Правила оказания услуги «Оценка степени защищенности объекта информационной инфраструктуры (тестирование на проникновение)»

Редакция действует со 02.06.2025

1. Правила оказания услуги «Оценка степени защищенности объекта информационной инфраструктуры (тестирование на проникновение)» (далее – Правила) являются неотъемлемой частью Договора об оказании услуг Центра кибербезопасности (далее – Договор).

Заказывая услугу «Оценка степени защищенности объекта информационной инфраструктуры (тестирование на проникновение)», 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:

Уязвимость — недостаток в программном обеспечении или средстве защиты информации, используя который, возможно нарушить работоспособность данного программного обеспечения или средства защиты информации, либо выполнить какие-либо несанкционированные действия в обход установленных разрешений в программном обеспечении и(или) в средстве защиты информации.

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

3. Услуга «Оценка степени защищенности объекта информационной инфраструктуры (тестирование на проникновение)» (далее – Услуга) – услуга по обеспечению кибербезопасности, которая включает:

оценку эффективности защищенности активов Клиента на предмет наличия уязвимостей;

ручную и (или) автоматизированную проверку возможностей эксплуатации уязвимостей;

моделирование кибератак на объекте информационной инфраструктуры Клиента.

4. По результатам оказания Услуги формируется отчет с описанием уязвимостей и рекомендациями по их устранению.

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

Для оценки степени защищенности объекта информационной инфраструктуры Клиент предоставляет следующую информацию:

количество активов, в отношении которых необходимо провести проверку;

тип активов;

идентификаторы активов (IP-адреса, программное обеспечение).

Процесс оценки степени защищенности объекта информационной инфраструктуры Клиента заключается в следующем:

удаленное определение сетевых сервисов;

подбор паролей к различным сервисам на основе словарей;

тестирование на известные уязвимости ПО.

Услуга оказывается при помощи специализированного ПО, которое в автоматическом и/или ручном режиме выполняет сканирование по заранее предоставленному Клиентом внешнему диапазону IP-адресов.

В процессе анализа результатов сканирования составляется отчет, в котором перечисляются уязвимости, требующие устранения, эксплуатация которых позволяет получать неавторизованный доступ к активам или производить кибератаки против их пользователей, производить отказ в обслуживании. В отчет включаются рекомендации по устранению уязвимостей.

7. Ограничения

Для оказания Услуги требуется наличие у Клиента необходимых технических возможностей для удаленного подключения МТС (наличие VPN – канала, организуемого Клиентом, соответствующего требованиям, установленным МТС).

Время проведения сканирования заранее обговариваются с Клиентом в срок не менее 3 (трех) дней до его начала и проходят строго в согласованные временные диапазоны.

Подтверждение наличия уязвимостей устанавливается совместно с Клиентом.

МТС вправе осуществлять эксплуатацию выявленных уязвимостей, когда это необходимо для окончательного подтверждения их наличия, исключительно с согласия Клиента.