БЮЛЛЕТЕНЬ ПО БЕЗОПАСНОСТИ – 28 НОЯБРЯ 2019 ГОДА

ПРАВИЛА ВЗАИМОДЕЙСТВИЯ «МАСТЕРКАРД» ООО С УЧАСТНИКАМИ ПС «МАСТЕРКАРД» И С ОПЕРАЦИОННЫМ ЦЕНТРОМ И ПЛАТЕЖНЫМ КЛИРИНГОВЫМ ЦЕНТРОМ ПРИ ВОЗНИКНОВЕНИИ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Оглавление

1. Задачи документа

Настоящий документ устанавливает Правила взаимодействия «Мастеркард» ООО с Участниками платежной системы «Мастеркард» и с Операционным центром и Платежным клиринговым центром при возникновении инцидентов информационной безопасности (далее – «Правила взаимодействия»).

2. Доступность документа

В целях достижения непротиворечивости процедур реагирования на инциденты информационной безопасности (далее – «Инциденты ИБ») всех участников информационного обмена, и, как следствие, обеспечения высокого уровня эффективности взаимодействия, Правила взаимодействия должны быть предоставлены всем Контрагентам-участникам информационного взаимодействия, а именно Участникам платежной системы «Мастеркард» и Операционному центру и Платежному клиринговому центру (совместно – «Контрагентам»). В случае внесения изменений в приведенные в данном документе Правила взаимодействия все указанные изменения должны быть доведены до Контрагентов, незамедлительно после утверждения данных изменений.

3. Термины, определения и сокращения

Инцидент ИБ – единичное событие или ряд нежелательных и непредвиденных событий информационной безопасности, в результате наступления которых нанесен ущерб компании и/или её контрагентам по информационному взаимодействию в виде финансовых потерь и/или реализации операционных и репутационных рисков, а также осуществлены атаки на информационные ресурсы, в результате чего произошли или могли произойти: утечка из информационных систем (далее – «ИС») конфиденциальной информации, нарушение работоспособности ИС, внесение несанкционированных изменений в состав данных или структуру ИС, системная утечка или разглашение данных клиентов из ИС и т.п., в результате которых велика вероятность массовой компрометации информации и/или деградация уровня информационной безопасности компании.

Событие информационной безопасности (далее – «Событие ИБ») – идентифицированный случай состояния системы, сервиса или сети, указывающий на возможное нарушение политики информационной безопасности или отказ средств защиты, либо ранее неизвестная ситуация, которая может быть существенной для безопасности.

4. Нормативные ссылки

Данная политика разработана в соответствии с документами «Базовая политика Информационной Безопасности «Мастеркард» ООО», «Правила платёжной системы «Мастеркард» в России» и с учетом внутренних документов «Мастеркард» ООО», регламентирующих вопросы информационной безопасности.

5. Область применения

Документ является руководством для Контрагентов в рамках функционирования бизнес-процессов платежной системы «Мастеркард».

6. Основные положения

В основе Правил взаимодействия лежат принципы, определенные в стандарте ГОСТ Р ИСО/МЭК ТО 18044:2007 (ISO/IEC TR 18044:2004 Information security incident management).

7. Управление Инцидентами ИБ

Управление Инцидентами ИБ включает в себя:

- Обнаружение и регистрация Инцидентов ИБ;
- Разрешение Инцидентов ИБ;
- Анализ или расследование Инцидентов ИБ.

7.1 Обнаружение и регистрация Событий ИБ

Обнаружение Инцидентов ИБ должно осуществляться Контрагентами в режиме 24x7.

Источником информации об Инциденте ИБ должно служить следующее:

- сообщения работников, клиентов, других Контрагентов, направленные ответственному сотруднику Контрагента в виде сообщений по электронной почте, служебных записок, писем, заявлений и т.д.;
- уведомления/сообщения ЦБ, иных органов, осуществляющих контроль или надзор за деятельностью Контрагента;
- данные, полученные на основании анализа журналов регистрации информационных систем, систем защиты.

В качестве Событий ИБ и/или подозрительной активности также могут рассматриваться, в том числе и следующие события:

- трудности и проблемы при работе с ресурсами ИС (нештатном функционировании программных и аппаратных средств ИС, нарушения целостности информации и т.п.);
- неполадки средств и систем обеспечения жизнедеятельности помещений;
- подозрительные, неадекватные (не совместимые с должностными обязанностями) действия сотрудников.

Сообщение об обнаруженном событии и/или подозрительной активности должно содержать как минимум:

- описание обнаруженного события и/или подозрительной активности;

- список активов предположительно вовлеченных в обнаруженное событие;
- оценку вероятности распространения обнаруженного события.

После фиксации события возможно проведение дополнительного сбора информации.

На основе собранной о событии информации, статистики Инцидентов ИБ, а также своего экспертного мнения ответственные лица Контрагента определяют, является ли выявленное событие Инцидентом ИБ, производят регистрацию Инцидента ИБ в соответствии с внутренними регламентами Контрагента и принимают решение о необходимости дальнейших действий по данному событию, о чем должны быть сделаны соответствующие отметки в журнале или системе регистрации Инцидентов ИБ.

В ходе проведения анализа Инцидента ИБ должна быть проведена классификация Инцидента ИБ.

В целях исключения неоднозначности классификации Инцидентов ИБ при обмене информации об Инцидентах ИБ рекомендуется использовать унифицированную Классификацию Инцидентов ИБ в соответствии с Таблицами 1 и 2:

Типы инцидентов Таблица 1

Типы Событий и Инцидентов ИБ	Описание
Административные	События и инциденты, связанные с административными нарушениями (в том числе нарушениями трудового распорядка и других корпоративных правил, а также с нарушениями сотрудниками правил ИБ)
Программно-технические	События и инциденты, связанные с работой программных и аппаратных средств, участвующих в бизнес-процессах компании, а также связанные с работой средств защиты информации. Программно-технические инциденты в качестве подтипов включают: • Несанкционированные подключения и несанкционированный доступ к ресурсам; • Атаки из внешних сетей; • Вирусные атаки; • Неавторизованное использование ресурсов.
Связанные с конфиденциальной информацией	События и инциденты, связанные с несанкционированным доступом или подозрением на доступ к конфиденциальной информации и, как следствие, с компрометацией таких данных (или АС, содержащей данные)

После определения типа Инцидента ИБ определяется критичность Инцидента ИБ по шкале, приведенной в Таблице 2, исходя из следующих сведений:

- информации об Инциденте ИБ;
- критичности активов, вовлеченных в Инцидент ИБ;
- прогнозируемой степени влияния Инцидента ИБ на ключевые свойства активов.

Критичность инцидентов Таблица 2.

Значение	Качественное значение	Целевое время разрешения	Описание
5	**Критичный**	**4 часа**	Инцидент ИБ, указывающий на событие, связанное с тем, что система была успешно атакована, затронуты критичные ресурсы, используемые платежной системой «Мастеркард». Это может привести к системной компрометации или раскрытию очень важной информации, нарушению работы критически серверов, приводящих к недоступности сервисов и полному непредставлению услуг. В этом случае планируются и реализуются корректирующие действия.
4	**Высокий**	**16 часов**	Инцидент ИБ указывает на событие, последствия которого могут привести компрометации данных системы. Указанный Инцидент ИБ должен быть исследован, по нему оперативно принимаются меры, с целью уменьшения риска, и снижения вероятности проведения успешной атаки. В этом случае планируются и реализуются корректирующие действия.
3	**Умеренный**	**48 часов**	Инцидент ИБ потенциально может привести к системной компрометации. Возможно, применение компенсирующих мер.
2	**Низкий**	**72 часа**	Инцидент ИБ, связан с низким риском. Проявлением может быть негласное получение данных о конфигурации систем, которые могут быть использованы впоследствии, и потенциально привести к компрометации данных системы. Компенсирующие меры, как правило, не требуются. Риск в этом случае может быть принят.
1	**Очень низкий**	**96 часов**	Инцидент ИБ, связанный с событием, представляющим интерес к системе, но не представляющим угрозу безопасности системы. К ним относятся, как правило, события информационного характера. К данной категории относятся так же инциденты административного типа, связанные с нарушениями трудового распорядка и других корпоративных правил, не связанных с ИС. Компенсирующих мер, не требуется. Риск принимается.

Дальнейшая обработка Инцидента ИБ производится в соответствии с внутренними правилами (регламентами) управления инцидентами Контрагента.

7.2 Оповещение об Инцидентах ИБ

После выявления Инцидента ИБ и его классификации, для уровней критичности инцидента «Критичный» и «Высокий» должно быть инициировано немедленное оповещение «Мастеркард» ООО по адресу

электронной почты Russia_IR@mastercard.com. Также сведения по Инцидентам ИБ с указанными уровнями критичности обязательно должны быть включены в оповещения, передаваемые Контрагентами на систематической основе в адрес «Мастеркард» ООО (см. п.7.3).

Для уровней критичности инцидента «Умеренный», «Низкий» и «Очень низкий» немедленное оповещение «Мастеркард» ООО не производится. Сведения по Инцидентам ИБ с указанными уровнями критичности обязательно должны быть включены в оповещения, передаваемые Контрагентами на систематической основе в адрес «Мастеркард» ООО (см. п.7.3).

7.3 Систематическое оповещение Контрагентами Оператора платежной системы «Мастеркард» о событиях и состоянии ИБ

Все Контрагенты обязаны уведомлять «Мастеркард» ООО на ежемесячной основе до 20-ого числа месяца, следующего за отчетным, о выявленных инцидентах, угрозах и уязвимостях в обеспечении защиты информации, связанных с нарушениями требований к обеспечению защиты информации в платежной системе при осуществлении переводов денежных средств, включая (но не ограничиваясь):

- о случаях компрометации шифровальных ключей,
- о случаях компрометации ключей к цифровой подписи,
- обнаружении вредоносного кода

по адресу электронной почты Russia_IR@mastercard.com. Формат данного уведомления определяется Контрагентами самостоятельно. При отсутствии вышеперечисленных инцидентов, угроз и уязвимостей в течении месяца по данному адресу оператора платежной системы Контрагентам следует отправлять уведомление в приведенный выше срок с подтверждением отсутствия указанный событий. В случае непредоставления указанной информации «Мастеркард» ООО оставляет за собой право применить к соответствующим Контрагентам штрафы в соответствии с разделом 3 Правил платежной системы «Мастеркард» в России.

7.4 Разрешение Инцидентов ИБ

Действия по разрешению Инцидентов ИБ производятся Контрагентами в зависимости от присвоенного значения критичности согласно внутренним правилам (регламентам) Контрагента по управлению Инцидентами ИБ.

При наступлении события, влияющего на уровень безопасности в информационных системах Контрагента и способных отразиться на уровне безопасности информационной инфраструктуры платежной системы «Мастеркард», уполномоченные сотрудники Контрагента должны организовать проведение внутреннего расследования.

Для Инцидентов ИБ, связанных с компрометацией конфиденциальной информации в информационных системах Контрагента, в обязательном порядке должно быть запланировано выполнение следующих действий:

- ограничить объем скомпрометированных данных;
- сохранить все доступные протоколы работ;
- создать резервную копию скомпрометированной системы для облегчения проведения дальнейшего расследования;
- протоколировать все выполняемые действия;
- осуществлять мониторинг всех систем обработки и передачи данных;
- оповестить правоохранительные органы (при необходимости);

Результаты расследования Инцидентов ИБ, о которых должно быть уведомлено «Мастеркард» ООО согласно абзацу 1 п.7.2, в обязательном порядке должны быть доведены до «Мастеркард» ООО путем включения указанной информации в состав очередного уведомления Контрагентом оператора платежной системы «Мастеркард» о событиях и состоянии безопасности Контрагента, предоставляемого на систематической основе (см. п.7.3).