Обеспечение безопасности при использовании внешних облачных сервисов

Риски кибербезопасности

- Утечка конфиденциальной информации
- Нарушение целостности активов (модификация и уничтожение информации)
- Недоступность активов (недоступность информационных систем, сбой в работе систем ИБ, недоступность облачных сервисов)
- Нарушение процессов управления кибербезопасностью (невыполнение требований КБ, некорректное выполнение процессов КБ)
- Нарушение управления доступом (нарушение предоставления прав доступа или парольной политики)

Риски, не относящиеся к кибербезопасности

- Отказ от ответственности поставщика облачного сервиса – ограничение или полный отказ от возмещения причиненного ущерба
- Невозможность сбора доказательной базы – отсутствие технической возможности сбора доказательств для предоставления в суде с целью возмещения ущерба, причиненного по вине поставщика облачного сервиса
- Регуляторный – нарушение требований регуляторов поставщиком или организацией при использовании облачного сервиса
- Потеря контроля – отсутствие технической возможности осуществления полного контроля над информацией, размещенной в облачном сервисе, и соблюдением поставщиком требований к ее защите
- Геополитический – изменение политической ситуации в стране, с территории которой предоставляется облачный сервис, влияющее на его качество

Меры компенсации рисков кибербезопасности

Область управления	Собственный ЦОД	Публичное облако		
		IaaS	PaaS	SaaS
Пользователи	Ролевые модели, многофакторная аутентификация			
Данные	Шифрование, контроль передачи (DLP), мониторинг активности СУБД			
Приложения	Статический и динамический анализ защищенности, WAF			
Среда исполнения	Управление уязвимостями			
Операционная система	Защита от вредоносного ПО			
Виртуальная сеть	Сегментирование, межсетевое экранирование, выявление и предотвращение вторжений			
Средства виртуализации	Контроль действий привилегированных пользователей			
Серверы	Контроль конфигураций и целостности			
Подсистема хранения	Шифрование, резервное копирование			
Физическая сеть	Защита периметра и защита от DDoS, контроль конфигураций, анализ трафика			
Доступ в ЦОД	СКУД, видеонаблюдение			

Клиент

Поставщик услуги

Нормативная база

- Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
- Федеральный закон № 152–ФЗ «О персональных данных»
- Федеральный закон № 242-ФЗ «О внесении изменений в отдельные законодательные акты РФ по вопросам осуществления государственного контроля (надзора) и муниципального контроля»
- Приказ ФСТЭК России № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»
- Постановление Правительства РФ № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»
- ГОСТ Р 56938-2016 «Защита информации. Защита информации при использовании технологий виртуализации. Общие положения»
- ГОСТ ISO/IEC 17788-2016 «Информационные технологии (ИТ). Облачные вычисления. Общие положения и терминология»

Мировые практики

- NIST Special Publication 500-299 “NIST Cloud Computing Security Reference Architecture”
- NIST Special Publication 800-125 “Guide to Security for Full Virtualization Technologies”
- NIST Special Publication 800-125A “Security Recommendations for Hypervisor Deployment on Servers”
- NIST Special Publication 800-125B “Secure Virtual Network Configuration for Virtual Machine (VM) Protection”
- NIST Special Publication 800-144 “Guidelines on Security and Privacy in Public Cloud Computing”
- NIST Special Publication 800-145 “The NIST Definition of Cloud Computing”
- NIST Special Publication 800-146 “Cloud Computing Synopsis and Recommendations”
- NIST Special Publication 800-190 “Application Container Security Guide”
- Cloud Security Alliance (CSA) Security Guidance for Critical Areas of Focus in Cloud Computing v.4