

Коммерческие ЦОДы – пути решения проблемы злонамеренного инсайда



Юлия Смирнова
менеджер по развитию
направления компании
«Код Безопасности»

Проблемы в области обеспечения ИБ и нормативного соответствия могут стать серьезной преградой на пути развития рынка коммерческих ЦОДов. Клиенты ЦОДа должны быть уверены в том, что их данные надежно защищены, в том числе, в соответствии с действующим законодательством, требованиями регуляторов и отраслевыми стандартами в области ИБ. При этом даже единичный факт нарушения конфиденциальности и целостности данных клиента ЦОДа может отразиться на репутации его владельца, не обеспечившего необходимых мер по защите введенных ему данных.

Проблема злонамеренного инсайда

Консолидация данных сразу нескольких клиентов коммерческого ЦОДа увеличивает его привлекательность как для хакеров, так и злонамеренных инсайдеров. При этом угроза злонамеренного инсайда в ЦОДах намного выше, чем при размещении ИТ-ресурсов внутри организации. Ведь в рамках штатной работы ЦОДа физический доступ на его территорию могут получить различные группы лиц. Это персонал ЦОДа, не имеющий непосредственного доступа к информационным системам, представители других организаций, арендующие стойки или серверы, а также иные лица. Однако самую серьезную угрозу ИБ представляют администраторы, имеющие непосредственный доступ к информационным системам клиентов ЦОДа.

В защите ресурсов клиентов ЦОДа как от злонамеренного инсайда, так и от других угроз помогут продукты разработки компании «Код Безопасности».

Продукт	Класс СЗИ	Ценность для ЦОДа
vGate R2	СЗИ от НСД (защита платформы виртуализации)	Защита ресурсов клиентов виртуализированного ЦОДа
TrustAccess	Межсетевой экран	Защита от злонамеренного инсайда
Security Studio Endpoint Protection	Комплексное решение (МЭ + HIPS + антивирус)	Защита рабочих мест персонала и клиентов ЦОДа от сетевых вторжений, вредоносных программ и спама
HoneyPot Manager	Защита от вторжений на основе имитации данных	Выявление и пресечение попыток злонамеренного инсайда и хакерских атак
Код Безопасности: Инвентаризация	Соответствие стандартам	Обнаружение ПО, которое может использоваться для злонамеренного инсайда
Электронный замок «Соболь»	Средство доверенной загрузки	Защита от злонамеренного инсайда
СЗИ Secret Net	СЗИ от НСД	Защита рабочих мест персонала и клиентов ЦОДа от НСД
АПКШ «Континент»	МЭ и VPN	Организация защищенного взаимодействия клиентов с ЦОДом

Построение комплексной системы защиты персональных данных с применением сертифицированных СЗИ разработки компании «Код Безопасности» не только обеспечит соблюдение требований к защите персональных данных в ИСПДн любого класса, но и позволит избежать проблем совместимости и управления средствами защиты информации, используемыми компанией для нейтрализации угроз информационной безопасности.

Сценарий защиты ЦОДа от злонамеренного инсайда

На рисунке продемонстрирован один из возможных сценариев защиты ЦОДа с сервисной моделью предоставления ИТ-ресурсов.

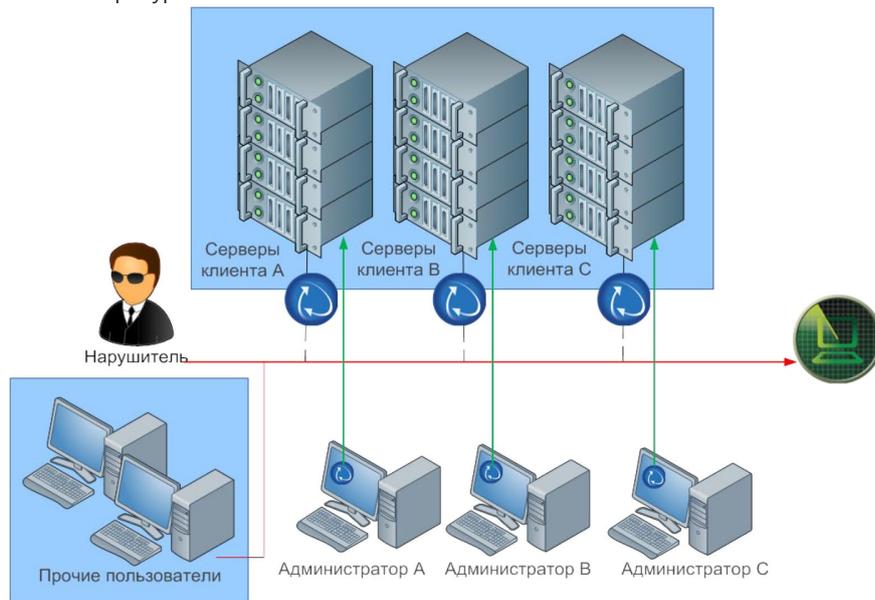
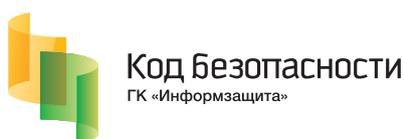


Рис. 1. Схема защиты ресурсов клиентов от злонамеренного инсайда

Распределенный межсетевой экран TrustAccess позволит защитить ресурсы клиентов ЦОДа, а также разграничить доступ администраторов к серверам разных клиентов (администратор сможет получить доступ только к тому серверу, который ему доверен для администрирования). Решение Honeypot Manager, в свою очередь, зафиксирует попытки прочих пользователей получить доступ к ресурсам клиентов, что позволит выявить и пресечь попытки злонамеренного инсайда внутри ЦОДа.

С помощью сертифицированных продуктов разработки компании «Код Безопасности» владельцы коммерческих ЦОДов могут не только обеспечить защиту доверенных им ресурсов от злонамеренного инсайда и хакерских атак, но и предложить своим клиентам дополнительную услугу по выполнению требований регуляторов и отраслевых стандартов в области ИБ. Решения компании «Код Безопасности» также обеспечат эффективную защиту ЦОДов, которые используют современные технологии виртуализации и облачных вычислений.



Почтовый адрес: 127018, Россия, Москва, а/я 55.

Адрес офиса в Москве: ул. Образцова, д. 38.

Адрес офиса в Санкт-Петербурге: Свердловская наб., д. 44.

Тел.: +7 (495) 980-2345 (многоканальный), факс: +7 (495) 980-2345.

E-mail: info@securitycode.ru

Запрос дополнительной информации о продуктах: info@securitycode.ru

По вопросам стоимости и покупки продуктов sales@securitycode.ru

По вопросам партнерства и сотрудничества info@securitycode.ru

Вы можете узнать подробную информацию о продуктах на сайте www.securitycode.ru

О компании «Код Безопасности»

Компания «Код Безопасности» – российский разработчик программных и аппаратных средств, обеспечивающих безопасность информационных систем, а также их соответствие требованиям международных и отраслевых стандартов. «Код Безопасности» входит в группу компаний «Информзащита» – признанного лидера в сфере информационной безопасности – и является преемником её многолетних наработок в области создания средств защиты информации для государственных и коммерческих заказчиков.