АБИСС
Ассоциация пользователей стандартов
по информационной безопасности

PKI ФОРУМ

Аудит информационной безопасности как инструмент подтверждения уровня надежности электронной подписи

Харыбина Анастасия Андреевна
Председатель Ассоциации АБИСС
Руководитель AKTIV.CONSULTING

Требования по ИБ для ДТС и УЦ

В рамках законодательства РФ (63-ФЗ)

ДТС (ст.18.1)

- Сертифицированные средства ДТС и ЭП
- Конфиденциальность, целостность и доступность при обработке, хранении и передаче информации

УЦ (ст.16)

- Сертифицированные средства УЦ, ЭП, защиты канала
- Специалисты с ИТ/ИБ образованием для работы с ЭП

В рамках обзорных визитов (ст. 5 Соглашения)

- Периодичность 1 раз в год
- Органы гос.власти, ДТС, УЦ (с привлечением иных организаций)
- Перечень организаций и что проверять — за 3 месяца
- По результатам — заключение

Невозможно предъявлять требования к партнерской стороне, не предъявляя эти же требования к себе. Следующий шаг – разработка таких требований совместно с коллегами из стран-партнеров.

Оценка соответствия требованиям

Объекты оценки — участники трансграничного электронного документооборота (ДТС, УЦ ДТС)

Основные бизнес-процессы

- ДТС — подтверждение действительности ЭП, проверка соответствия сертификатов требованиям, проверка полномочий, подпись квитанции
- УЦ — выдача сертификатов, управление их жизненным циклом, проверка сертификатов

Процессы информационной безопасности

- Управление функцией ИБ (PDCA)
- Защита информации (управление доступом, защита сети, управление инцидентами и т.д.)
- Обеспечение операционной надежности и управление рисками ИБ
- Безопасная разработка и ИТ/ИБ аутсорсинг
- и т.д.

Необходимо определить, на основе чего считаем, что объект оценки соответствует требованиям. Кто и как проводит оценку?

Практика аудита ИБ в РФ

Терминологическая коллизия:
термин «аудит» закреплен в 307-ФЗ и ориентирован на проверку финансовой отчетности, поэтому в документах по информационной безопасности используется термин «оценка соответствия».

Классификация:

- Виды аудита — управленческий, технический, комплаенс
- Аффилированность аудитора — внешний, внутренний
- Требования по проведению — обязательный, добровольный

Комлаенс-аудит ИБ:

- Субъекты КИИ (187-ФЗ, 235 и 239 Приказы ФСТЭК России) — добровольный аудит
- Операторы персональных данных (152-ФЗ и связанные НПА) — добровольный аудит
- Организации КФО (серия ГОСТ 57580 и связанные Положения Банка России) — обязательный аудит

Опыт финансовой отрасли

Обязательная оценка соответствия (с 2018 года)

- ГОСТ по защите информации (реализовано), ГОСТ по операционной надежности (в ближайшее время)
- Сроки прохождения — 1 раз в 1–3 года в зависимости от уровня критичности организации
- Требования к аудиторам — наличие лицензии ТЗКИ (подпункты «б» - контроль защищенности, «д» - проектирование защищенных систем, «е» - внедрение СЗИ)

Проблемы качества проводимых оценок:

- Недобросовестные заказчики и исполнители, соглашающиеся на формальные отчеты по оценке соответствия
- Большинство лицензиатов ТЗКИ не обладают знаниями и экспертизой по основным бизнес и технологическим процессам
- Демпинг делает затруднительным обеспечение проведения качественных оценок соответствия
- Нет санкций со стороны регулятора за некачественное проведение оценок соответствия и утверждения отчетов
- Нет листинга аудиторов и организаций, оказывающих услуги по оценке, которым можно доверять

Сфера аудита ИБ в настоящее время выпадает из процесса регулирования со стороны государства.

Саморегуляция и система добровольной сертификации

Без саморегуляции со стороны рынка не решить эту проблему, но необходима поддержка со стороны регуляторов.

Ассоциация АБИСС с 2020 года прорабатывает вопрос с ДИБ Банка России. В настоящее время работа ведется по двум направлениям:

01 Разработка ГОСТ по проведению оценок соответствия

- Требования к организациям и специалистам (процессы управления деятельностью по аудиту и квалификационные требования)
- Требования к процедуре оценки (от планирования и сбора свидетельств до формирования выводов и написания подробного отчета)

02 Создание Системы добровольной сертификации

- Объекты сертификации — знания физических лиц, услуги юридических лиц)
- Описание правил получения сертификата, его периодического подтверждения и отзыва
- Разработка экзамена, методических рекомендаций и учебных программ
- Определение правил взаимодействия СДС и Банка России

Аудит ИБ при трансграничном ЭДО

Необходима разработка гармонизированных требований по ИБ, включая функциональную надежность, для всех операторов доверенных сервисов

Оценка соответствия требованиям

- В рамках аккредитации со стороны государства при условии периодических оценок соответствия (требует создания инфраструктуры и доработки регуляторики, а также согласия стран-партнеров доверять таким оценкам)
- В рамках системы добровольной сертификации, где объектами сертификации являются операторы доверенных сервисов (требует создания СДС, деятельность которой признается странами-партнерами, с учетом мировых практик – WebTrust, eIDAS)
- В рамках проведения аудита независимой стороной, где заказчиком является оператор доверенного сервиса одной страны, а объектом аудита оператор другой страны (требует разработки общей методики оценки, а также аккредитации аудиторов в странах-партнерах)

Необходимо выбрать единую прозрачную процедуру оценки, которая будет признаваться всеми странами-партнерами.

Спасибо
за внимание!

АБИСС
Ассоциация пользователей стандартов
по информационной безопасности

kharybina@abiss.ru
kharybina@aktiv.consulting

www.abiss.ru
www.aktiv.consulting

+7 495 925-77-90
+7 903 687-90-59

Харыбина Анастасия Андреевна
Председатель Ассоциации АБИСС
Руководитель AKTIV.CONSULTING