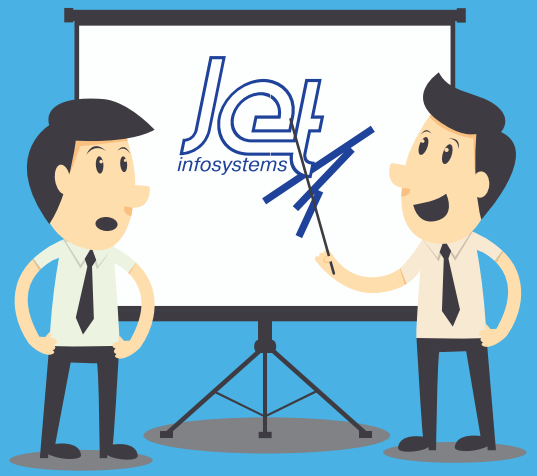
Подготовлено компанией «Инфосистемы Джет»
E-mail: is@jet.su
Тел.: +7 (495) 411-7601

СТО БР ИББС 2014:
АКТУАЛЬНЫЕ ИЗМЕНЕНИЯ

Компания «Инфосистемы Джет» представляет комментарии, посвященные изменениям в стандартах Банка России – СТО БР ИББС–1.0–2014, СТО БР ИББС–1.2–2014.

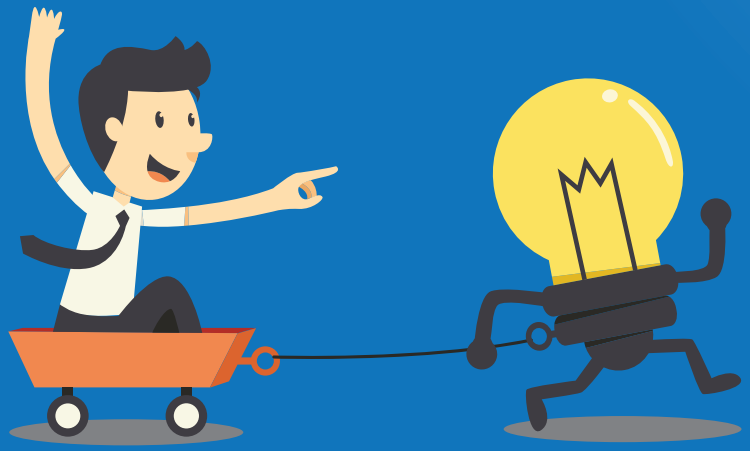
Комментарии основаны на оценках ведущих экспертов компании «Инфосистемы Джет» в области выполнения проектов по приведению в соответствие требованиям регуляторов.

В комментариях представлены ключевые нововведения стандартов Банка России, которые могут оказать влияние на методику оценки соответствия комплексу стандартов, а также на способы выполнения банками требований по информационной безопасности (ИБ).



С 1 июня 2014 года вступили в силу новые редакции стандартов Банка России (СТО БР ИББС–1.0–2014, СТО БР ИББС–1.2–2014), определяющие требования к банкам по информационной безопасности (ИБ) и методику оценки соответствия.

Комплекс стандартов является обязательным для тех, кто уже к нему присоединился, а это более 500 банков.



ОСНОВНЫЕ НОВОВВЕДЕНИЯ:

- требования в области защиты ПДн приведены в соответствие действующему законодательству, а также Банк России признает неактуальными угрозы безопасности ПДн, связанные с наличием недекларированных возможностей в системном и прикладном ПО;
- ряд новых требований предполагает внедрение дополнительных средств защиты, таких как средства защиты от утечек информации и системы противодействия мошенничеству;
- состав оцениваемых показателей изменился с 423 до 490; кроме того, в результатах аудита необходимо учитывать показатели из Положения Банка России от 9 июня 2012 г. №382–П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств ...».

ОБЗОР

Содержание стандартов Банка России – СТО БР ИББС–1.0–2014, СТО БР ИББС–1.2–2014 – дополнилось рядом новых положений, обновления коснулись почти всех разделов стандарта.

В своих комментариях мы выделили пять основных направлений, изменения в которых могут оказать существенное влияние на развитие систем информационной безопасности в российских банках:

01 Инфраструктурная безопасность и новые технологии

02 Изменения в методике оценки соответствия

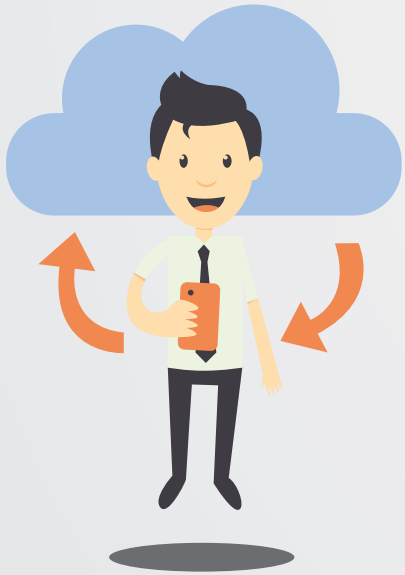
03 Обеспечение безопасности ПДн

04 Борьба с мошенничеством

05 Защита от утечек информации

Далее мы расскажем подробнее об изменениях по каждому из направлений.

01 ИНФРАСТРУКТУРНАЯ БЕЗОПАСНОСТЬ И НОВЫЕ ТЕХНОЛОГИИ



В стандарте СТО БР ИББС появился ряд новых положений по обеспечению безопасности базовой информационной инфраструктуры.

Появились требования, касающиеся эксплуатации автоматизированных банковских систем (АБС): внедрение процедур контроля отсутствия уязвимостей в оборудовании и ПО АБС, внесение изменений в АБС и систему обеспечения ИБ (п. 7.3.9 [1]).

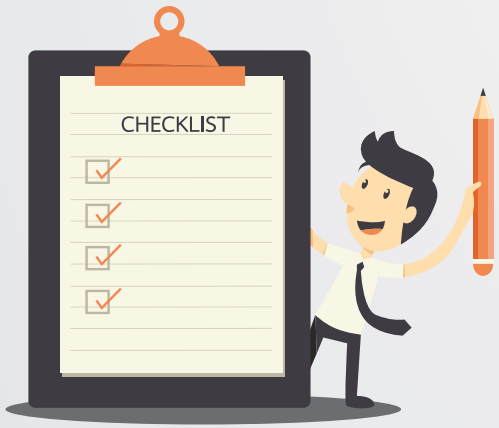
Подсистема обеспечения ИБ при управлении доступом и регистрацией дополнилась требованиями:

- контроля использования технологий беспроводного доступа к информации и защиты беспроводных соединений (п. 7.4.3 [1]);
- контроля использования мобильных устройств для доступа к информации (п. 7.4.3 [1]);
- разделения сегментов вычислительных сетей, в том числе создаваемых с использованием технологии виртуализации (п. 7.4.5 [1]).

Разделение сегментов необходимо для обеспечения независимого выполнения банковских платежных и информационных технологических процессов разной степени критичности, в том числе процессов, включающих обработку персональных данных в ИСПДн.

02

ИЗМЕНЕНИЯ В МЕТОДИКЕ ОЦЕНКИ СООТВЕТСТВИЯ



Согласно новой редакции стандарта к защищаемым активам относится информация, необходимость защиты которой указана и в Положении Банка России №382–П. Теперь при оценивании частных показателей в рамках групповых показателей М1–М7 для банковского платежного технологического процесса следует учитывать актуальные результаты последней по времени проверки на соответствие требованиям к обеспечению защиты информации при осуществлении переводов (п. 7.1.9 [2] Положения Банка России №382–П).

То есть теперь выполнение требований Положения 382–П впрямую влияет на уровень оценки по стандарту. Для упрощения понимания влияния показателей по 382–П на оцениваемые показатели по стандарту Банка России разработана специальная таблица соответствия частных показателей требованиям к обеспечению защиты информации при осуществлении переводов денежных средств.

Изменения также коснулись самой методики оценки соответствия. В прежней редакции в формуле расчета групповых показателей присутствовал коэффициент значимости (не применялся он только при расчете показателя, касающегося обработки ПДн). В новой методике оценки указанный коэффициент упразднен, по аналогии с методикой оценки соответствия из Положения Банка России №382–П введен корректирующий коэффициент, а в приложении с показателями ИБ появилось три категории проверки в зависимости от вида предъявляемых требований.

03 ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПДн

Существенно претерпел изменения раздел стандарта, касающийся обеспечения безопасности ПДн.

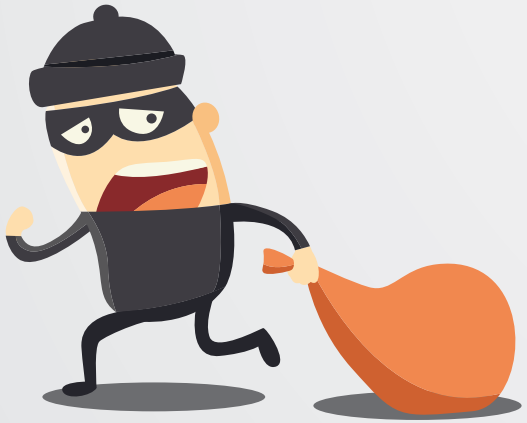
Разработка модели угроз позиционируется как непрерывный процесс: банки теперь должны регулярно пересматривать модели угроз и нарушителей ИБ (п. 6.12 [1]).

Раздел, посвященный обеспечению ИБ банковских технологических процессов, в рамках которых обрабатываются ПДн, переработан с учетом положений постановления Правительства РФ от 1 ноября 2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». Угрозы первого и второго типов, связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном ПО, используемом в ИСПДн, признаются Банком России неактуальными для банков (п. 7.11.4 [1]).

Выбор сертифицированных средств защиты информации для обеспечения безопасности ПДн необходимо осуществлять в соответствии с требованиями приказа ФСТЭК России от 18 февраля 2013 г. №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (п. 7.11.8 [1]).

Раздел «Особенности оценки степени выполнения требований стандарта, регламентирующих защиту ПДн в информационных системах персональных данных», а также приложение с уточняющими вопросами для оценки соответствия требованиям по защите ПДн в новой редакции отсутствуют.

04 БОРЬБА С МОШЕННИЧЕСТВОМ



«Намеки» на необходимость использования специализированных antifraud-решений есть в нескольких пунктах стандарта. Остановимся подробнее на требованиях по выявлению неправомерных или подозрительных операций и транзакций.

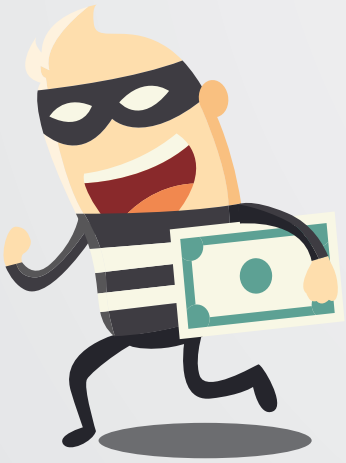
ПУНКТ СТАНДАРТА [1]	СОДЕРЖАНИЕ ТРЕБОВАНИЯ
7.4.4	В организации БС РФ должны быть определены, выполняться, регистрироваться и контролироваться правила и процедуры мониторинга ИБ, анализа и хранения данных о действиях и операциях, позволяющие выявлять неправомерные или подозрительные операции и транзакции. Для проведения процедур мониторинга ИБ и анализа данных о действиях и операциях следует использовать специализированные программные и (или) технические средства.
7.6.6	При осуществлении дистанционного банковского обслуживания должны применяться защитные меры, предотвращающие возможность подмены авторизованного клиента злоумышленником в рамках сеанса работы.
7.8.6	Комплекс защитных мер банковского платежного технологического процесса должен предусматривать в том числе: - контроль, направленный на исключение возможности совершения злоумышленных действий, в частности двойной ввод, сверка, установление ограничений в зависимости от суммы совершаемых операций.
7.8.7	Для систем дистанционного банковского обслуживания должны применяться защитные механизмы, реализующие: - снижение вероятности выполнения непреднамеренных или случайных операций или транзакций авторизованными клиентами.

БОРЬБА С МОШЕННИЧЕСТВОМ
продолжение

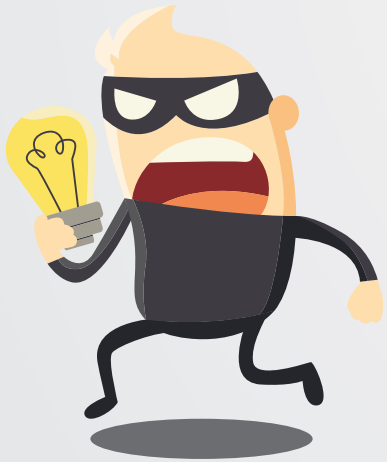
В новой версии стандарта эти пункты дополнены упоминанием мониторинга ИБ совместно с выявлением подозрительных транзакций, а также новыми показателями для оценки соответствия, в том числе из Положения Банка России №382–П.

В таблице ниже представлены частные показатели оценок, имеющие отношение к противодействию мошенническим операциям.

№ ЧАСТОТНОГО ПОКАЗАТЕЛЯ ИБ [2]	СОДЕРЖАНИЕ ПОКАЗАТЕЛЯ
М5.13	Применяются ли при осуществлении дистанционного банковского обслуживания защитные меры, предотвращающие возможность подмены авторизованного клиента злоумышленником в рамках сеанса работы?
М3.22	Определены ли, выполняются ли, регистрируются ли и контролируются ли в организации БС РФ правила и процедуры мониторинга ИБ, анализа и хранения данных о действиях и операциях, позволяющие выявлять неправомерные или подозрительные операции и транзакции?
М3.31	Используются ли для проведения процедур мониторинга ИБ и анализа данных о действиях и операциях специализированные программные и (или) технические средства?
М3.32	Зафиксированы ли критерии выявления неправомерных или подозрительных действий и операций, используемые при проведении процедур мониторинга ИБ и анализа данных о действиях и операциях?

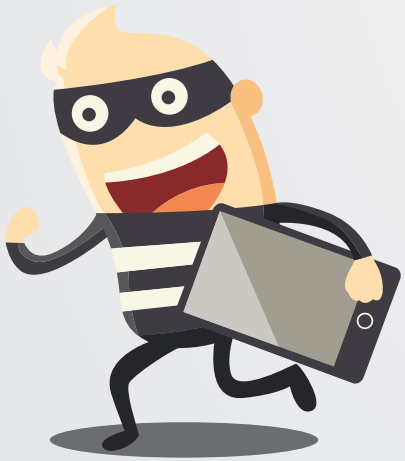


БОРЬБА С МОШЕННИЧЕСТВОМ
продолжение



№ ЧАСТОТНОГО ПОКАЗАТЕЛЯ ИБ [2]	СОДЕРЖАНИЕ ПОКАЗАТЕЛЯ
М3.33	Применяются ли процедуры мониторинга ИБ и анализа данных о действиях и операциях, использующие зафиксированные критерии выявления неправомерных или подозрительных действий и операций, на регулярной основе, например, ежедневно, ко всем выполненным операциям (транзакциям)?
М5.13	Применяются ли при осуществлении дистанционного банковского обслуживания защитные меры, предотвращающие возможность подмены авторизованного клиента злоумышленником в рамках сеанса работы?
М7.6	Предусматривает ли комплекс защитных мер банковского платежного технологического процесса защиту платежной информации от искажения, фальсификации, переадресации, несанкционированного уничтожения, ложной авторизации электронных платежных сообщений?
М7.12	Предусматривает ли комплекс защитных мер банковского платежного технологического процесса контроль, направленный на исключение возможности совершения злоумышленных действий, в частности двойной ввод, сверка, установление ограничений в зависимости от суммы совершения операций?
М7.18	Применяются ли для систем дистанционного банковского обслуживания процедуры, реализующие снижение вероятности выполнения непреднамеренных или случайных операций или транзакций авторизованными клиентами?

04 БОРЬБА С МОШЕННИЧЕСТВОМ
окончание



В стандарте есть требование (п. 7.4.4 [1]) к использованию специализированных программных или технических средств для проведения процедур мониторинга ИБ и анализа данных с целью выявления неправомерных действий. В прежней редакции стандарта это было указано в качестве рекомендации.

Системы дистанционного банковского обслуживания сами по себе не имеют встроенных механизмов для реализации требуемого функционала по умолчанию.

Для эффективного выявления подозрительных транзакций используются специализированные средства, позволяющие создавать профиль авторизованного пользователя и обнаруживать отклонения от стандартных параметров.

Применение таких средств обусловлено рядом объективных причин:

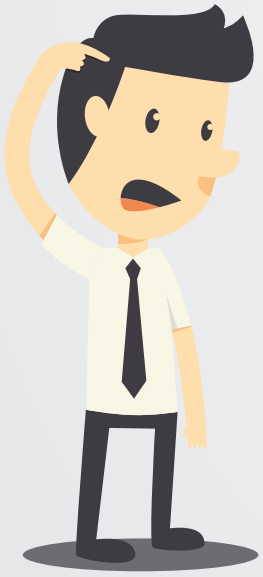
- высокие требования к производительности решения;
- формирование надежного и эффективного профиля клиента;
- отсутствие рычагов воздействия на antifraud-механизмы, встроенные в системы дистанционного банковского обслуживания.

05 ЗАЩИТА ОТ УТЕЧЕК ИНФОРМАЦИИ

В новой редакции стандарта окончательно укоренилось понятие защиты от утечек информации, а также появились новые требования в этом направлении.

ПУНКТ СТАНДАРТА [1]	СОДЕРЖАНИЕ ТРЕБОВАНИЯ
7.4.8	В организации банковской системы РФ должен быть определен, выполняться и контролироваться порядок использования съемных носителей информации.
7.6.2	Должны быть определены, выполняться, регистрироваться и контролироваться процедуры подключения и использования ресурсов сети Интернет.
7.6.9	Электронная почта должна архивироваться. Целями создания архивов электронной почты являются: - контроль информационных потоков, в том числе с целью предотвращения утечек информации; - использование архивов при проведении разбирательств по фактам утечек информации.

ЗАЩИТА ОТ УТЕЧЕК ИНФОРМАЦИИ
продолжение

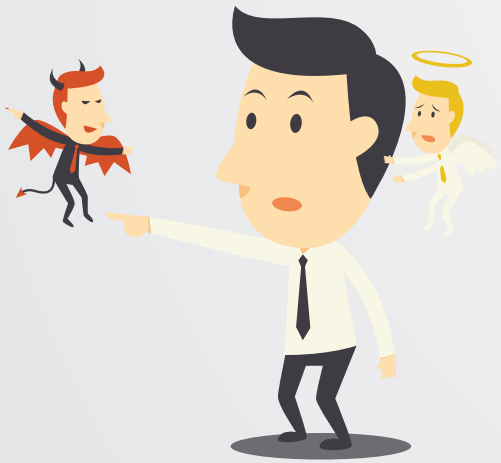


Частные показатели оценок деятельности по защите от утечек информации представлены в таблице.

№ ЧАСТОТНОГО ПОКАЗАТЕЛЯ ИБ [2]	СОДЕРЖАНИЕ ПОКАЗАТЕЛЯ
М3.18	Определены ли, выполняются ли, регистрируются ли и контролируются ли правила и процедуры выявления и блокирования несанкционированного перемещения (копирования) информации, в том числе баз данных, файловых ресурсов, виртуальных машин?
М3.40	Определен ли, выполняется ли и контролируется ли в организации банковской системы РФ порядок использования съемных носителей информации?
М5.6	Определены ли, выполняются ли, регистрируются ли и контролируются ли в организации банковской системы РФ процедуры подключения и использования ресурсов сети Интернет?
М5.10	Определены ли и выполняются ли процедуры протоколирования посещения ресурсов сети Интернет работниками организации банковской системы РФ?
М5.11	Доступны ли данные о посещенных сотрудниками организации банковской системы РФ ресурсов сети Интернет работникам службы ИБ?
М5.20	Осуществляется ли архивирование электронной почты с целью: - контроля информационных потоков, в том числе с целью предотвращения утечек информации; - использования архивов при проведении разбирательств по фактам утечек информации?

05

ЗАЩИТА ОТ УТЕЧЕК ИНФОРМАЦИИ
окончание



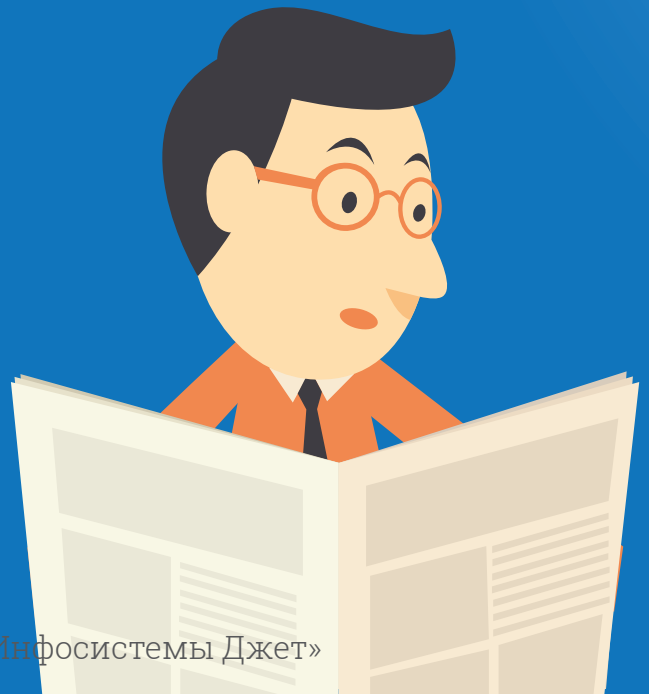
Для выполнения указанных выше требований стандарта можно использовать штатные средства базовой инфраструктуры: групповые политики домена, стандартные журналы почтового и прокси-серверов и др.

Однако, если говорить об удобном инструменте, который позволит ежедневно контролировать реальное соответствие требованиям, быстро и удобно изменять настройки в соответствии с развитием бизнеса банка, получать наглядную отчетность, – без специализированного решения не обойтись.

Упомянутый в требованиях и частных показателях функционал наиболее полно может быть реализован средствами класса DLP, которые позволяют:

- удобно контролировать использование съемных носителей и логировать все действия, производимые с ними;
- осуществлять гибкую настройку правил доступа к ресурсам Интернет и вести понятную отчетность;
- создавать архив электронной корпоративной почты;
- осуществлять интеллектуальный анализ данных для проведения расследований по фактам утечек информации.

В ЗАКЛЮЧЕНИЕ:



Изменения объективно отражают актуальные угрозы современных информационных систем. В новой редакции стандарта наблюдается эволюционное развитие требований, которые позволят банкам постепенно развивать существующие системы защиты.

Стандарт очень гармонично дополнен тематикой обеспечения соответствия требованиям в области ИБ национальной платежной системы, что, безусловно, повышает его ценность.

В части защиты ПДн требования стандарта переработаны с учетом действующего законодательства и позволяют отказаться от высоких уровней защищенности, а значит, и от внедрения большого количества дорогостоящих подсистем ИБ.

ОБ АВТОРЕ:

Елена Козлова – руководитель направления Security Compliance в компании «Инфосистемы Джет».

Елена обладает более чем семилетним опытом выполнения проектов, связанных с направлением Security Compliance и защитой гостайны.

Образование в области информационной безопасности получила в ФГБОУ ВПО «Юго-Западный государственный университет».

Елена – автор ряда научных работ и статей, посвященных различным аспектам информационной безопасности.

БИБЛИОГРАФИЯ:

[1]. Стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения». СТО БР ИББС–1.0–2014.

[2]. Стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС–1.0–2014». СТО БР ИББС–1.2–2014.

О КОМПАНИИ «ИНФОСИСТЕМЫ ДЖЕТ»

Компания «Инфосистемы Джет» – один из крупнейших российских системных интеграторов – образована в 1991 году.

Основные направления деятельности компании: бизнес-решения и программные разработки, ИТ- и телекоммуникационная инфраструктура, информационная безопасность, ИТ-аутсорсинг и техническая поддержка, управление комплексными проектами и др.

Компания располагает региональными офисами в семи городах России — от Санкт-Петербурга и Краснодара до Владивостока, а также представительствами на Украине, в Казахстане, Азербайджане и Узбекистане.

О ЦЕНТРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Компания «Инфосистемы Джет» работает в сфере ИБ более 18 лет и на сегодняшний день обладает уникальным набором компетенций в данной области. Своей главной задачей компания ставит создание решений, обеспечивающих реальную безопасность бизнеса.

Центр информационной безопасности компании «Инфосистемы Джет» на рынке ИБ — это:

- реализация более 230 комплексных проектов в сфере ИБ в год;
- более 210 экспертов в области ИБ;
- № 1 на рынке ИБ-интеграции в коммерческих организациях (независимое аналитическое агентство Anti-Malware.ru, 2010);
- № 1 среди интеграторов по объему предоставления услуг ИБ на российском рынке (экспертное исследование «Рынок информационной безопасности Российской Федерации», 2013);
- уникальные собственные продукты, занимающие ведущие позиции в своих сегментах;
- оказание услуг аутсорсинга ИБ со строгими SLA.