Обеспечение безопасности в облаке: распределение ответственности между провайдером облачных услуг и заказчиком

Емельянников
Михаил Юрьевич,
Управляющий партнер

CLOUD & DIGITAL
TRANSFORMATION

23 МАРТА 2017 ГОДА
МОСКВА, ЦЕНТР DIGITAL OCTOBER

Информация ограниченного доступа в облаке. Что это?

- **персональные данные**
- **служебная тайна** органов власти
- **коммерческая тайна**
- **врачебная тайна** (облачные медицинские информационные системы и хранилища)
- **тайна страхования** (при покупке электронного полиса)
- …

Две основных проблемы

Безопасность

Местонахождение технических средств

Безопасность при аутсорсинге: общие требования

Обладатель информации, **оператор информационной системы** в случаях, установленных законодательством, обязаны обеспечить:

1) предотвращение НСД;

2) своевременное обнаружение фактов НСД;

3) предупреждение неблагоприятных последствий нарушения порядка доступа;

4) недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

5) возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие НСД;

6) постоянный контроль за обеспечением уровня защищенности информации.

Безопасность при аутсорсинге: ГИСы и МИСы

Приказ ФСТЭК 2013 года № 17

Лицо, **обрабатывающее информацию**, являющуюся государственным информационным ресурсом, по поручению обладателя информации (заказчика) или оператора и (или) **предоставляющее им вычислительные ресурсы** (мощности) для обработки информации на основании заключенного договора, **обеспечивает защиту информации** в соответствии с законодательством РФ об информации, информационных технологиях и о защите информации. В договоре должна быть предусмотрена обязанность уполномоченного лица обеспечивать защиту информации, являющейся государственным информационным ресурсом, **в соответствии с настоящими Требованиями**.

Обязанности заказчика

Постановление Правительства № 1119 2012 года	Приказ ФСТЭК № 17
Определить тип угроз безопасности персональных данных; Установить уровень защищенности персональных данных; Выбрать средства защиты информации для системы защиты персональных данных.	Классифицировать информационную систему по требованиям защиты информации; Определить угрозы безопасности информации, реализация которых может привести к нарушению безопасности информации в информационной системе, и разработать на их основе модель угроз безопасности информации; Определить требования к системе защиты информации информационной системы.

Для кого установлены территориальные ограничения

152-ФЗ	149-ФЗ	Приказ ФСТЭК № 17	Проект изменений в 149-ФЗ
Все операторы в период сбора и актуализации персональных данных (есть исключения)	Государственные органы, органы местного самоуправления, государственные и муниципальные унитарные предприятия, государственные и муниципальные учреждения	Государственные и муниципальные информационные системы	Органы государственной власти, органы управления государственным и внебюджетными фондами, органы местного самоуправления

Возникающие проблемы

- **Доступ** персонала облачного провайдера к обрабатываемым данным – это передача данных для обработки, поручение на их обработку или что-то другое?
- **Классификация** информационной системы, определение **уровня защищенности**, **моделирование угроз** и **построение** системы защиты – как выполнить требования законодательства?
- **Согласие** субъекта на обработку – надо ли получать и, если да, то как?

Возможные пути решения

Поручение обработки, даваемое заказчиком провайдеру

Запрет на доступ персонала к данным заказчика

Безопасность при аутсорсинге: общие требования

Обладатель информации, **оператор информационной системы** в случаях, установленных законодательством, обязаны обеспечить:

1) предотвращение НСД;

2) своевременное обнаружение фактов НСД;

3) предупреждение неблагоприятных последствий нарушения порядка доступа;

4) недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

5) возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие НСД;

6) постоянный контроль за обеспечением уровня защищенности информации.

Особенности поручения обработки персональных данных

Статья 6. Условия обработки персональных данных

3. Оператор вправе поручить обработку персональных данных другому лицу **с согласия субъекта** персональных данных, если иное не предусмотрено 152-ФЗ, **на основании** заключаемого с этим лицом **договора**.

Условия договора поручения на обработку персональных данных

В поручении оператора должны быть определены:

- **перечень действий** (операций) с персональными данными;
- **цели обработки** персональных данных;
- обязанность соблюдать **конфиденциальность** персональных данных;
- обязанность обеспечивать **безопасность** персональных данных при их обработке;
- **требования к защите** персональных данных в соответствии со ст.19 ФЗ «О персональных данных».

Запрет доступа

Персонал провайдера **не имеет доступа** к информации клиента и принимает меры по предотвращению физического доступа любых лиц к оборудованию и данным клиента (закреплено в договоре).

Исполнитель (провайдер облачных сервисов) не знает, какие данные обрабатывает заказчик.

Это значит, что **нет и поручения обработки**.

Ключевая проблема

Но заказчик **не может смоделировать актуальные угрозы** для облачной инфраструктуры и выбрать средства защиты, используемые на сетевом уровне!

НИКОГДА!

Однако формирование частной модели актуальных угроз в целом является **прерогативой оператора.**

Что должен сделать заказчик – обладатель информации

- определить **тип актуальных угроз** и **класс защищенности** информационной системы (**уровень защищенности** ИСПДн);
- определить **состав мер безопасности** из набора базовых и адаптивных, согласовать и отразить в договоре с провайдером, какие меры безопасности принимаются провайдером;
- построить **частную модель актуальных угроз** для **своего сегмента** ИС;
- реализовать систему защиты **в своем сегменте ИС**.

Что может и должен сделать отечественный провайдер

- получить **лицензии ФСТЭК, ФСБ, Минсвязи**;
- определить **тип актуальных угроз**, максимальный **уровень защищенности**) для облака;
- построить **частную модель актуальных угроз** для облака;
- **реализовать систему защиты** в облаке;
- представить заказчику возможность **развернуть дополнительные средства** безопасности (PaaS или IaaS);
- **помочь заказчику** с реализацией мер защиты на клиентской стороне.

Решает ли все проблемы перенос ИСПДн в российский ЦОД?

Да!

Но при условиях:

- отношения владельца ЦОДа и оператора урегулированы **договором**, соответствующим требованиям части 3 ст.6 ФЗ «О персональных данных»;
- в ЦОДе приняты **меры безопасности**, обеспечивающие выполнение требований к защите персональных данных;
- у владельца есть **лицензии ФСБ, ФСТЭК и Минкомсвязи**.

Что может и должен сделать зарубежный провайдер?

- предоставить оператору данные о том, какие **меры безопасности** обеспечиваются в облачной инфраструктуре;
- обеспечить при необходимости принятие **дополнительных мер безопасности** или представить заказчику возможность **развернуть дополнительные средства** безопасности (PaaS или IaaS);
- **отразить в договоре** обязанности по обеспечению мер **безопасности** и **конфиденциальности** обрабатываемых данных, порядок доступа к ним персонала и порядок взаимодействия провайдера с компетентными органами соответствующей юрисдикции.

ГОСТ или https с RSA?

- Определение актуальных угроза и формирование частной модели угроз – прерогатива владельца информации.
- Если угроза перехвата в канале связи актуальна или предотвращение НСД нельзя обеспечить без средств шифрования – необходимо использовать СКЗИ, реализующие ГОСТ.
- Зайдите на сайты gosuslugi.ru и nalog.ru.

Аттестовывать облако или нет?

Для обеспечения защиты информации применяются средства защиты информации, прошедшие оценку соответствия **в форме обязательной сертификации** на соответствие требованиям безопасности.

Для обеспечения защиты информации, содержащейся в информационной системе, проводятся следующие мероприятия:

- **аттестация** информационной системы по требованиям защиты информации и ввод ее в действие;
- обеспечение защиты информации в ходе эксплуатации **аттестованной** информационной системы.

Если услышанного сегодня недостаточно

Рецепты безопасности от Емельянникова

Блог российского эксперта в области информационной безопасности, защиты персональных данных, коммерческой тайны, государственного регулирования охраны конфиденциальности. Комментарии к «громким» событиям, связанным с утечкой данных и взломом компьютерных сетей.

ПДн после 1 сентября | Блог | Об агентстве | Наши проекты | Семинары и курсы

Курсы, семинары, выступления М.Емельянникова. Где? Когда?

16 октября - Персональные данные россиян после 1 сентября 2015 года, очно, семинар, Центр «Технологии управления бизнесом», Самара, 8(846) 372-00-30, 8(846) 972-06-40

19 октября - Персональные данные россиян после 1 сентября 2015 года, очно / вебинар, Учебный центр «Информзащита», Москва, (495) 980-2345, доб.04

20 октября - Сложные проблемы применения законодательства о

16 сентября 2015 г.

Станут ли владельцы российских ЦОДов богаче и счастливее после 1 сентября

В журнале "ЦОДы.РФ" №12 за 2015 год опубликована моя подробная статья «Станут ли владельцы российских ЦОДов богаче и счастливее после 1 сентября».

Первого сентября вступили в силу поправки в российское законодательство, вносимые самым обсуждаемым в этом, да и в прошлом году законом – 242-ФЗ с привычно-длинным названием «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях». Закон с легкой подачи

Об авторе

Михаил Юрьевич Емельянников

Москва, Russia

Эксперт в области информационной безопасности и безопасности бизнеса. Управляющий партнер Консалтингового агентства "Емельянников, Попова и партнеры"

Просмотреть профиль

Спасибо!
Вопросы?

Емельянников
Михаил Юрьевич
Управляющий партнер
+7 (495) 761 5865
info@mezp.ru
http://emeliyannikov.blogspot.ru/

Консалтинговое агентство
Емельянников, Попова и партнеры