«УТВЕРЖДЕНО»
Приказом Директора ТОО «PrimePay»
№ 26 от 17.09.2024 г.

_____ Доборяков К.Е.

ПОРЯДОК СОБЛЮДЕНІЯ МЕР ІНФОРМАЦІОННОЙ БЕЗОПАСНОСТІІ І ЗАЩІТЫ ІНФОРМАЦІІІ ОТ НЕСАНКЦІОНІРОВАННОГО ДОСТУПА В СІСТЕМЕ ЭЛЕКТРОННЫХ ДЕНЕГ

Алматы 2024 г.

1. **Платежная организация** обеспечивает создание и функционирование системы управления информационной безопасностью, являющейся частью общей системы управления платежной организации, предназначенной для управления процессом обеспечения информационной безопасности.

2. Основы обеспечения информационной безопасности

Система управления информационной безопасностью (СУИБ) - часть системы управления Платежной организации, основанная на подходе бизнес-рисков по созданию, внедрению, функционированию, мониторингу, поддержке и улучшению информационной безопасности.

Информационная безопасность - сохранение конфиденциальности, целостности и доступности информации.

Конфиденциальность - свойство информации, предполагающее обеспечение секретности и не доступности информации для не авторизованных на ее получение субъектов, включая процессы Платежной организации.

Доступность - свойство информации, быть доступной и готовой к использованию для авторизованных на это субъектов.

Целостность - свойство сохранения достоверности, неизменности и полноты информации.

Основной целью СУИБ минимизация ущерба в следствии нарушения целостности, конфиденциальности и доступности информации.

3. Система управления информационной безопасностью обеспечивает защиту информационных активов платежной организации, допускающую минимальный уровень потенциального ущерба для бизнес-процессов платежной организации. Платежная организация обеспечивает надлежащий уровень системы управления информационной безопасностью, ее развитие и улучшение.

В рамках деятельности по построению системы управлению информационной безопасности, Платежной организацией обеспечивается функционирование следующих процессов:

- Определения целей и задач системы управления информационной безопасностью;
- Определение направлений развития системы управления информационной безопасностью;
- Оценка рисков и угроз информационной безопасности Платежной организации;
- Разработки и применения компенсирующих мер по результатам оценки рисков и угроз информационной безопасности.

В рамках реализации системы управлению информационной безопасностью, Платежная организация проводит следующие мероприятия, но не ограничиваясь ими:

- выявление и реагирование на атаки в реальном времени;
- разрешение и анализ причин возникновения инцидентов информационной безопасности;
- управление доступом к активам;
- антивирусная защита;
- резервирование информационных систем и данных платежной организации;
- управление непрерывностью деятельности;
- регистрация, анализ и контроль событий информационной безопасности;
- выявление уязвимостей в информационных системах платежной организации, с использованием которых могут быть реализованы угрозы информационной безопасности;
- использование средств криптографической защиты информации;
- обеспечение физической безопасности активов;
- защита сетевого периметра;
- соблюдение условий всех программных лицензий, авторских прав и законов, касающихся интеллектуальной собственности.

В целях совершенствования системы управления информационной безопасностью периодически осуществляется анализ результатов функционирования системы.

4. Платежная организация в целях обеспечения конфиденциальности, целостности и доступности информации платежной организации осуществляет следующие функции:

- организует систему управления информационной безопасностью, осуществляет координацию и контроль деятельности по обеспечению информационной безопасности и мероприятий по выявлению и анализу угроз, противодействию атакам и расследованию инцидентов информационной безопасности;
- обеспечивает методологическую поддержку процесса обеспечения информационной безопасности;

- осуществляет выбор, внедрение и применение методов, средств и механизмов управления, обеспечения и контроля информационной безопасности в рамках своих полномочий;
- осуществляет сбор, консолидацию, хранение и обработку информации об инцидентах информационной безопасности;
- осуществляет анализ информации об инцидентах информационной безопасности;
- обеспечивает внедрение, надлежащее функционирование программно-технических средств, автоматизирующих процесс обеспечения информационной безопасности, а также предоставление доступа к ним;
- определяет ограничения по использованию привилегированных учетных записей;
- организует и проводит мероприятия по обеспечению осведомленности работников платежной организации в вопросах информационной безопасности;
- осуществляет мониторинг состояния системы управления информационной безопасностью платежной организации;
- периодически (но не реже одного раза в год) осуществляет информирование руководства платежной организации о состоянии системы управления информационной безопасностью платежной организации.

5. Программное обеспечение обеспечивает:

- надежное хранение информации, защиту от несанкционированного доступа, целостность баз данных и полную сохранность информации в электронных архивах и базах данных при полном или частичном отключении электропитания в любое время на любом участке оборудования;
- многоуровневый доступ к входным данным, функциям, операциям, отчетам, реализованным в программном обеспечении, предусматривающим как минимум, два уровня доступа: администратор и пользователь;
- контроль полноты вводимых данных полей обязательных к заполнению, необходимых для проведения и регистрации операций (при выполнении функций или операций без полного заполнения всех полей программа обеспечивает выдачу соответствующего уведомления);
- поиск информации по критериям и параметрам, определенным для данной информационной системы, с сохранением запроса, а также сортировку информации по любым параметрам (определенным для данной информационной системы) и возможность просмотра информации за предыдущие даты, если такая информация подлежит хранению в информационной системе;
- обработку информации и ее хранение по дате и времени;
- автоматизированное формирование форм отчетов, представляемых платежными организациями в Национальный Банк, а также отчетов о проведенных операциях;
- ведение и автоматизированное формирование журналов системы внутреннего учета. Программное обеспечение формирует журнал полностью, а также частично (на указанный диапазон дат, определенную дату);
- возможность резервирования и восстановления данных, хранящихся в учетных системах;
- возможность вывода выходных документов на экран, принтер или в файл;
- возможность обмена электронными документами;
- регистрацию и идентификацию происходящих в информационной системе событий с сохранением следующих атрибутов: дата и время начала события, наименование события, пользователь, производивший действие, идентификатор записи, дата и время окончания события, результат выполнения события.

6. Процедуры безопасности

6.1. В целях обеспечения безопасности предоставления Услуг, проведения Операций возможны только на карты, эмитированные банками на территории Республики Казахстан.

6.2. Предоставление Услуг производится в соответствии с процедурами безопасности, установленными настоящими Правилами и Договором.

6.3. ТОО «PrimePay» при оказании Услуг осуществляет сбор и обработку персональных данных с согласия субъекта персональных данных, за исключением случаев, предусмотренных Законом Республики Казахстан "О персональных данных и их защите".

6.4. Процедуры безопасности обеспечивают:

- Достоверную идентификацию клиента и его право на получение соответствующих Услуг;
- Выявление наличия искажений и (или) изменений в содержании электронных документов, на основании которых клиенту предоставляются услуги;
- Защиту от несанкционированного доступа к информации, составляющей банковскую тайну, и целостность данной информации.

6.5. Платеж является санкционированным, если он произведен лицом, которое имело полномочие совершить данный платеж, и не противоречит законодательству Республики Казахстан, а также при условии, если

указание принято банком отправителя денег с соблюдением установленного порядка защиты действий от несанкционированных платежей.

6.6. Предоставление Услуг является санкционированным в случае выполнения клиентом процедур безопасности, установленных настоящими Правилами и Договором.

6.7. Несанкционированным является платеж, осуществленный без соблюдения требований, установленных законодательством, а также с использованием поддельных платежных инструментов.

6.8. В качестве элементов защиты действий используются идентификационные коды, шифрование и иные способы защиты, не противоречащие законодательству Республики Казахстан.

6.9. ТОО «PrimePay» осуществляет мониторинг за соблюдением клиентами требований к защите информации, определенных Договором и настоящими Правилами.

7. Платежная организация управляет рисками информационной безопасности с указанием критериев приемлемого уровня по отношению к информационным активам. При реализации рисков информационной безопасности разрабатывается план мероприятий, направленный на минимизацию возникновения подобных рисков.

8. Информация об инцидентах информационной безопасности, полученная в ходе мониторинга деятельности по обеспечению информационной безопасности, подлежит консолидации, систематизации и хранению.

Срок хранения информации об инцидентах информационной безопасности составляет **не менее 5 (пяти) лет.**

Платежной организацией определяется порядок принятия неотложных мер к устранению инцидента информационной безопасности, его причин и последствий. В платежной организации ведется журнал учета инцидентов информационной безопасности с отражением всей информации об инциденте информационной безопасности, принятых мерах и предлагаемых корректирующих мерах.

9. Платежная организация предоставляет в Национальный Банк информацию о следующих выявленных инцидентах информационной безопасности:

- эксплуатация уязвимостей в прикладном и системном программном обеспечении;
- несанкционированный доступ в информационную систему;
- атака «отказ в обслуживании» на информационную систему или сеть передачи данных;
- заражение сервера вредоносной программой или кодом;
- совершение несанкционированного перевода денежных средств вследствие нарушения контролей информационной безопасности;
- инцидентах информационной безопасности, несущих угрозу стабильности деятельности платежной организации.

10. Информация об инцидентах информационной безопасности, указанных в пункте 9. настоящего документа, предоставляется платежной организацией в возможно короткий срок, **но не позднее 48 часов** с момента выявления, в виде карты инцидента информационной безопасности по форме.

Информация по обработанным инцидентам информационной безопасности представляется в электронном формате с использованием платформы Национального Банка для обмена событиями и инцидентами информационной безопасности.

На каждый инцидент информационной безопасности заполняется отдельная карта инцидента информационной безопасности.

11. Обязательства по обеспечению общей безопасности платежных услуг, защиты передаваемых данных и информации несет ТОО «PrimePay».

12. ТОО «PrimePay» обязуется соблюдать конфиденциальность в отношении всех переданных ему Мерчантами данных, а также данных, ставших ему известными в ходе использования ТОО «PrimePay» Покупателями/Клиентами, за исключением случаев предусмотренных Правилами и/или законодательством Республики Казахстан, а также случаев, когда такая информация является общеизвестной или раскрыта по требованию или с разрешения Мерчанта/Покупателя.

13. Мерчант обязуется незамедлительно уведомлять ТОО «PrimePay» о любых операциях, произведенных без его согласия. В случае непредоставления соответствующего уведомления в течении календарных суток с момента осуществления операции и направления ТОО «PrimePay» соответствующего уведомления, операция считается осуществленной Мерчантом.

14. Стороны признают сочетание аутентификационных данных (уникального идентификатора пользователя и пароля) аналогом собственноручной подписи, являющимся необходимым и достаточным условием подтверждения права Мерчанта на проведение Транзакций.