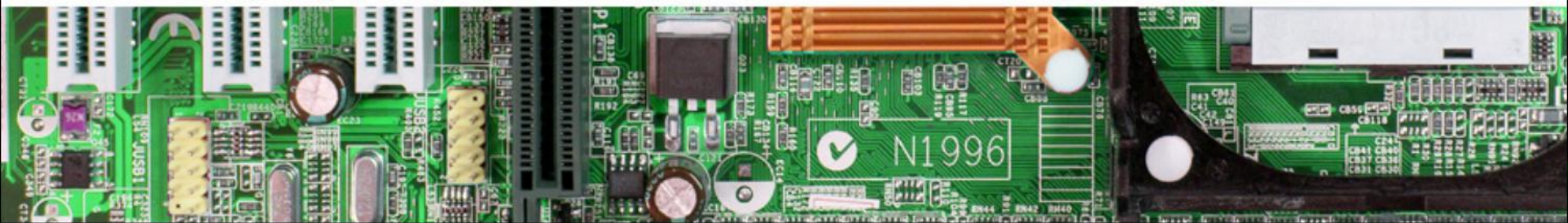
Информационная безопасность в банковском секторе: повышение уровня защищенности и выполнение требований регуляторов

Андрей Рыбин

Руководитель комплексных проектов

Global Trust Solutions

Продукты и услуги в области информационной безопасности



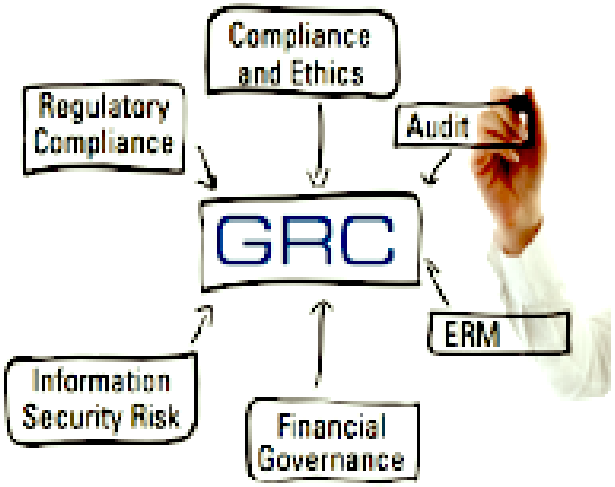
Самые актуальные угрозы для банковской сферы по мнению МВД

Основной мотив преступников - желание извлечения материальной прибыли. Практически все случаи неправомерного доступа к компьютерной информации и разработки вредоносного ПО направлены на хищения денежных средств. Злоумышленники используют:

- **скимминг**
- **заражение банкоматов**
- **DDoS атаки на онлайн-сервисы банков с параллельным проведением мошеннических операций**
- **использование вредоносного ПО для хищений со счетов юридических и физических лиц, а также создание бот-сетей**
- **многоярусные атаки на банки, процессинговые центры и банкоматы**
- **взлом ИТ-инфраструктур организаций, взаимодействующих с банками и платежными системами**

Global Trust Solutions

Актуальность концепции Governance - Risk management - Compliance для банков

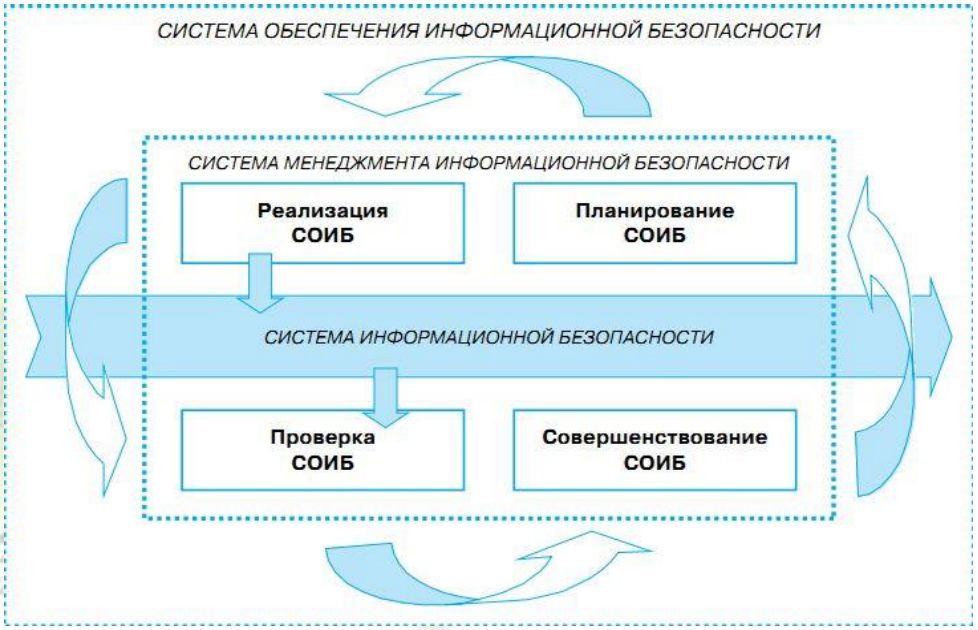


- **Функции высшего руководства банка (Governance) – указание целей и контроль их достижения**
- **Функция управления рисками (Risk management) – выясняется какие препятствия могут стать причиной нарушения сроков или сделать цель недостижимой, а также что банк рискует потерять на пути к цели. Выявленные риски обрабатываются**
- **Функция управления соответствием (Compliance) – выполнение множества внешних и внутренних правил, законов, стандартов и пр.**

Global Trust Solutions

Роль и место информационной безопасности в концепции GRC

- **Участие высшего руководства в вопросах обеспечения информационной безопасности**
- **Управление ИБ на основе анализа рисков (ISO 27001 и СТО БР ИББС)**
- **Управление соответствием требованиям 152-ФЗ, 382-П, стандарта Банка России СТО БР ИББС и стандарта безопасности данных индустрии платежных карт PCI DSS**



Global Trust Solutions

Участие высшего руководства в вопросах обеспечения ИБ

- Определение приемлемого уровня рисков
- Определение критериев принятия рисков
- Утверждение политики ИБ
- Поддержка и анализ СУИБ
- Распределение ключевых ролей и ответственности
- Общий контроль

Global Trust Solutions

Управление ИБ на основе анализа рисков (ISO 27001 и СТО БР ИББС)

- Что мы хотим защитить и почему?
- От кого мы хотим защититься?
- Какова вероятность возникновения и реализации угрозы при существующей инфраструктуре ИТ?
- Что мы потеряем (какой будет ущерб) при успешной реализации угрозы?
- Какой уровень риска мы имеем на сегодняшний день для каждой угрозы?

Global Trust Solutions

Управление соответствием требованиям регуляторов

Центральный Банк Российской Федерации

В настоящий момент приняты и введены в действие распоряжением Банка России следующие стандарты (совокупность указанных документов принято называть Комплексом БР ИББС):

- **СТО БР ИББС-1.0-2014. «Общие положения (5 редакция)**
- **СТО БР ИББС-1.1-2007. «Аудит информационной безопасности».**
- **СТО БР ИББС-1.2-2014. «Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0-2014 (4 редакция)»**

Общая доля кредитных организаций, принявших стандарт, ожидается на уровне 75-80%. Отказались внедрять стандарт 5-10% кредитных организаций. Заняли выжидательную позицию 10-15% (в основном, малые банки)

Global Trust Solutions

Управление соответствием требованиям регуляторов

Центральный Банк Российской Федерации

Кроме того, Банком России разработаны и введены следующие рекомендации в области стандартизации:

- **РС БР ИББС-2.0-2007. «Методические рекомендации по документации в области обеспечения информационной безопасности в соответствие с требованиями СТО БР ИББС-1.0».**
- **РС БР ИББС-2.1-2007. «Руководство по самооценке соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0».**
- **РС БР ИББС-2.2-2009. «Методика оценки рисков нарушения информационной безопасности».**

Global Trust Solutions

Управление соответствием требованиям регуляторов

Центральный Банк Российской Федерации

Для выполнения Федерального закона «О национальной платежной системе» 161-ФЗ в части защиты информации при осуществлении переводов денежных средств Центральным Банком было разработано Положение № 382-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств».

Проверки операторов платежных систем, являющихся кредитными организациями, проводятся на основании статьи 73 Федерального закона от 10 июля 2002 года N 86-ФЗ "О Центральном банке Российской Федерации (Банке России)"

Global Trust Solutions

Управление соответствием требованиям регуляторов

Законодательство в области защиты персональных данных

Более 90% организаций из реестра ЦБ РФ зарегистрированы в реестре РКН (по ПДн). Поправка (261-ФЗ) к 152-ФЗ «О персональных данных» узаконила СТО БР ИББС в качестве отраслевого стандарта обеспечения безопасности персональных данных. Кроме того, было так же утверждено право Банка России на разработку отраслевой модели угроз безопасности ПДн.

Однако техническая сторона вопроса защиты персональных данных, согласно 19 статье 152-ФЗ, устанавливается Правительством РФ, а не нормами СТО БР ИББС, что противоречит основной идеи создания отраслевого стандарта.

В ближайшее время статус СТО БР ИББС будет уточнён подзаконными нормативными актами Правительства, ФСТЭК, ФСБ, а также информационными письмами Банка России.

Global Trust Solutions

Управление соответствием требованиям регуляторов

Международный стандарт безопасности данных индустрии платежных карт PCI DSS

Требования стандарта распространяются на все компании, работающие с международными платёжными системами Visa и MasterCard.

С сентября 2006 года стандарт введён международной платёжной системой Visa на территории региона CEMEA (Центральная и Восточная Европа, Ближний Восток и Африка) как обязательный, соответственно, его действие распространяется и на Россию.

Поставщики услуг (процессинговые центры, платёжные шлюзы, интернет-провайдеры), работающие напрямую с VisaNet, должны пройти процедуру аудита на соответствие требованиям стандарта.

Global Trust Solutions

Построение СОИБ в банке

Система Обеспечения Информационной Безопасности банка представляет собой совокупность мер организационного и программно-технического уровня, направленных на защиту информационных ресурсов организации от угроз безопасности, ее создание включает в себя:

- **предварительное обследование**
- **создание Концепции обеспечения информационной безопасности;**
- **разработка Технического задания на создание СОИБ;**
- **техническое проектирование СОИБ;**
- **рабочее проектирование СОИБ поставка программных и технических средств защиты информации, ввод СОИБ в эксплуатацию, настройка всех компонентов и подсистем, проведение приемо-сдаточных испытаний;**
- **обучение пользователей и обслуживающего персонала;**
- **сопровождение СОИБ, техническая поддержка, аутсорсинг информационной безопасности.**

Global Trust Solutions

Аудит информационной безопасности банка

Аудит информационной безопасности является обязательным механизмом контроля для банков. Аудит позволяет руководству организации, ее акционерами и третьим сторонам получить объективную информацию о состоянии ее информационной безопасности.

- **Оценка соответствия состояния информационной безопасности требованиям стандарта Банка России СТО БР ИББС 1.0-2014;**
- **Оценка соответствия требованиям к защите персональных данных при их обработке в ИСПДн;**
- **Оценка соответствия требованиям к обеспечению защиты информации при осуществлении переводов денежных средств, установленных Положением Банка России от 09.06.2012 № 382-П.**

Global Trust Solutions

Аудит информационной безопасности банка

При проведении аудита достигаются следующие цели:

- Независимая оценка текущего состояния
- Идентификация и ликвидация уязвимостей
- Технико-экономическое обоснование механизмов безопасности
- Обеспечение соответствия требованиям действующего законодательства
- Минимизация ущерба от инцидентов безопасности

Ценность аудита состоит в:

- Независимости (никто не может эффективно контролировать и оценивать самого себя)
- Высокой квалификации экспертов, проводящих аудит
- Экономической целесообразности (дешевле привлечь стороннюю организацию для конкретной работы)
- Наличии официального аудиторского заключения, которое повышает степень доверия к организации

Global Trust Solutions

Аудит информационной безопасности банка

Аудит безопасности платежных систем по стандарту PCI DSS

Целью аудита является проверка соответствия платежных систем и поддерживающей их ИТ-инфраструктуры требованиям стандарта PCI DSS, определяющего 6 областей контроля и 12 основных требований по безопасности

Работы по аудиту на соответствие стандарту PCI DSS включают в себя три последовательных этапа:

- **Сбор исходных данных и анализ документации**
- **Анализ защищенности периметра и инфраструктуры**
- **корпоративной сети**
- **Проверка реализации Стандарта на объекте аудита**

Основные результаты работы:

- **Формирование общественного мнения о честном имени и стабильном положении банка**
- **Снижение величины рисков, связанных с компрометацией карточных систем**
- **Повышение осведомленности персонала банка в вопросах ИБ**

Global Trust Solutions

Защита информации в платежных системах

Согласно 382-П в банке должны быть реализованы требования из следующих областей контроля:

- **назначение и распределение ролей и ответственности за защиту информации в платежной системе**
- **защита информации на всех стадиях жизненного цикла объектов ИТ-инфраструктуры**
- **управление доступом к объектам ИТ-инфраструктуры**
- **защита информации от воздействия вредоносного кода**
- **защита информации при использовании сети Интернет**
- **использование средств криптографической защиты информации**
- **использование технологических мер защиты информации**
- **организация и функционирование службы информационной безопасности**
- **повышение осведомленности в области обеспечения защиты информации**
- **выявление и реагирование на инциденты**
- **определение и реализация порядка обеспечения защиты информации**
- **оценка выполнения требований к обеспечению защиты информации**
- **информирование об обеспечении в платежной СЗИ**
- **совершенствование системы защиты информации**

Global Trust Solutions

Защита информации в платежных системах

Для выполнения требований 161-ФЗ в банке проводятся следующие работы:

- **Оценка соответствия платежной системы требованиям по безопасности информации и разработка плана мероприятий по обеспечению соответствия**
- **Анализ защищенности платежной системы**
- **Оценка и обработка рисков информационной безопасности платежной системы**
- **Разработка комплекса организационно-распорядительных документов для обеспечения соответствия платежной системы организации требованиям по безопасности информации**
- **Разработка и внедрение технических решений по комплексу программно-технических средств защиты информации в платежной системе**

Global Trust Solutions

Авторские учебные курсы GlobalTrust

Авторские учебные курсы разрабатываются и проводятся экспертами GlobalTrust и охватывают вопросы управления рисками ИБ, аудита ИБ, построения системы управления ИБ и защиты персональных данных.

- **IS001 - Мастер-класс "Аудит информационной безопасности"**
- **IS002 - Мастер-класс "Управление рисками информационной безопасности в соответствии с требованиями международного стандарта ISO 27001"**
- **IS002s - Мастер-класс "Практикум по анализу рисков информационной безопасности"**
- **IS003 - Ликбез для членов управляющего комитета по информационной безопасности**
- **IS004 - Мастер-класс "Внедрение и сертификация СУИБ в соответствии с требованиями международного стандарта ISO 27001"**
- **IS005 - Обучающий семинар "Проблемные вопросы обработки и защиты персональных данных"**
- **IS006 - Обучающий семинар "Ликбез по защите персональных данных для банкиров"**
- **IS007 - Обучающий семинар "Аудит информационной безопасности организаций банковской системы РФ по требованиям стандарта СТО БР ИББС"**

Global Trust Solutions

Получение лицензий ФСТЭК и ФСБ

Компания GlobalTrust оказывает полный комплекс услуг по подготовке организаций к получению лицензий ФСТЭК и ФСБ России

- проведение консультаций по подготовке организации к лицензированию
- подготовка пояснительной записки
- подготовка перечня документов с пометкой «ДСП» (ФСТЭК России и ГОСТов)
- проведение работ по защите и аттестации автоматизированной системы (АС), состоящей из одного рабочего места на базе ПЭВМ
- проведение работ по защите и аттестации защищаемого помещения (только для ФСТЭК)
- поставка рекомендованных ФСТЭК России программных средств контроля защищенности информации (только для ФСТЭК)
- повышение квалификации сотрудников Заказчика или подбор персонала
- оформление лицензионного дела
- передача заявки и лицензионного дела во ФСТЭК или ФСБ России

Global Trust Solutions

Почему Global Trust ?

СЕРИЯ КИ 0073 НОМЕР 003609

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

ЛИЦЕНЗИЯ

НА ДЕЯТЕЛЬНОСТЬ ПО ТЕХНИЧЕСКОЙ ЗАЩИТЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

Регистрационный номер 1414 от 25 марта 2011 г.

Федеральная служба по техническому и экспортному контролю разрешает осуществление мероприятий и оказание услуг по технической защите конфиденциальной информации

Лицензия предоставлена Обществу с ограниченной ответственностью «ГлобалТраст Солюшнс» (ООО «ГлобалТраст»)

ОГРН 1037727011156, ИНН 7727241354

Адрес места нахождения:
117216, г. Москва, ул. Грина, д. 4, кв. 21

Адрес места осуществления лицензируемой деятельности:
123317, г. Москва, Пресненская набережная, д.10, офис № 444, кампус 1

Лицензия предоставлена на срок до 25 марта 2016 г.

на основании приказа ФСТЭК России от 25 марта 2011 г. № 166

Первый заместитель директора

В.Селин

Специализация GlobalTrust:

- **Аудит и оценка рисков ИБ**
- **Разработка и внедрение систем управления информационной безопасностью**

Статусы GlobalTrust:

- **Лицензиат ФСТЭК России**
- **Официальный дистрибьютор и бизнес-партнер Британского Института Стандартов (BSI)**
- **Разработчик русских редакций международных стандартов в области защиты информации и обеспечения непрерывности бизнеса**

Проекты GlobalTrust для банков:

- **Разработка и сертификация СУИБ и СУНБ в соответствии с ISO 27001, BS 25999, BS 25777**
- **Обеспечение соответствия СТО БР, 382-П, PCI DSS, 152-ФЗ**
- **Внедрение системы мониторинга действий пользователей корпоративной сети на базе Spector 360**

Global Trust Solutions

Контактная информация

РЫБИН АНДРЕЙ АЛЕКСАНДРОВИЧ

Руководитель комплексных проектов

123317, Россия, г.Москва,
Пресненская наб., блок С,
Бизнес-центр «Регус»
www.globaltrust.ru

Тел.: +7 (925) 203-95-11
Моб.: +7 (964) 627-02-67
Факс.: +7 (495) 967-76-00
rybin@globaltrust.ru

Global Trust Solutions