VI Уральский Форум
«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ БАНКОВ»
Республика Башкортостан, ДЦ «Юбилейный»
17-22 февраля 2014 года

Обновленные модели угроз для ДБО и PCI

Павел Головлев
paulmg69@gmail.com

Ассоциация Российских Банков

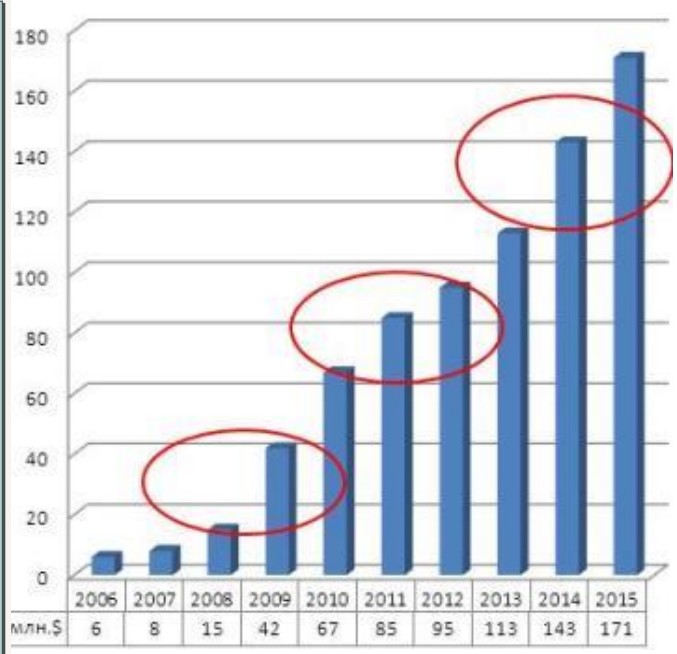
Член комитета по банковской безопасности АРБ
Член правления АРСИБ
Эксперт ассоциации BISA

DISCLAIMER

Мнение, высказанное в настоящем докладе, является личным мнением автора и может не совпадать ни с одной официальной позицией и даже быть ошибочным.

Защищаемые активы

Модель угроз для ДБО



Аналитический центр компании "Техносерв", 2012

Один инцидент на 250 тысяч платежей.
90% операторов не выявляют инцидентов.
8% операторов выявляют менее 10 инцидентов в месяц.
2% операторов выявляют более 10 инцидентов в месяц.

Удельная величина риска в системах ДБО составляет 0.001 коп./руб.
Средняя сумма одного инцидента может быть оценена в 250 т.руб.

Актуальность угроз для ДБО

1	Компрометация компьютеров, на которых установлено ДБО. **Нарушитель:** внешний злоумышленник.	**XX%🡻6%**
2	Компрометация ключей системы ДБО. **Нарушитель:** сотрудник компании клиента.	**XX%🡻5%**
3	Мошеннические действия со стороны Клиента. **Нарушитель:** Клиент.	**XX%🡹5%**
4	Мошеннические действия со стороны лица, получившего доступ к сети Банка (как внутренний - законный, так и внешний – незаконный). **Нарушитель:** Сотрудник банка, обладающий законными правами, и третье лицо, не обладающее законными правами	**XX%🡹3%**
5	Прямая атака на систему ДБО с целью создания подложного документа. **Нарушитель:** Внешний нарушитель	**XX%🡹1%**
6	Подделка документов для получения ключей к системе ДБО клиента юридического лица. **Нарушитель:** сотрудник компании клиента.	**XX%🡹1%**
7	Подделка документов для получения ключей к системе ДБО клиента юридического лица. **Нарушитель:** сотрудник операционного подразделения Банка.	**XX%**
	Прочие угрозы	***XX%***

Эффективность защитных мер для ДБО

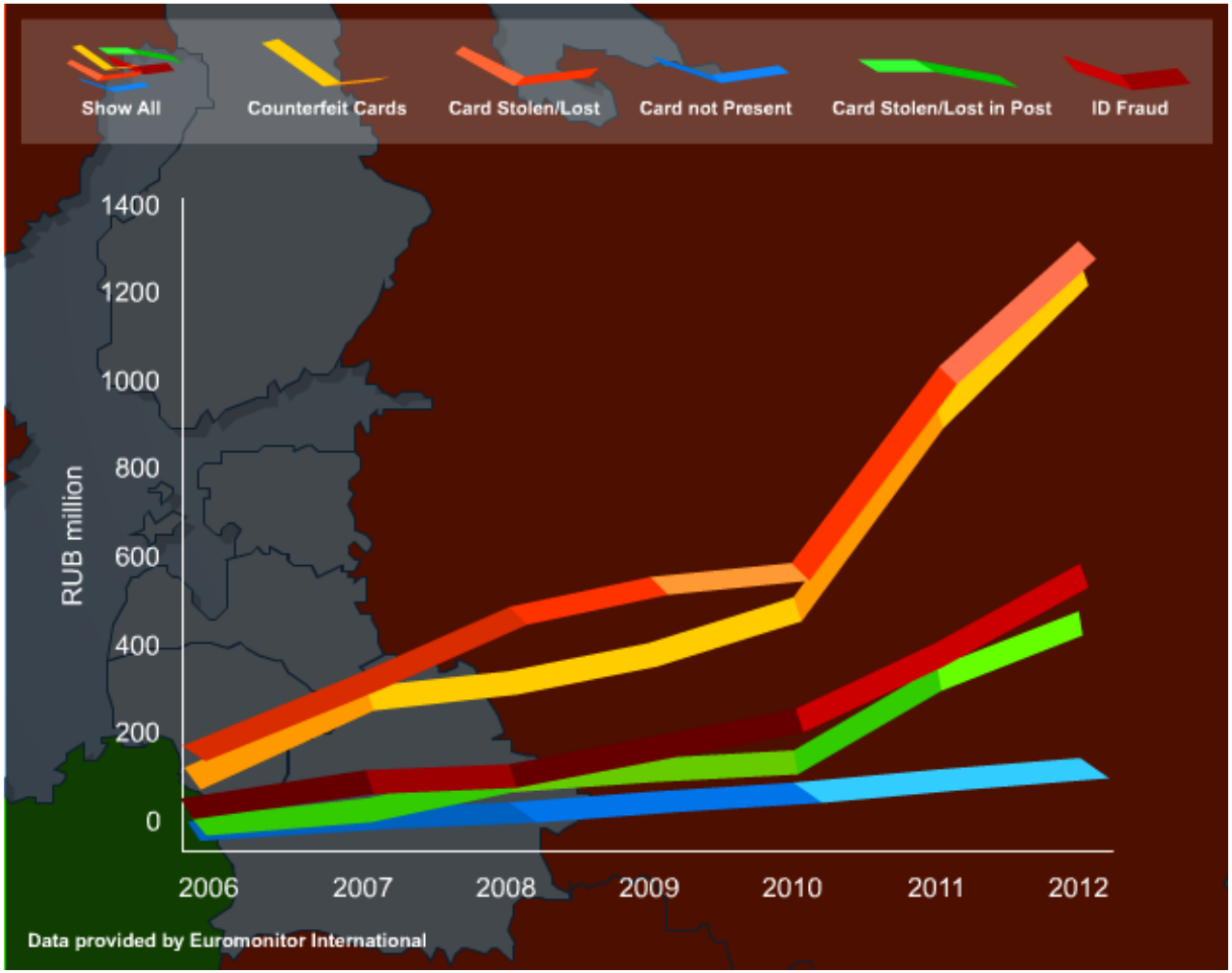
1	Наличие в Банке системы FRAUD-мониторинга, отслеживающей нестандартные операции клиента.	**XX.xx%↓0.11%**
2	Карантин на реальное исполнение операции (задержка от уведомления клиента до реального исполнения документа).	**XX.xx%↑11.33 %**
3	Осуществление Банком информирования клиентов обо всех операциях совершенных от их имени.	**XX.xx%↓0.04%**
4	Реализация в системе ДБО у клиента двух разнесенных рабочих мест (оператора и контролера).	**XX.xx%↑4.87%**
5	Наличие в Банке системы FRAUD-мониторинга, разрешающей операции клиента только с доверенными контрагентами (белый список).	**XX.xx%↑2.86%**
6	Использование оборудования с неизвлекаемыми ключами.	**XX.xx%↓3.58%**
7	Наличие в Банке системы FRAUD-мониторинга, отслеживающей операции клиента с подозрительными контрагентами (черный список).	**XX.xx%↑3.99%**
8	В договоре с клиентом указываются лимиты операций клиента, что позволяет снизить максимальный размер ущерба.	**XX.xx%↑3.68%**

9	Использование клиентом оборудования (работоспособность оборудования должна регулярно проверяться) ограничивающего входящий и исходящий интернет-трафик только с доверенными сайтами.	**XX.xx%↓0.95%**
10	Использование клиентом антивирусных программ (антивирусные базы должны регулярно обновляться, регулярно должно осуществляться полное сканирование компьютера, работоспособность антивируса должна проверяться).	**XX.xx%↓0.96%**
11	Использование клиентом антивирусных программ проверки почтовых сообщений (антивирусные базы должны регулярно обновляться, работоспособность антивируса должна проверяться).	**XX.xx%↓3.34%**
12	Использованием на компьютере клиента средств контроля целостности операционной системы и программных компонентов, задействованных при работе в системе ДБО.	**XX.xx%↑3.07%**
13	Контроль на компьютере клиента работы учетных записей с расширенными правами (администраторов).	**XX.xx%↑6.59%**
14	Запрет работы за компьютером клиента недоверенного персонала.	**XX.xx%↑4.05%**

15	Разработка и распространение материалов (мультимедиа, брошюры, плакаты, заставки и т.д.), повышающих бдительность клиентов.	**XX.xx%↓2.06%**
16	Осуществление Клиентом программы проверки лояльности сотрудников.	**XX.xx%↑4.88%**
17	Контроль оформляемых документов на ЭЦП (побайтовое сравнение электронной и бумажной версии).	**XX.xx%↑4.15%**
18	Использование клиентом DLP-систем, сохраняющих в теневых копиях поступающие в компьютер данные.	**XX.xx%↑4.43%**
19	Запрет клиентом на использование в DLP-системах средств подмены сертификатов сайтов.	**XX.xx%↑4.73%**
20	Контроль сроков действия ключей и сроков полномочий.	**XX.xx%↑3.29%**
21	Контроль функционирования механизмов авторизации в Банке.	**XX.xx%↑2.04%**
22	Анализ защищенности серверов ДБО.	**XX.xx%↑1.85%**
23	Анализ защищенности АБС.	**XX.xx%↑2.39%**
24	Использование в Банке средств протоколирования действий.	**XX.xx%↑1.31%**

25	Наличие в Банке системы FRAUD-мониторинга, отслеживающей использование новых ключей.	**XX.xx%↑0.67%**
26	Наличие в договоре обязанности клиента по обращению в правоохранительные органы.	**XX.xx%↑1.65%**
27	Наличие процедуры сверки выданных ключей к системе ДБО у Банка и у клиента. (Следует учесть, что клиент у клиента может не быть соглашения с Банком об использовании системы ДБО.)	**XX.xx%↑0.13%**
28	Осуществление Банком программы проверки лояльности сотрудников.	**XX.xx%↑0.44%**
29	Использование в Банке DLP-решений.	**XX.xx%↑0.06%**

Модель угроз для PCI



Source: FICO™ Banking Analytics Blog. Data provided by Euromonitor International.

Удельный риск:15 коп./1000 руб.

Актуальность угроз для PCI

1	Хищение авторизационных данных карты при ее использовании в сети Интернет.	**XX%↑2%**
2	Перехват авторизационных карточных данных при использовании банкоматов, POS-терминалов, терминалов самообслуживания с помощью установки скиммера.	**XX%↓5%**
3	Хищение карты у клиента.	**XX%↑1%**
4	Снятие наличных по поддельным картам.	**XX%↑3%**
5	Физическая атака на банкомат.	**XX%↓6%**
6	Мошенничество в точке продаж.	**XX%↓1%**
7	Выпуск карт на подставных лиц.	**XX%↑1%**
8	Cash Trapping.	**XX%↓1%**
9	Cash Trapping – Reversal.	**XX%**
10	Недоступность процессинга.	**XX%**
11	Ложный банкомат.	**XX%↑3%**
12	Ложный терминал.	**XX%↑3%**

13	Физическая кража авторизационных карточных данных до выдачи их клиенту.	**XX%↑2%**
14	Перехват авторизационных карточных данных при использовании банкоматов, POS-терминалов, терминалов самообслуживания, удаленное управление устройствами с помощью установки вредоносного программного обеспечения или постороннего оборудования.	**XX%↓2%**
15	Компрометация процессинга.	**XX%↓1%**
16	Перехват авторизационных карточных данных при использовании банкоматов, POS-терминалов, терминалов самообслуживания на сетевом уровне.	**XX%↑1%**
17	Компрометация криптографических ключей банкомата/терминала и/или криптомаршрутизатора.	**XX%↑1%**
	Прочие угрозы	***XX%***

Эффективность защитных мер для PCI

1	Информирование клиента по операциям, проведенным с использованием банковских карт.	**XX.xx%↑3.82%**
2	Установка устройств в защищенных местах.	**XX.xx%↓6.67%**
3	Использование технологии 3DS (или аналогичной).	**XX.xx%↑3.36%**
4	Разработка и распространение материалов (мультимедиа, брошюры, плакаты, заставки и т.д.), повышающих бдительность клиентов.	**XX.xx%↑3.27%**
5	Использование видеофиксации окружающей обстановки рядом с устройствами.	**XX.xx%↑0.05%**
6	Контроль за работоспособностью устройств в режиме 24*7.	**XX.xx%↓2.88%**
7	Фрод-мониторинг.	**XX.xx%↑0.11%**
8	Периодический осмотр устройств.	**XX.xx%↓0.68%**
9	Анализ финансовых потоков.	**XX.xx%↑1.11%**
10	Установка пассивного и активного антискиммингового оборудования.	**XX.xx%↓2.38%**
11	Корректная установка ограничений на объем операций.	**XX.xx%↓1.13%**
12	Страхование банкоматов.	**XX.xx%↓4.77%**

13	Раздельное хранение клиентом карты и пин-кода.	**XX.xx%↓0.71%**
14	Ограничение на авторизацию по магнитной полосе для чиповой карты в устройстве, поддерживающем чиповую авторизацию.	**XX.xx%↑0.9%**
15	Установка сигнализации на банкомат.	**XX.xx%↓3.19%**
16	Раздельное хранение идентификационных и авторизационных данных карт.	**XX.xx%↑1.06%**
17	Раздельная инкассация идентификационных и авторизационных данных карт.	**XX.xx%↑1.04%**
18	Раздельная выдача идентификационных и авторизационных данных карт клиенту.	**XX.xx%↑0.83%**
19	Двойной контроль документов.	**XX.xx%↓0.12%**
20	Безопасное хранение криптографических ключей.	**XX.xx%↑0.9%**
21	Установка и проверка требований по доступности процессинга.	**XX.xx%↓0.3%**
22	Отказ от доступа в тамбуры по картам.	**XX.xx%↑0.44%**

23	Назначение ответственных за использование криптографических ключей.	**XX.xx%↑0.72%**
24	Проведение нагрузочных исследований процессинга.	**XX.xx%↓0.87%**
25	Контроль предприятий, принимаемых на эквайринг.	**XX.xx%↓0.35%**
26	Очистка входящего трафика.	**XX.xx%↑0.31%**
27	Учет криптографических ключей.	**XX.xx%↑0.49%**
28	Контроль устройств.	**XX.xx%↑0.78%**
29	Раздельное изготовление идентификационных и авторизационных данных карт.	**XX.xx%↑1.14%**
30	Выполнение требований PCI DSS.	**XX.xx%↓0.42%**
31	Регулярное подтверждение PCI DSS.	**XX.xx%↓0.14%**
32	Использование антивирусной защиты.	**XX.xx%↓0.03%**

33	Использование средств контроля целостности кода.	**XX.xx%🡻1.29%**
34	Активация карты клиентом после получения.	**XX.xx%🡹0.95%**
35	Анализ регламентов техобслуживания процессинга.	**XX.xx%🡻0.6%**
36	Использование стойкой криптографии (3DES).	**XX.xx%🡹0.85%**
37	Физическая защита эмбосерных.	**XX.xx%🡹0.99%**
38	Доступ в эмбосерные возможен при наличии не менее 2-х человек.	**XX.xx%🡹0.99%**
39	Контроль USB устройств.	**XX.xx%🡻0.95%**
40	Учет и контроль идентификационных и авторизационных данных.	**XX.xx%🡹0.82%**
41	Контроль операций с банкоматом.	**XX.xx%🡻0.56%**
42	Система видеонаблюдения в эмбосерных.	**XX.xx%🡹0.93%**

43	Обучение персонала эквайринговых предприятий.	**XX.xx%🡻0.92%**
44	Использование средств контроля целостности оборудования.	**XX.xx%🡻0.68%**
45	Анализ программного кода приложений на наличие потенциальных уязвимостей.	**XX.xx%🡻0.33%**
46	Контроль учетных записей пользователей устройств.	**XX.xx%🡻0.37%**
47	Раздельное изготовление, хранение, передача и ввод компонент ключей.	**XX.xx%🡹0.2%**
48	Проход в эмбосерные через шлюзовые камеры.	**XX.xx%🡹0.76%**
49	Использование для генерации ключей HSM.	**XX.xx%🡹0.08%**
50	Физическая защита средств изготовления ключей.	**XX.xx%🡹0.07%**
51	Гарантированное уничтожение носителей после ввода ключей.	**XX.xx%🡹0.12%**
52	Регламентация одежды для людей, работающих в эмбосерных.	**XX.xx%🡹0.31%**

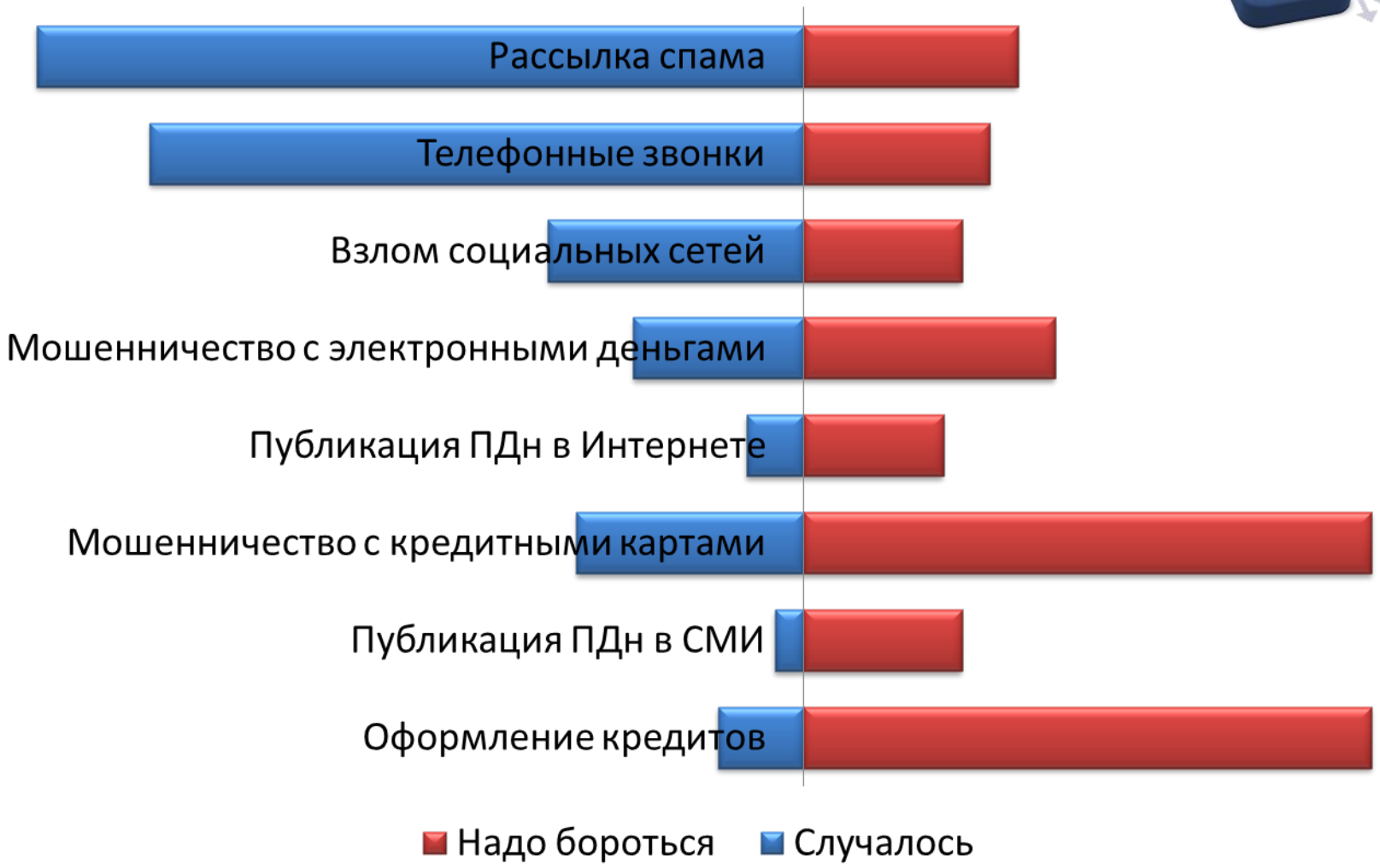
Модели угроз для клиентских средств

ПРАКТИЧЕСКОЕ ПРИМЕНЕНИЕ:

1)Валовый объем платежей за год: 1 трлн. руб.
2)Удельный риск мошенничества: 1коп/1000руб.
3)Сумма «под риском»: 10 млн.руб.
4)Прогноз риска
5)Эффективность защитных мер:
6)Остаточный риск
7)Прогноз остаточного риска
8)Стоимость защитных мер
9)TSO
10)ROI
11)…….

$$K = 1 - \prod_{i=1}^{n} (1 - Ki)$$

Модель угроз для ПДн



(Источник данных: «ФОМнибус» – опрос граждан РФ от 18 лет и старше. 7 апреля 2013. 43 субъекта РФ, 100 населенных пунктов, 1500 респондентов. Интервью по месту жительства. Статпогрешность не превышает 3,6%.)

Актуальность угроз для ПДн

Актуальные классы вреда для субъектов ПДн

Актуальные классы угроз для ПДн

39) Осуществление несанкционированного доступа к персональным данным путем использования методов социального инжиниринга к легальным субъектам доступа.

13) Осуществление несанкционированного доступа к персональным данным с использованием уязвимостей, вызванных недостатками организации защиты персональных данных.

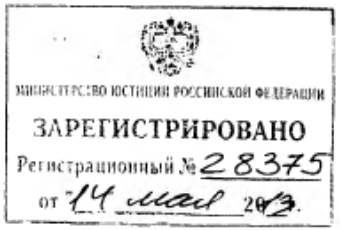
46) Осуществление несанкционированного доступа к персональным данным путем внедрения вредоносного программного обеспечения.

7) Утрата (потеря) накопителей с персональными данными, включая переносные персональные компьютеры пользователей информационной системы персональных данных.

3) Использование системного и прикладного программного обеспечения автоматизированных рабочих мест пользователей информационной системы персональных данных, приводящее к несанкционированному доступу к персональным данным.

4) Осуществление несанкционированного доступа к персональным данным в ходе сопровождения, модернизации и (или) вывода из эксплуатации компонентов информационной системы персональных данных.

Эффективность защитных мер для ПДн



ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК России)

П Р И К А З

«18» февраля 2013 г. Москва № 21

Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

В соответствии с частью 4 статьи 19 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (Собрание законодательства Российской Федерации, 2006, № 31, ст. 3451; 2009, № 48, ст. 5716; № 52, ст. 6439; 2010, № 27, ст. 3407; № 31, ст. 4173, ст. 4196; № 49, ст. 6409; 2011, № 23, ст. 3263; № 31, ст. 4701) и Положением о Федеральной службе по техническому и экспортному контролю, утвержденным Указом Президента Российской Федерации от 16 августа 2004 г. № 1085 (Собрание законодательства Российской Федерации, 2004, № 34, ст. 3541; 2006, № 49, ст. 5192; 2008, № 43, ст. 4921; № 47, ст. 5431; 2012, № 7, ст. 818),

П Р И К А З Ы В А Ю:

1. Утвердить прилагаемые Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

ВОПРОСЫ?

Павел Головлев
paulmg69@gmail.com

Член комитета по банковской безопасности АРБ
Член правления АРСИБ
Эксперт ассоциации BISA