Правила оказания услуги «Расследование киберинцидента»

Редакция действует с 11.06.2025

1. Правила оказания услуги «Расследование киберинцидента» (далее – Правила) являются неотъемлемой частью Договора об оказании услуг Центра кибербезопасности (далее – Договор).

Заказывая услугу «Расследование киберинцидента», 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.

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

3. Услуга «Расследование киберинцидента» (далее – Услуга) – услуга по обеспечению кибербезопасности, которая заключается в установлении источника и последствий одного киберинцидента, вызванного кибератакой на объект информационной инфраструктуры Клиента.

4. По результатам оказания Услуги формируется отчет с результатами расследования киберинцдиента.

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. Порядок оказания Услуги

6.1. При обработке киберинцидента МТС проводит сбор информации по инциденту у Клиента, который предоставляет следующие данные:

местонахождение Клиента, филиала Клиента, в котором зафиксирован инцидент.

время возникновения киберинцидента.

информационная система, IP-адреса, MAC-адреса, FQDN-имена хостов, относящихся к киберинциденту.

контактные данные сотрудника Клиента (ФИО, тел., адрес эл.почты), ответственного за эксплуатацию систем, которые относятся к инциденту.

6.2. После сбора первичной информации по инциденту МТС приступает к сбору расширенной информации по киберинциденту, которая включает в себя:

сбор дополнительных данных о фигурантах инцидента (события с фигурантами в других информационных, инфраструктурных системах-источниках, системах защиты информации за предшествующий период от 1 месяца; имеющиеся доступы/роли/привилегии; наличие ранее зафиксированных инцидентов ИБ).

сбор дополнительных данных об активах - участниках инцидента (зафиксированные события и инциденты ИБ, результаты автоматизированных сканирований, проверок и аудитов).

сбор другой дополнительной информации.

Данная работа ведется совместно с Клиентом. Качество расследования зависит от данных, предоставляемых Клиентом.

6.3. По результатам собранной информации проводится расследование киберинцидента.

В процессе расследования инцидента МТС, устанавливает:

хронологию событий, повлекших за собой возникновение киберинцидента.

причины, из-за которых возник киберинцидент.

последствия киберинцидента.

6.4. МТС помимо анализа киберинцидента и установления актива - участника инцидента и причин инцидента, формирует набор технических рекомендаций, позволяющих предотвратить или снизить вероятность возникновения аналогичных инцидентов в дальнейшем.

Клиент анализирует предоставленную ему информацию, принимает решение о применимости выданных рекомендаций в своей Инфраструктуре и проводит предложенные технические мероприятия.

Предложенный механизм предотвращения анализируется МТС и Клиентом на возможность повторного применения при возникновении киберинцидента и фиксируется в системе Центра кибербезопасности МТС, описывающей профиль системы.

6.5. Ограничения при проведении расследования:

Расследование киберинцидента проводится удаленно. Расследование инцидентов на площадке Клиента осуществляется за дополнительную плату.

Время выработки рекомендаций может быть увеличено по согласованию сторон в случае, если выданные МТС рекомендации оказались неприменимыми на Инфраструктуре Клиента в силу особенностей архитектуры, ресурсных либо бюджетных ограничений.

Выдаваемые МТС рекомендации основываются на общих архитектурных и инфраструктурных положениях обеспечения информационной безопасности и не включают в себя детализированных настроек специфического оборудования либо приложений Клиента. Анализ применимости рекомендаций и разработка инструкций для специфических приложений является ответственностью Клиента.