Соглашение об уровне обслуживания (SLA)
услуги «Доступ к системе сбора и корреляции событий (SIEMaaS)»

Содержание

1. ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Время анализа и реагирования на обращение – период времени, начиная с зафиксированного факта Обращения Клиента в Центре поддержки Компании, до определения и классификации Обращения и начала работ по данному обращению, с уведомлением Клиента по электронной почте.

Время обработки и выполнения обращения – период времени с момента зафиксированного факта Обращения Клиента в Центре поддержки Компании до факта полного выполнения работ, указанных в Обращении, и устранения проблемы или предложения альтернативного решения задачи/проблемы.

Глобальная недоступность Услуги – недоступность Услуги (массовые инциденты с приоритетом – Критический), связанная с форс-мажором или обстоятельствами непреодолимой силы (определения указаны в договоре об оказании Услуги), препятствующими Компании предоставить Услугу Клиенту.

Интерфейсы Компании – перечень регламентируемых способов и точек коммуникации с Компанией.

Инцидент – любое непредвиденное событие, не являющееся частью стандартного (штатного) использования программ и/или программно–аппаратных комплексов, которое вызывает или может вызвать прерывание предоставления или снижение качества используемых Услуг Клиентом.

Услуга SIEMaaS (далее – Услуга) – предоставление доступа к SIEMaaS на базе программного обеспечения IBM QRadar, размещенной в аттестованном сегменте, с заявленными логическими единицами услуги.

Логическая единица услуги – количество учетных записей SIEMaaS, количество событий, обрабатываемых в секунду (далее – EPS), количество источников событий.

Обращение – зарегистрированный факт любого обращения или инцидента со стороны Клиента или потребителя Услуги, через интерфейсы Компании. В данном соглашении имеет категории – обращение на предоставление информации, обращение на обслуживание, обращение на изменение, инцидент.

Отчетный период технической поддержки – период времени продолжительностью 3 календарных месяца в рамках срока действия настоящего соглашения. Отсчет периода начинается с момента начала оказания Услуг.

Период ограниченной поддержки - период времени, в течение которого обращения регистрируются, обращения и инциденты с приоритетом Высокий и Критический решаются, обработка остальных обращений производится в основной период поддержки. Период ограниченной поддержки является частью периода функционирования.

Период поддержки - период времени, в течение которого сотрудник технической поддержки выполняет обработку обращений потребителей Услуги - Клиента. Период поддержки является частью периода функционирования.

Период технического обслуживания - период времени, в течение которого не гарантируется функционирование объектов Услуги (Информационные системы, ПО, оборудование), вследствие возможного проведения регламентных и технических работ. Период технического обслуживания не входит в период функционирования. Период технического обслуживания согласовывается с Клиентом дополнительно.

Период функционирования - период времени, в течение которого компоненты, обеспечивающие предоставление Услуги, (Информационные системы, программное обеспечение (далее - ПО), оборудование) функционируют. Обработка обращений выполняется на уровне их регистрации. Выполнение обращений выполняется в период поддержки.

Пользователь – сотрудник Клиента или другое лицо, уполномоченное Клиентом пользоваться Услугой.

ПО – программное обеспечение.

Техническая поддержка – совокупность действий и итераций по настройке и обслуживанию обращений Клиента, направленных на обеспечение стабильной и бесперебойной работы информационных систем и сервисов в зоне ответственности Компании.
Учетные данные - набор регистрационных данных клиента, включая номер договора, имя пользователя, пароль и URL доступа к порталу самообслуживания.
Центр обработки данных (далее - ЦОД), расположенный по адресу г. Минск, ул. Танковая, 11, представляет собой специализированное помещение, в котором реализована совокупность решений, технологий и организационных процедур, ориентированных на предоставление информационных сервисов и услуг с заданными параметрами качества. ЦОД соответствует классу отказоустойчивости TIER III (сертифицирован Uptime Institute Tier III Design, Tier III Facility).
Центр поддержки – система обмена сообщениями между Клиентом и Компанией предоставляемой Услуги путем передачи запросов через Интерфейсы Компании.

2. ПРЕДМЕТ СОГЛАШЕНИЯ

Настоящее Соглашение является неотъемлемой частью Договора об оказании услуг информационной безопасности, заключенного между Компанией и Клиентом, и определяет порядок и условия предоставления Клиенту технической поддержки в отношении предусмотренной Договором Услуги, а также требования к качеству Услуги и сервисов, выполнение которых гарантирует Компания.
В соглашении определяются состав и области допустимых значений показателей качества Услуги, размеры и порядок компенсации в случае нарушения гарантий по настоящему Соглашению.
Во всём остальном, что не предусмотрено условиями настоящего Соглашения, Стороны руководствуются условиями Договора.

3. ПОДДЕРЖКА И ПРЕДОСТАВЛЕНИЕ УСЛУГ

3.1. Интерфейсы подачи Обращения в Центр поддержки

Все Обращения Клиента, в обязательном порядке, должны подаваться утвержденным способом с использованием следующих интерфейсов/сервисов Компании:

Интерфейс/сервис	**Контактная информация**
Телефон	**150 – далее в голосовом меню 3, затем 6.**
Электронная почта Центра поддержки	**sd@a1data.by**
Электронная почта Отдела продаж	**sales@a1data.by**

Все обращения по Услуге могут быть приняты Компанией только от Пользователей Клиента.
Для идентификации Клиента или уполномоченных Пользователей Клиента при обращении через интерфейсы Компании в обязательном порядке необходимо сообщить информацию, указанную при заключении Договора на оказание Услуги, а именно:

- УНП;
- лицевой счет;
- учётные данные Клиента (наименование учетной записи пользователя);
- дополнительную информацию согласно инструкции пользователя.

В случае если информация, переданная Клиентом Компании, не соответствует действительности (УНП, Лицевой счет и Учётные данные не совпадают), Компания вправе отказать в обслуживании и выполнении обращения Клиента.
В случае если Клиент не имеет возможности воспользоваться порталом самообслуживания в связи с утерей Учётных данных или в результате самостоятельного некорректного изменения учётных данных, для восстановления Учётных данных Клиенту необходимо обратиться через интерфейсы Компании для перегенерации Учётных данных со стороны Компании.

В целях повышения уровня обслуживания Клиенту рекомендуется предоставить в обращении следующую информацию:

- подробное описание ситуации, вызвавшей обращение (по возможности со скриншотами и/или графическим пояснением в форматах .jpg/.gif/.png или в других графических форматах);
- пошаговое описание действий по воспроизведению Инцидента (если применимо);
- ФИО, e-mail, телефон обратившегося лица.
- Учётные данные для доступа к порталу мониторинга (опционально по запросу Компании).

После обработки и выполнения обращения Клиенту необходимо будет изменить учетные данные, предоставленные им. Компания не несет ответственности за действия, совершенные с использованием учетных данных Клиента после обработки и выполнения обращения.

3.2. Способы управления обращениями

В рамках данного Соглашения выделяются четыре категории обращений:

Обращение на предоставление информации – запрос на предоставление технической информации об Услугах, включая отчёты, журналы доступа (в зависимости от программного обеспечения Компании и наличия технической возможности) направляется по адресу: sd@a1data.by, обращения по остальным (общим вопросам) вопросам – по адресу: sales@a1data.by

Обращение на изменение - обращение Клиента, связанное с изменением состава и/или объема предоставляемых Услуг, направляется по адресу: sd@a1data.by.

Обращение на обслуживание – запрос на проведение дополнительных работ, входящих в состав услуги, направляется Клиентом в письменной форме через интерфейсы Компании по адресу: sd@a1data.by. Запрос на проведение дополнительных работ (не входящих в состав Услуги), направляется Клиентом в письменной форме через интерфейсы Компании по адресу: sales@a1data.by.

Инцидент (Критический, Высокий, Обычный) – обращение о событии, влияющем на предоставление Услуг направляется по адресу: sd@a1data.by

Описание критичностей и влияний Инцидента на предоставляемую Услугу:	
Критический	Инцидент, приводящий к полной недоступности Услуг в связи с неисправностью оборудования, сети, инженерных систем и/или инфраструктуры Компании.
Высокий	Обращение на устранение неисправности, повлекшей за собой частичную недоступность, существенное ограничение доступного функционала или замедление доступа к Услугам, предоставляемым одному Клиенту.
Обычный	Обращение на устранение неисправности, которая не оказывает существенного влияния на использование Услуг Клиентом.

Компания вправе в одностороннем порядке изменить приоритет инцидента, преобразовать инцидент в обращение (Обращение на предоставление информации, Обращение на изменение) в случае некорректной его классификации Клиентом, с обязательным уведомлением Клиента по электронной почте.

3.3. Приоритет обработки обращений, сроки, гарантии.

Порядок обработки обращения, определяется приоритетом. Гарантированное время реагирования, обработки и выполнения обращений (в отчётном периоде), за исключением случаев глобальной недоступности Услуги:

Категория обращения	Приоритет	Время анализа и реагирования на обращение, в минутах	Максимальное время обработки и выполнения обращения, минуты
Инцидент	Критический	30	720
	Высокий	60	1440
	Обычный	120	2160
Обращение на изменение стандартное	Низкий	120 (только в рабочее время)	1440 (только в рабочее время)
Обращение на обслуживание	Низкий	480 (только в рабочее время)	N/A
Обращение на предоставление информации	Н/Д	1440	N/A

3.4. Периоды обслуживания

В таблице описаны периоды поддержки и обслуживания Услуги:

Период поддержки	24 часа в сутки, 7 календарных дней в неделю, включая праздники и выходные дни.
Период ограниченной поддержки	С 17:30 до 8:30 по местному времени (UTC+3.00)
Период функционирования	круглосуточно - 24 часа в день, 7 дней в неделю, 365/366 дней в году.
Период технического обслуживания	Профилактические работы по техническому обслуживанию, связанные с прерыванием сервиса выполняются специалистами Компании в часы наименьшей нагрузки, с обязательным оповещением по электронной почте Клиента не менее чем за 48 часов до выполнения работ. Суммарное время профилактических работ не может превышать 4 часа в месяц.
Период экстренного технического обслуживания	Работы по экстренному техническому обслуживанию, связанные с глобальными рисками для систем информационной безопасности и непрерывности бизнеса, выполняются специалистами Компании в рабочее время с обязательным оповещением по электронной почте Клиента не менее чем за 2 часа до начала работ.

3.5. Метрики, параметры качества и уровня доступности Услуги

В данном разделе приводится перечень параметров предоставления Услуги.

Компания гарантирует доступность и штатное функционирование компонентов Услуги, входящих в зону ответственности Компании: системы управления уязвимостями, окружения Услуги на уровне Вспомогательных сервисов ЦОД. За работоспособность внешнего сенсора несет ответственность Клиент.

Компания гарантирует Клиенту выполнение и соблюдение обязательств, указанных в пп.3.2, 3.3, 3.4 настоящего соглашения, которые входят в зону ответственности Компании и определяются как штатное функционирование Центра поддержки и Технической поддержки предоставляемой и поддерживаемой Услуги.

Оценка доступности Услуги и ее компонент производится на основании анализа данных, полученных из собственных систем мониторинга и других информационных систем Компании (ITSM системы, системы учёта обращений и инцидентов, системы мониторинга инфраструктуры ЦОД и т.д.)
При возникновении споров о качестве предоставляемой Услуги, приоритетными являются данные систем мониторинга Компании, а также данные журналов (логов) систем мониторинга и отчётов из информационных систем Компании.

3.6. Доступность Услуги и ответственность Компании
Основным показателем качества Услуги является Доступность Услуги за отчетный период технической поддержки.
Доступность Услуги определяется по следующей формуле:
Период доступности Услуги = (Т период — Т недоступности) /Т период* 100%
Т период — время предоставления Услуги за отчётный период технической поддержки.
Т недоступности — время недоступности Услуги за отчетный период технической поддержки.
Услуга считается недоступной с момента получения обращения Клиента об инциденте и до отправки ответа на обращение о восстановлении доступности (с учётом факта подтверждения инцидента со стороны Компании путём оповещения Клиента на этапе обработки и реагирования на инцидент). Оповещение о недоступности приходит от Клиента путём обращения в службу технической поддержки Компании через интерфейсы указанных в п.3.1 настоящего Соглашения.
При расчете времени недоступности Услуги не учитываются периоды недоступности, возникшие по вине Клиента, а также периоды Технического обслуживания (п.3.4).
Единственным официальным и достоверным источником измерения данного показателя является отчет Компании.
Компания гарантирует соблюдение Доступности Услуг в каждом отчётном периоде технической поддержки предоставления Услуги Клиенту на уровне не менее параметров, указанных в таблице ниже:

Категория	Доступность	Период	Возможная недоступность	Безотказная работа
Доступность Услуги SIEMaaS	99%	Отчётный период технической поддержки	21ч 54м 52с	90д 9ч 32м 26с

При расчёте используются следующие усреднённые значения:
30.437 дней в месяце, 91.311 день в квартале, 82.621 дня в полугодии, 365.243 дней в году.

При снижении показателя ниже согласованного значения в конце отчётного периода технической поддержки наступает ответственность Компании, описанная в таблице ниже:

Доступность Услуги (%) в отчётном периоде технической поддержки	Количество дней безвозмездного пользования Услугой Клиентом в период, следующий за отчётным (компенсация)
99%> Доступность Услуги> =98%	15 дней
98%> Доступность Услуги> =95%	25 дней
Доступность Услуги <95%	1 месяц

Для получения компенсации на основании отчёта Клиенту необходимо в течение 90 (девяноста) дней с момента окончания отчётного периода технической поддержки направить Обращение в Центр поддержки через интерфейсы Компании (п.3.1), в котором необходимо указать период недоступности Услуги и/или превышения сроков оказания технической поддержки, а также сообщить о желании получить компенсацию. В теме обращения следует указать «Компенсация по SLA».

В течение 15 (пятнадцати) рабочих дней от даты получения данного Обращения Компания обязуется предоставить Клиенту ответ, в котором будут указаны условия предоставления компенсации или мотивированный отказ от её предоставления.
Компенсация предоставляется в период, следующий за отчетным, в виде определенного количества дней (в зависимости от показателя доступности Услуги в отчётном периоде технической поддержки) безвозмездного пользования Услугой.

4. ОГРАНИЧЕНИЯ ПРЕДОСТАВЛЕНИЯ УСЛУГИ (ГРАНИЦЫ ОТВЕТСТВЕННОСТИ SLA)

4.1. Зоны ответственности

В зоне ответственности **Компании** находятся:

- вся инфраструктура, ПО промежуточного слоя, ПО приложений и данные приложений, выделенного коллектора событий (Event Collector), расположенные в центре обработки данных Компании;
- заведение в SIEM источников событий;
- ежедневное резервное копирование событий и конфигураций Клиента в период с 0:00 по 3:00.

В зоне ответственности **Клиента** находятся:

- сохранность учетных записей Клиента и корректность конфигурации в SIEM;
- программно-аппаратный комплекс Bel VPN для доступа к порталу самообслуживания Услуги;
- обеспечение подключения к сети общего пользования;
- удаленный коллектор событий (Disconnected Log Collector).

Компания не несет ответственности за:

- мониторинг доступности любых систем и программного обеспечения, размещенного у Клиента;
- качество каналов связи и соединений с Интернет, находящихся вне зоны ответственности и контроля Компании;
- деятельность Клиента, связанную с использованием SIEM.

5. ТРЕБОВАНИЕ К ПОЛЬЗОВАТЕЛЯМ УСЛУГИ СО СТОРОНЫ КЛИЕНТА

5.1. Требования к квалификации

Пользователи должны обладать базовыми навыками использования персонального компьютера и офисного программного обеспечения, четко следовать инструкциям по использованию Услуги.
В целях ускорения обработки обращений Пользователям рекомендовано выполнять озвученные специалистами технической поддержки действия и предоставлять всю информацию, необходимую для обеспечения своевременной и профессиональной технической поддержки Услуги.

5.2. Знание документации

Пользователям Услуги рекомендуется ознакомиться с документами, регламентирующими оказание Услуги.

6. ПРОЦЕДУРЫ

6.1. Процедура изменения Соглашения

Данное Соглашение является неотъемлемой частью Договора об оказании Услуг информационной безопасности.

Во всём остальном, что не предусмотрено условиями настоящего Соглашения, Стороны руководствуются условиями Договора и Порядком оказания Услуги «Доступ к системе сбора и корреляции событий (SIEMaaS)».

Компания вправе в одностороннем порядке изменять настоящее Соглашение.

6.2. Предоставление отчётности Клиенту

Отчёт о качестве предоставления услуги за период и/или другая информация из систем мониторинга Компании, предоставляется по запросу Клиента по электронной почте в течении 15 рабочих дней с момента получения запроса.

6.3. Процедура прекращения предоставления Услуги

Процедура прекращения предоставления услуги Клиенту осуществляется путём расторжения Договора на оказание услуги, по основаниям и в порядке, предусмотренном в Договоре.