

# АБИСС



**Ассоциация пользователей  
стандартов по информационной  
безопасности АБИСС**

# Что такое АБИСС

Сообщество профессионалов, ключевой задачей которых является развитие и совершенствование сферы применения стандартов информационной безопасности



## Члены ассоциации (ИТ/ИБ компании)



## Сообщество АБИСС (поднадзорные организации)

- Финансовые организаций
- Субъекты критической информационной инфраструктуры
- Операторы персональных данных и государственных информационных систем
- **3 200** КОНТАКТОВ



## Регуляторы (ИБ-сфера и отраслевые)

- ФСТЭК, ФСБ, Минцифры, Роскомнадзор
- Банк России, Минпромторг, Минэнерго и т.д.

# Система добровольной сертификации

В 2023 году на Уральском форуме «Кибербезопасность в финансах» Банком России и АБИСС было принято решение о формировании совместной рабочей группы «Системы внешнего аудита информационной безопасности»

## Выполнено:

- ✓ Стандарт по оценке соответствия (требования к проверяющей организации и процессу оценки соответствия): СТО АБИСС
- ✓ Процедура добровольной сертификации для компаний-аудиторов, а также система аттестации для аудиторов
- ✓ Сертификация в СДС по ГОСТ р 57580.1.2: специалисты

## Разрабатывается:

- ✓ Сертификация в СДС по ГОСТ р 57580.1.2: компании
- ✓ Публикация ГОСТ.Х. от ЦБ РФ
- ✓ Развитие СДС на новые направления: ГОСТ 3,4,5

# Инициативы АБИСС

## Планируемые инициативы

- ✓ Система аудита информационной безопасности
- ✓ Разработка методики управления поставщиками ПО

## Разработка образовательных курсов

- ✓ Разработка учебных курсов в рамках СДС
- ✓ Участие в магистерской программе по ИБ
- ✓ Участие в проведении КиберКурса Банка России

## Гармонизация требований

- ✓ Оценка уровня зрелости по методологии ФСТЭК
- ✓ Участие в работе технических комитетов по ИБ
- ✓ Формирование предложений по правкам в регуляторику и запрос разъяснений

## 5-ая ежегодная конференция АБИСС

- ✓ При участии ФСТЭК, Минцифры, Банка России
- ✓ 700 участников из финансовой отрасли, промышленности, ТЭК, транспорта и т.д.
- ✓ Сайт: <https://conf.abiss.ru/>

## Обучающие инициативы от экспертов АБИСС

- ✓ Регулярные практические вебинары по реализации ИБ-требований: 350-400 слушателей
- ✓ Создание консультационного портала по регуляторике ИБ

# АБИСС

## Контактная информация



shubina@abiss.ru



www.abiss.ru



+7 916 581-84-60

**Варвара Шубина,**

Руководитель по маркетингу  
Ассоциации АБИСС



# АБИСС

## Безопасная работа с подрядчиками: как выстроить и чем помогут методические рекомендации

**Анна Коробецкая,**  
Ведущий консультант по информационной безопасности  
АО «Инфосистемы Джет»

# Ключевые проблемы работы с подрядчиком



## ДОСТУП К ИНФРАСТРУКТУРЕ

- Скомпрометированные учетные записи, выданные подрядчику
- Избыточные права и административный доступ
- Остановка бизнес-процессов из-за действий подрядчика



Хакеры скомпрометировали рабочее место одного из клиентов (подрядчика) и использовали легитимный функционал системы «Контур.Диадок» для рассылки загрузчика вредоноса



## ДОСТУП К ДАННЫМ

Неконтролируемый канал утечки:

- конфиденциальная информация
- персональные данные
- конфигурационные данные
- исходный код и интеллектуальная собственность



В августе 2024 года Минтруду присудили штраф за утечку ПДн, которая произошла вследствие взлома подрядчика — он имел легитимный доступ к инфраструктуре Минтруда



## ЛЕГИТИМНОСТЬ

В ходе работ подрядчик может выполнять критичные действия:

- изменять конфигурации
- отключать средства защиты
- загружать и удалять файлы



Активность хакеров в сети "Аэрофлота" была замечена и предприняты меры, но инфраструктура подрядчика была "вычищена" плохо, что позволило злоумышленникам вернуться и через пару месяцев повторно обосноваться в системах авиакомпании

# Как выглядит практика работы с подрядчиками в мире

01

Знай всех своих подрядчиков  
(и их подрядчиков)

02

Дай им ровно столько  
доступа, сколько нужно

04

Отключи мгновенно, как  
только они больше не нужны

03

Контролируй их в реальном  
времени (технически и  
юридически)



# Как выглядит практика работы с подрядчиками в мире – на что обратить внимание

Управление на основе рисков

Принцип "Никогда не доверяй, всегда проверяй"

Управление доступом и идентификацией

Юридически обязательства в контрактах

Непрерывный мониторинг

Регулярная переоценка и аудит

Совместный план реагирования на инциденты

Безопасное завершение отношений

# Как выглядит практика работы с подрядчиками в мире – на что обратить внимание

- Разделите всех подрядчиков на категории по критичности
- Ведите централизованный реестр всех подрядчиков, включая субподрядчиков

Принцип "Никогда не доверяй, всегда проверяй"

Управление доступом и идентификацией

Юридически обязательства в контрактах

Непрерывный мониторинг

Регулярная переоценка и аудит

Совместный план реагирования на инциденты

Безопасное завершение отношений

# Как выглядит практика работы с подрядчиками в мире – на что обратить внимание

- Разделите всех подрядчиков на категории по критичности
- Ведите централизованный реестр всех подрядчиков, включая субподрядчиков

- Соблюдайте принцип минимальных привилегий
- Доступ подрядчика должен ограничиваться изолированными сегментами

Управление доступом и идентификацией

Юридически обязательства в контрактах

Непрерывный мониторинг

Регулярная переоценка и аудит

Совместный план реагирования на инциденты

Безопасное завершение отношений

# Как выглядит практика работы с подрядчиками в мире – на что обратить внимание

- Разделите всех подрядчиков на категории по критичности
- Ведите централизованный реестр всех подрядчиков, включая субподрядчиков

- Соблюдайте принцип минимальных привилегий
- Доступ подрядчика должен ограничиваться изолированными сегментами

- Многофакторная аутентификация для всех удаленных подключений
- Отзыв доступа должен быть автоматизирован и срабатывать немедленно по окончании контракта

Юридически  
обязательства в  
контрактах

Непрерывный  
мониторинг

Регулярная переоценка  
и аудит

Совместный план  
реагирования на  
инциденты

Безопасное завершение  
отношений

# Как выглядит практика работы с подрядчиками в мире – на что обратить внимание

- Разделите всех подрядчиков на категории по критичности
- Ведите централизованный реестр всех подрядчиков, включая субподрядчиков

- Соблюдайте принцип минимальных привилегий
- Доступ подрядчика должен ограничиваться изолированными сегментами

- Многофакторная аутентификация для всех удаленных подключений
- Отзыв доступа должен быть автоматизирован и срабатывать немедленно по окончании контракта

- Пропишите требования к шифрованию, уведомлению об инцидентах и право на аудит
- Наличие актуальных сертификатов (таких как ISO 27001, SOC 2 и др.)

Непрерывный мониторинг

Регулярная переоценка и аудит

Совместный план реагирования на инциденты

Безопасное завершение отношений

# Как выглядит практика работы с подрядчиками в мире – на что обратить внимание

- Разделите всех подрядчиков на категории по критичности
- Ведите централизованный реестр всех подрядчиков, включая субподрядчиков

- Соблюдайте принцип минимальных привилегий
- Доступ подрядчика должен ограничиваться изолированными сегментами

- Многофакторная аутентификация для всех удаленных подключений
- Отзыв доступа должен быть автоматизирован и срабатывать немедленно по окончании контракта

- Пропишите требования к шифрованию, уведомлению об инцидентах и право на аудит
- Наличие актуальных сертификатов (таких как ISO 27001, SOC 2 и др.)

- Используйте инструменты для отслеживания цифрового риска подрядчика
- Отслеживайте риски, исходящие от субподрядчиков

Регулярная переоценка и аудит

Совместный план реагирования на инциденты

Безопасное завершение отношений

# Как выглядит практика работы с подрядчиками в мире – на что обратить внимание

- Разделите всех подрядчиков на категории по критичности
- Ведите централизованный реестр всех подрядчиков, включая субподрядчиков

- Соблюдайте принцип минимальных привилегий
- Доступ подрядчика должен ограничиваться изолированными сегментами

- Многофакторная аутентификация для всех удаленных подключений
- Отзыв доступа должен быть автоматизирован и срабатывать немедленно по окончании контракта

- Пропишите требования к шифрованию, уведомлению об инцидентах и право на аудит
- Наличие актуальных сертификатов (таких как ISO 27001, SOC 2 и др.)

- Используйте инструменты для отслеживания цифрового риска подрядчика
- Отслеживайте риски, исходящие от субподрядчиков

- Пересматривайте риски не реже раза в год, а также при значимых изменениях в услугах подрядчика или регуляторных требованиях

Совместный план реагирования на инциденты

Безопасное завершение отношений

# Как выглядит практика работы с подрядчиками в мире – на что обратить внимание

- Разделите всех подрядчиков на категории по критичности
- Ведите централизованный реестр всех подрядчиков, включая субподрядчиков

- Соблюдайте принцип минимальных привилегий
- Доступ подрядчика должен ограничиваться изолированными сегментами

- Многофакторная аутентификация для всех удаленных подключений
- Отзыв доступа должен быть автоматизирован и срабатывать немедленно по окончании контракта

- Пропишите требования к шифрованию, уведомлению об инцидентах и право на аудит
- Наличие актуальных сертификатов (таких как ISO 27001, SOC 2 и др.)

- Используйте инструменты для отслеживания цифрового риска подрядчика
- Отслеживайте риски, исходящие от субподрядчиков

- Пересматривайте риски не реже раза в год, а также при значимых изменениях в услугах подрядчика или регуляторных требованиях

- Имейте согласованные DRP и плановые с критическими подрядчиками
- Кризисные планы должны учитывать сценарий недоступности или ухода подрядчика

Безопасное завершение отношений

# Как выглядит практика работы с подрядчиками в мире – на что обратить внимание

- Разделите всех подрядчиков на категории по критичности
- Ведите централизованный реестр всех подрядчиков, включая субподрядчиков

- Соблюдайте принцип минимальных привилегий
- Доступ подрядчика должен ограничиваться изолированными сегментами

- Многофакторная аутентификация для всех удаленных подключений
- Отзыв доступа должен быть автоматизирован и срабатывать немедленно по окончании контракта

- Пропишите требования к шифрованию, уведомлению об инцидентах и право на аудит
- Наличие актуальных сертификатов (таких как ISO 27001, SOC 2 и др.)

- Используйте инструменты для отслеживания цифрового риска подрядчика
- Отслеживайте риски, исходящие от субподрядчиков

- Пересматривайте риски не реже раза в год, а также при значимых изменениях в услугах подрядчика или регуляторных требованиях

- Имейте согласованные DRP и плановые с критичными подрядчиками
- Кризисные планы должны учитывать сценарий недоступности или ухода подрядчика

- Убедитесь, что подрядчик вернул или уничтожил все данные заказчика
- Убедитесь, что удалены все VPN-токены, SSH-ключи и сервисные учетные записи

# Российская практика не столь обширная

01

## ПРЯМЫЕ АНАЛОГИ МЕЖДУНАРОДНЫХ СТАНДАРТОВ

- ГОСТ Р ИСО/МЭК 27036-1-2021 (ISO/IEC 27036-1)
- ГОСТ Р 59215-2020 (ISO/IEC 27036-3)

02

## ОТРАСЛЕВАЯ СПЕЦИФИКА

- СТО БР ИББС-1.4-2018
- Положение Банка России № 716-П
- Указание Банка России от 22 октября 2024 г. № 6906-У
- ГОСТ Р 57580.3-2022
- ГОСТ Р 56939-2024
- Приказ ФСТЭК № 117

## В ЧЕМ ОТЛИЧИЕ ОТ МИРОВОЙ ПРАКТИКИ

- Основным драйвером выступает регулятор
- Компания несет ответственность за своего подрядчика
- Отсутствует единый подход к регулированию
- Предотвращение инцидентов с подрядчиком, через ужесточение доступа и технический контроль на стороне компании

# Методические рекомендации для выравнивания подхода

01

## Как выстроить процесс

Взаимодействие с подрядчиками рассматривается через жизненный цикл для охвата возможных рисков ИБ на каждом из этапов

02

## Как и кого проверять

Основой подход к оценке рейтинга ИБ подрядчика является ранжирование подрядчиков по уровню их критичности и выбор целесообразного типа проверки

03

## Что регулировать

В зависимости от определенного рейтинга ИБ расширяются требования к подрядчику и закрепляются на уровне договора

# Что учесть при работе с подрядчиками

## Основная цель этапа

Закрепление правил выбора и взаимодействия с подрядчиками, учитывая аспекты обеспечения ИБ

## Что делаем

- ✓ Определяем кого можем привлекать и на какие работы
- ✓ Закрепляем внутри компании подход (методологию) по безопасной работе с подрядчиками, как минимум:
  - уровни критичности
  - способы проверки ИБ
  - требования ИБ
- ✓ Инвентаризируем имеющихся подрядчиков и их доступы в нашу инфраструктуру



# Что учесть при работе с подрядчиками

## Основная цель этапа

Проведение оценки критичности подрядчиков и их рейтинга ИБ до начала взаимодействия с ними

## Что делаем

- ✓ Проводим оценку ИБ подрядчика соизмеримую возможному риску:
  - Заполнение и проверка опросника
  - Сторонний или собственный аудит
  - Оценка цифрового риска с помощью специальных сервисов
  - Оценка из открытых источников
  - Тестирование на проникновение
- ✓ По результатам оценки выбираем дополнительные требования и компенсирующие меры



# Что учесть при работе с подрядчиками

## Основная цель этапа

Формализация ответственности и обязательств по обеспечению ИБ и реагированию на инциденты ИБ

## Что делаем



Закрепляем на уровне договора следующие аспекты:

- взаимодействие подрядчика с конфиденциальной информацией
- совместное реагирование на инциденты ИБ
- правила безопасной работы в инфраструктуре компании
- право на аудит
- штрафные санкции за нарушение требований ИБ или допущение инцидента ИБ



# Что учесть при работе с подрядчиками

## Основная цель этапа

Минимизация риска неправомерного доступа к ресурсам через учетные данные подрядчика

## Что делаем

- ✓ Прорабатываем и реализуем различные схемы подключения подрядчика в зависимости от уровня критичности
- ✓ Доводим до работников подрядчика, которым предоставляется доступ или передаются конфиденциальные данные, правила безопасной работы с фиксацией факта ознакомления
- ✓ Ставим на мониторинг ИТ-активы, с которыми взаимодействует подрядчик



# Что учесть при работе с подрядчиками

## Основная цель этапа

Мониторинг и выявление неправомерного доступа к ресурсам через учетные данные подрядчика

## Что делаем

- ✓ Контролируем соблюдение требований ИБ работниками подрядчика
- ✓ Анализируем результаты мониторинга действий работников подрядчика в нашей инфраструктуре на предмет компрометации или злонамеренных действий
- ✓ Регулярно проводим переоценку уровня критичности подрядчиков
- ✓ Актуализируем реестр подрядчиков



# Что учесть при работе с подрядчиками

## Основная цель этапа

Блокировка доступов подрядчика к ИТ-инфраструктуре и данным

## Что делаем

- ✓ Контролируем уничтожение критичной информации, переданной подрядчику
- ✓ Контролируем своевременность блокировки доступов подрядчиков
- ✓ Возвращаем контроль над управлением ИС и ИТ-инфраструктурой



# Подрядчик в инфраструктуре - потенциальный нарушитель

01

## УЖЕСТОЧАЕМ И ТЕХНИЧЕСКИ КОНТРОЛИРУЕМ ДОСТУП

- Выделяем для подрядчиков отдельный изолированный контур
- Организуем доступ подрядчика с использованием виртуальных рабочих столов или jump-хостов
- Подключаем второй фактор для удаленного доступа подрядчиков
- Соблюдаем принцип минимальных привилегий
- Разрешаем доступ только с определенного IP-или MAC-адреса
- Контролируем сессии с использованием PAM-решения
- Используем для передачи файлов VDR, интегрированное с DLP и песочницей

02

## ВВОДИМ ДОПОЛНИТЕЛЬНЫЙ МОНИТОРИНГ

- Подключаем к системе мониторинга событий источников, с которыми работает подрядчик
- Разрабатываем правила детектирования для определения нетипичного поведения учетных записей подрядчика, например:
  - вход из неожиданных стран или geographic IP-адресов
  - вход вне рабочего времени
  - входа с одной учетной записи из нескольких мест в одно и то же время
  - изменение прав доступа без согласования
  - скачивание или загрузка большого объема данных

# Как сделать выбор подрядчика исходя из защищенности



## Оценка критичности подрядчиков

- ✓ Транслирование критичности ИТ-актива на подрядчика
- ✓ Определение критичности подрядчика по критериям
- ✓ Экспертная оценка критичности подрядчика



## Определение рейтинга ИБ подрядчика

- ✓ Выбор способа оценки рейтинга ИБ
- ✓ Анализ результатов оценки и определение рейтинга ИБ:
  - низкий
  - достаточный
  - средний
  - высокий



## Принятие решения о дальнейшей работе

- ✓ Применение результатов как стоп-фактора
- ✓ Расширение требований ИБ к подрядчику
- ✓ Выбор дополнительных мер защиты

# Способы оценки рейтинга ИБ подрядчика

Уровень критичности подрядчика

НИЗКИЙ

СРЕДНИЙ

ВЫСОКИЙ

КРИТИЧЕСКИЙ

Опросный лист  
о состоянии ИБ

Информация о  
состоянии ИБ  
из открытых  
источников

Внешний аудит  
ИБ

Анализ  
цифровых  
рисков

Практический  
анализ  
защищенности  
(пентест)

Релевантные способы оценки рейтинга ИБ подрядчика

# Как определяем рейтинг ИБ

## УРОВЕНЬ КРИТИЧНОСТИ ПОДРЯДЧИКА

РЕЙТИНГ ИБ ↓	УРОВЕНЬ КРИТИЧНОСТИ ПОДРЯДЧИКА			
	Низкий	01 Средний	Высокий	Критический
Низкий				
03 Достаточный		02 Набран максимальный балл		
Средний				
Высокий				

01

Определили критичность подрядчика и выбрали способ оценки

02

Проанализировали результат оценки и сопоставили с вариантами ячеек в матрице

03

Сопоставили какому значению соответствует в столбце рейтинг ИБ

# Бинго сложностей при реализации

нет ресурса для  
проверки подрядчиков

все подрядчики  
«критичные»

подрядчик не хочет  
проходить оценку

нет бюджета для  
отдельного доступа под  
подрядчиков

нельзя проверить  
удаление данных

инвентаризация – это  
долго

дополнительный  
мониторинг – трата  
ресурсов

«Исполнитель  
обязуется исполнять  
требования  
внутренних ЛНА  
Заказчика»

регулятор такого не  
требует

# АБИСС

## Контактная информация



aa.korobetskaya@jet.su



<https://jet.su>



+7 (495) 411-76-01

**Анна Коробецкая,**

Ведущий консультант по информационной безопасности  
АО «Инфосистемы Джет»

