ТОО «Интернет-компания PS»

Условия использования услуги

Оперативный центр Информационной безопасности (ОЦИБ)

Версия от 01.12.2023

www.ps.kz

Настоящие условия («Условия»):

- устанавливают порядок предоставления Заказчику услуг Оперативного центра информационной безопасности («Услуга»);
- являются неотъемлемой частью Публичного договора, опубликованного по адресу: https://www.ps.kz/agreements/offer («Оферта»).

Предоставляемая Услуга в соответствии с НК РК 03–2019 «Общий классификатор видов экономической деятельности», введенном в действие Министерством индустрии и инфраструктурного развития Республики Казахстан с 1 января 2020 года, включена в подкласс 62.09.2.

Термины, которые используются, но не определены в Условиях, имеют значение, присвоенное им в Оферте и в разделе «Помощь» на Сайте Исполнителя: https://www.ps.kz/faq. Условия содержат пункты с активными гиперссылками на веб-страницы с более подробной информацией, которые являются неотъемлемой частью Условий.

Исполнитель вправе без какого-либо специального уведомления вносить изменения в Условия, в связи с чем Заказчик обязуется регулярно отслеживать эти изменения. Действующая редакция Условий размещена по адресу: https://www.ps.kz/agreements/soc-sla.pdf. Использование Заказчиком Услуги после изменения Условий является подтверждением его согласия с их новой редакцией.

1. Состав Услуги

1.1. Исполнитель осуществляет мониторинг Информационно-коммуникационной инфраструктуры Заказчика для выявления и предотвращения инцидентов по информационной безопасности, а Заказчик принимает и оплачивает оказанные услуги.

1.2. В состав Услуги входят:

- мониторинг событий информационной безопасности;
- регистрация и классификация подозрений на инцидент информационной безопасности;
- сбор необходимых данных для анализа подозрения на инцидент информационной безопасности;
- анализ подозрений на инцидент информационной безопасности с целью его идентификации;
- составление рекомендаций реагирования на инциденты информационной безопасности;
- администрирование технических инструментов SOC;
- развитие инфраструктуры SOC;
- улучшение и обновление сигнатур и правил реагирование на события информационной безопасности.

1.3. В состав Услуги не входят:

- активное реагирование на инциденты информационной безопасности со стороны оборудования и сервисов заказчика.

2. Порядок оказания Услуги

2.1. Заказчик направляет письмо с запросом на услугу на адрес info@ps.kz.

2.2. Исполнитель уточняет первоначальные параметры Услуги, наличие технической возможности для ее предоставления и направляет в адрес Заказчика опросный лист.

2.3. После получения заполненного опросного листа Исполнитель формирует окончательный заказ, выставляя счет на оплату.

2.4. Заказчик оплачивает выставленный счет и уведомляет об этом Исполнителя.

2.5. Исполнитель производит установку и настройку инфраструктуры оперативного центра информационной безопасности. После этого Исполнитель направляет в адрес Заказчика инструкции по подключению источников информации к ОЦИБ. По окончанию подключения, Исполнитель начинает предоставление Услуги с даты, согласованной с Заказчиком.

2.6. Исполнитель обеспечивает мониторинг информационной безопасности в течение всего срока действия Договора, с учетом ограничений, предусмотренных для проведения планового и внепланового технического обслуживания.

2.7. Исполнитель получает информацию о состоянии информационной безопасности, включая информацию об инцидентах, и направляет указанные сведения в карточке инцидента Заказчику через мессенджер Telegram или через иные согласованные Сторонами каналы связи.

2.8. Карточка инцидента содержит информацию о характере, уровне, времени инцидента, его краткое описание и, в зависимости от характера уведомлений системы мониторинга, может включать рекомендации по обработке инцидента.

2.9. Заказчик обязуется уведомить Исполнителя о плановых профилактических работах, проводимых Заказчиком самостоятельно, не менее, чем за 24 (двадцать четыре) часа до момента проведения работ. В таких случаях Исполнитель не реагирует на отчеты системы мониторинга, возникших в результате Плановых работ Заказчика, без соответствующего запроса Заказчика в Тикет-системе.

2.10. При оказании Услуг Исполнитель гарантирует обеспечить ключевые параметры предоставления услуг. Перечень ключевых параметров:

Уровни приоритета

Критический	Элементы, требующие немедленных действий, такие как признаки DDOS-атаки, признаки успешной атаки, компрометация сети или учетной записи или свидетельства продолжающейся эпидемии вредоносного ПО.
Высокий/Средний	Элементы, требующие немедленных действий, такие как серьезное нарушение политики, незначительная вирусная эпидемия (более 1 узла, но все же небольшая, ограниченная группа) или другие подобные риски и угрозы.
Низкий	Элементы, требующие не срочного внимания, такие как незначительные нарушения политики ИБ, единичное появление вируса или угроза с низким риском, затрагивающее 1 узел.

Обязательства по уровню обслуживания

Приоритет	Время обнаружения инцидента	Время подтверждения инцидента
Критический	15 минут	Не более 1 часа с момента обнаружения
Высокий	15 минут	Не более 1 часа с момента обнаружения
Средний	15 минут	Не более 2 часов с момента обнаружения
Низкий	30 минут	Не более 4 часов с момента обнаружения

3. Оплата Услуги

3.1. Стоимость Услуги определяется согласно тарифным планам Исполнителя и фиксируется в счете, автоматически выставляемом Заказчику за очередной период.

3.2. Заказчик осуществляет предоплату очередного периода предоставления Услуги до его начала, в ином случае предоставление Услуги прекращается.

3.3. В случае отказа Заказчика от Услуги Исполнитель по его запросу осуществляет перерасчет и возвращает неиспользованные средства на Лицевой счет.

4. Уровень оказания и параметры Услуги

Гарантированная доступность (без учета плановых работ)	99,8% в год (не более 18 часов простоя)
Сбор/прием/хранение/обработка событий ИБ	24/7

Мониторинг и анализ событий, выявление инцидентов	8/5 / 24/7
Мониторинг работоспособности	24/7
Выявление инцидентов	8/5 / 24/7
Отправка периодических отчетов на почту	Да
Телефонный звонок при инцидентах	Да
Оповещения в мессенджерах	Да

4.1. Виды работ:

- **плановые работы** — регламентные организационные и технические мероприятия Исполнителя по мониторингу, настройке и обновлению IT-инфраструктуры;
- **внеплановые работы** — экстренные организационные и технические мероприятия Исполнителя нерегламентированной продолжительности с целью устранения сбоев и неполадок в IT-инфраструктуре.

Работы	Уведомления	Время проведения
Плановые	не менее, чем за 48 часов до начала работ	в часы наименьшей нагрузки (с 01:00 до 06:00 GMT+6)
Внеплановые	по факту	в любое время суток, по необходимости

4.2. Работа Исполнителя с обращениями:

Критичность	Время решения	Период обслуживания
Высокая	До 24 часов	Круглосуточно, 7 дней в неделю
Средняя	До 24 часов	Круглосуточно, 7 дней в неделю
Низкая	До 24 часов	В будние дни с 10:00 до 19:00

5. Условия компенсации

5.1. В случае недоступности Услуги по вине Исполнителя и обращения Заказчика, направившего посредством Тикет-системы сообщение с указанием даты и суммарного времени простоя, сумма компенсации определяется согласно п. 5.3.

5.2. Если Исполнитель располагает собственными данными о времени простоя, он вправе использовать эти данные. Разногласия о времени простоя разрешаются путем переговоров сторон.

5.3. Компенсируется каждый час простоя в размере 1% от суммы ежемесячного платежа Заказчика за Услугу:

- стоимость Услуги в месяц / 100 × количество часов
- при этом общая сумма компенсации не может превышать 100% стоимости Услуги в месяц. Компенсация начисляется на Лицевой счет в виде бонусов.

5.4. Компенсация может выражаться в выплате денежных средств Заказчику только в случае его отказа от дальнейшего использования Услуги и проведения сверки взаиморасчетов.

5.5. Не подлежит компенсации простой:

- связанный с обстоятельствами непреодолимой силы и иными обстоятельствами, произошедшими не по вине Исполнителя;
- вызванный действиями (бездействием) Заказчика;

- произошедший по причине отказа ПО, разработанного третьими лицами или являющегося собственностью (либо арендуемого) Заказчиком;
- вызванный сбоями системы сетевых служб, находящимися за пределами прямого контроля Исполнителя, а также задержками распространения информации об обновлении DNS-записей;
- связанный с проведением работ, согласно п. 4.1.