Правила оказания услуги «Подключение объекта информационной инфраструктуры к Центру кибербезопасности»

Редакция действует со 02.06.2025

1. Правила оказания услуги «Подключение объекта информационной инфраструктуры к Центру кибербезопасности» (далее – Правила) являются неотъемлемой частью Договора об оказании услуг Центра кибербезопасности (далее – Договор).

Заказывая услугу «Подключение объекта информационной инфраструктуры к Центру кибербезопасности», 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.

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.

Средство защиты информации (СЗИ) — техническое, программное средство, вещество и(или) материал, предназначенные или используемые для защиты информации.

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 «Подключение объекта информационной инфраструктуры к Центру кибербезопасности» (далее – Услуга) заключается в подключении объекта информационной инфраструктуры (его активов) к системе сбора и обработки событий информационной безопасности (SIEM) Центра кибербезопасности МТС в соответствии с типами и записями, указанными в приложении к Положению о порядке информационного взаимодействия элементов национальной системы обеспечения кибербезопасности, утвержденными приказом ОАЦ от 25.07.2023 № 130.

Оказание Услуги возможно только при условии заказа услуги «Обследование информационной инфраструктуры» (за исключением подключения дополнительных активов ранее подключенного к Центру кибербезопасности объекта информационной инфраструктуры).

4. Ограничения при оказании Услуги

Подключение активов проводится удаленно. МТС подключает активы Клиента к системе сбора и обработки событий информационной безопасности (SIEM) в согласованные сроки при условии своевременного выполнения работ со стороны Клиента, а также при наличии у Клиента необходимых технических возможностей (оборудование для организации и организация туннеля доступа к активам (равнозначно также, «VPN», «VPN – канал», организуемый Клиентом), серверное оборудование и т.д.). Подключение с выездом на площадку Клиента осуществляется за дополнительную плату.

Клиент должен обеспечить выполнение требований по кибербезопасности объектов информационной инфраструктуры государственных органов и иных организаций, изложенных в приложении 4 к приказу ОАЦ 25.07.2023 № 130, для подключения активов к Центру кибербезопасности МТС.

Подключение актива производится только при наличии технической возможности получения событий информационной безопасности, необходимых для реализации сценариев обнаружения киберинцидентов. Наличие технической возможности определяется МТС с использованием консультаций Клиента.

Сроки подключения зависят от своевременного завершения настроек передачи необходимых данных (логов) для анализа в систему Центра кибербезопасности и выполнения иных необходимых

работ на стороне Клиента (далее – готовность Инфраструктуры Клиента). МТС начинает выполнять работы только после готовности Инфраструктуры Клиента. Сроки, в течение которых должна быть обеспечена готовность Инфраструктуры Клиента, Стороны согласовывают в Заказе.

МТС определяет и согласовывает с Клиентом необходимый уровень логирования актива в соответствии с типами и записями, указанными в приложении к Положению о порядке информационного взаимодействия элементов национальной системы обеспечения кибербезопасности, утвержденными приказом ОАЦ от 25.07.2023 № 130, для реализации требуемых сценариев. При отсутствии технической возможности использовать рекомендованный уровень логирования МТС совместно с Клиентом определяет необходимость и порядок решения киберинцидентов.

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.

7. Особенности первоначального подключения объекта информационной инфраструктуры к Центру кибербезопасности:

7.1. При первоначальном подключении МТС со своей стороны:

1) по результатам оказания услуги «Обследование информационной инфраструктуры» согласовывает с Клиентом итоговый перечень подключаемых активов;

2) совместно с Клиентом подключается по организованному и предоставленному Клиентом туннелю доступа к активам, настраивает защищенное соединение между ними, сервером сбора логов Клиента и системой Центра кибербезопасности МТС с целью передачи логов с активов Клиента, передачу логов на сервер сбора логов Клиента и с него в систему Центра кибербезопасности МТС в режиме реального времени;

3) направляет в адрес Клиента инструкции по настройке журналирования на соответствующих ИТ и ИБ-системах (для стандартных активов);

4) подключает события с активов, которые передаются на заранее подготовленные Клиентом сервера, соответствующие требованиям, установленным МТС;

5) проводит подключение активов к системе сбора и обработки событий информационной безопасности (SIEM);

6) совместно с Клиентом адаптирует правила выявления инцидентов ИБ, включающий в себя:

– корреляционные правила, позволяющие выявлять соответствующий сценарий обнаружения инцидентов;

– логику определения событий, относящихся к одному/разным инцидентам, в рамках одного сценария;

– определение степени критичности инцидентов;

7) проводит совместно с Клиентом профилирование сетевой и хостовой активности для минимизации ложных срабатываний.

7.2. При первоначальном подключении Клиент со своей стороны обязуется:

осуществить установку серверов для сбора логов с активов с техническими характеристиками, определенными МТС. Лицензии на ОС и другое прикладное ПО Клиент оплачивает самостоятельно;

организовать и предоставить уполномоченному сотруднику МТС удаленный доступ – туннель доступа на сервера с целью настройки сбора логов с активов. В случае отказа Клиента предоставить данный доступ, Клиент самостоятельно проводит работы по установке и настройке. Ответственность за корректность работы в таком случае лежит на Клиенте;

организовать сетевой доступ и передачу данных между активами и серверами сбора логов, установленными на стороне Клиента;

осуществить настройку журналирования на активах и организовать передачу событий на сервера сбора логов, установленные на стороне Клиента;

осуществить дальнейшую эксплуатацию и настройку средств СЗИ. Клиент может обратиться за консультациями по настройке к МТС;

обеспечить выполнение требований по кибербезопасности объектов информационной инфраструктуры государственных органов и иных организаций, изложенных в приложении 4 к

приказу ОАЦ 25.07.2023 № 130, для подключения объекта информационной инфраструктуры к Центру кибербезопасности МТС;

предоставить информацию об активах, необходимую для их определения в сценариях обнаружения киберинцидентов.

8. Особенности подключения дополнительных активов к Центру кибербезопасности:

8.1. Для подключения дополнительных активов к Центру кибербезопасности Клиент предоставляет следующую информацию:

тип актива;

информация по получению данных с актива (IP-адрес, данные доступа);

список сценариев обнаружения киберинцидентов, которые необходимо контролировать в рамках данного актива;

дополнительную информацию, необходимую для определения актива в сценариях обнаружения киберинцидентов.

8.2. МТС совместно с Клиентом оценивает техническую возможность сбора требуемых событий с целевого актива и согласовывает механизм и способ подключения.

8.3. МТС оценивает достаточность предоставленной информации для выполнения работ и составления документов и вносит изменения в сценарии обнаружения киберинцидентов с учетом подключения нового актива.

8.4. МТС и Клиент выполняют требуемые настройки на SIEM-системе и активе для его подключения.

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