УТВЕРЖДАЮ
Генеральный директор
ООО «НЕТФОКС»
Богданов А.Г.
_____
«___»_____ 20___г.

Регламент 6
к Договору об оказании услуг
Введено в действие
03 апреля 2017 г.

Политика безопасности

Содержание:

1. **Используемые термины**
Политика информационной безопасности - Совокупность требований и правил по обеспечению информационной безопасности системы для объекта информационной безопасности системы, разработанных в целях противодействия нарушителю информационной безопасности по реализации угроз информационной безопасности системы с учетом ценности защищаемой информационной сферы и стоимости системы обеспечения информационной безопасности системы.
Угроза информационной безопасности-Возможное воздействие нарушителя информационной безопасности на информационную систему, не предотвращение, не обнаружение и не ликвидация последствий которого средствами информационной системы может привести к ухудшению заданного уровня качества службы или к ухудшению заданных качественных характеристик функционирования ИС и, как следствие, к нанесению ущерба государству, пользователю или оператору ИС.
Виртуальный частный (корпоративный) центр обработки данных - Ресурсы, сгруппированные для определенных бизнес целей - все сервисы ЦОД (хостинг, хранение и обработка данных и т.д.), реализованные в облачной инфраструктуре и доступные через веб-интерфейс.
Взломщик - Лицо или группа, которая стремится воздействовать на конфиденциальность, целостность и доступность данных.
Уязвимость - Параметр, характеризующий возможность нанесения описываемой системе повреждений любой природы теми или иными внешними средствами или факторами.
ДДОС-атака - Атака на вычислительную систему с целью довести её до отказа, то есть создание таких условий, при которых легитимные (правомерные) пользователи системы не могут получить доступ к предоставляемым системой ресурсам (серверам), либо этот доступ затруднен.
Мониторинг безопасности в реальном времени - Получение и анализ информации о состоянии ресурсов системы обеспечения информационной безопасности с помощью специальных средств контроля в реальном масштабе времени.

Операционная система - Комплекс управляющих и обрабатывающих программ, которые, с одной стороны, выступают как интерфейс между устройствами вычислительной системы и прикладными программами, а с другой стороны — предназначены для управления устройствами, управления вычислительными процессами, эффективного распределения вычислительных ресурсов между вычислительными процессами и организации надёжных вычислений.
Отказоустойчивость - Способность системы предоставлять и обеспечивать приемлемый уровень сервиса в условиях отказов (ненамеренных, намеренных или вызванных естественных путем).
Виртуальный хостинг - Услуга по предоставлению ресурсов для размещения информации на сервере.
Виртуальные серверы - программный комплекс, эмулирующий работу сервера, и обладающий набором вычислительных ресурсов. Количество доступных вычислительных ресурсов (параметры Услуги) определяется Тарифом.
Термины и определения, не оговоренные в настоящем разделе, соответствуют терминам и определениям, приведенным в Договоре

2. Общие положения
Данный регламент регулирует взаимоотношения, относительно политики информационной безопасности Исполнителя предоставляемых услуг Заказчику.
3. Область применения
Виртуальный хостинг, виртуальные сервера, размещение оборудование, аренда оборудования, доступ к оборудованию.
4. Цель
Повышение отказоустойчивости используемых ресурсов. Обеспечение безопасного функционирования ресурсов Исполнителя.
Определение более четких рамок ответственности сторон при возникновении угроз информационной безопасности для ресурсов Исполнителя, ДДОС-атаках. Определение алгоритмов при возникновения угроз.
5. Взаимодействие
В случае обнаружение, уязвимостей, вредоносных файлов (удаляются), подозрительных файлов, ДДОС-атак, услуга предоставляемая Заказчику может быть заблокирована. В зависимости от степени опасности, блокировка производится полностью, либо частично, на усмотрение Исполнителя.
Исполнитель производит отправку уведомления Заказчику, с копией в личный кабинет, форма свободная.
В случае повторного инцидента услуга блокируется без возможности включения и удаляется без восстановления.

6. Расследование инцидентов
Объем сохраняемой и предоставления информации об инциденте определяет Исполнитель. Информация о происшедших инцидентах предоставляется в ограниченном виде, либо не предоставляется, используется только для служебного пользования. Алгоритм выявления вредоносных файлов не предоставляется.

7. Ответственность
Исполнитель не несет ответственности за упущенную выгоду и иные риски в связи с блокировкой услуг предоставляемых заказчику.
Заказчик несет ответственность в соответствии с законодательством Российской Федерации.