персонального состава временной администрации по управлению кредитной организацией Открытое Акционерное общество "ЕВРОСИБ БАНК" ОАО "ЕВРОСИБ БАНК" (г. Санкт-Петербург)

В связи с производственной необходимостью и в дополнение к приказу Банка России от 07.07.2014 № ОД-1660 "О назначении временной администрации по управлению кредитной организацией Открытое Акционерное общество "ЕВРОСИБ БАНК" ОАО "ЕВРОСИБ БАНК" (г. Санкт-Петербург) в связи с отзывом лицензии на осуществление банковских операций"

ПРИКАЗЫВАЮ:

1. Вывести с 29 июля 2014 года из состава временной администрации по управлению кредитной организацией Открытое Акционерное общество "ЕВРОСИБ БАНК" Мишина Антона Владимировича — эксперта 1 категории сектора технической защиты информации отдела безопасности и защиты информации Отделения 1 Москва.

2. Руководителям территориальных учреждений Банка России довести в установленном порядке содержание настоящего приказа до сведения всех кредитных организаций, расположенных на подведомственной территории, в срок не позднее рабочего дня, следующего за днем его получения.

3. Пресс-службе Банка России (Граник А.В.) опубликовать настоящий приказ в "Вестнике Банка России" в десятидневный срок с момента принятия и дать для средств массовой информации соответствующее сообщение.

И.О. ПРЕДСЕДАТЕЛЯ ЦЕНТРАЛЬНОГО БАНКА
РОССИЙСКОЙ ФЕДЕРАЦИИ Г.И. ЛУНТОВСКИЙ

28 июля 2014 года № ОД-1925

ПРИКАЗ
Об уточнении персонального состава временной администрации по управлению кредитной организацией Открытое акционерное общество Банк "Западный" ОАО Банк "Западный" (г. Москва)

В связи с производственной необходимостью и в дополнение к приказу Банка России от 21.04.2014 № ОД-767 "О назначении временной администрации по управлению кредитной организацией Открытое акционерное общество Банк "Западный" ОАО Банк "Западный" (г. Москва) в связи с отзывом лицензии на осуществление банковских операций"

ПРИКАЗЫВАЮ:

1. Вывести с 29 июля 2014 года из состава временной администрации по управлению кредитной организацией Открытое акционерное общество Банк "Западный" Ходакову Татьяну Алексеевну — ведущего экономиста Отдела по надзору за деятельностью кредитных организаций ГУ Банка России по Новгородской области, Шаленко Ирину Михайловну — юрисконсульта 1 категории Юридического сектора ГУ Банка России по Томской области, Сергееву Светлану Ивановну — ведущего экономиста Отдела лицензирования деятельности кредитных организаций и контроля за операциями на рынке ценных бумаг ГУ Банка России по Алтайскому краю, Липай Юлию Анатольевну — экономиста 1 категории экономического отдела ГРКЦ ГУ Банка России по Свердловской области, Новоселову Татьяну Викторовну — бухгалтера 1 категории сектора обслуживания клиентов Отдела бухгалтерского учета и расчетов РКЦ Единый в г. Екатеринбург ГУ Банка России по Свердловской области, Зайцеву Анну Анатольевну — ведущего экономиста сектора межбанковских расчетов отдела бухгалтерского учета и отчетности Отделения Тамбов, Добронравова Дмитрия Сергеевича — ведущего экономиста сектора рефинансирования кредитных организаций сводно-экономического отдела Отделения Тамбов, Стефанову Елену Борисовну — ведущего экономиста отдела банковского надзора Отделения Тверь, Бахтилова Вячеслава Александровича — ведущего экономиста сектора мониторинга банковской деятельности, финансовых рынков и валютного контроля Отделения Тверь, Сычеву Елену Владимировну — ведущего экономиста отдела банковского надзора Отделения Тамбов и Балагову Анну Викторовну — ведущего экономиста экономического аппарата РКЦ г. Пятигорск ГУ Банка России по Ставропольскому краю.

2. Ввести с 29 июля 2014 года в состав временной администрации по управлению кредитной организацией Открытое акционерное общество Банк “Западный” Певневу Евгению Анатольевну — главного экономиста Отдела лицензирования деятельности кредитных организаций и контроля за операциями на рынке ценных бумаг ГУ Банка России по Алтайскому краю.

3. Руководителям территориальных учреждений Банка России довести в установленном порядке содержание настоящего приказа до сведения всех кредитных организаций, расположенных на подведомственной территории, в срок не позднее рабочего дня, следующего за днем его получения.

4. Пресс-службе Банка России (Граник А.В.) опубликовать настоящий приказ в “Вестнике Банка России” в десятидневный срок с момента принятия и дать для средств массовой информации соответствующее сообщение.

И.О. ПРЕДСЕДАТЕЛЯ ЦЕНТРАЛЬНОГО БАНКА
РОССИЙСКОЙ ФЕДЕРАЦИИ Г.И. ЛУНТОВСКИЙ

СООБЩЕНИЕ
об исключении АБ “Сир” (ОАО) из реестра банков — участников системы обязательного страхования вкладов

Государственная корпорация “Агентство по страхованию вкладов” сообщает, что в связи с отзывом у Акционерного Банка “Сир” (открытое акционерное общество) АБ “Сир” (ОАО) (регистрационный номер по Книге государственной регистрации кредитных организаций 1904, номер по реестру банков — участников системы обязательного страхования вкладов 585) лицензии Банка России и завершением Агентством процедуры выплаты возмещения по вкладам Правление Агентства приняло решение (от 25.07.2014 протокол № 84) об исключении указанного банка из реестра банков — участников системы обязательного страхования вкладов с 08.07.2014 на основании информации Банка России от 23.07.2014 № 33-3-16/6743 о государственной регистрации банка в связи с его ликвидацией на основании решения суда (запись в Едином государственном реестре юридических лиц от 08.07.2014 № 2141400006724).

29 июля 2014 года № ОД-1947

ПРИКАЗ
О приостановлении действия лицензии на осуществление посреднической деятельности в качестве страхового брокера Общества с ограниченной ответственностью “Страховой брокер “Пересвет”

В связи с уклонением Общества с ограниченной ответственностью “Страховой брокер “Пересвет” от получения предписания Банка России от 14.04.2014 № 015-53-3/2670, на основании пункта 4 статьи 32.6 Закона Российской Федерации от 27.11.1992 № 4015-1 “Об организации страхового дела в Российской Федерации”, в соответствии с Федеральным законом от 10.07.2002 № 86-ФЗ “О Центральном банке Российской Федерации (Банке России)”

ПРИКАЗЫВАЮ:

1. Приостановить до устранения выявленных нарушений действие лицензии от 20.09.2011 СБ-Ю № 4258 77 на осуществление посреднической деятельности в качестве страхового брокера Общества с ограниченной ответственностью “Страховой брокер “Пересвет” (регистрационный номер по единому государственному реестру субъектов страхового дела 4258; место нахождения: 109156, г. Москва, ул. Генерала Кузнецова, д. 18, корп. 2, пом. XXIII; ИНН 7721731190; ОГРН 1117746587298).

2. Установить срок для устранения выявленных нарушений 10 календарных дней с даты вступления настоящего приказа в силу.

3. Пресс-службе Банка России (Граник А.В.) опубликовать настоящий приказ в “Вестнике Банка России” в течение 10 рабочих дней со дня его принятия и дать для средств массовой информации соответствующее сообщение.

ПЕРВЫЙ ЗАМЕСТИТЕЛЬ ПРЕДСЕДАТЕЛЯ
ЦЕНТРАЛЬНОГО БАНКА РОССИЙСКОЙ ФЕДЕРАЦИИ С.А. ШВЕЦОВ

СООБЩЕНИЕ
об итогах проведения кредитного аукциона по предоставлению кредитов, обеспеченных нерыночными активами, по плавающей процентной ставке

Центральный банк Российской Федерации 28 июля 2014 года провел кредитный аукцион по предоставлению кредитов, обеспеченных нерыночными активами, по плавающей процентной ставке на следующих условиях:

срок предоставления денежных средств — 12 месяцев (дата предоставления кредита Банка России — 30 июля 2014 года, дата погашения — 29 июля 2015 года). Способ проведения аукциона — голландский. Максимальный объем предоставляемых денежных средств — 500,0 млрд. рублей.

В кредитном аукционе приняли участие 17 кредитных организаций из 12 регионов России. На кредитный аукцион были поданы заявки с предложением процентных ставок в диапазоне от 8,25 до 10,25% годовых. Объем спроса на кредитном аукционе составил 495,0 млрд. рублей.

По итогам кредитного аукциона установлена ставка отсечения в размере 8,25% годовых.

Процентная ставка, по которой удовлетворяются заявки, — 8,25% годовых.

Объем предоставленных денежных средств по итогам кредитного аукциона — 495,0 млрд. рублей.

Аукцион проведен в соответствии со ст. 46 Федерального закона от 10.07.2002 № 86-ФЗ “О Центральном банке Российской Федерации (Банке России)” и Положением Банка России от 12 ноября 2007 года № 312-П “О порядке предоставления Банком России кредитным организациям кредитов, обеспеченных активами или поручительствами”.

28.07.2014

Зарегистрировано
Министерством юстиции
Российской Федерации
25 июля 2014 года
Регистрационный № 33282

20 июня 2014 года № 3289-У

УКАЗАНИЕ

О требованиях к порядку учета денежных требований, являющихся предметом залога по облигациям, и денежных сумм, зачисленных на залоговый счет

Настоящее Указание в соответствии со статьей 40^{1} Федерального закона "О банках и банковской деятельности" (в редакции Федерального закона от 3 февраля 1996 года № 17-ФЗ) (Ведомости Съезда народных депутатов РСФСР и Верховного Совета РСФСР, 1990, № 27, ст. 357; Собрание законодательства Российской Федерации, 1996, № 6, ст. 492; 1998, № 31, ст. 3829; 1999, № 28, ст. 3459, ст. 3469; 2001, № 26, ст. 2586; № 33, ст. 3424; 2002, № 12, ст. 1093; 2003, № 27, ст. 2700; № 50, ст. 4855; № 52, ст. 5033, ст. 5037; 2004, № 27, ст. 2711; № 31, ст. 3233; 2005, № 1, ст. 18, ст. 45; № 30, ст. 3117; 2006, № 6, ст. 636; № 19, ст. 2061; № 31, ст. 3439; № 52, ст. 5497; 2007, № 1, ст. 9; № 22, ст. 2563; № 31, ст. 4011; № 41, ст. 4845; № 45, ст. 5425; № 50, ст. 6238; 2008, № 10, ст. 895; 2009, № 1, ст. 23; № 9, ст. 1043; № 18, ст. 2153; № 23, ст. 2776; № 30, ст. 3739; № 48, ст. 5731; № 52, ст. 6428; 2010, № 8, ст. 775; № 27, ст. 3432; № 30, ст. 4012; № 31, ст. 4193; № 47, ст. 6028; 2011, № 7, ст. 905; № 27, ст. 3873, ст. 3880; № 29, ст. 4291; № 48, ст. 6728, ст. 6730; № 49, ст. 7069; № 50, ст. 7351; 2012, № 27, ст. 3588; № 31, ст. 4333; № 50, ст. 6954; № 53, ст. 7605, ст. 7607; 2013, № 11, ст. 1076; № 19, ст. 2317, ст. 2329; № 26, ст. 3207; № 27, ст. 3438, ст. 3477; № 30, ст. 4084; № 40, ст. 5036; № 49, ст. 6336; № 51, ст. 6683, ст. 6699; 2014, № 6, ст. 563; № 19, ст. 2311, ст. 2317), пунктами 8 и 9 статьи 27^{3-1} Федерального закона от 22 апреля 1996 года № 39-ФЗ "О рынке ценных бумаг" (Собрание законодательства Российской Федерации, 1996, № 17, ст. 1918; 2001, № 33, ст. 3424; 2002, № 52, ст. 5141; 2004, № 27, ст. 2711; № 31, ст. 3225; 2005, № 11, ст. 900; № 25, ст. 2426; 2006, № 1, ст. 5; № 2, ст. 172; № 17, ст. 1780; № 31, ст. 3437; № 43, ст. 4412; 2007, № 1, ст. 45; № 18, ст. 2117; № 22, ст. 2563; № 41, ст. 4845; № 50, ст. 6247, ст. 6249; 2008, № 52, ст. 6221; 2009, № 1, ст. 28; № 18, ст. 2154; № 23, ст. 2770; № 29, ст. 3642; № 48, ст. 5731; № 52, ст. 6428; 2010, № 17, ст. 1988; № 31, ст. 4193; № 41, ст. 5193; 2011, № 7, ст. 905; № 23, ст. 3262; № 27, ст. 3880; № 29, ст. 4291; № 48, ст. 6728; № 49, ст. 7040; № 50, ст. 7357; 2012, № 25, ст. 3269; № 31, ст. 4334; № 53, ст. 7607; 2013, № 26, ст. 3207; № 30, ст. 4043, ст. 4082, ст. 4084; № 51, ст. 6699; № 52, ст. 6985) устанавливает требования к порядку учета денежных требований, являющихся предметом залога по облигациям, обеспеченным залогом таких денежных требований (далее — облигации), и к порядку учета денежных сумм, зачисленных на залоговый счет.

1. Учет денежных требований, являющихся предметом залога по облигациям, осуществляется:

лицом, в том числе кредитной организацией, которое, не являясь кредитором по указанным денежным требованиям, на основании договора с эмитентом облигаций осуществляет получение и перевод поступивших от должников денежных средств и (или) осуществляет иные права кредиторов (далее — обслуживающая организация);

эмитентом облигаций;

кредитной организацией, в которой открыт залоговый счет эмитента.

2. Учет денежных требований, являющихся предметом залога по облигациям, осуществляется путем ведения реестра. В реестре должны содержаться следующие сведения о денежных требованиях, являющихся предметом залога по облигациям.

2.1. Вид договора (основания для предъявления требований к должникам об уплате денежных средств по кредитным договорам, договорам займа и (или) иным обязательствам, включая права, которые возникнут в будущем из существующих или из будущих обязательств) (далее — договор).

2.2. Обеспечение, предоставленное по денежному требованию, если такое обеспечение предоставляется.

2.3. Информация, позволяющая идентифицировать денежные требования (в том числе номер договора, дата заключения договора).

2.4. Основная сумма долга либо иные сведения, позволяющие определить основную сумму долга, а также процентная ставка или правила ее определения в соответствии с условиями договора.

2.5. Дата приобретения денежного требования эмитентом.

2.6. Срок уплаты суммы требования или, если эта сумма подлежит уплате по частям, сроки (периодичность) соответствующих платежей и размер каждого из них либо

условия, позволяющие определить эти сроки и размеры платежей.

2.7. Сведения о нарушениях сроков исполнения обязательств, включая дату возникновения и количество дней каждого нарушения.

2.8. Сумма (размер) неисполненного обязательства, в том числе основная сумма долга и размер процентов, которые должны быть уплачены.

2.9. Сведения об учете залога прав денежного требования путем регистрации уведомлений о залоге.

2.10. Иные сведения, предусмотренные решением о выпуске облигаций.

3. В реестре, ведение которого осуществляется обслуживающей организацией, в том числе являющейся кредитной организацией, в которой открыт залоговый счет эмитента, помимо сведений, указанных в пункте 2 настоящего Указания, должны содержаться следующие сведения об эмитенте и выпуске (дополнительном выпуске) облигаций:

полное и сокращенное фирменные наименования эмитента в соответствии с его учредительными документами;

основной государственный регистрационный номер и дата государственной регистрации эмитента, наименование органа, осуществившего государственную регистрацию эмитента;

идентификационный номер налогоплательщика эмитента;

дата выдачи и номер лицензии, в случае если ее наличие является условием осуществления соответствующего вида деятельности;

государственный регистрационный номер выпуска эмиссионных ценных бумаг и дата государственной регистрации, а в случае если выпуск (дополнительный выпуск) эмиссионных ценных бумаг не подлежит государственной регистрации, — идентификационный номер и дата его присвоения.

Если на дату утверждения решения о выпуске (дополнительном выпуске) облигаций денежные требования, являющиеся предметом залога по облигациям, еще не перешли от предшествующего кредитора к эмитенту, в реестре должны также содержаться сведения о предшествующем кредиторе, предусмотренные абзацами вторым—пятым настоящего пункта.

4. Если ведение реестра осуществляется обслуживающей организацией, не являющейся кредитной организацией, в которой открыт залоговый счет эмитента, эмитент ведет учет денежных требований, являющихся предметом залога по облигациям, отражающий сведения, указанные в подпунктах 2.1, 2.5 и 2.7 пункта 2 настоящего Указания.

5. Внесение сведений в реестр осуществляется не позднее рабочего дня, следующего за днем их получения.

6. Эмитент ведет учет зачисленных на залоговый счет денежных сумм, если ведение такого учета не было поручено кредитной организации, в которой открыт залоговый счет эмитента.

7. Эмитент вправе поручить ведение учета денежных требований, являющихся предметом залога по облигациям, и денежных сумм, зачисленных на залоговый счет эмитента, кредитной организации, в которой открыт залоговый счет эмитента. Кредитная организация, которой эмитентом поручено ведение учета денежных требований, осуществляет такой учет в соответствии с пунктом 3 настоящего Указания.

8. Реестр и учет зачисленных на залоговый счет эмитента денежных сумм, а также учет денежных требований в соответствии с пунктом 4 настоящего Указания ведутся на электронных носителях при условии обеспечения возможности предоставления содержащихся в реестре сведений или сведений об учитываемых денежных средствах (денежных требованиях) на бумажных носителях. При этом организация, ведущая реестр и (или) учет, обеспечивает хранение и защиту всех сведений, внесенных в реестр, или сведений об учитываемых денежных средствах (денежных требованиях), в том числе путем обязательного создания резервной копии не реже одного раза в месяц.

9. Программно-технические средства, предназначенные для ведения реестра и учета денежных требований в соответствии с пунктом 4 настоящего Указания, должны позволять формировать документы, содержащие внесенные сведения обо всех или об отдельных денежных требованиях, на любой момент или за любой период времени.

10. Программно-технические средства, предназначенные для учета зачисленных на залоговый счет эмитента денежных сумм, должны позволять формировать документы, содержащие сведения обо всех или об отдельных поступивших денежных суммах, на любой момент или за любой период времени.

11. Настоящее Указание вступает в силу по истечении 10 дней после дня его официального опубликования в “Вестнике Банка России”.

ПРЕДСЕДАТЕЛЬ
ЦЕНТРАЛЬНОГО
БАНКА
РОССИЙСКОЙ
ФЕДЕРАЦИИ Э.С. НАБИУЛЛИНА

Зарегистрировано
Министерством юстиции
Российской Федерации
22 июля 2014 года
Регистрационный № 33196

25 июня 2014 года № 3294-У

УКАЗАНИЕ

О порядке применения к операторам платежных систем штрафов, предусмотренных статьями 82^4, 82^5 Федерального закона от 10 июля 2002 года № 86-ФЗ "О Центральном банке Российской Федерации (Банке России)"

На основании статей 82^4 и 82^5 Федерального закона от 10 июля 2002 года № 86-ФЗ "О Центральном банке Российской Федерации (Банке России)" (Собрание законодательства Российской Федерации, 2002, № 28, ст. 2790; 2003, № 2, ст. 157; № 52, ст. 5032; 2004, № 27, ст. 2711; № 31, ст. 3233; 2005, № 25, ст. 2426; № 30, ст. 3101; 2006, № 19, ст. 2061; № 25, ст. 2648; 2007, № 1, ст. 9, ст. 10; № 10, ст. 1151; № 18, ст. 2117; 2008, № 42, ст. 4696, ст. 4699; № 44, ст. 4982; № 52, ст. 6229, ст. 6231; 2009, № 1, ст. 25; № 29, ст. 3629; № 48, ст. 5731; 2010, № 45, ст. 5756; 2011, № 7, ст. 907; № 27, ст. 3873; № 43, ст. 5973; № 48, ст. 6728; 2012, № 50, ст. 6954; № 53, ст. 7591, ст. 7607; 2013, № 11, ст. 1076; № 14, ст. 1649; № 19, ст. 2329; № 27, ст. 3438, ст. 3476, ст. 3477; № 30, ст. 4084; № 49, ст. 6336; № 51, ст. 6695, ст. 6699, № 52, ст. 6975; 2014, № 19, ст. 2311, ст. 2317) (далее — Федеральный закон "О Центральном банке Российской Федерации (Банке России)") настоящее Указание устанавливает порядок применения Банком России к операторам платежных систем штрафов, предусмотренных статьями 82^4, 82^5 Федерального закона "О Центральном банке Российской Федерации (Банке России)" (далее при совместном упоминании — штрафы).

1. Штрафы применяются к операторам платежных систем по основаниям, предусмотренным статьями 82^4, 82^5 Федерального закона "О Центральном банке Российской Федерации (Банке России)".

2. Решение о взыскании штрафов с операторов платежных систем принимается Председателем Банка России, его заместителем, курирующим структурное подразделение Банка России, осуществляющее функции надзора за операторами платежных систем, руководителем территориального учреждения Банка России, осуществляющего надзор за операторами платежных систем, или лицами, их замещающими.

3. Штраф, предусмотренный статьей 82^4 Федерального закона "О Центральном банке Российской Федерации (Банке России)", взыскивается с оператора платежной системы за каждый день приостановления (прекращения) в одностороннем порядке оказания услуг платежной инфраструктуры участнику (участникам) платежной системы и его (их) клиентам в размере, не превышающем величину, предусмотренную статьей 82^4 Федерального закона "О Центральном банке Российской Федерации (Банке России)".

4. Штраф, предусмотренный статьей 82^5 Федерального закона "О Центральном банке Российской Федерации (Банке России)", взыскивается с оператора платежной системы, не являющейся национально значимой платежной системой, в размере невнесенного обеспечительного взноса либо внесенного не в полном размере обеспечительного взноса в сумме недоплаты.

5. Требования об уплате штрафов оформляются предписаниями Банка России, в которых указываются: фамилия, имя, отчество (Ф.И.О.) должностного лица Банка России, принявшего решение о взыскании штрафа за приостановление (прекращение) в одностороннем порядке оказания услуг платежной инфраструктуры участнику (участникам) платежной системы и его (их) клиентам, взыскании штрафа за невнесение, внесение не в полном размере обеспечительного взноса операторами платежных систем, не являющихся национально значимыми платежными системами; полное наименование и регистрационный номер оператора платежной системы, выявленные нарушения, являющиеся основанием для взыскания штрафа, со ссылкой на соответствующие федеральные законы и принятые в соответствии с ними нормативные акты Банка России; требование об уплате штрафа, сумма штрафа, дата (даты) приостановления (прекращения) в одностороннем порядке оказания услуг платежной инфраструктуры участнику (участникам) платежной системы и его (их) клиентам, срок для уплаты штрафа, реквизиты счета для уплаты штрафа.

6. Предписание Банка России направляется оператору платежной системы, допустившему нарушение, в срок, не превышающий два месяца с момента выявления нарушения.

7. Взыскание штрафа, предусмотренного статьей 82^4 Федерального закона "О Цен-

тральном банке Российской Федерации (Банке России)", с оператора платежной системы, не являющейся национально значимой платежной системой, осуществляется посредством списания денежных средств со специального счета по учету обеспечительного взноса оператора платежной системы, открытого в Банке России, на основании инкассового поручения, составленного Банком России в соответствии с Положением Банка России от 19 июня 2012 года № 383-П "О правилах осуществления перевода денежных средств", зарегистрированного Министерством юстиции Российской Федерации 22 июня 2012 года № 24667, 14 августа 2013 года № 29387, 19 мая 2014 года № 32323 ("Вестник Банка России" от 28 июня 2012 года № 34, от 28 августа 2013 года № 47, от 28 мая 2014 года № 46), с учетом следующих особенностей:

в реквизите "Плательщик" указывается полное или сокращенное наименование оператора платежной системы;

в реквизите "Сч. №" плательщика указывается номер специального счета по учету обеспечительного взноса оператора платежной системы, не являющейся национально значимой платежной системой, открытого в подразделении Банка России;

в реквизите "Назначение платежа" указываются сведения о предписании Банка России, на основании которого осуществляется уплата штрафа.

8. Штрафы, взысканные в соответствии с настоящим Указанием, уплачиваются (зачисляются) в бюджетную систему Российской Федерации.

9. С оператора платежной системы, не являющейся национально значимой платежной системой, штраф, предусмотренный статьей 82^4 Федерального закона "О Центральном банке Российской Федерации (Банке России)", взыскивается за период после дня, следующего за днем, в который оператор платежной системы, не являющейся национально значимой платежной системой, должен внести на счет по учету обеспечительного взноса сумму первого ежеквартального отчисления для формирования обеспечительного взноса в соответствии с Положением Банка России от 12 июня 2014 года № 423-П "Об обеспечительных взносах операторов платежных систем, не являющихся национально значимыми платежными системами", зарегистрированным Министерством юстиции Российской Федерации 20 июня 2014 года № 32820 ("Вестник Банка России" от 26 июня 2014 года № 60).

10. Настоящее Указание вступает в силу по истечении 10 дней после дня его официального опубликования в "Вестнике Банка России".

ПРЕДСЕДАТЕЛЬ
ЦЕНТРАЛЬНОГО
БАНКА
РОССИЙСКОЙ
ФЕДЕРАЦИИ Э.С. НАБИУЛЛИНА

25 июля 2014 года № 3341-У

УКАЗАНИЕ
О признании инфраструктурных организаций финансового рынка системно значимыми

Настоящее Указание на основании Федерального закона от 10 июля 2002 года № 86-ФЗ “О Центральном банке Российской Федерации (Банке России)” (Собрание законодательства Российской Федерации, 2002, № 28, ст. 2790; 2003, № 2, ст. 157; № 52, ст. 5032; 2004, № 27, ст. 2711; № 31, ст. 3233; 2005, № 25, ст. 2426; № 30, ст. 3101; 2006, № 19, ст. 2061; № 25, ст. 2648; 2007, № 1, ст. 9, ст. 10; № 10, ст. 1151; № 18, ст. 2117; 2008, № 42, ст. 4696, ст. 4699; № 44, ст. 4982; № 52, ст. 6229, ст. 6231; 2009, № 1, ст. 25; № 29, ст. 3629; № 48, ст. 5731; 2010, № 45, ст. 5756; 2011, № 7, ст. 907; № 27, ст. 3873; № 43, ст. 5973; № 48, ст. 6728; 2012, № 50, ст. 6954; № 53, ст. 7591, ст. 7607; 2013, № 11, ст. 1076; № 14, ст. 1649; № 19, ст. 2329; № 27, ст. 3438, ст. 3476, ст. 3477; № 30, ст. 4084; № 49, ст. 6336; № 51, ст. 6695, ст. 6699; № 52, ст. 6975; 2014, № 19, ст. 2311, ст. 2317) устанавливает порядок признания Банком России инфраструктурных организаций финансового рынка (далее — ИОФР) системно значимыми.

1. Для целей настоящего Указания к ИОФР относятся следующие организации:

центральный контрагент;

центральный депозитарий;

расчетный депозитарий;

саморегулируемая организация, клиринговая организация или биржа, осуществляющие ведение реестра договоров, предусмотренных пунктом 6 статьи 51^5 Федерального закона от 22 апреля 1996 года № 39-ФЗ “О рынке ценных бумаг” (Собрание законодательства Российской Федерации, 1996, № 17, ст. 1918; 2001, № 33, ст. 3424; 2002, № 52, ст. 5141; 2004, № 27, ст. 2711; № 31, ст. 3225; 2005, № 11, ст. 900; № 25, ст. 2426; 2006, № 1, ст. 5; № 2, ст. 172; № 17, ст. 1780; № 31, ст. 3437; № 43, ст. 4412; 2007, № 1, ст. 45; № 18, ст. 2117; № 22, ст. 2563; № 41, ст. 4845; № 50, ст. 6247, ст. 6249; 2008, № 44, ст. 4982; № 52, ст. 6221; 2009, № 1, ст. 28; № 18, ст. 2154; № 23, ст. 2770; № 29, ст. 3642; № 48, ст. 5731; № 52, ст. 6428; 2010, № 17, ст. 1988; № 31, ст. 4193; № 41, ст. 5193; 2011, № 7, ст. 905; № 23, ст. 3262; № 27, ст. 3880; № 29, ст. 4291; № 48, ст. 6728; № 49, ст. 7040; № 50, ст. 7357; 2012, № 25, ст. 3269; № 31, ст. 4334; № 53, ст. 7607; 2013, № 26, ст. 3207; № 30, ст. 4043, ст. 4082, ст. 4084; № 51, ст. 6699; № 52, ст. 6985) (далее — репозитарий).

2. Признание ИОФР системно значимой осуществляется на основании информации, подтверждающей ее соответствие критериям признания инфраструктурных организаций финансового рынка системно значимыми, установленным в приложении к настоящему Указанию (далее — критерии).

3. Соответствие ИОФР критериям определяется Департаментом финансовой стабильности Банка России раз в календарный квартал на основании данных форм отчетности ИОФР, указанных в приложении к настоящему Указанию, а также информации, полученной от ИОФР по запросам Банка России.

4. В случае соответствия ИОФР хотя бы одному из критериев Департамент финансовой стабильности Банка России с участием Департамента рынка ценных бумаг и товарного рынка Банка России в течение 10 рабочих дней с даты установления факта соответствия подготавливает докладную записку о признании ИОФР системно значимой, содержащую обоснование признания ИОФР соответствующей критерию (критериям), и представляет ее для рассмотрения и принятия решения Председателю Банка России или лицу, его замещающему.

Решение о признании ИОФР системно значимой оформляется приказом Банка России, подписываемым Председателем Банка России или лицом, его замещающим (далее — приказ Банка России).

ИОФР признается системно значимой с даты подписания соответствующего приказа Банка России.

4.1. При принятии решения о признании ИОФР системно значимой Департамент финансовой стабильности Банка России в срок не позднее пяти рабочих дней с даты принятия такого решения подготавливает и направляет в ИОФР уведомление о принятом Банком России решении.

4.2. Банк России в течение 10 рабочих дней с даты принятия решения о признании ИОФР системно значимой размещает соответствующую информацию на официальном сайте Банка России в информационно-телекоммуникационной сети “Интернет” и опубликовывает ее в “Вестнике Банка России”.

5. В случае если ранее признанная системно значимой ИОФР не соответствует ни одному из критериев в течение двух последних календарных кварталов, Департамент финансовой стабильности Банка России с участием Департамента рынка ценных бумаг и товарного рынка Банка России в течение 10 рабочих дней с даты установления факта несоответствия подготавливает доклад-

ную записку об отзыве решения о признании ИОФР системно значимой, содержащую обоснование несоответствия ИОФР ни одному из критериев, и представляет ее для рассмотрения и принятия решения Председателю Банка России или лицу, его замещающему.

Решение о признании ИОФР утратившей системную значимость оформляется приказом Банка России.

ИОФР признается утратившей системную значимость с даты подписания соответствующего приказа Банка России.

5.1. При принятии решения о признании ИОФР утратившей системную значимость Департамент финансовой стабильности Банка России в срок не позднее пяти рабочих дней с даты принятия такого решения подготавливает и направляет в ИОФР уведомление о принятом Банком России решении.

5.2. Банк России в течение 10 рабочих дней с даты принятия решения о признании ИОФР утратившей системную значимость размещает соответствующую информацию на официальном сайте Банка России в информационно-телекоммуникационной сети “Интернет” и опубликовывает ее в “Вестнике Банка России”.

6. Настоящее Указание вступает в силу по истечении 10 дней после дня его официального опубликования в “Вестнике Банка России”.

ПРЕДСЕДАТЕЛЬ
ЦЕНТРАЛЬНОГО
БАНКА
РОССИЙСКОЙ
ФЕДЕРАЦИИ Э.С. НАБИУЛЛИНА

Приложение
к Указанию Банка России
от 25 июля 2014 года № 3341-У
“О признании инфраструктурных организаций
финансового рынка системно значимыми”

Критерии признания инфраструктурных организаций финансового рынка системно значимыми

1. ИОФР может быть признана системно значимой в случае соответствия хотя бы одному из следующих трех критериев:

критерий уникальности: ИОФР единолично осуществляет определенные законодательством Российской Федерации функции в качестве ИОФР;

критерий значимости для единой государственной денежно-кредитной политики: ИОФР обеспечивает операции Банка России;

критерий значимости на финансовом рынке: ИОФР удовлетворяет количественным абсолютному и относительному критериям значимости ИОФР на финансовом рынке, определенным в соответствии с пунктом 2 и пунктом 3 настоящего приложения, одновременно.

2. ИОФР удовлетворяет абсолютному критерию значимости ИОФР на финансовом рынке, в случае когда значение итогового абсолютного показателя значимости ИОФР на финансовом рынке (далее — ИАПЗ) выше медианного значения ИАПЗ по всем ИОФР соответствующего вида.

2.1. ИАПЗ для каждой ИОФР определяется как простое среднее арифметическое значение за последние четыре квартала по соответствующему абсолютному показателю значимости (далее — АПЗ) для каждой ИОФР. В случае если ИОФР осуществляла деятельность менее четырех кварталов, то ИАПЗ рассчитывается как простое среднее арифметическое значение за кварталы, предшествующие дате расчета показателя.

2.2. АПЗ для центрального контрагента является количество сделок, заключенных участниками клиринга за квартал в рамках договоров, стороной которых является центральный контрагент, по состоянию на отчетную дату квартала.

2.3. АПЗ для расчетного депозитария является совокупная рыночная стоимость (в случае отсутствия рыночной стоимости — номинальная стоимость) активов в рублевом эквиваленте, учитываемых расчетным депозитарием на счетах депо, по состоянию на отчетную дату квартала.

2.4. АПЗ для репозитария является количество договоров, представленных информирующими лицами и зарегистрированных в реестре договоров за квартал, по состоянию на отчетную дату квартала.

3. ИОФР удовлетворяет относительному критерию значимости ИОФР на финансовом рынке, в случае когда значение итогового относительного показателя значимости ИОФР на финансовом рынке (далее — ИОПЗ) выше медианного значения ИОПЗ по всем ИОФР соответствующего вида.

3.1. ИОПЗ для каждой ИОФР определяется как простое среднее арифметическое значение за последние четыре квартала по соответствующему относительному показателю значимости (далее — ОПЗ) для каждой ИОФР. В случае если ИОФР осуществляла деятельность менее четырех кварталов, то ИОПЗ рассчитывается как простое среднее арифметическое значение за кварталы, предшествующие дате расчета показателя.

3.2. ОПЗ для каждой ИОФР рассчитывается на ежеквартальной основе по формуле:

$$ОПЗ = K_i \times O_i,$$

где:

K_i:

для центральных контрагентов — доля обслуживаемых центральным контрагентом участников клиринга в общем количестве обслуживаемых участников клиринга среди центральных контрагентов по состоянию на отчетную дату квартала, в процентах;

для расчетных депозитариев — доля обслуживаемых расчетным депозитарием депонентов в общем количестве обслуживаемых депонентов среди расчетных депозитариев по состоянию на отчетную дату квартала, в процентах;

для репозитариев — доля обслуживаемых репозитарием клиентов в общем количестве обслуживаемых клиентов среди репозитариев по состоянию на отчетную дату квартала, в процентах;

i — порядковый номер ИОФР соответствующего вида;

O_i:

для центральных контрагентов — доля центрального контрагента в обороте по совершенным участниками клиринга операциям в общем обороте по совершенным участниками клиринга операциям среди центральных контрагентов за соответствующий период, в процентах;

для расчетных депозитариев — доля расчетного депозитария в обороте по совер-

шенным операциям по поручениям депонентов в общем обороте по совершенным операциям по поручениям депонентов среди расчетных депозитариев за соответствующий период, в процентах;

для репозитариев — доля в обороте по договорам, предоставленным информирующими лицами и зарегистрированным в реестре договоров репозитария, в общем обороте по указанным договорам среди репозитариев за соответствующий период, в процентах. Оборот по договорам, представленным информирующими лицами и зарегистрированным в реестре договоров репозитария, рассчитывается исходя из сумм сделок по соответствующим договорам.

Обороты, необходимые для расчета O_i, определяются в рублевом эквиваленте, рассчитанном по официальному курсу иностранной валюты по отношению к рублю, установленному Банком России на дату расчета O_i, по всем совершенным операциям (по всем предметам договоров).

АПЗ и ОПЗ для каждой ИОФР рассчитываются за каждый квартал из четырех кварталов, предшествующих дате расчета, или, в случае если ИОФР осуществляла деятельность менее четырех кварталов, за каждый квартал, предшествующий дате расчета показателя, на основании данных формы № 1100 "Квартальный отчет профессионального участника рынка ценных бумаг", составленной в соответствии с Положением "Об отчетности профессиональных участников рынка ценных бумаг", утвержденным Постановлением Федеральной комиссии по рынку ценных бумаг и Министерства финансов Российской Федерации от 11 декабря 2001 года № 33/109н "Об утверждении Положения об отчетности профессиональных участников рынка ценных бумаг", зарегистрированным Министерством юстиции Российской Федерации 25 декабря 2001 года № 3125, 31 декабря 2009 года № 15936 (Российская газета от 16 января 2002 года, от 17 января 2002 года, от 26 января 2010 года), а также информации, получаемой Банком России на основании Указания Банка России от 30 апреля 2014 года № 3253-У "О порядке ведения реестра договоров, заключенных на условиях генерального соглашения (единого договора), сроках предоставления информации, необходимой для ведения указанного реестра, и информации из указанного реестра, а также предоставления реестра договоров, заключенных на условиях генерального соглашения (единого договора), в Центральный банк Российской Федерации (Банк России)", зарегистрированного Министерством юстиции Российской Федерации 26 мая 2014 года № 32434 ("Вестник Банка России" от 4 июня 2014 года № 52), а также иных документов и (или) информации, полученной от ИОФР по запросам Банка России.

РЕКОМЕНДАЦИИ В ОБЛАСТИ
СТАНДАРТИЗАЦИИ
БАНКА РОССИИ

РС БР ИББС-2.6-2014

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА СТАДИЯХ ЖИЗНЕННОГО ЦИКЛА АВТОМАТИЗИРОВАННЫХ БАНКОВСКИХ СИСТЕМ

Дата введения: 2014-09-01

Москва
2014

Предисловие

ПРИНЯТЫ И ВВЕДЕНЫ в действие Распоряжением Банка России от 10 июля 2014 года № Р-556.

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) организациям банковской системы Российской Федерации (БС РФ) требуется принимать меры к обеспечению информационной безопасности (ИБ) автоматизированных банковских систем (АБС) на всех стадиях их жизненного цикла.

Принятие мер к обеспечению ИБ на стадиях жизненного цикла АБС осуществляется с целью выполнения следующих основных задач:

— обеспечение реализации в АБС необходимых требований к обеспечению ИБ, установленных законодательством Российской Федерации, в том числе нормативными актами Банка России, СТО БР ИББС-1.0, внутренними документами организации БС РФ;
— снижение рисков нарушения ИБ, связанных с наличием уязвимостей в АБС;
— контроль обеспечения ИБ в рамках эксплуатации АБС;
— снижение рисков нарушения ИБ, в том числе рисков утечки информации, на этапе сопровождения, модернизации АБС и вывода из эксплуатации АБС;
— оперативная модернизация АБС в случае выявления недопустимых рисков нарушения ИБ, связанных с ее эксплуатацией.

С целью установления рекомендаций по выполнению указанных задач настоящий документ устанавливает положения:

— по организации работ на этапах жизненного цикла АБС, в том числе обеспечивающей возможность контроля с целью установления доверия к проведению указанных работ и, соответственно, доверия к реализации обеспечения ИБ в АБС;
— по составу типовых недостатков в реализации требований к обеспечению ИБ в АБС, создающих условия для возникновения недопустимых рисков нарушения ИБ при эксплуатации АБС (далее – типовые недостатки в обеспечении ИБ АБС);
— по составу, содержанию и порядку проведения работ по контролю исходного кода программного обеспечения АБС, оценке защищенности АБС и по контролю параметров настроек технических защитных мер (выявление ошибок конфигурации).

РС БР ИББС-2.6-2014

РЕКОМЕНДАЦИИ В ОБЛАСТИ СТАНДАРТИЗАЦИИ БАНКА РОССИИ

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА СТАДИЯХ ЖИЗНЕННОГО ЦИКЛА АВТОМАТИЗИРОВАННЫХ БАНКОВСКИХ СИСТЕМ

Дата введения: 2014-09-01

1. Область применения

Настоящие рекомендации распространяются на организации БС РФ, реализующие требования СТО БР ИББС-1.0 по обеспечению ИБ на этапах жизненного цикла АБС в рамках построения (совершенствования) системы обеспечения ИБ, а также на организации, привлекаемые организациями БС РФ для выполнения работ на стадиях жизненного цикла АБС.

Настоящий документ применяется в организациях БС РФ и иных организациях путем включения ссылок на него и (или) прямого использования устанавливаемых в нем положений во внутренних документах и договорах, заключаемых организацией БС РФ.

Рекомендательный статус документа допускает, что по решению организации БС РФ вместо его отдельных положений могут применяться иные положения, обеспечивающие эквивалентный (аналогичный) уровень обеспечения ИБ в АБС на различных стадиях их жизненного цикла.

2. Нормативные ссылки

В настоящих рекомендациях в области стандартизации Банка России использованы нормативные ссылки на следующие документы:

СТО БР ИББС-1.0;

Рекомендации в области стандартизации Банка России “Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения ИБ” (РС БР ИББС-2.2).

3. Термины и определения

В настоящих рекомендациях применяются термины в соответствии со СТО БР ИББС-1.0, а также следующие термины с соответствующими определениями:

3.1. **Доверие** — состояние уверенности в том, что АБС соответствует установленным для нее требованиям к обеспечению ИБ.

3.2. **Функция обеспечения ИБ** — реализованная функциональная возможность одного или нескольких компонентов АБС, связанная с обеспечением ИБ.

3.3. **Интерфейс (использования) функции обеспечения ИБ** — описание и реализация способов использования функций обеспечения ИБ.

3.4. **Функциональные требования к обеспечению ИБ** — требования к функциям обеспечения ИБ компонентов АБС, а также интерфейсам их использования.

4. Обозначения и сокращения

АБС — автоматизированная банковская система
АРМ — автоматизированное рабочее место
СУБД — система управления базами данных
ТЗ — техническое задание
ЧТЗ — частное техническое задание
ИБ — информационная безопасность
БС РФ — банковская система Российской Федерации

5. Общие положения

5.1. В рамках настоящих рекомендаций АБС рассматривается как взаимосвязанная совокупность программно-технических средств: телекоммуникационного оборудования, средств вычислительной техники, системного программного обеспечения, прикладного программного обеспечения, а также средств защиты информации.

Основные функциональные возможности АБС, обеспечивающие автоматизацию банковских информационных и платежных технологических процессов, в том числе существенные защитные меры, реализуются одним или несколькими специализированными банковскими приложениями, входящими в состав АБС. Остальные компоненты, в том числе системное программное обеспечение, средства вычислительной техники, средства защиты информации, рассматриваются как обеспечивающая среда функционирования специализированных банковских приложений (далее — обеспечивающие компоненты АБС).

5.2. Обеспечение ИБ в АБС реализуется использованием функций обеспечения ИБ компонентов АБС, которое заключается в применении и эксплуатации защитных мер специализированных банковских приложений, а также защитных мер всех обеспечивающих компонентов АБС. Совокупность защитных мер специализированных банковских приложений АБС и защитных мер всех обеспечивающих компонентов АБС определяется как подсистема ИБ АБС.

Следует учитывать, что обеспечивающие компоненты АБС могут использоваться для обеспечения эксплуатации нескольких разных специализированных банковских приложений, соответственно, функции обеспечения ИБ таких обеспечивающих компонентов могут использоваться в разных АБС, а их защитные меры включаются в подсистемы ИБ разных АБС.

5.3. С учетом того, что обеспечивающие компоненты АБС могут являться объектом целенаправленных действий со стороны злоумышленника, обеспечение ИБ на этапах жизненного цикла АБС требует реализации мероприятий как для специализированных банковских приложений, так и для всех обеспечивающих компонентов АБС.

При организации работ на стадиях жизненного цикла АБС рекомендуется учитывать, что в ряде случаев обеспечивающие компоненты АБС создаются разными организациями, большая их часть поставляется как есть и организация — разработчик специализированных банковских приложений (далее — разработчик) не располагает полной и достоверной информацией о корректности реализации функций безопасности обеспечивающих компонентов АБС.

5.4. В соответствии с требованиями СТО БР ИББС-1.0 жизненный цикл АБС разделяется на следующие стадии:

1) разработка технического задания (ТЗ);
2) проектирование;
3) создание и тестирование;
4) приемка и ввод в действие;
5) эксплуатация;
6) сопровождение и модернизация;
7) снятие с эксплуатации.

5.5. Доверие к реализации обеспечения ИБ в АБС возможно только при наличии определенных свидетельств полноты и корректности проведения мероприятий по обеспечению ИБ на стадиях жизненного цикла компонентов АБС, как минимум специализированных банковских приложений. В качестве свидетельств доверия рекомендуется рассматривать:

— регламенты, используемые для организации деятельности по обеспечению ИБ на этапах жизненного цикла АБС;
— документированные результаты выполнения деятельности по обеспечению ИБ на этапах жизненного цикла АБС.

На каждой стадии жизненного цикла формируется собственный набор свидетельств доверия, по результатам оценки которых может быть принято решение о полноте и корректности реализации требований к обеспечению ИБ, предъявляемых к АБС.

5.6. Организацию работ по созданию АБС, включая подсистему ИБ, рекомендуется осуществлять с учетом положений комплекса стандартов и руководящих документов на автоматизированные системы “Информационная технология”, в том числе ГОСТ 34.601-90 “Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания” (далее — ГОСТ 34.601-90).

6. Стадия разработки технического задания

6.1. Основной задачей на стадии разработки ТЗ в части обеспечения ИБ является определение требований к обеспечению ИБ для создаваемой АБС для включения в состав ТЗ (далее — требования ТЗ к обеспечению ИБ).

Следует учитывать, что на данной стадии, как правило, отсутствует полная информация, необходимая для установления конкретных функциональных требований к обеспечению ИБ, реализуемых компонентами АБС. Установление конкретных функциональных требований к обеспечению ИБ возможно только после того, как будут определены основные технические решения создаваемой АБС. В связи с этим требования ТЗ к обеспечению ИБ рекомендуется формулировать в общем (неявном) виде, без привязки к конкретным реализациям, но при этом требования должны быть четко определены в объеме, достаточном для их однозначного понимания.

6.2. Формирование требований ТЗ к обеспечению ИБ рекомендуется осуществлять с учетом положений ГОСТ 34.602-89 “Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы”.

6.3. Требования ТЗ к обеспечению ИБ определяются (составляются) на основе требований к обеспечению ИБ, установленных законодательством Российской Федерации, в том числе нормативными актами Банка России, СТО БР ИББС-1.0, внутренними документами организации БС РФ, которые должны быть реализованы для создаваемой АБС.

Определение состава документов, требования к обеспечению ИБ которых используются для формирования ТЗ к обеспечению ИБ, рекомендуется осуществлять на основе данных:

- о типах информации (информационных активов), предполагаемых к обработке и (или) хранению в АБС;
- о составе банковских технологических процессов организации БС РФ, для автоматизации которых она создается;
- о технологиях и средствах обработки информации, предполагаемых к использованию для реализации АБС (в случае наличия подобных данных).

6.4. При определении требований ТЗ к обеспечению ИБ рекомендуется установить:

- необходимость и целесообразность применения средств защиты информации, сертифицированных по требованиям безопасности информации;
- необходимость и целесообразность привлечения для проведения работ по созданию, модернизации, эксплуатации и выводу из эксплуатации АБС организации, имеющей лицензии на деятельность по технической защите конфиденциальной информации.

6.5. При формировании требований ТЗ к обеспечению ИБ дополнительно рекомендуется осуществить предварительный анализ актуальных угроз безопасности информации. На данном этапе рекомендуется формулировать угрозы ИБ в самом общем виде в терминах бизнес-процессов, операций и функций организации БС РФ.

В случае если на данной стадии могут быть сформированы функциональные требования к обеспечению ИБ по нейтрализации рассмотренных актуальных угроз или компенсации возможного ущерба, рекомендуется включить указанные требования в состав ТЗ к обеспечению ИБ.

6.6. В состав требований ТЗ к обеспечению ИБ рекомендуется включать требования к использованию функций обеспечения ИБ обеспечивающих компонентов АБС, используемых для обеспечения ИБ специализированных банковских приложений разных АБС, со стороны специализированных банковских приложений (требования к интеграции специализированных банковских приложений с разделяемыми обеспечивающими компонентами АБС).

6.7. Среди прочего в состав требований ТЗ к обеспечению ИБ рекомендуется включать:

- требования к обеспечению ИБ, связанные с назначением и распределением ролей в АБС;
- требования к обеспечению ИБ, связанные с управлением доступом и регистрацией;
- требования к обеспечению ИБ, связанные с защитой от воздействия вредоносного кода;
- требования к обеспечению ИБ, связанные с использованием общедоступных сетей и каналов передачи данных;
- требования к обеспечению ИБ, связанные с использованием средств криптографической защиты информации;

— требования к обеспечению ИБ, связанные с реализацией контроля эксплуатации применяемых защитных мер;
— требования к обеспечению ИБ, связанные с реализацией мониторинга ИБ, в том числе для выявления инцидентов ИБ в АБС;
— требования к безопасным технологиям обработки информации (технологическим мерам защиты информации).

6.8. ТЗ на создаваемую АБС рекомендуется как основной источник требований к обеспечению ИБ на стадии проектирования АБС.

7. Стадия проектирования АБС

7.1. Основными задачами на стадии проектирования АБС в части обеспечения ИБ являются:

— установление и документирование функциональных требований, реализуемых компонентами АБС, обеспечивающих выполнение требований ТЗ к обеспечению ИБ;
— определение состава функций обеспечения ИБ, реализуемых разделяемыми обеспечивающими компонентами АБС;
— выбор состава защитных мер (технических и (или) организационных), реализующих функции обеспечения ИБ в соответствии с функциональными требованиями к обеспечению ИБ в привязке к компонентам АБС, в том числе выбор средств защиты информации, сертифицированных на соответствие требованиям по безопасности информации;
— первичное определение параметров настройки технических защитных мер (стандартов конфигураций);
— определение и документирование интерфейсов использования функций обеспечения ИБ, реализованных в компонентах АБС;
— первичное определение правил эксплуатации технических защитных мер, включая правила их обновления, управления и контроля параметров их настройки;
— определение требований (состав и содержание) к регламентам реализации организационных защитных мер;
— первичное определение состава ролей субъектов доступа АБС (эксплуатирующего персонала, пользователей, программных процессов), состав ресурсов доступа (баз данных, файловых ресурсов, виртуальных машин, иных ресурсов доступа), прав доступа ролей субъектов доступа (чтение, запись, выполнение или иные типы доступа) при осуществлении доступа к ресурсам доступа;
— первичное определение требований к кадровому обеспечению подсистемы ИБ АБС.

7.2. Проектирование АБС в части обеспечения ИБ рекомендуется начинать с разработки архитектуры подсистемы ИБ АБС, в которую рекомендуется включать описание:

— предполагаемой реализации требований ТЗ к обеспечению ИБ компонентами проектируемой АБС;
— предполагаемого использования функций обеспечения ИБ разделяемых обеспечивающих компонентов АБС;
— предполагаемого взаимодействия компонентов АБС для обеспечения ИБ в АБС.

Разработку архитектуры АБС для обеспечения ИБ следует осуществлять на основе:

— данных о разделении АБС на компоненты, составе и функциях специализированных банковских приложений и обеспечивающих компонентов АБС;
— идентификации (для стандартных) или описания (для разрабатываемых в составе АБС или самостоятельно разрабатываемых) интерфейсов взаимодействия между компонентами АБС;
— данных о программном обеспечении АБС, в том числе системном, которое является покупным коробочным (для АБС, создаваемых путем адаптации специализированного прикладного обеспечения, — данные о пакетах специализированных прикладных программ).

7.3. Проектирование подсистемы ИБ АБС рекомендуется выполнять с учетом целесообразности реализации:

— централизованного управления и контроля технических защитных мер, в том числе в части обновления программного обеспечения, обновления применяемых сигнатурных баз, установления и контроля параметров их настройки;
— интеграции АБС с инфраструктурными компонентами мониторинга ИБ и выявления инцидентов ИБ, применяемыми в организации БС РФ, для чего в состав функциональных требований к обеспечению ИБ рекомендуется включить требования к составу данных мониторинга ИБ, генерируемых компонентами АБС в процессе эксплуатации АБС;

— максимально возможной степени использования функций обеспечения ИБ разделяемых обеспечивающих компонентов АБС.

При проектировании подсистемы ИБ АБС не рекомендуется планировать необоснованную модернизацию эксплуатируемых разделяемых обеспечивающих компонентов АБС. В случае проведения модернизации указанных компонентов рекомендуется организация и проведение работ по модернизации и тестированию в части обеспечения ИБ всех АБС, использующих разделяемый обеспечивающий компонент, подвергшийся модернизации.

7.4. На этапе проектирования рекомендуется установить функциональные требования к обеспечению ИБ, включая:

— функциональные требования к обеспечению ИБ специализированных банковских приложений;
— функциональные требования к обеспечению ИБ обеспечивающих компонентов разрабатываемой АБС;
— требования к использованию функций обеспечения ИБ разделяемых обеспечивающих компонентов АБС.

Функциональные требования к обеспечению ИБ рекомендуется документировать в частном ТЗ на АБС (далее — ЧТЗ подсистемы ИБ АБС).

Если функциональные требования к обеспечению ИБ установлены на стадии разработки ТЗ, их повторное документирование в ЧТЗ подсистем ИБ АБС нецелесообразно.

7.5. С целью обеспечения полноты реализации требований ТЗ к обеспечению ИБ рекомендуется выполнять процедуры контроля соответствия требований ТЗ к обеспечению ИБ и функциональных требований к обеспечению ИБ, включенных в ЧТЗ подсистемы ИБ.

Функциональные требования ЧТЗ подсистемы ИБ АБС рекомендуется разделять на категории с учетом выполнения пункта 7.4 настоящего документа и документировать в отдельных подразделах ЧТЗ подсистемы ИБ АБС.

В случаях, когда к различным составным частям АБС предъявляются одинаковые функциональные требования, рекомендуется дублировать их в соответствующих подразделах ЧТЗ подсистемы ИБ АБС.

7.6. Функциональные требования ЧТЗ подсистемы ИБ АБС рекомендуется рассматривать в качестве основного документа, на соответствие которому оцениваются свидетельства доверия, формируемые на последующих стадиях жизненного цикла АБС.

7.7. При проектировании подсистемы ИБ АБС рекомендуется определение и оформление стандартов конфигурации — документов, содержащих перечень и эталонные значения конфигурационных параметров компонентов АБС, в том числе технических защитных мер. Принятие стандартов конфигурации и контроль соответствия фактических значений параметров конфигурации их эталонным значениям — основной способ предотвращения уязвимостей, вызванных ошибками настройки компонентов АБС.

С целью формирования стандартов конфигурации обеспечивающих компонентов АБС, являющихся серийно выпускаемым программным обеспечением, в том числе операционными системами, системами управления базами данных, иным системным программным обеспечением, рекомендуется использовать стандартизованные справочники параметров конфигураций в части обеспечения ИБ, например National Checklist Program Repository [1].

7.8. Для АБС, компоненты которых предполагается размещать на средствах вычислительной техники клиентов организации БС РФ, рекомендуется определение и документирование:

— состава компонентов, передаваемых на сторону клиента;
— мер, принимаемых для обеспечения целостности программных компонентов, передаваемых на сторону клиента;
— требований к среде функционирования компонентов АБС на стороне клиента;
— требований и порядка передачи клиентом информации о проблемах и инцидентах ИБ, возникших при использовании клиентом компонентов АБС;
— требований и способов обновления компонентов АБС, эксплуатируемых на стороне клиента, а также требований к обновлению среды их функционирования.

7.9. На этапе разработки технического проекта разрабатывается проектная документация, включающая в себя проектную документацию на подсистему ИБ АБС. Определение состава и структуры проектной документации АБС рекомендуется осуществлять с учетом положений руководящего документа РД 50-34.698-90 “Автоматизированные системы. Требования к содержанию документов”, а также ГОСТ 34.201-89 “Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем” и ГОСТ 19.201-78 “Единая система программной документации. Техническое задание. Требования к содержанию и оформлению”.

7.10. Проектную документацию подсистемы ИБ АБС рекомендуется разрабатывать с соблюдением следующих принципов:

— проектная документация должна содержать документированные результаты выполнения задач, установленных в пункте 7.1 настоящего документа;
— проектная документация должна предоставлять возможность проведения контроля полноты и корректности реализации функций обеспечения ИБ в соответствии с требованиями ЧТЗ подсистемы ИБ АБС в реализованных проектных решениях.

8. Стадия создания и тестирования АБС

8.1. Основными задачами на стадии создания и тестирования АБС в части обеспечения ИБ являются:

— управление версиями и изменениями разрабатываемых специализированных банковских приложений;
— обеспечение ИБ среды разработки и тестирования компонентов АБС;
— тестирование (проведение предварительных испытаний) компонентов АБС, в том числе специализированных банковских приложений;
— тестирование (проведение предварительных испытаний) компонентов АБС, предназначенных для эксплуатации на средствах вычислительной техники клиентов организации БС РФ;
— разработка эксплуатационной документации.

8.2. Основными рекомендуемыми целями применения управления версиями и изменениями разрабатываемых программных компонентов АБС в части обеспечения ИБ являются:

— контроль соответствия реализации определенных требований ЧТЗ на подсистему ИБ АБС в определенной версии (сборке) разрабатываемых специализированных банковских приложений;
— формализация порядка хранения исходных файлов и работы с ними, а также принятие мер, препятствующих несанкционированному внесению изменений в версии специализированных банковских приложений.

8.3. Для обеспечения управления версиями и изменениями разрабатываемых специализированных банковских приложений рекомендуется использовать систему управления версиями и изменениями, позволяющую осуществлять:

— маркировку (присвоение номеров) промежуточных версий разрабатываемых специализированных банковских приложений;
— идентификацию исходных файлов, используемых для сборки каждой промежуточной версии разрабатываемых специализированных банковских приложений, в том числе файлов исходного кода, ресурсных файлов, файлов документации;
— маркировку версий (редакций) исходных файлов.

8.4. Для обеспечения ИБ среды разработки и тестирования компонентов АБС рекомендуется обеспечить защиту от следующих угроз ИБ:

— несанкционированное внесение изменений в исходные файлы разрабатываемого программного обеспечения;
— приостановка процесса разработки и тестирования, приводящая к нарушению сроков выпуска окончательной (финальной) разрабатываемой версии программного обеспечения, в том числе вследствие нарушения работоспособности средств разработки, уничтожения части исходных файлов;
— несанкционированное ознакомление третьих лиц с исходными файлами и программной документацией, а также иная утечка информации в процессе разработки компонентов АБС;
— утрата прав (лицензий) на использование средств разработки.

Для противодействия угрозам разработчикам рекомендуется принять и документировать меры защиты, включающие:

— обеспечение контроля физического доступа к средствам вычислительной техники, используемым на стадии разработки и тестирования программных компонентов АБС;
— выделение сегментов вычислительных сетей, в которых располагаются средства вычислительной техники, используемые на стадии разработки специализированных банковских приложений;
— выделение сегментов вычислительных сетей, в которых располагаются средства вычислительной техники, используемые на стадии тестирования специализированных банковских приложений и обеспечивающих компонентов АБС;

— организацию и контроль изоляции и информационного взаимодействия сегмента разработки, сегмента тестирования и сегментов вычислительных сетей, в которых располагаются средства вычислительной техники, используемые для реализации банковских технологических процессов;
— управление доступом к ресурсам, средствам разработки и тестирования специализированных банковских приложений, в том числе исходным файлам;
— регистрацию и контроль действий с исходными файлами специализированных банковских приложений;
— организацию антивирусной защиты;
— контроль использования коммуникационных портов средств вычислительной техники.

8.5. В среде разработки и тестирования не рекомендуется использование реальных данных, полученных в результате реализации банковских технологических процессов.

В случае если для тестирования необходимы данные, максимально приближенные к реальным, рекомендуется формирование тестовых массивов данных путем необратимого обезличивания, маскирования и (или) искажения сведений, полученных в результате реализации банковских технологических процессов. Не рекомендуется использование в тестировании каких-либо данных, в отношении которых на основании законодательства Российской Федерации, в том числе нормативных актов Банка России, внутренних документов организации БС РФ и (или) договоров с клиентами и контрагентами, распространяется требование к обеспечению ИБ.

8.6. Тестирование полноты и корректности реализации требований ЧТЗ на подсистему ИБ АБС рекомендуется проводить в три стадии:
— непосредственно в ходе разработки программных компонентов АБС;
— перед выпуском финальной версии разрабатываемых программных компонентов АБС;
— в ходе предварительных испытаний АБС.

8.7. В ходе тестирования в рамках разработки специализированных банковских приложений рекомендуется проводить автономную проверку корректности реализации требований ЧТЗ подсистемы ИБ АБС к разрабатываемым специализированным банковским приложениям. Взаимодействие разрабатываемых специализированных банковских приложений с обеспечивающими компонентами АБС и их функциями обеспечения ИБ при этом, как правило, не тестируется, а сами обеспечивающие функции эмулируются с помощью тест-программ. Данное тестирование рекомендуется проводить разработчиками в среде разработки специализированных банковских приложений.

8.8. Перед выпуском финальной версии специализированных банковских приложений рекомендуется проводить тестирование полноты и корректности выполнения требований ЧТЗ на подсистему ИБ АБС к разрабатываемым специализированным банковским приложениям с учетом взаимодействия с обеспечивающими компонентами АБС, в том числе разделяемыми. Данное тестирование рекомендуется проводить разработчикам в тестовой среде, включающей в себя все компоненты АБС, размещенные и настроенные в соответствии с проектной документацией, и воспроизводящей близкие к реальным условия их эксплуатации.

8.9. Для тестирования разрабатываемых специализированных банковских приложений рекомендуется разработать и поддерживать в актуальном состоянии программу тестирования, включающую в себя проверку выполнения всех требований к обеспечению ИБ, установленных в ЧТЗ на подсистему ИБ АБС, в том числе при некорректных значениях входных данных, неработоспособности функций обеспечения ИБ прочих обеспечивающих компонентов АБС и иных возможных нештатных режимах функционирования АБС. Программа тестирования должна идентифицировать все тесты и демонстрировать соответствующими тестами полноту выполнения требований ЧТЗ на подсистему ИБ АБС.

Для каждого теста должна быть документирована методика тестирования, составляемая на основе информации об интерфейсах функций обеспечения ИБ, включающая исходные данные, последовательность проверочных действий, ожидаемый результат выполнения теста и критерии успешного или неуспешного выполнения теста.

Факт выполнения теста должен подтверждаться протоколом тестирования, содержащим дату тестирования, указание на методику тестирования, использованные при выполнении теста исходные данные, полученный результат и решение об успешном или неуспешном выполнении теста.

К моменту выпуска финальной версии разрабатываемых программных компонентов АБС корректность реализации их функций безопасности должна подтверждаться протоколами тестирования, демонстрирующими успешное выполнение всех тестов, предусмотренных программой тестирования.

8.10. Для программных компонентов АБС, реализующих банковский платежный технологический процесс или предназначенных для обработки персональных данных или иной информации, в отношении которой законодательством Российской Федерации или решением организации БС РФ установлено требование об обеспечении безопасности, рекомендуется перед проведением предварительных испытаний осуществлять контроль исходного кода с целью выявления типовых ошибок программирования и иных дефектов, приводящих к возникновению уязвимостей.

Рекомендации к проведению контроля исходного кода приведены в приложении 2 к настоящему документу.

8.11. В ходе предварительных испытаний АБС рекомендуется проведение независимого или совместного с разработчиком полного тестирования с целью проверки полноты и корректности реализации всех требований ЧТЗ на подсистему ИБ АСБ применительно ко всем компонентам АБС. Предварительные испытания рекомендуется проводить в тестовой среде, включающей в себя все компоненты АБС, конфигурированные и настроенные в соответствии с проектной документацией, и воспроизводящей близкие к реальным условия их эксплуатации.

Предварительные испытания рекомендуется проводить в соответствии с программой и методикой испытаний, в которой для каждого интерфейса каждой функции обеспечения ИБ должны быть предусмотрены процедуры тестирования, соответствующие этому интерфейсу. Тестирование должно подтверждать корректность:

— реализации функции обеспечения ИБ при доступе к ней через тестируемый интерфейс;
— вызовов необходимых функций обеспечения ИБ компонентов АБС, в том числе разделяемых.

Тесты должны демонстрировать соответствие результатов выполнения функции обеспечения ИБ на заданных наборах исходных данных требованиям безопасности, заданным в ЧТЗ.

8.12. Проведение предварительных испытаний рекомендуется осуществлять с учетом положений стандарта ГОСТ 34.603-92 “Информационная технология. Виды испытаний автоматизированных систем”.

8.13. По результатам выполнения стадии создания и тестирования АБС рекомендуется провести необходимые корректировки проектной документации на АБС.

8.14. В состав эксплуатационной документации, включая инструкции эксплуатационного персонала, в том числе администратора ИБ АБС, рекомендуется включать следующие сведения:

— описание состава защитных мер в привязке к компонентам АБС;
— описание состава, требований к размещению, параметров настройки (стандартов конфигураций) технических защитных мер;
— описание правил эксплуатации технических защитных мер, включая правила их обновления, управления и контроля их эксплуатации, в том числе параметров их настройки;
— требования и регламенты реализации организационных защитных мер;
— требования к кадровому обеспечению подсистемы ИБ АБС, описание ролей и функций эксплуатирующего персонала;
— требования к составу и содержанию организационных мероприятий, необходимых к проведению для обеспечения развертывания и эксплуатации подсистемы ИБ АБС, в том числе мероприятий по назначению ролей эксплуатационного персонала, обучению, информированию и повышению осведомленности эксплуатационного персонала и пользователей;
— описание правил и процедур обеспечения информационной безопасности при снятии с эксплуатации АБС или по окончании обработки информации.

8.15. Для АБС, компоненты которых предполагается размещать на средствах вычислительной техники клиентов организации БС РФ, в состав эксплуатационной документации рекомендуется включение отдельных документов, предназначенных для регламентации эксплуатации компонентов АБС на стороне клиента:

— описание состава компонентов АБС, эксплуатируемых на стороне клиента;
— порядок реализации мер, принимаемых для обеспечения целостности специализированных банковских приложений и обеспечивающих компонентов АБС, передаваемых на сторону клиента;
— требования к составу, версиям и необходимым настройкам в части обеспечения ИБ программного обеспечения среды функционирования компонентов АБС на стороне клиента;
— порядок обновления компонентов АБС, эксплуатируемых на стороне клиента, а также требования к обновлению программных компонентов среды их функционирования;
— требования к составу, версиям, обновлению и настройкам технических защитных мер, применяемых на стороне клиента.

9. Стадия приемки и ввода в действие

9.1. Основными задачами на стадии приемки и ввода в действие в части обеспечения ИБ являются:

— контроль развертывания компонентов АБС в информационной инфраструктуре организации БС РФ, используемой для реализации банковских технологических процессов (далее — промышленная или производственная среда);
— проведение опытной эксплуатации;
— устранение недостатков в реализации требований ЧТЗ на подсистему ИБ АБС;
— проведение приемочных испытаний.

9.2. Для контроля развертывания компонентов АБС в промышленной среде рекомендуется:

— обеспечить контроль корректности версий и целостности специализированных банковских приложений при передаче из среды разработки и тестирования в промышленную среду;
— обеспечить контроль выполнения требований проектной и эксплуатационной документации в части размещения и установления параметров настройки технических защитных мер, реализации организационных защитных мер, определения и назначения ролей.

9.3. Опытную эксплуатацию АБС рекомендуется проводить с учетом положений ГОСТ 34.603-92.

9.4. В рамках проведения опытной эксплуатации в части обеспечения ИБ рекомендуется проведение проверки корректности функционирования подсистемы ИБ АБС в промышленной среде, а также проверки возможности реализации на этапе эксплуатации положений проектной и эксплуатационной документации в части:

— контроля эксплуатации технических защитных мер, включая правила их обновления, управления и контроля параметров их настройки;
— контроля реализации организационных защитных мер;
— требований к кадровому обеспечению подсистемы ИБ АБС.

9.5. Дополнительно в рамках проведения опытной эксплуатации рекомендуется проведение комплексной оценки защищенности, включающей проведение:

— тестирования на проникновение;
— выявления известных уязвимостей компонентов АБС.

Комплексную оценку защищенности рекомендуется проводить без уведомления персонала, задействованного в опытной эксплуатации АБС, что среди прочего позволит оценить готовность персонала к выполнению требований документов организации БС РФ в части реагирования на инциденты ИБ.

Рекомендации к проведению оценки защищенности приведены в приложении 3 к настоящему документу.

9.6. По результатам опытной эксплуатации рекомендуется:

— документально зафиксировать состав выявленных недостатков в реализации подсистемы ИБ АБС;
— по каждому недостатку провести оценку рисков и принять решение о возможности их устранения на стадии эксплуатации;
— составить планы устранения недостатков в реализации подсистемы ИБ АБС;
— провести мероприятия по устранению критичных с точки зрения обеспечения ИБ недостатков в реализации подсистемы ИБ АБС.

9.7. После устранения недостатков в реализации подсистемы ИБ АБС рекомендуется принятие решения о составе и необходимости проведения мероприятий по повторному тестированию и опытной эксплуатации АБС и (или) ее компонентов с учетом выполненных доработок и уровня критичности устраняемых недостатков.

9.8. По результатам опытной эксплуатации рекомендуется рассмотреть необходимость доработки проектной и (или) эксплуатационной документации и в случае необходимости выполнить такую доработку.

9.9. После устранения критичных недостатков в реализации подсистемы ИБ АБС, выявленных в ходе опытной эксплуатации, проводятся приемочные испытания. Определение состава и порядка проведения приемочных испытаний рекомендуется осуществлять с учетом положений ГОСТ 34.603-92.

9.10. Приемочные испытания проводятся на основе результатов предварительных испытаний, опытной эксплуатации и результатов устранения критических недостатков, выявленных на стадии опытной эксплуатации. Кроме того, в рамках приемочных испытаний могут проводиться выборочные мероприятия по тестированию функций обеспечения ИБ, предусмотренные к проведению в рамках предварительных испытаний.

10. Стадия эксплуатации

10.1. Основными задачами на стадии эксплуатации в части обеспечения ИБ являются:

— контроль состава, мест размещения и параметров настроек технических защитных мер;
— контроль выполнения правил эксплуатации технических защитных мер, включая правила обновления и управления;
— контроль выполнения регламентов реализации организационных защитных мер;
— контроль реализации мер, принимаемых для обеспечения целостности специализированных банковских приложений и обеспечивающих компонентов АБС, передаваемых на сторону клиента, а также доведения до клиентов необходимых документов, входящих в состав эксплуатационной документации;
— контроль соблюдения требований к кадровому обеспечению подсистемы ИБ АБС;
— контроль выполнения организационных мероприятий, необходимых для обеспечения эксплуатации подсистемы ИБ АБС, в том числе мероприятий по назначению ролей эксплуатационного персонала, обучению, информированию и повышению осведомленности эксплуатационного персонала и пользователей;
— контроль готовности эксплуатационного персонала к эксплуатации подсистемы ИБ АБС;
— контроль информирования пользователей о правилах эксплуатации подсистемы ИБ АБС;
— периодическая оценка защищенности АБС (проведение мероприятий по выявлению типичных уязвимостей программных компонентов АБС, тестирование на проникновение);
— мониторинг сообщений об уязвимостях АБС и реагирование на них.

Рекомендации к проведению контроля параметров настроек технических защитных мер (выявление ошибок конфигурации) приведены в приложении 4 к настоящему документу.

10.2. Периодичность проведения работ по оценке защищенности определяется решением организации БС РФ. Для АБС, используемых для реализации банковского платежного технологического процесса, рекомендуется проведение комплексной оценки защищенности не реже одного раза в год.

10.3. Сообщения об уязвимостях программного обеспечения могут быть получены из различных источников, таких как:

— уведомления, публикуемые центрами реагирования на компьютерные инциденты (например, уведомления CERT [2]), платежными системами (например, уведомления платежной системы VISA [3]), производителями технических и программных средств (например, уведомления компании ORACLE [4]);
— уведомления, публикуемые в общедоступных базах данных уязвимостей, а также распространяемые по подписке;
— сообщения об уязвимостях в АБС, направляемые сторонними специалистами в адрес организации БС РФ или публикуемые ими в общедоступных источниках, для чего рекомендуется предусматривать способы оперативной связи с соответствующими специалистами организацией БС РФ.

10.4. Рекомендуется организовать выполнение деятельности по:

— идентификации АБС, компонентом которых является программное обеспечение с выявленными уязвимостями;
— определению степени критичности выявленных уязвимостей для реализации банковских технологических процессов организации БС РФ;
— принятию решений об устранении уязвимости в рамках мероприятий по сопровождению и модернизации АБС в случае ее подтверждения.

11. Сопровождение и модернизация АБС

11.1. Основными задачами на стадии сопровождения и модернизации АБС в части обеспечения ИБ являются:

— обеспечение проверки в тестовой среде работоспособности подсистемы ИБ АБС после обновления компонентов АБС, выполненных в рамках сопровождения АБС;
— обеспечение доработки эксплуатационной документации при изменении применяемых версий обеспечивающих компонентов АБС;
— предотвращение утечки информации в рамках работ по сопровождению АБС, в том числе с участием сторонних организаций;
— предотвращение утечки информации при передаче средств вычислительной техники на ремонт в сторонние организации;

— обеспечение контроля полноты проведения мероприятий на стадиях жизненного цикла АБС при ее модернизации.

11.2. Для предотвращения утечки информации в рамках работ по сопровождению (модернизации) АБС, в том числе с участием сторонних организаций, рекомендуется организовать контроль лиц, осуществляющих работы по сопровождению (модернизации) АБС, со стороны работников организации БС РФ с возложением ответственности за выполнение несанкционированных и (или) нерегламентированных операций, выполняемых в рамках сопровождения (модернизации), на указанных работников организации БС РФ.

11.3. Модернизация АБС включает в себя в необходимом объеме стадии разработки технического задания, проектирования, создания и тестирования, приемки и ввода в действие.

12. Стадия снятия с эксплуатации

12.1. Основными задачами на стадии снятия с эксплуатации в части обеспечения ИБ являются:

— контроль соблюдения правил и процедур обеспечения информационной безопасности при снятии с эксплуатации АБС;

— архивирование информации, содержащейся в АБС, в случае необходимости ее дальнейшего использования;

— гарантированное уничтожение (стирание) данных и остаточной информации с машинных носителей информации АБС и (или) уничтожение машинных носителей информации АБС в случаях, предусмотренных законодательством РФ, в том числе нормативными актами Банка России, внутренними документами организации БС РФ.

Приложение 1

Типовые недостатки в реализации функций безопасности автоматизированных систем

1. Общие недостатки АБС и банковских приложений

1.1. Управление доступом

1.1.1. Наличие у пользователя прав доступа, не являющихся безусловно необходимыми для выполнения технологических операций, предусмотренных его ролью в организации БС РФ.

1.1.2. Наличие у технологической учетной записи, от имени которой функционирует составная часть АБС, прав доступа, не являющихся безусловно необходимыми для выполнения операций, предусмотренных для этой составной части АБС проектной документацией.

1.1.3. Наличие в АБС учетных технологических записей со стандартными паролями, задаваемыми автоматически при установке программного обеспечения.

1.1.4. Реализация в АБС дискреционной, мандатной или иных моделей управления доступом вместо ролевой модели.

1.1.5. Отсутствие в АБС встроенных средств формирования отчетов о пользователях и их привилегиях.

1.1.6. Реализация функций управления доступом только на уровне АБС.

1.1.7. Наличие в графическом интерфейсе пользователя АБС элементов управления, предназначенных для выполнения операций, права на выполнение которых у пользователя отсутствуют.

1.1.8. Отсутствие ограничений на количество одновременных подключений (сессий) пользователя в АБС. Упрощает использование нарушителями учетных записей, принадлежащих сотрудникам организации БС РФ.

1.2. Идентификация и аутентификация

1.2.1. Отсутствие аутентификации серверной стороны при взаимодействии пользователя с АБС и составных частей АБС между собой.

1.2.2. Взаимодействие составных частей АБС без аутентификации инициатора взаимодействия.

1.2.3. Использование протоколов аутентификации, допускающих незащищенную передачу аутентификационных данных пользователей (в том числе передачу их открытым текстом или с использованием обратимых преобразований).

1.2.4. Выполнение в алгоритмах аутентификации сужающих преобразований аутентификационных данных (например, приведение букв идентификатора пользователя и (или) пароля к одному регистру, ограничение количества значащих символов пароля).

1.2.5. Использование предсказуемых идентификаторов (например, производных от имени и фамилии пользователя, совпадающих с идентификаторами в адресах электронной почты, порядковых номеров, формирование идентификаторов по единому алгоритму).

1.2.6. Отсутствие принудительного ограничения на минимальную сложность паролей (например, ограничение минимальной длины пароля, наличие символов различных классов, несовпадение пароля с идентификатором пользователя, несовпадение нового пароля с одним из ранее использовавшихся).

1.2.7. Использование при создании новых учетных записей единого первоначального пароля или формирование таких паролей по единому алгоритму, а также отсутствие механизма принудительной смены первоначального пароля при первом входе пользователя в систему.

1.2.8. Хранение в АБС паролей пользователей с использованием обратимых преобразований. При несанкционированном доступе нарушителя к ОС или СУБД серверных компонентов АБС приводит к компрометации всех учетных записей данной АБС и отдельных учетных записей в остальных АБС организации БС РФ.

1.2.9. Использование процедур самостоятельного восстановления или смены забытых пользователями паролей.

1.2.10. Отсутствие предварительной аутентификации при смене пароля пользователем. В ряде случаев делает возможным обход аутентификации путем задания нарушителем нового пароля пользователя.

1.2.11. Отображение символов пароля при вводе.

1.2.12. Отсутствие противодействия автоматизированному подбору идентификаторов и паролей пользователей, в том числе:

— отсутствие автоматического временного блокирования учетной записи при превышении заданного количества неуспешных попыток аутентификации;
— отсутствие механизмов, исключающих возможность автоматизированного подбора паролей (например, CAPTCHA).

1.2.13. При автоматическом блокировании учетной записи в случае превышения заданного количества неуспешных попыток аутентификации — отсутствие автоматического разблокирования учетной записи по истечении заданного интервала времени, что позволяет нарушителю блокировать доступ пользователей в АБС.

1.2.14. Необходимость выполнения отдельных программных модулей АБС с правами администратора операционной системы. При наличии уязвимостей программного кода приложения позволяет нарушителю получить полный контроль над приложением и операционной системой.

1.2.15. Аутентификация пользователей средствами программного кода автоматизированного рабочего места (далее — АРМ) при отсутствии аутентификации пользователя серверными компонентами АБС, что делает возможным обход аутентификации нарушителем.

1.2.16. Наличие аутентификационных данных, необходимых для доступа компонентов АБС к прочим АБС организации БС РФ, в программном коде компонентов АБС и (или) в доступных пользователям конфигурационных файлах.

1.2.17. Использование протоколов взаимодействия, уязвимых для перехвата и повторного использования постаутентификационных данных (хеш-значений паролей, идентификаторов сессии, аутентификационных маркеров и т.п.), уязвимых к перехвату и повторному использованию.

1.3. Регистрация событий и просмотр журналов регистрации событий

1.3.1. Отсутствие или отключение средств синхронизации времени операционной системы.

1.3.2. Отсутствие механизмов регистрации отдельных типов событий, существенных для расследования инцидентов, в том числе:

— создание новых учетных записей и изменение прав доступа учетных записей;
— неуспешные операции (например, ошибки аутентификации, недостаточные права доступа при выполнении операций, недоступность интерфейсов составных частей АБС);
— срабатывание функций безопасности, направленных на противодействие компьютерным атакам (например, автоматическое блокирование учетных записей, автоматическое завершение сессий, поступление некорректных исходных данных на внешние и интерфейсы АБС);
— выполнение операций, предусмотренных моделью угроз в качестве составной части реализации угрозы.

1.3.3. Отсутствие в данных журналов регистрации событий существенных сведений о регистрируемых событиях, позволяющих установить обстоятельства наступления события.

1.3.4. Наличие в данных журналов регистрации событий конфиденциальных и чувствительных данных (пароли пользователей, данные платежных карт и т.п.).

1.3.5. Регистрация отдельных событий только составными частями АБС, потенциально доступными нарушителю (например, АРМ пользователя, общедоступные веб-серверы).

1.3.6. Хранение журналов регистрации событий в незащищенном виде (например, в общедоступном пользователям для изменения файле или таблице базы данных).

1.3.7. Возможность изменения пользователями параметров регистрации событий.

1.3.8. Отсутствие встроенных или специализированных средств анализа журналов регистрации событий, в том числе поиска событий по заданным критериям (по имени и идентификатору пользователя, дате, времени и т.д.).

1.3.9. Отсутствие механизмов оперативного уведомления администраторов АБС о событиях, имеющих признаки инцидента безопасности.

1.4. Обработка ввода и вывода

1.4.1. Отсутствие предварительной проверки корректности входных данных (например, проверки ограничений на длину текстовых строк, отсутствия в них недопустимых символов и комбинаций символов, соответствия числовых значений граничным условиям).

1.4.2. Наличие в видимых пользователями сообщениях об ошибках чувствительной информации (например, аутентификационных данных, сведений, идентифицирующих программное обеспечение составных частей АБС, диагностической информации).

1.4.3. Отсутствие проверки корректности выходных данных, в том числе:

— возможность формирования серверными компонентами АБС исполняемых файлов и сценариев на основе задаваемых пользователями исходных данных;

— возможность включения в выходные данные, передаваемые между составными частями АБС, фрагментов, не соответствующих спецификациям протоколов взаимодействия и (или) используемых для эксплуатации типовых уязвимостей.

1.5. Криптографическая защита

1.5.1. Использование для взаимодействия составных частей АБС (в том числе размещенных в пределах контролируемой зоны) протоколов, не обеспечивающих криптографическую защиту данных.

1.5.2. Отсутствие технологической возможности использования приложением сертифицированных СКЗИ при выполнении операций, требующих криптографической защиты данных (в том числе и в случаях, когда возможность использования несертифицированных СКЗИ предусмотрена решением руководства организации БС РФ).

1.5.3. При использовании приложением сертифицированных СКЗИ — выполнение криптографических операций с использованием программного интерфейса, характерного только для определенной модели СКЗИ.

1.5.4. Использование процедур генерации криптографических ключей, допускающих возможность копирования симметричного ключа и (или) закрытой части асимметричного ключа пользователем.

1.5.5. Использование для генерации псевдослучайных последовательностей (например, для формирования идентификаторов сессий, challenge-запросов, GUID) программных генераторов, не входящих в состав СКЗИ.

1.5.6. Использование СКЗИ в режимах и условиях, не предусмотренных эксплуатационной документацией СКЗИ.

1.6. Безопасная архитектура и разработка

1.6.1. Отказ от использования в программном коде компонентов АБС механизмов защиты, предоставляемых архитектурой процессора, операционной системой и средствами компиляции кода (например, защиты от переполнения буфера, защиты от нарушения обработки исключений, защиты от исполнения кода в сегментах стека и данных, случайного размещения сегментов в адресном пространстве).

1.6.2. Использование функций стандартных библиотек, уязвимых к атакам переполнения буфера, при наличии аналогичных функций с встроенной защитой.

1.6.3. Отсутствие предварительной инициализации переменных и структур данных при выделении оперативной памяти.

1.6.4. Присутствие в операционной системе, СУБД, серверных компонентах прикладного ПО функционирующих и доступных для взаимодействия сетевых служб, использование которых не предусматривается проектной документацией.

1.7. Защита данных

1.7.1. Отсутствие в АБС механизмов очистки остаточной информации при удалении данных.

1.7.2. Отсутствие защиты от несанкционированного доступа к разделяемым ресурсам операционной системы (например, к разделяемой памяти, именованным каналам, отображаемым в памяти файлам).

1.7.3. Некорректное использование средств синхронизации доступа к разделяемым ресурсам операционной системы (например, критических секций, семафоров).

1.8. Конфигурация безопасности

1.8.1. Отсутствие механизмов защиты от несанкционированного доступа к настройкам приложения.

1.8.2. Отсутствие возможности экспорта настроек приложения в формат, пригодный для анализа специалистом.

1.9. Контроль целостности и достоверности

1.9.1. Отсутствие в АБС средств контроля целостности программного кода и корректности настроек составных частей АБС.

1.9.2. Отсутствие механизмов обработки ошибок и отката к предыдущему состоянию при выполнении отдельных операций.

1.9.3. Отсутствие механизмов перевода АБС в аварийный режим функционирования при выявлении нарушения целостности программного кода или некорректности настроек.

1.9.4. Отключение отдельных функций безопасности при переводе АБС в аварийный режим функционирования.

1.9.5. Отсутствие механизмов генерации диагностической информации при переводе АБС в аварийный режим функционирования.

2. Типовые недостатки приложений дистанционного банковского обслуживания и электронных средств платежа

2.1. Идентификация и аутентификация

2.1.1. Использование однофакторной аутентификации при выполнении финансовых операций.

2.1.2. Предсказуемый алгоритм формирования однократных паролей и (или) возможность повторного использования однократных паролей.

2.2. Безопасность транзакций

2.2.1. Использование для подтверждения транзакций средств авторизации (например, простой электронной подписи), допускающих возможность формирования подтверждения третьими лицами, в том числе сотрудниками организации БС РФ.

2.2.2. Выбор механизмов авторизации следует осуществлять исходя из критичности транзакций и возможных проблем, которые могут быть связаны с обеспечением аутентичности и целостности данных. Примерами недостатков в реализации механизмов авторизации могут являться:

- отсутствие средств подтверждения для неплатежных операций, влияющих на платежный процесс (создание шаблонов платежных поручений, ведение справочников реквизитов получателей платежей, изменение лимитов и т.п.);
- использование для формирования электронной цифровой подписи ключевых носителей, допускающих экспорт закрытой части ключа подписи;
- отсутствие возможности подписания электронных платежных поручений юридических лиц электронными подписями двух уполномоченных лиц;
- возможность повторного использования электронного платежного документа;
- отсутствие сквозного контроля электронных подписей в электронном платежном документе на всех этапах его обработки.

3. Типовые недостатки веб-приложений

3.1. Размещение компонентов веб-приложения

3.1.1. Размещение в единой демилитаризованной зоне веб-серверов и иных составных частей нескольких АБС.

3.1.2. Хранение данных, используемых веб-сервером, а также журналов регистрации событий на системном разделе жесткого диска.

3.1.3. Совместное расположение журналов регистрации событий и системных файлов.

3.1.4. Наличие на веб-сервере тестовых приложений и сценариев, а также программных компонентов, не входящих в состав АБС.

3.2. Управление сессиями

3.2.1. Использование предсказуемых идентификаторов сессий.

3.2.2. Возможность повторного использования идентификатора сессии (в том числе использование одинаковых идентификаторов в нескольких сессиях одного пользователя, неизменность идентификатора сессии после повторной аутентификации пользователя).

3.2.3. Возможность использования идентификатора сессии после ее завершения.

3.2.4. Раскрытие идентификаторов сессий, в том числе передача идентификаторов в незашифрованном виде, а также включение идентификаторов в записи журналов регистрации событий, в сообщения об ошибках.

3.3. Управление доступом

3.3.1. Отсутствие контроля доступа на уровне идентификаторов ресурсов (URI), в том числе возможность несанкционированного доступа к отдельным разделам и объектам веб-сайта путем указания их URI в веб-браузере пользователя.

3.3.2. Возможность просмотра содержимого каталогов веб-сайта в случаях, когда такой просмотр не является необходимым.

3.3.3. Использование при обработке данных в формате XML внешних сущностей (External Entity), внешних параметров сущностей (External Parameter Entity) и внешних описаний типа документа (External Doctype).

3.4. Защита данных

3.4.1. Отсутствие в параметрах веб-формы, предназначенных для ввода конфиденциальной информации, директив, запрещающих кеширование данных.

3.4.2. Передача конфиденциальной и аутентификационной информации в сообщениях HTTP-GET.

3.4.3. Отсутствие атрибута HTTPOnly у параметров cookie, значения которых не должны быть доступны сценариям, выполняемым веб-браузером.

3.4.4. Отсутствие атрибута secure у параметров cookie, содержащих чувствительную информацию.

3.5. Обработка ввода и вывода

3.5.1. Отсутствие проверки корректности вводимых пользователем данных или выполнение такой проверки только сценариями, исполняемыми веб-браузером.

3.5.2. Отсутствие директивы, определяющей используемую кодировку в заголовках сообщений HTTP, а также использование разных кодировок для разных источников входных данных.

3.5.3. Отказ от использования встроенных средств проверки корректности входных параметров, реализованных в стандартных программных библиотеках.

3.5.4. Отсутствие или отключение средств предотвращения атак, связанных с использованием типовых уязвимостей веб-приложений.

3.5.5. Отсутствие средств контроля корректности входных данных, предназначенных для последующей обработки программными модулями, допускающими интерпретацию команд (SQL, XPath, LINQ, LDAP, командная оболочка ОС и т.п.).

3.5.6. Отсутствие преобразования специальных символов, предусмотренного спецификациями языка HTML (например, замены символов ‘<’ и ‘>’ специальными символами языка HTML).

4. Типовые недостатки систем управления базами данных

4.1. Функционирование и доступность протоколов взаимодействия с СУБД, использование которых не предусмотрено проектной документацией.

4.2. Возможность доступа составных частей АБС к функциям СУБД без аутентификации.

4.3. Наличие у администраторов СУБД учетных записей операционной системы с правами, не являющимися безусловно необходимыми для обслуживания СУБД.

4.4. Наличие у технологических учетных записей, используемых составными частями АБС для доступа к СУБД, прав, не являющихся безусловно необходимыми для выполнения предусмотренных документацией операций.

4.5. Установка СУБД на сервер, используемый другими составными частями АБС.

4.6. Размещение СУБД в демилитаризованной зоне, в которую возможен непосредственный доступ внешних пользователей.

4.7. Возможность доступа к системным таблицам и конфигурационным настройкам у пользователей, не являющихся администраторами.

4.8. Наличие в СУБД демонстрационных баз данных, поставляемых в составе дистрибутива программного обеспечения СУБД.

4.9. Размещение данных нескольких приложений в одном разделе СУБД в случае, когда такое размещение не предусмотрено явно проектной документацией.

5. Типовые недостатки операционных систем

5.1. Управление доступом

5.1.1. Отсутствие ограничений по составу пользователей, имеющих право удаленного доступа к операционной системе, и IP-адресам, с которых разрешен такой доступ.

5.1.2. Использование незащищенных и слабозащищенных протоколов удаленного доступа к операционной системе (например, TELNET, PPTP).

5.1.3. Возможность доступа к настройке параметров операционной системы, заданий, журналу событий, системным файлам у пользователей, не являющихся администраторами ОС.

5.1.4. Задание индивидуальных прав доступа к объектам операционной системы отдельным пользователям (вместо включения этих пользователей в соответствующие группы).

5.1.5. Возможность интерактивного входа в систему для системных учетных записей, использующихся приложениями и сервисами.

5.1.6. Наличие у пользователя, не являющегося администратором ОС, прав на чтение и (или) модификацию файлов в домашних каталогах остальных пользователей.

5.1.7. Отсутствие дисковых квот для учетных записей (включая технологические учетные записи).

5.1.8. Несоответствие настроек операционной системы рекомендациям разработчика по ее безопасной настройке.

5.1.9. Наличие в операционных системах серверных компонентов АБС программного обеспечения, не предусмотренного эксплуатационной документацией.

5.2. Идентификация и аутентификация

5.2.1. Отображение на приглашении для входа в систему сведений, на основе которых могут быть установлены имена пользователей операционной системы или получены какие-либо сведения о паролях пользователей.

5.2.2. Возможность доступа к операционной системе без аутентификации через вспомогательные и (или) редко используемые интерфейсы (serial-порты и т.п.).

5.2.3. Отсутствие аутентификации пользователя при доступе к параметрам BIOS, параметрам загрузчика ядра ОС, входе в режим восстановления системы (safe mode, single-user mode и т.п.).

5.3. Управление системой

5.3.1. Отключение в настройках ядра операционной системы механизмов, настройки ядра, предотвращающих выполнение кода в области данных и стека.

5.3.2. Отключение в настройках ядра операционной системы функции очистки файла/раздела подкачки виртуальной памяти.

5.3.3. Включенная в настройках операционной системы возможность выгрузки образов областей памяти (дампов) на диск.

5.3.4. Включенная в настройках операционной системы возможность гибернации (перехода в ждущий режим).

5.3.5. Отключение встроенного межсетевого экрана операционной системы, отсутствие в настройках встроенного межсетевого экрана правил фильтрации, блокирующих взаимодействие, не предусмотренное эксплуатационной документацией АБС, и отключение используемых средств защиты сторонних производителей.

6. Типовые недостатки телекоммуникационного оборудования

6.1. При возможности выбора операционной системы для установки на телекоммуникационное оборудование — установка операционных систем с заведомо избыточными функциональными возможностями.

6.2. Использование в телекоммуникационной инфраструктуре АБС коммутационного оборудования, не обеспечивающего возможность отключения неиспользуемых интерфейсов и контроль подключения сетевых устройств (например, по MAC-адресам или с использованием протокола IEEE 802.1x), защиту от атак типа ARP spoofing, разделение сети на сегменты с использованием технологии VLAN.

6.3. Настройка сегментов VLAN, допускающая присутствие в одном сегменте АРМ пользователей и серверов АБС, а также АРМ пользователей и АРМ администраторов АБС.

7. Типовые недостатки технологий виртуализации

7.1. Возможность доступа к данным виртуальных машин (например, настройкам виртуального аппаратного обеспечения, образам дисков) пользователей, не являющихся администраторами сервера виртуализации.

7.2. Предоставление виртуальным машинам доступа к разделяемым ресурсам операционной системы сервера виртуализации в случаях, когда такой доступ не предусмотрен явно эксплуатационной документацией АБС.

7.3. Отсутствие средств мониторинга объема свободных ресурсов сервера виртуализации.

7.4. Отсутствие ограничения удаленного доступа администраторов сервера виртуализации путем ограничения IP-адресов, с которых разрешен доступ, и сетевого интерфейса для доступа администраторов.

7.5. Использование для удаленного администрирования сервера виртуализации сетевых интерфейсов, используемых виртуальными машинами.

7.6. Хранение журналов регистрации событий средств виртуализации в каталогах, доступных на чтение и (или) запись виртуальным машинам.

7.7. Использование в виртуальных машинах образов жестких дисков с динамически изменяемым размером.

7.8. Непосредственный доступ виртуальных машин к физическим дискам и логическим томам памяти сервера виртуализации.

7.9. Использование в графическом интерфейсе сервера виртуализации расширенных механизмов обмена данными между виртуальными машинами и сервером виртуализации (например, drag and drop, copy and paste).

7.10. Использование расширенных механизмов обмена данными между виртуальными машинами (например, программного интерфейса сервера виртуализации, виртуальных сокетов).

7.11. Возможность изменения пользователем режима загрузки виртуальной машины.

РС БР ИББС-2.6-2014

Приложение 2

Рекомендации к проведению контроля исходного кода

1. Общие положения

1.1. Контроль кода (code review) — мероприятия, осуществляемые в отношении определенных частей исходного текста (исходного кода) программы для ЭВМ, созданных одним или несколькими разработчиками, другим (не создававшим эту часть кодов) разработчиком или назначенным в установленном порядке иным имеющим требуемую подготовку специалистом, и которые состоят в детальной проверке (изучении, анализе, исследовании) соответствующих исходных кодов с целью выявления неизвестных уязвимостей, в том числе связанных с ошибками программирования, нарушений установленных требований, а также иных существенных дефектов.

1.2. Объектом исследования являются тексты программ разрабатываемых компонентов АБС, в первую очередь тексты программ специализированных банковских приложений.

1.3. Контроль кода может в обоснованных случаях проводиться несколькими лицами, в том числе при участии создавшего и (или) модифицировавшего проверяемый код разработчика.

1.4. Контроль кода может осуществляться лицом, проверяющим код, как вручную, в том числе с использованием приемов эффективного чтения программного кода (code reading), так и с применением методов и средств автоматизированного анализа исходного кода, в том числе обеспечивающих:

— статический анализ кода;
— динамический анализ кода.

2. Контроль кода вручную

2.1. Контроль (проверка) исходного кода вручную обеспечивается просмотром, изучением и оценкой кода лицом, отличным от его разработчика. Оценка кода может включать в себя:

— оценку соответствия кода требованиям, предъявляемым к структурированию и оформлению кода, именованию объектов, разделению на модули, использованию специальных средств обеспечения качества кода, предусмотренных используемыми языками программирования и средствами разработки;
— оценку полноты и качества документирования кода, включая документирование заголовков программных модулей, прототипов функций и структур данных, комментарии к выполнению существенных операций;
— оценку соответствия алгоритмов, реализованных в исходном коде, программной документации, в том числе выявление явных недекларированных возможностей (программных закладок), ошибок программного кода, попыток запутывания (обфускации) программного кода и использования иных приемов, затрудняющих проведение контроля.

2.2. Методы эффективного чтения кода включают двойное чтение (сначала понять общую структуру, запомнить основные обозначения и соглашения, затем читать снова, выявляя дефекты, несоответствия), использование сценариев и др.

2.3. Помимо приемов индивидуальной проверки кода, существуют методы эффективной организации взаимодействия участников контроля кода, в том числе прослеживания (walkthrough), инспекции кода (code inspections) и др. Они являются достаточно ресурсоемкими и для их применения нужны соответствующие навыки, но при рациональном использовании они могут быть весьма эффективны в случаях, требующих особого внимания.

3. Статический анализ кода

3.1. Статический анализ кода (static_program_analysis) проводится с использованием автоматизированных средств (программных инструментов) и направлен на идентификацию потенциально опасных фрагментов кода, в том числе:

— вызовов функций, методов, процедур (далее — функции) с передачей им в качестве аргументов данных, вводимых пользователем или принимаемых из внешних источников;
— текстов функций преобразования форматов данных;
— вызовов системных функций и функций обеспечения ИБ разделяемых обеспечивающих компонентов АБС, в том числе функций обеспечения ИБ операционной системы и специализированных технических защитных мер, функций ввода/вывода, управления памятью и системными ресурсами;

— текстов функций, осуществляющих проверку прав доступа и принятие решений, основанных на значениях атрибутов безопасности;
— текстов функций, самостоятельно реализующих функциональность обеспечения ИБ, в том числе криптографические функции, аутентификацию пользователей и проверку прав доступа, генерацию данных мониторинга ИБ;
— текстов функций, предусматривающих установление соединения с внешними компонентами с передачей им аутентификационных данных;
— текстов обработчиков ошибок и исключений.

3.2. В ходе статического анализа кода рекомендуется проводить поиск типовых ошибок программирования (недостаточная проверка входных параметров функций, включение аутентификационных данных непосредственно в текст программ, некорректное преобразование типов, недостаточная обработка ошибок и исключений), а также определяются статические пути исполнения программы.

4. Динамический анализ кода

4.1. Динамический анализ кода осуществляется путем выполнения или эмуляции выполнения программы на определенной совокупности наборов тестовых исходных данных. Перед выполнением или в процессе выполнения программа иногда инструментируется путем дополнения ее функциями трассировки выполнения для задания и контроля инвариантов, предусловий, постусловий и др. Динамический контроль проводится с использованием специализированных автоматизированных средств и может включать в себя, в частности:
— исследование особенностей исполнения потенциально опасных функций при задании заведомо некорректных аргументов;
— построение динамических путей исполнения программы и идентификацию точек принятия решений, существенных для выполнения функций обеспечения ИБ;
— поиск чувствительной информации в оперативной памяти и в аргументах функций;
— исследование особенностей исполнения программы при типовых атаках (переполнение буфера, внедрение операторов SQL в данные, используемые для формирования запросов к СУБД).

5. Дополнительные практические аспекты контроля кода

5.1. Вне зависимости от применяемых способов и методов анализа кода при его осуществлении рекомендуется использование классификаторов типовых ошибок программирования, а также способов выявления различных типов ошибок, например каталог Common Weakness Enumeration [5].

5.2. Выявленным в рамках контроля кода уязвимостям в коде разрабатываемых компонентов АБС целесообразно присваивать оценку степени их критичности (например, высокая, средняя, низкая) для обеспечения ИБ организации БС РФ. Для каждой выявленной уязвимости с учетом ее критичности принимается решение о доработке программного компонента АБС (и о приоритетности доработки) или о принятии рисков, связанных с наличием уязвимости.

5.3. Результаты контроля кодов оформляются протоколами контроля кода (название этих документов может быть иным), подписываемыми разработчиками — непосредственными исполнителями разработки проверенного исходного кода и лицами, участвовавшими в его проверке (контролерами кода), с отражением в протоколе сведений о дате мероприятия, проверенной части исходных кодов, выявленных уязвимостях и иных дефектах (при наличии), повторном контроле кодов с подтверждением устранения выявленных уязвимостей, дефектов.

Примечание. Протоколы контроля кода и иные подобные документы целесообразно оформлять в виде информации в электронной форме, созданной, переданной и надежно сохраненной в предусмотренной для данного вида информации (документов) системе электронного документооборота (например, в архиве сообщений электронной почты), с реквизитами (название, уникальный номер, подписи, даты и др.), позволяющими при аудите предъявлять ее в качестве электронного документа (комплекта документов), подписанного простыми электронными подписями, а также при необходимости изготавливать и заверять ее копии на бумажном носителе. (Требование об оформлении протоколов изначально на бумажном носителе или с усиленными электронными подписями может блокировать систематическое выполнение контроля кода.)

5.4. Мероприятия по контролю кода планируются и осуществляются в отношении всего подлежащего контролю измененного или вновь созданного исходного кода с уведомлением и в необходимых случаях при участии представителей службы ИБ в качестве контролеров кода.

Приложение 3

Рекомендации к проведению оценки защищенности

Оценка защищенности заключается в исследовании АБС или ее компонентов, целью которого является выявление уязвимостей, которые могут быть использованы злоумышленником для реализации угроз ИБ. Выделяются следующие основные методы оценки защищенности:

— тестирование на проникновение;
— выявление известных уязвимостей программного обеспечения.

1. Тестирование на проникновение

1.1. Описание метода

1.1.1. Тестирование на проникновение является основным методом оценки защищенности, охватывающим все аспекты функционирования подсистемы ИБ АБС, включая действия персонала по реагированию на инциденты ИБ и противодействие компьютерным атакам.

1.1.2. Достоинствами тестирования на проникновение как метода оценки защищенности являются:

— высокая достоверность сведений о выявленных уязвимостях за счет фактического подтверждения возможности их использования злоумышленником;
— достаточность результатов исследования для оценки критичности выявленных уязвимостей;
— наглядность получаемых результатов.

Недостатками тестирования на проникновение являются:

— способность исследователя воспроизводить только действия нарушителя, равного или уступающего по квалификации, как следствие — высокие требования к квалификации исследователя и низкая достоверность сведений об отсутствии уязвимостей;
— низкая степень автоматизации действий исследователя, как следствие — высокие трудозатраты по сравнению с другими способами оценки защищенности.

1.1.3. При тестировании на проникновение исследователь выполняет поиск уязвимостей АБС, воспроизводя действия злоумышленника. Перед началом работ для исследователя создаются условия, эквивалентные тем, в которых действует потенциальный злоумышленник. Условия проведения тестирования на проникновение различаются по следующим показателям:

— наличие прав доступа у исследователя в АБС;
— расположение исследователя относительно сетевого периметра защиты АБС;
— стратегия предоставления исследователю информации об АБС.

1.1.4. Тестирование на проникновения подразделяется на исследования с предоставлением доступа к АБС и без предоставления такого доступа. При исследовании с предоставлением доступа исследователю предоставляются учетные записи для доступа к АБС. При исследовании без предоставления доступа к АБС задача самостоятельного получения учетных записей пользователей АБС является составной частью тестирования на проникновение.

1.1.5. По расположению исследователя относительно сетевого периметра АБС тестирование на проникновение разделяется на внешнее и внутреннее. При внутреннем тестировании на проникновение исследователю предоставляется возможность подключения к телекоммуникационному оборудованию в точке, находящейся внутри сетевого периметра защиты организации БС РФ и обеспечивающей возможность сетевого взаимодействия с составными частями АБС. При внешнем тестировании на проникновение начальные действия исследователя ограничены только сетевыми протоколами взаимодействия с АБС, доступными извне сетевого периметра защиты организации БС РФ. При отсутствии в АБС интерфейсов для взаимодействия извне сетевого периметра задача самостоятельного преодоления сетевого периметра защиты организации БС РФ является составной частью тестирования на проникновение.

1.1.6. При тестировании на проникновение могут использоваться две стратегии предоставления исследователю информации об АБС. При стратегии черного ящика исследователь оперирует только теми сведениями об АБС, которые получены им самостоятельно в ходе тестирования на проникновение. При стратегии белого ящика исследователю заблаговременно предоставляется вся доступная информация об АБС, включая при наличии проектную и эксплуатационную документацию, исходные коды программных компонентов АБС и возможность просмотра параметров настройки компонентов АБС.

1.1.7. Рекомендуется проведение тестирования на проникновение только с уведомлением эксплуатирующего персонала организации БС РФ с исключением возможности активного противодействия исследователю.

1.1.8. Перед проведением тестирования на проникновение рекомендуется определить начальные условия его проведения. Рекомендуется учитывать, что максимальная полнота оценки достигается при внутреннем тестировании на проникновение с использованием предоставленного доступа к АБС и стратегией белого ящика. Тестирование на проникновение при таких начальных условиях рекомендуется проводить на стадии приемки и ввода в эксплуатацию, а также после каждой модернизации АБС.

1.1.9. Любые действия, выполнение которых способно причинить ущерб организации БС РФ, выполняются только после их подтверждения руководством организации БС РФ.

1.1.10. В ходе тестирования на проникновение возможно получение исследователем доступа к сведениям, охраняемым в соответствии с законодательством РФ и нормативными документами организации БС РФ. Трудовые договоры с работниками организации БС РФ, договоры оказания услуг с организациями, проводящими тестирование на проникновение, должны включать в себя:

— требование о сохранении конфиденциальности сведений, доступ к которым потенциально может быть получен в ходе тестирования на проникновение, в соответствии с законодательством РФ, в том числе нормативными актами Банка России и документами организации БС РФ;
— распределение и установление ответственности для случаев, когда выполнение действий в рамках тестирования на проникновение приведет к негативным последствиям и ущербу для организации БС РФ.

1.1.11. Отчет о тестировании на проникновение должен содержать:

— описание начальных условий исследования и постановку задачи;
— описание последовательности действий, которые приводили к выявлению уязвимостей или изменению возможностей исследователя, а также решения об отказе от выполнения запрашиваемых действий;
— описание выявленных уязвимостей, оценку степени их критичности для обеспечения ИБ организации БС РФ;
— рекомендации по устранению выявленных уязвимостей.

1.2. Содержание работ по тестированию на проникновение

1.2.1. Тестирование на проникновение включает в себя следующие направления исследований:

— оценка защищенности сетевого периметра, сетевых устройств и протоколов;
— оценка защищенности беспроводных сетей;
— оценка защищенности веб-приложений;
— оценка защищенности операционных систем;
— оценка защищенности систем управления базами данных (СУБД);
— оценка защищенности средств виртуализации;
— оценка защищенности специализированных банковских приложений;
— оценка защищенности мобильных устройств.

1.2.2. При проведении оценки защищенности сетевого периметра, сетевых устройств и протоколов рекомендуются следующие мероприятия:

— идентификация доступных исследователю сетевых устройств и протоколов взаимодействия;
— идентификация типов устройств, а также семейств и версий программного обеспечения, реализующего сетевые протоколы, на основе предоставляемой ими информации и особенностей их реакции на взаимодействие;
— поиск интерфейсов удаленного доступа и прочих интерфейсов взаимодействия, доступность которых из данной точки не предусмотрена требованиями ИБ организации БС РФ или практикой создания защищенных автоматизированных систем;
— проверка возможностей перенаправления сетевого трафика с использованием особенностей протоколов канального и сетевого уровня, протоколов автоматического взаимного согласования параметров телекоммуникационного оборудования, создания ложных сетевых служб автоматической адресации, разрешения имен, создания ложных сетевых служб;
— подбор данных аутентификации (имен пользователей, паролей, ключей) для доступа к сетевым службам на основе словарей стандартных и часто встречающихся значений;

— перехват и повторная отправка данных аутентификации;
— проверка возможности обхода средств защиты сетевого периметра путем изменения значимых полей сетевых пакетов, туннелирования и шифрования данных, перегрузки журналов событий СЗИ незначащей информацией;
— идентификация доступных веб-интерфейсов и нестандартных протоколов взаимодействия для последующего анализа.

1.2.3. При проведении оценки защищенности беспроводных сетей рекомендуются следующие мероприятия:

— прослушивание трафика, в том числе обнаружение доступных беспроводных сетевых устройств и их идентификаторов, определение текущей зоны радиовидимости, сбор информации о клиентских устройствах (например, MAC-адреса), сбор доступных идентификаторов сетей, определение применяемых алгоритмов шифрования;
— рассылка пробных запросов (например, для перебора идентификационных данных устройств) и анализ ответов на пробные запросы;
— выявление недостатков в настройке встроенных средств криптографической защиты беспроводных устройств;
— навязывание клиентским устройствам ложных точек доступа или дубликатов точек доступа.

1.2.4. При проведении оценки защищенности веб-приложений рекомендуются следующие мероприятия:

— выявление уязвимостей, связанных с раскрытием чувствительной информации о приложении, в том числе путем отправки некорректных сообщений, анализа стандартных системных сообщений об ошибках, поиска чувствительной информации в коде и комментариях веб-страниц;
— получение сведений о структуре файловой системы перебором путей и имен файлов (полный перебор, перебор по словарю, проверка наличия стандартных файлов используемых платформ и средств разработки, поиск резервных копий файлов);
— проверка корректности обработки специальных символов в параметрах запроса (символы форматирования вывода, перевода строки и возврата каретки, перехода в вышестоящий каталог, двойное URL-кодирование);
— проверка корректности обработки параметров различной длины;
— проверка корректности обработки числовых параметров, в том числе не предусмотренных технологией обработки больших величин, отрицательных и нулевых значений;
— проверка корректности приведения и преобразования типов параметров;
— проверка корректности обработки различного представления пользовательских данных, в том числе дублирование заголовков запроса, дублирование параметров сценария;
— проверка корректности обработки параметров универсального идентификатора ресурса (URI — uniform resource identifier), в том числе возможности подключения произвольного внешнего источника данных, или перенаправления на внешний или внутренний веб-сайт, возможности обращения к сетевым протоколам, возможности замены полного пути к ресурсу на относительный;
— проверка наличия ошибок, связанных с обработкой загружаемых файлов, в том числе с обработкой имен файлов без расширения, несоответствием расширения типу файла, альтернативными расширениями для файлов одного типа, специальными символами (включая нулевой символ) в имени файла;
— проверка корректности исполнения сценариев при манипулировании входными параметрами, в том числе атрибутами безопасности, используемыми при управлении доступом;
— проверка возможности подбора аутентификационных данных (паролей, включая словарные, идентификаторов сессий, атрибутов, используемых для восстановления паролей);
— проверка корректности обработки идентификаторов сессий пользователей, в том числе обработки событий завершения сессии, интервалов неактивности, сопоставление идентификатора сессии с дополнительными атрибутами, прямо или косвенно идентифицирующими пользователя или его рабочее место, предотвращение повторного и множественного использования идентификаторов сессий;
— проверка корректности реализации механизмов авторизации;
— проверка корректности противодействия атакам на клиентские приложения, в том числе с использованием межсайтового выполнения сценариев и подделки межсайтовых запросов;

— проверка корректности обработки входных параметров сценариев при внедрении в них команд операционных систем, синтаксических конструкций языков программирования и разметки;
— проверка невозможности обхода средств межсетевого экранирования прикладного уровня путем фрагментации данных, смешивания параметров, замены алгоритма кодирования и формата представления данных, замены специальных символов их альтернативными представлениями.

1.2.5. При проведении оценки защищенности операционных систем рекомендуются следующие мероприятия:

— идентификация сетевых служб операционной системы по типовым атрибутам (стандартные параметры сетевых протоколов, характерный отклик на установление соединения, характерные особенности реализации сетевых протоколов), наличия характерных служебных сообщений в сетевом трафике;
— проверка корректности ограничения доступа к сетевым службам операционной системы, в том числе с использованием анонимного/гостевого доступа, подбора паролей, перехвата и повторного/множественного использования авторизационных маркеров;
— проверка корректности противодействия подбору паролей, в том числе оценка возможности злоумышленника блокировать учетные записи пользователей множественными неуспешными попытками аутентификации;
— проверка возможности получения злоумышленником чувствительной информации с помощью служебных сетевых протоколов (SNMP, RPC, CIFS);
— проверка возможности реализации компьютерных атак с использованием уязвимостей сетевых служб, а для автоматизированных рабочих мест — и прикладного программного обеспечения.

При наличии у исследователя доступа к интерфейсам управления операционной системой оценка защищенности дополнительно включает в себя:

— возможность загрузки операционной системы в специальном режиме или с отчуждаемого носителя (при физическом доступе к средству вычислительной техники), а также загрузку операционной системы в специальном режиме (например, в режиме восстановления);
— получение имен пользователей;
— просмотр данных журналов регистрации событий и остаточной информации (удаленных файлов, образов оперативной памяти, сохраняемых при сбоях);
— поиск аутентификационных данных пользователей в остаточной информации, конфигурационных параметрах программного обеспечения, исходном коде приложений и скриптов;
— проверку возможности передачи управления операционной системой удаленному компьютеру с установлением реверсивного соединения и туннелированием сетевых протоколов;
— проверку возможности повышения привилегий с использованием локально эксплуатируемых уязвимостей и ошибок в настройке программного обеспечения;
— перенаправление и прослушивание сетевого трафика в доменах коллизий анализируемого средства вычислительной техники путем подделки таблиц протокола ARP, подложных серверов динамической конфигурации оборудования и разрешения имен.

1.2.6. При проведении оценки защищенности СУБД рекомендуются следующие мероприятия:

— проверка корректности функционирования механизмов идентификации, аутентификации и управления доступом при взаимодействии с интерфейсами управления СУБД, в том числе блокирования анонимного и гостевого доступа, отсутствие стандартных учетных записей и учетных записей со словарными паролями;
— проверка корректности обработки модифицированных входящих запросов, включая замену параметров протокола, вставку специальных символов и команд операционной системы в параметры входящих запросов языка SQL;
— эксплуатация уязвимостей в сетевых службах СУБД.

При наличии доступа к интерфейсам управления операционной системы и СУБД дополнительно проводятся:

— проверка корректности прав доступа к файлам СУБД;
— проверка контроля целостности исполняемых файлов СУБД, включая защиту от подмены файлов;
— поиск чувствительной информации (в том числе паролей пользователей) в служебных файлах (файлы баз данных, журналов, резервных копий, конфигурации, истории команд), а также переменных системных процессов СУБД;

— эксплуатация уязвимостей в хранимых процедурах, направленная на повышение привилегий, выполнение произвольных команд или прямой доступ к содержимому таблиц, изменение системных настроек;
— проверка возможности использования хранимых процедур для доступа к защищаемым объектам СУБД и операционной системы;
— проверка корректности обработки нестандартных значений параметров хранимых процедур (передача произвольных значений параметров, внедрение операторов SQL и команд PL/SQL, T-SQL, использование курсоров; передача значений параметров различной длины);
— проверка возможности чтения чувствительной информации приложений, включая восстановление паролей пользователей СУБД и приложений из хеш-значений.

1.2.7. При проведении оценки защищенности средств виртуализации рекомендуются мероприятия по проверке возможности доступа к интерфейсам управления средой виртуализации и защищаемым объектам, в том числе:
— проверка возможности подбора паролей к интерфейсам управления;
— проверка корректности прав доступа пользователей к объектам виртуализации, включая проверку возможности несанкционированного чтения и изменения виртуальных дисков, образов оперативной памяти, конфигурационных файлов и снимков виртуальных машин;
— использование уязвимостей гипервизора и средств управления средой виртуализации.

1.2.8. При проведении оценки защищенности специализированных банковских приложений рекомендуются следующие мероприятия:
— прослушивание сетевого трафика и поиск в нем чувствительной информации, включая пароли и хеш-значения паролей пользователей, идентификаторы сессий, авторизационные маркеры, криптографические ключи;
— запуск программ с различными параметрами, в том числе нестандартными, в том числе с использованием значений различной длины, дублирование отдельных параметров с присвоением им разных значений, включение в значения параметров специальных символов, команд операционной системы, операторов интерпретируемых языков программирования;
— мониторинг характера взаимодействия приложения с операционной системой в процессе функционирования, включая идентификацию файлов данных, содержащих чувствительную информацию, трассировку системных вызовов;
— проверка прав доступа к файлам данных, содержащим чувствительную информацию, а также контроль целостности исполняемых файлов приложения.

1.2.9. При проведении оценки защищенности мобильных устройств рекомендуются следующие мероприятия:
— проверка наличия чувствительной информации в файлах данных, журналах регистрации событий, в оперативной памяти устройства, а также передачи чувствительной информации в незашифрованном виде;
— проверка возможности чтения ключей шифрования и электронной подписи, а также записи и замены сертификатов ключей;
— идентификация протоколов взаимодействия и проверка возможности принудительного навязывания устройству использования незащищенных версий протоколов (HTTP вместо HTTPS, TELNET вместо SSH, SSH1 вместо SSH2);
— проверка корректности обработки мобильным приложением входящих параметров, в том числе с использованием значений различной длины, дублирование отдельных параметров с присвоением им разных значений, включение в значения параметров специальных символов, команд операционной системы, операторов интерпретируемых языков программирования.

2. Выявление известных уязвимостей

2.1. Выявление известных уязвимостей включает в себя:
— выявление известных уязвимостей в сетевых службах;
— выявление типовых уязвимостей в веб-приложениях;
— выявление известных уязвимостей в программном обеспечении;
— выявление учетных записей с паролями, содержащимися в словарях, используемых при проведении исследования.

Данный метод оценки защищенности может являться составной частью метода тестирования на проникновение, не требует наличия у исследователя специальных навыков и допускает полную автоматизацию.

2.2. Известные уязвимости могут быть выявлены следующими способами:

— идентификацией наименований и версий программного обеспечения АБС и поиском в базах данных известных для них уязвимостей;
— запуском тест-программ (эксплойтов), воспроизводящих в полном объеме или частично выполнение компьютерных атак с использованием известных уязвимостей.

2.3. В зависимости от начальных условий для выявления известных уязвимостей могут использоваться стратегии черного ящика и белого ящика.

При стратегии черного ящика исследователю предоставляется доступ к составным частям АБС на уровне протокола IP. Предметом исследования являются уязвимости сетевых служб компонентов АБС, доступных исследователю.

При стратегии белого ящика исследователю предоставляется доступ к интерфейсам управления операционными системами, телекоммуникационным оборудованием, СУБД и серверами приложений с необходимыми правами доступа. Предметом исследования являются все уязвимости программных компонентов АБС, сведения о которых содержатся в используемой исследователем базе данных уязвимостей.

При стратегии белого ящика исследования могут проводиться как с использованием автоматизированных средств анализа защищенности, так и вручную, при стратегии черного ящика исследования проводятся с использованием автоматизированных средств.

2.4. К достоинствам выявления известных уязвимостей как метода оценки защищенности относятся:

— высокая достоверность сведений о выявленных уязвимостях при использовании стратегии белого ящика;
— высокая степень автоматизации, низкие требования к квалификации исследователя при использовании автоматизированных средств анализа защищенности;
— пригодность результатов исследования для оценки степени возможности реализации угроз и степени тяжести последствий из реализации;
— воспроизводимость исследования.

Недостатками выявления известных уязвимостей как метода оценки защищенности являются:

— низкая достоверность сведений о выявленных уязвимостях при использовании стратегии черного ящика;
— возможность сбоев и отказов в функционировании компонентов АБС при проведении исследования с использованием стратегии черного ящика;
— необходимость предоставления исследователю привилегированного доступа к составным частям АБС при использовании стратегии белого ящика.

2.5. Выявление известных уязвимостей в сетевых службах производится при использовании стратегии черного ящика. Исследование включает в себя:

— идентификацию серверов и рабочих мест по их IP-адресам или именам;
— идентификацию сетевых протоколов, доступных для взаимодействия;
— идентификацию программ, обеспечивающих реализацию указанных сетевых протоколов, с определением их наименований и версий по информации, передаваемой при сетевом взаимодействии;
— выборку из базы данных уязвимостей, относящихся к идентифицированным версиям программ;
— выявление уязвимостей сетевых служб путем запуска потенциально применимых к ним эксплойтов.

2.6. Выявление типовых уязвимостей в веб-приложениях производится при использовании стратегии черного ящика. Исследование включает в себя выявление следующих типов уязвимостей:

— инъекции, в особенности SQL-инъекции, OS Command, LDAP и XPath-инъекции;
— подбор аутентификационных данных;
— небезопасная передача данных, в том числе в процессе аутентификации;
— ошибки в контроле доступа (например, небезопасные прямые ссылки на объекты, невозможность ограничения доступа по URL и обход директорий);
— межсайтовый скриптинг (XSS);
— подделка межсайтовых запросов (CSRF);
— расщепление запроса HTTP, сокрытие ответа HTTP;
— открытое перенаправление;
— раскрытие информации о директориях/сценариях;
— предсказуемое расположение ресурсов;

— идентификация приложений;
— чтение произвольных файлов;
— раскрытие чувствительной информации;
— обратный путь в директориях;
— переполнение буфера.

Исследование производится путем анализа данных веб-форм, отправки веб-серверу тестовых запросов с варьируемыми значениями параметров запроса и анализа ответов.

2.7. Идентификация известных уязвимостей программного обеспечения выполняется с использованием стратегии белого ящика. Исследование включает в себя:

— инвентаризацию программного обеспечения, установленного на исследуемом техническом средстве, с идентификацией наименований и версий программ, а также установленных обновлений безопасности;
— выборку из базы данных уязвимостей, относящихся к идентифицированным версиям программ;
— исключение из полученной выборки уязвимостей, устранение которых обеспечено установленными обновлениями безопасности.

2.8. Выявление учетных записей с паролями, содержащимися в словарях, используемых при проведении исследования с использованием стратегий как черного ящика, так и белого ящика. При использовании стратегии черного ящика производятся попытки аутентификации с использованием имен и паролей из используемого словаря. При использовании стратегии белого ящика производятся выборка хеш-значений паролей из конфигурационных файлов, таблиц баз данных и сравнение их с хеш-значениями паролей из используемого словаря.

2.9. По результатам исследования разрабатывается отчет, содержащий:

— перечень компонентов АБС;
— перечень выявленных уязвимостей, оценку степени их критичности для обеспечения ИБ организации БС РФ;
— рекомендации по устранению выявленных уязвимостей.

Оценку критичности уязвимостей рекомендуется определять в соответствии с методикой Common Vulnerability Scoring System (CVSS).

Приложение 4

Рекомендации к проведению контроля параметров настроек технических защитных мер (выявление ошибок конфигурации)

1. Выявление ошибок конфигурации направлено на поддержание корректности функционирования подсистемы ИБ АБС. Для этого в составе рабочей документации АБС или в качестве отдельных внутренних документов организации БС РФ разрабатываются и утверждаются стандарты конфигурации программных и аппаратных компонентов АБС. Выявление ошибок конфигурации — исследование, направленное на поиск несоответствий между фактическими значениями параметров технических мер защиты и их эталонными значениями, установленными в стандартах конфигурации.

2. Исследователю должен быть предоставлен доступ к интерфейсам программных компонентов АБС, в том числе к операционной системе, специализированным банковским приложениям или альтернативный способ получения фактических параметров настройки технических мер защиты.

3. Исследование проводится с использованием стратегии белого ящика. Исследование может проводиться вручную или с использованием автоматизированных средств анализа защищенности. Ошибки конфигурации выявляются путем получения фактических значений параметров настроек и сравнения их с эталонными значениями. При этом:

— в случае, если фактическое значение параметра настройки задано явно, производится его сравнение с эталонным значением;
— в случае, если фактическое значение параметра конфигурации не задано или задано неявно, производится вычисление эффективного значения параметра настройки, которое затем сравнивается с эталонным значением.

Если параметр настройки не задан явно, устройство или программа использует значение по умолчанию, которое может зависеть от модели устройства или версии программы. В ряде случаев фактические параметры настройки задаются не явно, а в виде выражений, результаты вычисления которых зависят от фактических значений других параметров, переменных окружения. В этих случаях в ходе исследования должны быть определены эффективные значения параметров настройки с учетом особенностей их определения в рамках исследуемого компонента АБС.

4. Достоинствами данного метода являются:

— высокая достоверность сведений о выявленных несоответствиях стандартам конфигурации;
— высокая степень автоматизации, низкие требования к квалификации исследователя при использовании автоматизированных средств анализа;
— воспроизводимость исследования.

5. Недостатками данного метода являются:

— невозможность в ряде случаев оценить потенциал реализации каких-либо угроз при несоответствии отдельных настроек стандартам конфигурации. Одним из источников разработки стандартов конфигурации являются рекомендации разработчиков программного и аппаратного обеспечения. Как правило, разработчики не раскрывает информацию об угрозах, реализация которых становится возможной при невыполнении этих рекомендаций;
— необходимость предоставления исследователю привилегированного доступа к компонентам АБС;
— высокие требования к квалификации исследователя в случае, когда необходимо вычисление эффективных значений параметров конфигурации, а также в случае проведения исследования без использования автоматизированных средств анализа.

6. По результатам исследования разрабатывается отчет, содержащий перечень исследованных компонентов АБС, перечень выявленных несоответствий стандартам конфигурации и рекомендации по их устранению.

7. В случае если изменение параметров настройки не было вызвано технической необходимостью, рекомендуется проведение оперативной перенастройки компонентов АБС.

Если изменение параметров настройки было вызвано технической необходимостью и возврат к эталонным значениям может повлечь нарушение функционирования АБС, рекомен-

дуется проведение оценки критичности влияния значений параметров настройки на защищенность АБС. В случае отсутствия такого влияния или несущественного увеличения рисков нарушения ИБ рекомендуется внесение соответствующих изменений в эксплуатационную документацию (стандарты конфигурации). В случае существенного увеличения рисков нарушения ИБ рекомендуется проведение модернизации АБС или ее отдельных компонентов.

Библиография

1. National Checklist Program Repository [Электронный ресурс]: офиц. сайт. США. URL: http://web.nvd.nist.gov/view/ncp/repository (дата посл. обращения: 25.03.2014).
2. Уведомления CERT [Электронный ресурс]: офиц. сайт. URL: http://www.us-cert.gov/ncas/bulletins (дата посл. обращения: 25.03.2014).
3. Alerts, Bulletins & Webinars [Электронный ресурс]: офиц. сайт. США. URL: http://usa.visa.com/merchants/risk_management/cisp_alerts.html#anchor_3 (дата посл. обращения: 25.03.2014).
4. Critical Patch Updates, Security Alerts and Third Party Bulletin [Электронный ресурс]: офиц. сайт. США. URL: http://www.oracle.com/technetwork/topics/security/alerts-086861.html (дата посл. обращения: 25.03.2014).
5. CCE List — Archive [Электронный ресурс]: офиц. сайт. США. URL: http://cce.mitre.org/lists/cce_list.html (дата посл. обращения: 25.03.2014).

ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ

ВЕСТНИК БАНКА РОССИИ

Нормативные акты и оперативная информация
Центрального банка Российской Федерации

№ 70 (1548)

31 ИЮЛЯ 2014

МОСКВА

Учредитель — Центральный банк Российской Федерации
107016, Москва, ул. Неглинная, 12
Адрес официального сайта Банка России: *http://www.cbr.ru*
Тел. 8 (495) 771-43-73, факс 8 (495) 623-83-77, e-mail: *mvg@cbr.ru*

Издание зарегистрировано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций. Регистрационный номер ПИ № ФС77-47238

Издатель и распространитель: ЗАО "АЭИ "ПРАЙМ"
119021, Москва, Зубовский б-р, 4
Тел. 8 (495) 974-76-64, факс 8 (495) 637-45-60, *www.1prime.ru,* e-mail*: sales01@1prime.ru*

Отпечатано в ООО "ЛБЛ Маркетинг Про"
125080, Москва, Ленинградское ш., 46/1

Москва, 2014