Специализированный облачный сервис для малых КО и НКО

Особенности сегмента малых и средних финансовых организаций

ТРЕБОВАНИЯ РЕГУЛЯТОРА

Обязательность выполнения:

- Положения 382-П
- Базовых требований комплекса СТО ИББС
- ГОСТ 57580.1-2017
- Стандарт PCI DSS.3 (в зависимости от объема операций)
- Положения № 242-П
- Указания № 3097-У

Аудит по ИБ

ОСОБЕННОСТИ ОРГАНИЗАЦИЙ СЕГМЕНТА

- Малая штатная численность организаций;
- Отсутствие компетенций в сфере IT и ИБ;
- Различная организационная структура;
- Небольшой бюджет;
- Разнообразное и неунифицированное техническое оснащение, отсутствие типизации;
- Непрозрачные отношения со службами технической поддержки.

ПРОБЛЕМЫ и СЛЕДСТВИЯ

Риски непрохождения аудита, ведущие к росту норматива достаточности базового капитала банка
Риски реализации успешных атак, вызывающих ущерб
Высокая стоимость работ
Сложность реализации требований по безопасности собственными ресурсами
Рост нагрузки на бюджет за счет приема на работу дорогостоящих непрофильных специалистов по IT и ИБ

ВЫХОД

ПЕРЕХОД НА ЦЕНТРАЛИЗОВАННУЮ УДАЛЕННУЮ ОБРАБОТКУ И НА ЦЕНТРАЛИЗОВАННЫЕ СЕРВИСЫ БЕЗОПАСНОСТИ

Аудит ИБ в банках

Шаги Банка России по запуску рынка внешнего аудита

I. Нормативно определены четыре направления проведения внешнего аудита:

- → оценка выполнения требований к обеспечению защиты информации при осуществлении переводов денежных средств (не реже раза в 2 года);
- → сертификация (во ФСТЭК) прикладного ПО, используемого при переводе денежных средств (однократно и после существенных изменений);
- → анализ (сканирование) уязвимостей ИБ объектов информационной инфраструктуры (1 раз в год);
- → тестирование на проникновение (1 раз в год).

II. Нормативно и на уровне ГОСТ Р установлены:

- → требования по безопасности
- → методики проведения аудита

III. Начало работ по проведению аудита **с 1 июля 2018 года**

IV. Готовится Положение ЦБ РФ об установлении размера дополнительных резервов для компенсации операционных рисков по ИБ. Определен механизм снижения резервов за счет результатов аудита ИБ. **Ввод в действие с 1 июля 2020 года.**

V. Готовится **список из 50 организаций,** рекомендуемых Банком России для проведения аудита в КО.

VI. Прорабатывается вопрос создания **системы добровольной сертификации**

VII. Прорабатывается вопрос **создания СРО.**

ПРОБЛЕМЫ МАЛЫХ ОРГАНИЗАЦИЙ

- → затратность
- → сложность
- → риски непрохождения аудита

Компенсация проблем и рисков – перенос обработки в облако, типизация

Возникает устойчивый долговременный процесс аудита

Предложения для малых организаций

1 **Переход к сервису доверенного защищенного взаимодействия и доверенной защищенной облачной обработки**

2 **Предоставление в пользование:**
Системы защищенного удаленного доступа (терминальный режим, VDI). Система может быть развернута на компьютерах, имеющихся в организации

3 **Централизованное представление сервисов:**

a. Безопасности.
b. Администрирования и поддержки работоспособности оборудования.
c. Обеспечения катастрофоустойчивости и отказоустойчивости в соответствии с согласованными параметрами.
d. Обеспечения текущей деятельности НФО

4 **Состав сервисов безопасности:**

a. Обеспечение возможности обработки персональных данных в соответствии с требованиями ФЗ и нормативных документов регуляторов;
b. Хранение данных в облачном сервисе (частном выделенном для пользователя сегменте облака ….) в зашифрованном на ключе пользователя виде;
c. Шифрование канала связи до АРМ пользователя;
d. Антивирусная защита;
e. Защита от НСД и DDoS-атак;
f. Противодействие кибератакам, сервисы СОА;
g. Обеспечение выполнения требований стандартов и требований регулятора по информационной безопасности;
h. Подготовка отчетности о выполнении требований по безопасности для ЦБ РФ;
i. Проведение разбора и обработки инцидентов безопасности, восстановление нарушенного уровня безопасности;
j. Предоставление сервиса страхования рисков нарушения безопасности

ВЫГОДЫ И ПРЕИМУЩЕСТВА

a. Полная необходимая функциональность с высоким уровнем безопасности;
b. Использование уже имеющегося оборудования;
c. Существенно дешевле, чем держать специалистов по информатизации и информационной безопасности в штате организации;
d. Квалифицированное обслуживание и поддержка;
e. Соответствие требованиям по безопасности, установленным регулятором;
f. Страховая защита.

ХАРАКТЕРИСТИКИ СЕРВИСА ДОСТУПА К РЕСУРСАМ

a. Доступность 99,999. Обеспечивается защитой оборудования провайдера от кибератак.
b. Работа через единого телекоммуникационного оператора

Модель развертывания и обслуживания в «облаке», реализуемые сервисы безопасности

Специализированное «общественное облако», находящееся под контролем доверенного оператора.

Модель обслуживания - SaaS (Программное обеспечение как услуга)— потребителю предоставляется прикладное программное обеспечение провайдера, доступное из различных клиентских устройств или посредством тонкого клиента. Контроль и управление предоставленной физической и виртуальной инфраструктурой облака, в том числе сети, серверов, операционных систем, хранения, или даже индивидуальных возможностей приложения (за исключением ограниченного набора пользовательских настроек конфигурации приложения) осуществляется облачным провайдером.

Такие предложения известны. (Ростелеком, ЦФТ, Диасофт и т.д.).
Причины неудачи – отсутствие гарантий доверия в предлагаемых решениях.
SaaS в части ИБ целесообразно доверять аттестованному по ФСТЭК, ГОССОПКА и ФИНЦЕРТ оператору.

Реализуемые в системе сервисы безопасности:

- управления и контроля прав доступа
- идентификации, аутентификации и авторизации
- предоставления привилегированного доступа эксплуатационному персоналу
- защиты вычислительной инфраструктуры
- защиты сетевой инфраструктуры
- защиты от воздействий вредоносного кода
- предотвращения утечек информации
- мониторинга и анализа событий информационной безопасности
- управления ключевыми системами средств криптографической защиты информации.

Основные вопросы, требующие обязательной проработки

- Выбор способа владения облака и собственника
- Обеспечение резервирования систем и данных.
- Системы доступа, почты и архивного хранения
- Обеспечение работы удаленного пользователя в Облаке, у том числе, когда каналы регионального телекоммуникационного оператора недостаточно стабильны.
- Подготовка регламентов проведения тематических проверок, аудита, тестирований.
- Обеспечение конфиденциальности данных, обрабатываемых в облаке. Управление доступом к ним со стороны пользователя. Ответственность перед пользователем.
- Подготовка регламента реагирования на инциденты, порядок и правила проведения расследований.
- Создание СОС, SIEM, услуги аутсорсинга
- Проработка вопросов переноса опердня, подсистем ДБО, карточного процессинга , транспортных проектов, школьных карт, кампусов, систем лояльностив виртуальную среду
- Подготовка регламента предоставления ресурсов пользователю оператором Облака.
- Создание системы поддержки клиентов первого уровня в пределах шаговой доступности (физическая замена и подключение оборудования и т.д.).
- Разработка механизма покрытия убытков, возникающих в результате сбоев системы безопасности и реализации атак. Страхование рисков информационной безопасности.
- Отработка приемлемых свидетельства доверия безопасности

→ **Обяза-тельные условия обеспе-чения общего доверия**

Вопросы безопасности

ДОКУМЕНТЫ, УСТАНАВЛИВАЮЩИЕ ТРЕБОВАНИЯ ПО ЗАЩИТЕ И ФИКСИРУЮЩИЕ СОСТОЯНИЕ ЗАЩИЩЕННОСТИ СИСТЕМЫ

Базовые требования по безопасности	Требования к ГИС	Требования ФЗ № 187-ФЗ
ГОСТ Р 57580.1—2017	Приказ ФСТЭК России от 11 февраля 2013 г. № 17 Приказ ФСТЭК России от 15 февраля 2017 г. № 27	17 НПА ФСТЭК, ФСБ и МКС
Проект ГОСТ Р Методика оценки соответствия»		
ГОСТ Р 56938-2016		
СТО БР ИББС-1.0 — 2014, СТО БР ИББС-1.1-2007»		
Положение Банка России от 9 июня 2012 г. № 382-П		
Положение Банка России от 24 августа 2016 г. № 552-П		

СОСТАВЛЯЮЩИЕ, ОБЕСПЕЧИВАЮЩИЕ ГАРАНТИИ ДОВЕРИЯ К ПЕРЕДЛАГАЕМОМУ СЕРВИСУ

СВИДЕТЕЛЬСТВА ДОВЕРИЯ К СЕРВИСУ ОБЛАЧНОЙ ОБРАБОТКИ

1. Наличие Сертификатов соответствия ФСТЭК и ФСБ на используемое оборудование и ПО, включая средства обеспечения безопасности и контроля.
2. Наличие аттестатов соответствия требованиям безопасности информации для следующих объектов:
   - → ИТС - составляющей
   - → Облачной – составляющей.
3. Свидетельство компетенции организации, выполняющей работы по безопасности.

СВИДЕТЕЛЬСТВА ДОВЕРИЯ К КО СО СТОРОНЫ РЕГУЛЯТОРА

Наличие акта аудита ИБ его ИТС, размещенной в облачной среде, проведенного по документам ЦБ РФ

ГАРАНТИИ ПОКРЫТИЯ УЩЕРБА В СЛУЧАЕ УСПЕШНОЙ РЕАЛИЗАЦИИ АТАКИ:

Страхование рисков предоставления услуг информационной безопасности

Схема взаимодействия корпоративного центра ГосСОПКА (центра мониторинга) с подконтрольными объектами

Основные сервисы

1.Обеспечение заданной доступности сервисов в условиях воздействия компьютерных атак.

2.Защита ИТС (АИС) клиентов сети Комкор от компьютерных атак, выявление атак типа APT (длительных целенаправленных атак), атак «нулевого дня».

3.Взаимодействие с ГЦ ГосСОПКА.

4.Взаимодействие с FINSERT.

5.Расследование инцидентов информационной безопасности.

6.Мониторинг состояния информационной безопасности оборудования клиента (сетевое оборудование, сервера, АРМы), включая:
•доступность подконтрольного оборудования;
•целостность ПО;
•загруженность оборудования и его элементов;
•инвентаризацию ресурсов;
•анализ журналов регистрации;
•анализ системных журналов.

7.Управление ресурсами в ходе проверок и инцидентов.

8.Сканирование уязвимостей.

9.Предоставление отчетов по результатам работы и оперативное взаимодействие с клиентами в режиме работы 24x7x365.

Преимущества решения «Форпост»

Архитектурно - ПО линейки "Форпост" спроектировано с учётом построения быстродействующей территориально распределённой, иерархически масштабируемой системы противодействия киберугрозам с централизованным управлением, с сохранением возможности управления "на местах" при выходе единого центра управления из строя.

Удалённые компоненты системы защищены от подмены и прослушивания за счёт использования криптографических технологий.

Быстродействие компонент систем противодействия компьютерным атакам не уступает лучшим аналогичным системам, за счёт разработки собственных планировщиков загрузки процессорных ядер.

Наличие универсального пользовательского интерфейса, позволяющего использовать консоли управления с использование как "толстого", так и "тонкого", с использованием WEB интерфейса, клиентов;

Работоспособность в среде виртуализации. Высокие показатели быстродействия.

90 % программного кода является собственной разработкой

Схема размещения ПАК «ФОРПОСТ» и ПК «Фантом-VIP» на сети АО «КОМКОР»

ОСНОВНЫЕ ХАРАКТЕРИСТИКИ СЕТИ «КОМКОР-Банк»

Число кредитных организаций, казначейств, особых клиентов :
250
Шифрование:
Точка-точка
Количество сетевого оборудования:
2 высокоскоростных катастрофоустойчивых узла доступа (по 2 независимых ВОЛС на каждый) и холодный резерв сетевого оборудования
Средняя задержка: **4 мс**
Скорость:
по требованию клиентов
Доступность для крупных банков, например, Сбербанка:
99,97

→ Цель - сокращение времени реакции персонала на инциденты ИБ и снижение рисков ИБ в сети КОМКОР- БАНК, в том числе, полной потери доступности платежной системы Банка России

Результаты испытаний и выводы

С ИСПОЛЬЗОВАНИЕМ ЛИНЕЙКИ ПРОДУКТОВ ПАК «ФОРПОСТ» и ПК «ФАНТОМ- VIP» РАЗРАБОТКИ АО «РНТ», ПРОВОДИЛИСЬ ПРОВЕРКИ :

- На действующем телекоммуникационном оборудовании АО «Комкор» в рамках сети «Комкор-банк» ;
- На ЦОД «Комкор», на российской сертифицированной ФСТЭК России платформе виртуализации «Горизонт-ВС»

По результатам испытаний подготовлен соответствующий протокол.

- **РЕЗУЛЬТАТЫ ИСПЫТАНИЙ:**
  - Показана работоспособность ПАК «Форпост» и «ФАНТОМ - VIP» при их размещении в сети «Комкор-Банк», в двух вариантах (ПАК, виртуальная среда ЦОД).
  - Заявленные в эксплуатационной документации функции ПАК «ФОРПОСТ», в том числе реализация собственных механизмов защиты, реализуются полностью.
  - Проверки заявленной функциональности по базовым требованиям ГОСТР 57580.1-2017 прошли успешно.
  - Линейка ПАК «Форпост» не уступает по характеристикам используемому в настоящий момент импортному ПО, контролирующему состояние сети Комкор-Банк.
  - Обеспечивается информационная безопасность рабочих мест операторов от НСД и кибератак атак на базе ПАК «Фантом-VIP»
  - Целесообразно и возможно использовать ПАК «Фантом-VIP» в качестве универсальной платформы для защищенного доступа клиентов (абонентов) к облачным сервисам.

- УСТАНОВКА НА ОБОРУДОВАНИИ ОАО «КОМКОР» ПАК «ФОРПОСТ» И «ФАНТОМ - VIP» ПОЗВОЛЯЮТ РЕШИТЬ СЛЕДУЮЩИЕ ЗАДАЧИ:
  - Обеспечить выполнение требований статей 4, 10 и 11 ФЗ № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», а также положений нормативных актов ФСТЭК и государственных стандартов Российской Федерации.
  - Обеспечить достаточный уровень защищенности от кибератак инфраструктуры телекоммуникационного оператора, предоставляющего услуги финансовым структурам и Банку России (каналы связи и ЦОД) и как следствие – обеспечивается требуемая доступность сервисов с использованием СОА ПАК «Форпост» и ПАК «ФАНТОМ - VIP» не ниже 99,99.
  - Предложить новый экономически выгодный сервис защиты от компьютерных атак с использованием уже имеющихся каналов связи и размещаемых в защищенном ЦОД оператора связи ПАК «Форпост» и ПАК«ФАНТОМ»
  - Обеспечить возможность предоставления финансовым организациям облачных защищенных сервисов для решения задачи обеспечения взаимодействия на финансовом рынке, включая сервисы защищенного доступа и полноценной функциональности (аутентификация, внешний и внутренний документоборот, платежи, электронная подпись, долговременное хранение электронных документов, технологии блокчейн).

ТЕРРИТОРИЯ БЕЗОПАСНОСТИ СЕЙЧАС ИЛИ НИКОГДА!

129515, Москва,
2-я Останкинская улица, д.6
+7 (495) 777 75 77
rnt@rnt.ru
www.rnt.ru

РОССИЙСКИЕ НАУКОЁМКИЕ ТЕХНОЛОГИИ