Управляя технологиями, приближаем будущее!

Конференция: «152 ФЗ – основные ловушки и способы разминирования»

Методическое пособие для ИТ Директора

К конференции мы подготовили методическое пособие, которое имеется у каждого из присутствующих здесь.

Мы рассчитываем, что данное методическое пособие, будет иметь продолжение, если оно вызовет интерес.

Свои заявки, мнения, предложения по пособию просим высылать на адрес:

fz152@4cio.ru

Секция № 1

Программный комитет:

ФИО	Компания
Алмазов Андрей	Телеком Сервис
Зверянская Екатерина	VDEL Ltd.
Конопкин Николай	Leta IT
Кочуров Дмитрий	Мечел
Сапрыкина Виктория	ПрофМедиа Менеджмент
Сумманен Карл	ВТБ
Тагиев Аркадий	ВНИИНС
Устюжанин Дмитрий	Билайн

Секция № 1

Панельная дискуссия.
Ключевые вопросы встающие перед ИТ подразделением, в связи с реализацией 152 ФЗ.

Ведущая: **В. Сапрыкина**, Начальник Отдела Информационных Технологий, ПрофМедиа Менеджмент.

Эксперты:
Н. Конопкин, Заместитель директора Департамента внедрения и консалтинга, LETA IT Company
Д.Устюжанин, Руководитель департамента информационной безопасности, CISSP, MBCI, Beeline

Вопрос № 1

Классификация систем. Есть ли документы, определяющие точный перечень ПДн?
Например, ФИО + год рождения – это какой класс, ФИО + фото + телефон – какой класс и т.п.
Где тонкая грань между 2 и 3 классом?

Обязательная аттестация систем определенных классов, подходы к аттестации для различных типов ИС (медицина, страхование и т.п.). Что будет, если не пройти обязательную аттестацию. Как проходит процедура аттестации. С какими документами и условиями оператор должен подойти к аттестации. Реально ли сделать все своими силами – экспертная оценка?

Вопрос № 2

Нужна ли сертификация ПО, с помощью которого обрабатываются ПДн и которое не является средством защиты. И с какого момента ПО можно назвать средством защиты. (Пояснение: производители и интеграторы пользуясь неоднозначностью ситуации и предлагают внедрение версий бухгалтерских и кадровых систем, прошедших сертификацию. Насколько это нужно)?

Какие системы можно не сертифицировать. ОС - это система обработки или защиты? Можно ли обновлять сертифицированное ПО.?

Вопрос № 3

Нужна ли сертификация ПО, с помощью которого обрабатываются ПДн и которое не является средством защиты. И с какого момента ПО можно назвать средством защиты. (Пояснение: производители и интеграторы пользуясь неоднозначностью ситуации и предлагают внедрение версий бухгалтерских и кадровых систем, прошедших сертификацию. Насколько это нужно)?

Какие системы можно не сертифицировать. ОС - это система обработки или защиты? Можно ли обновлять сертифицированное ПО?

Вопрос № 4

Организация провела обследование ИС, определила и утвердила класс системы.
Может ли надзорный орган оспорить это и требовать изменить повысить) класс?

Как это происходит, на каком основании, какие механизмы?

Как проходит сама проверка?

Вопрос № 5

Структура предприятия : Головная (управляющая) Компания и филиалы в рамках одного Юридического лица.

В этом случае уведомление за себя и все филиалы рассылается Головной компанией?

Как оформляется передача данных между филиалами?

Что делать в случае Холдинговой структуры?

Вопрос № 6

Сертификация аппаратной части.

Надо ли заменять все или достаточно поставить сертифицированную железку «для галочки»?

Насколько сложнее сертифицировать свое оборудование самому нежели чем заменять на то, что уже сертифицировано под нужных класс?

Вопрос № 7

Практика применения санкций.
Не проще ли будет оспорить возможные взыскания в суде, чем тратить сейчас деньги на реализацию?

Чем это грозит компании?

Если компания – интегратор, которая имеет лицензию ФСТЭК провела обследование и выдала сертификат с нарушениями ошибочными заключениями как распространяется ответственность?

Вопрос № 8

Передача ПДн третьим лицам (партнерам, вышестоящей организации).

Как это регламентировать?
Какие должны быть документы и как защищать каналы передачи в случае, например, использования почты для передачи файлов с данными?

Вопрос № 9

Модель угроз.

Что такое типовая модель угроз?
Порядок разработки?

Для каждой ли ИС она отдельно разрабатывается и утверждается?

Что можно отнести к специальной ИС и как разрабатывать для нее модель угроз?

Вопрос № 10

В каких случаях необходимо использовать криптозащиту и всегда ли при использовании криптозащиты надо получать лицензию ФСБ?

Что делать при передаче данных через Интернет, ВОЛС?

Действительно ли при трансграничной передаче использовать шифрованные каналы не обязательно, а при передаче из ИС в ИС, расположенных в разных комнатах надо?