Правила оказания услуги «Мониторинг и управление событиями информационной безопасности»

Редакция действует с 11.06.2025

1. Правила оказания услуги «Мониторинг и управление событиями информационной безопасности» (далее – Правила) являются неотъемлемой частью Договора об оказании услуг Центра кибербезопасности (далее – Договор).

Заказывая услугу «Мониторинг и управление событиями информационной безопасности», Клиент подтверждает свое ознакомление и согласие с настоящими Правилами и Договором и принимает их.

МТС вправе в одностороннем порядке изменять Правила, публикуя изменения на Интернет-сайте МТС. С момента публикации таких изменений новая редакция Правил становится неотъемлемой частью Договора.

2. В Правилах применяются основные термины и их определения в значениях, установленных законодательством Республики Беларусь о кибербезопасности, Договором а также следующие термины и их определения:

Актив – информация или ресурс Клиента, входящий в состав объекта информационной инфраструктуры.

Перерыв – это временная недоступность услуги «Мониторинг и управление событиями информационной безопасности» для Клиента.

Плановые регламентные работы – комплекс профилактических работ по поддержанию бесперебойной работы Инфраструктуры МТС.

Событие информационной безопасности — идентифицированное появление определенного состояния объекта информационной инфраструктуры, указывающего на возможное нарушение политик информационной безопасности или отказ защитных мер, или возникновение неизвестной ранее ситуации, которая может иметь отношение к безопасности.

Срочные работы – комплекс внеплановых работ, которые требуется проводить оперативно для устранения или предупреждения аварийных ситуаций на Инфраструктуре МТС.

EPS (events per second - количество событий в секунду) — совокупный поток данных от информационных систем и средств защиты клиента, поступающий в SIEM для последующей корреляции и выявления событий информационной безопасности.

IP-адрес — уникальный адрес, который идентифицирует устройство в Интернете или локальной сети Клиента.

SIEM (Security information and event management - управление событиями и информацией о безопасности) — система сбора и обработки событий информационной безопасности.

3. Услуга «Мониторинг и управление событиями информационной безопасности» (далее – Услуга) – услуга по обеспечению кибербезопасности, которая включает:

круглосуточный автоматизированный сбор, обработку, накопление, систематизацию данных о кибербезопасности объекта информационной инфраструктуры Клиента, направленные на обнаружение, предотвращение и минимизацию последствий кибератак;

круглосуточное выявление, предупреждение и исследование кибератак и вызванных ими киберинцидентов на объекте информационной инфраструктуры Клиента;

блокировку IP-адресов, являющихся источниками событий информационной безопасности (при наличии технической возможности у МТС и предоставлении Клиентом удаленного доступа к собственной инфраструктуре);

консультативную поддержку Клиента при выявлении киберинцидента;

сбор, обработку, анализ и обобщение информации о состоянии кибербезопасности на объекте информационной инфраструктуры Клиента;

хранение информации о событиях информационной безопасности объекта информационной инфраструктуры в течение 1 (одного) года;

разработку по объекту информационной инфраструктуры регламента обеспечения кибербезопасности и плана мероприятий по реагированию на киберинциденты.

В Услугу не входит: а) предоставление имущественных прав на систему сбора и обработки событий информационной безопасности (SIEM); б) выделение виртуальных вычислительных

ресурсов МТС Cloud для размещения системы сбора и обработки событий информационной безопасности (SIEM) и ресурсов для хранения событий информационной безопасности.

Оказание Услуги возможно только после оказания услуг «Обследование информационной инфраструктуры» и «Подключение объекта информационной инфраструктуры к Центру кибербезопасности».

4. По результатам оказания Услуги формируются ежемесячные отчеты о событиях информационной безопасности и о состоянии кибербезопасности на объекте информационной инфраструктуры Клиента;

5. Для заказа Услуги Клиенту необходимо заполнить опросный лист и подписать Заказ.

Обработка заявок на подключение Услуги производится в рабочее время (с 8:30 до 17:30 с понедельника по четверг и с 8:30 до 16:15 в пятницу, кроме праздничных и выходных дней). В случае поступления заявки в нерабочее время – в течение следующего рабочего дня.

6. Сроки оказания Услуг определяются в Заказе.

По договоренности Сторон Клиенту может быть предоставлен полный функционал услуги в рамках тестового периода. Тестовый период действует до подписания акта о начале оказания услуги «Мониторинг и управление событиями информационной безопасности», но не более 1 (одного) месяца с начала его предоставления, если иное не будет отдельно согласовано между МТС и Клиентом.

Тестовый период предоставляется Клиенту единожды, повторное тестирование Услуги невозможно.

7. МТС обеспечивает предоставление Услуги 24 часа в сутки, 7 дней в неделю, 365 (366) дней в году.

Название параметра	Значение параметра	
Обработка и анализ поступающих событий информационной безопасности	Анализ событий в реальном времени в соответствие с правилами корреляции	
Время предоставления Клиенту информации о киберинциденте с момента его фиксации в системе Центра кибербезопасности МТС	Высокий уровень	До 1 часа
	Низкий уровень	До 2 часов

Допустимые сроки Перерывов при проведении Плановых регламентных работ и Срочных работ:

Наименование работ	Продолжительность и интервалы между Перерывами	Сроки с способ уведомления Клиента
Плановые регламентные работы	Суммарная продолжительность Перерывов - не более 48 (сорока восьми) часов в год	Не менее чем за 24 (двадцать четыре) часа до начала Перерыва одним или несколькими способами, указанными в пункте 7 Правил
Срочные работы	Время Перерыва равно фактическому времени, необходимому для устранения / предотвращения аварийных ситуаций и/или неисправностей	Непосредственно перед началом Перерыва одним или несколькими способами, указанными в пункте 7 Правил

Если недоступность Услуги вызвана причинами, не предусмотренными пунктом 17 Договора, Клиент имеет право требовать перерасчет стоимости данной услуги с момента превышения МТС сроков Перерывов при проведении Плановых регламентных или Срочных работ.

Для получения компенсации Клиенту необходимо в течение 30 (тридцати) календарных дней с момента обнаружения недоступности Услуги и/или превышения сроков Перерывов, направить в МТС соответствующее требование с указанием периода недоступности услуги и/или превышения сроков Перерывов.

В течение 10 (десяти) рабочих дней с даты получения вышеуказанного требования МТС предоставляет ответ, в котором будут указаны условия предоставления Клиенту компенсации за недоступность Услуги и/или превышение сроков Перерывов или мотивированный отказ от ее предоставления.

8. Порядок оказания Услуги

8.1. Мониторинг событий ИБ:

8.1.1. МТС в режиме 24х7 осуществляет мониторинг всех событий ИБ Клиента, фиксируемых в системе Центра кибербезопасности МТС, передачу в автоматическом режиме в Национальный центр

кибербезопасности сведений, предусмотренных приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 25.07.2023 № 130; передачу Клиенту сведений от Национального центра кибербезопасности.

При возникновении киберинцидента МТС проводит первичный анализ данных с целью обработки ложных срабатываний сценария. Если МТС принято решение о ложном срабатывании, соответствующий инцидент закрывается с техническим обоснованием причин, информация о нем и причинах его закрытия предоставляется в рамках регулярной отчетности системы Центра кибербезопасности МТС.

При дальнейшей обработке киберинцидента МТС по правилам приказа Оперативно-аналитического центра при Президенте Республики Беларусь от 25.07.2023 № 130 устанавливает критичность инцидента, исходя из данных, полученных при анализе. Критичность в результате данного анализа может быть изменена в сторону как увеличения, так и уменьшения по результатам согласования.

По итогам проведенной обработки МТС информирует Клиента о факте возникновения киберинцидента. При этом работы по анализу инцидента не прекращаются, если в этом есть необходимость.

После информирования Клиента о факте инцидента, МТС продолжает установление причин и источника инцидента, если это возможно.

МТС вправе запросить у Клиента дополнительную информацию об инфраструктуре или событиях информационной безопасности в случае, если она требуется для анализа киберинцидента.

Сотрудники Клиента вправе запросить дополнительную информацию о причинах и источнике киберинцидента, если данная информация может быть получена средствами системы Центра кибербезопасности МТС, из информации об Инфраструктуре, переданной МТС, или общедоступных источников информации.

По итогам анализа предоставленной информации сотрудники Клиента подтверждают достаточность полученных им данных, и МТС завершает работы по анализу инцидента.

8.1.2. Ограничения

МТС гарантирует корректность обработки только по киберинцидентам, зафиксированным в системе Центра кибербезопасности МТС;

в случае если инцидент информационной безопасности не попадает под согласованный набор критериев выявления, работы по его анализу не входят в состав услуги;

время реакции на киберинцидент отсчитывается от момента фиксации инцидента в системе Центра кибербезопасности МТС;

время анализа киберинцидента может быть увеличено в случае, если сотрудниками Клиента запрошена обработка большого количества данных в системе Центра кибербезопасности МТС или внешних систем-источников информации.

время анализа не включает в себя работы Клиента по верификации и оценке полноты предоставленных МТС данных;

мониторинг выполняется удаленно. Выезд на площадку Клиента осуществляется за дополнительную плату.

8.2. Подключение дополнительных активов осуществляется в соответствии с Правилами оказания услуги по подключению объекта информационной инфраструктуры к Центру кибербезопасности.

8.2. Отключение актива от Центра кибербезопасности:

8.2.1. Клиент инициирует запрос на отключение актива, предоставляя следующую информацию:

тип актива;

идентификатор актива (IP-адрес, программное обеспечение).

8.2.2. МТС проводит анализ существующих сценариев обнаружения инцидентов и информирует Клиента, если отключение актива приводит к их модификации либо исключению из списка контролируемых киберинцидентов.

8.2.3. В случае необходимости МТС и Клиент проводят изменение состава киберинцидентов на SIEM-системе и активе для его отключения.

8.2.4. Ограничения

Время, необходимое Клиенту для согласования изменений в списке контролируемых сценариев обнаружения инцидентов и проведение требуемых работ на активе для его отключения, не

учитывается в метриках отключения актива.

8.3. Реализация новых правил обнаружения киберинцидентов по запросу Клиента:

8.3.1. Клиент инициирует запрос на реализацию нового правила обнаружения киберинцидентов, предоставляя следующую информацию:

общее описание и критерии возникновения киберинцидента;

типы и записи событий информационной безопасности для выявления киберинцидента.

8.3.2. МТС анализирует техническую возможность реализации правила в рамках Инфраструктуры Клиента в системе Центра кибербезопасности МТС, привлекая Клиента для более детальной проработки сценария.

8.3.3. МТС и Клиент согласовывают итоговый сценарий обнаружения киберинцидента по новому правилу, определяют его критичность и процесс взаимодействия по инциденту в соответствии с положениями приказа ОАЦ от 25.07.2023 № 130.

8.3.4. МТС выполняет работы по реализации нового правила, производя настройки системы Центра кибербезопасности МТС.

8.3.5. По завершению подключения и проверки работоспособности МТС проводит изменение системы Центра кибербезопасности МТС, описывающей профиль услуг, заказанных Клиентом.

8.3.6. Ограничения:

Если реализация правила требует подключения дополнительных активов, то для реализации данного правила требуется сначала подключить эти активы.

При подключении нового правила обнаружения Клиенту выделяется тестовый период отладки инцидента (2 недели), в течение которого происходит дополнительная кастомизация правила.

8.4. Реализация новых правил обнаружения киберинцидентов по инициативе МТС:

8.4.1. МТС информирует Клиента о расширении списка правил обнаружения инцидентов в рамках системы Центра кибербезопасности МТС указывая следующую информацию:

общее описание и критерии возникновения киберинцидента

тип активов для выявления киберинцидента;

критичность инцидента.

8.4.2. Клиент анализирует предоставленную информацию и принимает решение о включении новых правил в список контролируемых. Если адаптация сценариев под требования Клиента требует дополнительной информации, Клиент предоставляет ее МТС.

8.4.3. МТС включает контроль событий по новым правилам выявления киберинцидентов для Инфраструктуры Клиента, производя необходимые настройки системы Центра кибербезопасности МТС.

8.4.4. По завершению подключения и проверки работоспособности МТС проводит изменение системы Центра кибербезопасности МТС, описывающей профиль услуг, заказанных Клиентом.

8.4.5. Ограничения

Если реализация правила требует подключения дополнительных активов, то для реализации данного правила требуется сначала подключить эти активы.

При подключении нового правила обнаружения Клиенту выделяется тестовый период отладки инцидента (2 недели), в течение которого происходит дополнительная кастомизация правила.

9. При обеспечении кибербезопасности объекта информационной инфраструктуры Клиента, в том числе реализации мероприятий по выявлению, предупреждению кибератак и вызванных ими киберинцидентов, реагированию на такие киберинциденты, МТС вправе потребовать от Клиента:

– представления документов (их копий) и (или) иной информации, в том числе технического характера, связанных с функционированием объекта информационной инфраструктуры.

Клиент предоставляет МТС документы (их копии), иную информацию не позднее дня, следующего за днем предъявления требования;

– обеспечения беспрепятственного доступа сотрудников МТС в помещения и иные объекты (на территории), в которых размещен (функционирует) объект информационной инфраструктуры, а также к программно-техническим средствам (в том числе удаленно), с помощью которых обеспечивается их функционирование.

10. МТС до подписания акта о начале оказания услуги «Мониторинг и управление событиями информационной безопасности» разрабатывает по каждому подключаемому объекту информационной инфраструктуры Клиента регламент обеспечения кибербезопасности объекта информационной инфраструктуры и план мероприятий по реагированию на киберинциденты.

В регламенте должны быть предусмотрены, в т.ч.:

порядок представления в МТС документов (их копий) и (или) иной информации, в том числе технического характера, связанных с функционированием объекта информационной инфраструктуры Клиента;

порядок обеспечения беспрепятственного доступа сотрудников МТС в помещения и на иные объекты (на территории), в которых размещен (функционирует) объект информационной инфраструктуры, а также к программно-техническим средствам (в том числе удаленно), с помощью которых обеспечивается их функционирование;

порядок автоматизированных сбора, обработки, накопления, систематизации и хранения сведений о событиях информационной безопасности и данных о киберинцидентах, выявления и регистрации киберинцидентов.

Клиент утверждает регламент и пересылает его МТС в течение 2 (двух) рабчих дней с момента его получения. С момента утверждения регламент является неотъемлемой частью Договора.