ООО «RAQAMLI BIZNES AGREGATOR»

«УТВЕРЖДАЮ»

10 января 2023 год

Директор Толаганов А.А.

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПЛАТЕЖНОЙ ОРГАНИЗАЦИИ

ООО «RAQAMLI BIZNES AGREGATOR»

Ташкент 2023

Оглавление

Глава 1. Введение

1.1. Настоящая Политика информационной безопасности ООО «RAQAMLI BIZNES AGREGATOR» (далее - Политика) определяет цели и принципы обеспечения информационной безопасности, излагает основные направления и требования по защите информации, является основой для обеспечения режима информационной безопасности, служит руководством при разработке соответствующих внутренних документов ООО «RAQAMLI BIZNES AGREGATOR» (далее - Платежной организации).

1.2 Нормативно-правовую основу Политики составляют положения законодательства Республики Узбекистан по вопросам использования информационных систем и информационной безопасности, а также требования международных стандартов управления информационной безопасностью.

1.3. Положения Политики обязательны для исполнения всеми работниками платежной организации, а также должны доводиться до сведения клиентов и иных третьих лиц, имеющих доступ к информационным системам и документам платежной организации, в той их части, которая непосредственно взаимосвязана с платежном организации и их деятельностью.

1.4. Политика охватывает все информационные системы и документы, владельцем и пользователем которых является платежной организации. Платежной организации обеспечивает создание и функционирование системы управления информационной безопасностью, предназначенной для управления процессом обеспечения информационной безопасности. Обеспечение информационной безопасности - одно из условий для успешного осуществления коммерческой деятельности Платежной организации.

1.5. Информационная безопасность (далее - ИБ) Платежной организации - состояние защищенности электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры от внешних и внутренних угроз, которые могут привести к материальному ущербу, нанести ущерб репутации Платежной организации или повлечь нанесение иного ущерба Платежной организацию, его учредителям, работникам или клиентам.

1.6. Являясь элементом общей политики руководства Платежной организации, ИБ основывается на требованиях бизнеса, разрабатывается и реализуется в соответствии с общими правилами управления рисками в Платежной организации. Нарушения в данной области могут привести к серьезным последствиям, включая потерю доверия со стороны клиентов и снижению конкурентоспособности.

1.7. Обеспечение ИБ включает в себя применение всех доступных средств и инструментов в рамках компетенций работников Платежной организации, направленных на защиту информации и поддерживающей ее инфраструктуры.

1.8. Неотъемлемой частью организации ИБ является непрерывный контроль эффективности предпринимаемых мер, определение для работников перечня недопустимых действий (бездействия), возможных последствий и ответственности.

Глава 2. Нормативные ссылки

2.1. Политика и система ИБ в целом основываются на следующих нормативно-правовых актах и международных стандартах (в данном разделе указаны основные нормативные акты, непосредственно влияющие на процесс создания системы ИБ Платежной организации в целом, в то же время существует ряд документов, который либо описывает стратегические аспекты развития ИБ на государственном уровне, либо регламентирует правила по информационной защите отдельных направлений деятельности):

- Закон Республики Узбекистан от 11 декабря 2003 г., № 560-II «Об информатизации»;
- Закон Республики Узбекистан от 11 декабря 2003 года № 562-II «Об электронной цифровой подписи»;
- Закон Республики Узбекистан от 29 апреля 2004 года № 611-II «Об электронном документообороте»;
- Закон Республики Узбекистан от 30 августа 2003 г. № 530-II «О банковской тайне»;
- Закон Республики Узбекистан от 04 апреля 2006 года № ЗРУ-30 «О защите информации в автоматизированной банковской системе»;
- Закон Республики Узбекистан от 11 сентября 2014 года №374 «О коммерческой тайне»;
- Закон Республики Узбекистан от 02 июля 2019 года № №ЗРУ-547 «О персональных данных»;
- Постановление Президента Республики Узбекистан от 3 апреля 2007 года № ПП-614 «О мерах по организации криптографической защиты информации в Республике Узбекистан»;
- Постановление Президента Республики Узбекистан от 8 июля 2011 года № ПП-1572 «О дополнительных мерах по защите национальных информационных ресурсов»;
- Постановление Кабинета Министров Республики Узбекистан от 22 ноября 2005 года № 256 «О совершенствовании нормативно-правовой базы в сфере информатизации»;

- Постановление Кабинета Министров Республики Узбекистан от 4 мая 2011 года № 126 «О мерах по внедрению и использованию единой защищенной электронной почты и системы электронного документооборота в исполнительном аппарате Кабинета Министров, органах государственного и хозяйственного управления, государственной власти на местах»;
- Постановление Кабинета Министров Республики Узбекистан от 14 июня 2013 года №170 «О дополнительных мерах по реализации Постановления Президента Республики Узбекистан от 8 июля 2011 года № ПП-1572 «О дополнительных мерах по защите национальных информационных ресурсов»;
- Постановление Кабинета Министров Республики Узбекистан от 16 октября 2015 года №295 «Об утверждении Положения о порядке организации и обеспечения безопасности конфиденциальной информации на объектах информатизации Республики Узбекистан»;
- Постановление Правления Центрального Банка Республики Узбекистан от 25 января 2020 года № 2/4 Об утверждении Положения о защите информации в автоматизированных банковских системах коммерческих банков Республики Узбекистан;
- O'z DSt ISO/IEC 13335-1:2009 Информационная технология. Методы обеспечения безопасности. Управление безопасностью информационно-коммуникационных технологий. (Часть1). Концепции и модели управления безопасностью информационно - коммуникационных технологий;
- O'z DSt ISO/IEC 15408-1:2016 Информационная технология. Методы обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель;
- O'z DSt ISO/IEC 15408-2:2016 Информационная технология. Методы обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности;
- O'z DSt ISO/IEC 15408-3:2016 Информационная технология. Методы обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности;
- O'z DSt ISO/IEC 27000:2014 «Информационная технология. Методы обеспечения безопасности. Системы управления информационной безопасностью. Обзор и словарь»;
- O'z DSt ISO/IEC 27001:2016 «Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования»;

- O'z DSt ISO/IEC 27002:2016 «Информационная технология. Методы обеспечения безопасности. Практические правила управления информационной безопасности»;
- O'z DSt ISO/IEC 27003:2014 «Информационная технология. Методы обеспечения безопасности. Руководство по внедрению системы управления информационной безопасностью»;
- O'z DSt ISO/IEC 27005:2013 «Информационная технология. Методы обеспечения безопасности. Управление рисками информационной безопасности»;
- O'z DSt 3388:2019 Информационная технология. Методы обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем управления информационной безопасности;
- O'z DSt ISO/IEC 27007:2015 Информационная технология.
- Методы обеспечения безопасности. Руководящие указания по аудиту систем управления информационной безопасностью;
- O'z DSt ISO/IEC 27010:2015 Информационная технология. Методы обеспечения безопасности. Руководство по управлению информационной безопасностью при коммуникациях между отраслями и организациями;
- O'z DSt ISO/IEC 27011:2014 «Информационная технология. Методы обеспечения безопасности. Руководящие указания по управлению информационной безопасностью в организациях телекоммуникаций»;
- O'z DSt 3386:2019 Информационная технология. Методы обеспечения безопасности. Управление инцидентами информационной безопасности. Часть 1. Принципы менеджмента инцидентов;
- O'z DSt 3387:2019 Информационная технология. Методы обеспечения безопасности. Управление инцидентами информационной безопасности. Часть 2. Руководящие указания по планированию и подготовке к реагированию на инциденты;
- O'z DSt 2814:2014 «Информационная технология. Автоматизированные системы. Классификация по уровню защищенности от несанкционированного доступа к информации»;
- O'z DSt 2815:2014 «Информационная технология. Межсетевые экраны. Классификация по уровню защищенности от несанкционированного доступа к информации»;
- O'z DSt 2816:2014 «Информационная технология. Классификация программного обеспечения средств защиты информации по уровню контроля отсутствия не декларированных возможностей»;
- O'z DSt 2817:2014 «Информационная технология. Средства вычислительной техники. Классификация по уровню защищенности от несанкционированного доступа к информации»;

- O'z DSt 2927:2015 «Информационная технология. Информационная безопасность. Термины и определения»;
- O'z DSt 1047:2018 «Информационная технология. Термины и определения»;
- Методические пособия по разработке политики информационной безопасности на территории Республики Узбекистан (Приложение №10 к протоколу Республиканской комиссии по координации реализации Комплексной программы развития Национальной информационно-коммуникационной системы Республики Узбекистан на 2013-2020 годы от 23 февраля 2016 года № 7);
- «Регламент взаимодействия между Министерством по развитию информационных технологий и коммуникаций Республики Узбекистан и органами государственного и хозяйственного управления по реагированию и расследованию и предотвращению инцидентов информационной безопасности» (Приложение №1 и №2 к протоколу Технического совета по вопросам информационно коммуникационной безопасности Республики Узбекистан №7 от 17.11.2017 г.);
- «Требования обеспечения информационной безопасности органов государственного и хозяйственного управления, государственной власти на местах» (Приложение № 2 к протоколу Республиканской комиссии по координации реализации Комплексной программы развития национальной информационно-коммуникационной системы Республики Узбекистан на 2013- 2020 годы от 11 ноября 2017 года № 7);
- Постановление Правления ЦБ РУз Об утверждении положения о защите информации в автоматизированной банковской системе коммерческих банков Республики Узбекистан от 10.03.2020г. №3224

Глава 3. Термины и определения

3.1. В настоящем Положении используются следующие основные понятия:

авторизация — предоставление определенному лицу либо группе лиц права на выполнение определенных действий;

аутентификация — процедура подтверждения подлинности пользователя, программы, устройства или сведений;

идентификация — назначение идентификатора субъектам платежных систем и/или сравнение идентификаторов с установленным списком идентификаторов;

криптографический ключ — последовательность конфиденциальных символов, выполняющих шифрацию, дешифрацию, а

также проверку электронных ключей с помощью криптографических алгоритмов;

система дистанционного обслуживания — комплекс средств телекоммуникации, цифровых и информационных технологий, программных обеспечений и оборудования, обеспечивающих связь между пользователями платежных услуг и поставщиками данных услуг для пользования электронными услугами;

платеж – исполнение денежных обязательств наличными, либо перевод денежных средств с использованием платежных средств;

платежный агент — юридическое лицо, не являющееся банком и заключившее агентский договор на оказание платежных услуг с банком или платежной организацией;

платежный субагент — юридическое лицо, не являющееся банком, или индивидуальный предприниматель, заключивший с платежным агентом субагентский договор на оказание платежных услуг;

платежная организация — юридическое лицо, не являющееся банком, которое правомочно осуществлять деятельность по оказанию платежных услуг;

операторы платежных систем – юридическое лицо, осуществляющее деятельность по обеспечению работы платежной системы на территории Республики Узбекистан;

поставщики платежных систем — Центральный банк, банки, платежные организации, платежные субагенты Республики Узбекистан;

режим безопасности — установленный нормативно-правовыми актами порядок, обеспечивающий предупреждение незаконного использования конфиденциальных сведений организации, включающий в себя административно-правовые, организационные, инженерно-технические и другие меры.

Несанкционированный доступ – это преднамеренное противоправное получение доступа к ресурсу организации (сайту, программе, серверу, службе и т. д.) и завладение конфиденциальной информацией лицом, не имеющим прав доступа к данным.

Аппаратные средства защиты включают в себя всевозможные электронные, лазерные, оптические и прочие устройства, которые встраиваются в информационные и телекоммуникационные системы.

Программные средства защиты – это ПО, предназначенное для обнаружения и пресечения утечки информации. Такие программы могут быть простыми (одиночными) или комплексными.

Программно-аппаратные средства защиты подразумевают комплексное применение рассмотренных выше средств обеспечения целостности данных. Именно такой подход позволяет создать безопасные условия для деятельности компаний.

Криптографическая защита информации от несанкционированного проникновения обеспечивает безопасную передачу данных по корпоративной и глобальной сети. Шифрование защищает саму информацию, а не доступ к ней, поэтому считается самым надежным способом сохранения целостности данных.

Глава 4. Обозначения и сокращения

ИБ - Информационная безопасность

ПО – программное обеспечение;

СБ – Служба безопасности;

Глава 5. Область применения

5.1. Политика ИБ распространяется на всех сотрудников Платежной организации, включая практикантов, контрактников и внешних посетителей (клиенты, технический обслуживающий персонал и т.п.), которые по тем или иным причинам имеют легитимный доступ к ИР Платежной организации, его клиентов и корреспондентов. Также она применяется в отношении к АРМ персонала платежной организации, оргтехнике и другим ресурсам информационной структуры Платежной организации.

5.2. Политика, информационной безопасности не распространяется на информационные системы и объекты информатизации, предназначенные для передачи, обработки, хранения сведений, содержащих государственные секреты. Защита информации, содержащая государственные секреты, обеспечивается в соответствии с Законодательством Республики Узбекистан.

Глава 6. Цели и задачи

6.1. Основной целью, на достижение которой направлены все положения Политики, является минимизация ущерба от событий, таящих угрозу безопасности информации, посредством их предотвращения или сведения их последствий к минимуму.

6.2. Процесс создания надежной информационной защиты является непрерывным.

6.3. В целях обеспечения достаточно надежной системы ИБ необходима постоянная регулировка ее параметров, адаптация для отражения новых угроз, исходящих из внешней и внутренней среды. Не должно существовать каких-либо препятствий при внесении изменений в стандарты, процедуры или Политику по мере возникновения такой необходимости.

В соответствии с данным положением определяются следующие этапы цикла управления ИБ (модель PDCA: Plan-Do-Check-Act):

1) Plan - Планирование (разработка) - анализ рисков, определение Политики, целей, задач, процессов, процедур, программно-аппаратных средств, относящихся к управлению рисками и совершенствованию ИБ для получения результатов в соответствии с общей стратегией и целями Платежной организации;

2) Do - Реализация (внедрение и эксплуатация) - внедрение и эксплуатация Политики, механизмов контроля, процессов, процедур, программно-аппаратных средств;

3) Check - Проверка (мониторинг и анализ) - оценка, и там, где это применимо - измерение характеристик исполнения процессов в соответствии с Политикой, целями и практическим опытом, анализ изменения внешних и внутренних факторов, влияющих на защищенность информационных ресурсов, предоставление отчетов руководству для анализа;

4) Act - Корректировка (сопровождение и совершенствование) - принятие корректирующих и превентивных мер, основанных на результатах внутренних и внешних проверок состояния ИБ, требований со стороны руководства, иных факторов в целях обеспечения непрерывного совершенствования системы управления ИБ.

6.4. Построение системы управления ИБ Платежной организации и ее функционирование должны осуществляться в соответствии со следующими основными принципами:

1) законность - любые действия, предпринимаемые для обеспечения ИБ, осуществляются на основе действующего законодательства с применением всех дозволенных законодательством методов обнаружения, предупреждения, локализации и пресечения негативных воздействий на объекты защиты информации Платежной организации;

2) ориентированность на бизнес - ИБ рассматривается как процесс поддержки основной деятельности Платежной организации. Любые меры по

обеспечению ИБ не должны повлечь за собой серьезных препятствий деятельности Платежной организации;

3) непрерывность - применение средств управления системами защиты информации, реализация любых мероприятий по обеспечению информационной защиты Платежной организации должны осуществляться без прерывания или остановки текущих бизнес-процессов Платежной организации;

4) комплексность - обеспечение безопасности информационных ресурсов в течение всего их жизненного цикла на всех технологических этапах их использования во всех режимах функционирования;

5) обоснованность и экономическая целесообразность - используемые возможности и средства защиты должны быть реализованы на соответствующем уровне развития науки и техники, обоснованы с точки зрения заданного уровня безопасности и должны соответствовать предъявляемым требованиям и нормам. Во всех случаях стоимость мер

и систем ИБ должна быть меньше размера возможного ущерба от любых видов риска;

6) приоритетность - категорирование (ранжирование) всех информационных ресурсов Платежной организации по степени важности при оценке реальных, а также потенциальных угроз ИБ;

7) необходимое знание и наименьший уровень привилегий - пользователь получает минимальный уровень привилегий и доступ только к тем данным, которые являются необходимыми для выполнения им деятельности в рамках своих полномочий;

8) специализация - эксплуатация технических средств и реализация мер ИБ должны осуществляться профессионально подготовленными специалистами Платежной организации;

9) информированность и персональная ответственность - руководители всех уровней и исполнители должны быть осведомлены обо всех требованиях ИБ и несут персональную ответственность за выполнение этих требований и соблюдение установленных мер ИБ;

10) взаимодействие и координация - меры ИБ осуществляются на основе взаимосвязи соответствующих структурных подразделений Платежной организации, координации их усилий для достижения поставленных целей, а также установления необходимых связей с внешними организациями, профессиональными ассоциациями и сообществами, государственными органами, юридическими и физическими лицами;

11) Подтверждаемость - важная документация и все записи - документы, подтверждающие исполнение требований по ИБ и эффективность системы ее организации, должны создаваться и храниться с возможностью оперативного доступа и восстановления.

Глава 7. Основные положения

7.1. ИБ состоит из трех основных компонентов:

- конфиденциальность: свойство, указывающее на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации, и обеспечиваемое способностью системы (среды) сохранять указанную информацию в тайне от субъектов, не имеющих полномочий на доступ к ней;

- целостность: свойство информации, заключающееся в ее существовании

в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию);

- доступность: свойство, характеризующееся способностью своевременного беспрепятственного доступа к информации субъектов, имеющих на это надлежащие полномочия.

7.2. Политика ИБ предусматривает обеспечение ИБ на основе использования совокупности организационных, режимных, технических, программных и других методов и средств защиты

Глава 8. Объекты защиты

8.1. Основными объектами обеспечения ИБ в Платежная организация признаются следующие элементы:

1) информационные ресурсы платежной организации, его клиентов и корреспондентов, содержащие сведения, отнесенные в соответствии с действующим законодательством и внутренними нормативными документами Платежной организации и коммерческой тайне, персональным данным, финансовой информации, любой иной информации, необходимой для обеспечения нормального функционирования Платежной организации (далее - защищаемая информация);

2) средства и системы информатизации (средства вычислительной техники, информационно-вычислительные комплексы, сети, системы), на которых производится обработка, передача и хранение защищаемой информации;

3) программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное

обеспечение) автоматизированной системы Платежной организации, с помощью которых производится обработка защищаемой информации;

4) процессы Платежной организации, связанные с управлением и использованием информационных ресурсов;

5) помещения, в которых расположены средства обработки защищаемой информации;

6) рабочие помещения и кабинеты работников Платежной организации, помещения Платежной организации, предназначенные для ведения закрытых переговоров и совещаний;

7) персонал Платежной организации, имеющий доступ к защищаемой информации;

8) технические средства и системы, обрабатывающие открытую информацию, но размещенные в помещениях, в которых обрабатывается защищаемая информация.

8.2. Список пользователей информационных систем Платежной организации, их права и приоритеты на доступ к информации, заведен в матрицы доступов, полномочия к программным и техническим средствам предоставляются в соответствии с матрицами доступов подразделений Платежной организации, процессы регламентированы Правилами допустимого использования информационных ресурсов Платежной организации и Правилами управления логическим доступом к информационным ресурсам Платежной организации.

8.3. Подлежащая защите информация может:

1) размещаться на бумажных носителях;

2) существовать в электронном виде (обрабатываться, передаваться и храниться средствами вычислительной техники, записываться и воспроизводиться с помощью технических средств);

3) передаваться по телефону, телефаксу, телексу и т.п. в виде электрических сигналов;

4) присутствовать в виде акустических и вибросигналов в воздушной среде и ограждающих конструкциях во время совещаний и переговоров.

Глава 9. Риск и модель угроз информационной безопасности

I. Риски информационной безопасности

9.1. Риск ИБ - это потенциальная возможность использования уязвимостей актива или группы активов с конкретной угрозой для причинения ущерба

Платежной организацию. Для управления рисками ИБ необходимы соответствующие методы определения и обработки рисков, которые могут включать расчет затрат и экономического эффекта, требования законодательных актов, интересы заинтересованных сторон и другие соответствующие данные.

9.2. Процесс определения рисков, принятый в Платежная организация, включает идентификацию, сравнительную оценку риска, и назначение им приоритетов в соответствии с критериями принятия риска и важностью целей для Платежной организации. Результаты определен рисков ИБ помогут руководству принять решения относительно управления рисками ИБ, назначения приоритетов при управлении рисками ИБ и внедрения соответствующих средств управления безопасностью для защиты от этих рисков.

9.3. Для оценки риска, процесс определения рисков включает систематический метод оценки величины риска (анализ риска) и процесс сравнения предполагаемого риска с соответствующими критериями риска. Определение риска должно выполняться периодически, это позволит своевременно учитывать изменения требований ИБ и возникновение рискованных ситуаций, а также произошедшие существенные изменения. Для определения риска следует использовать методы, обеспечивающие сопоставимые и воспроизводимые результаты.

9.4. Для эффективного определения риска ИБ четко определяется область его действия. Определение риска ИБ будет взаимосвязано с определениями рисков для других областей деятельности (при необходимости). До начала обработки рисков устанавливается критерии принятия рисков. Риск принимается, если определено, что его уровень низкий или стоимость его обработки для Платежной организации экономически невыгодна, эти критерии документируются.

9.5. После определения риска для каждого идентифицированного риска должно быть принято решение об его обработке. К возможным опциям обработки рисков относятся:

- применение соответствующих средств управления для снижения рисков;

- осознанное и объективное принятие рисков, если они однозначно удовлетворяют требованиям и критериям принятия рисков Платежной организации;

- разделение совместных рисков с другими сторонами, например, страховщиками или поставщиками.

9.6. После принятия решения об обработке рисков используются соответствующие средства управления, которые прежде были выбраны и внедрены. При случаях доступа сторонних организаций к информационным активам Платежной организации и средствам обработки информации необходимого по производственным причинам, а также, в случае получения товаров и услуг от сторонних организаций, проводится анализ рисков для определения возможных последствий для безопасности информации и требований к средствам управления. Такие мероприятия следует согласовывать и определять в договорах со сторонней организацией.

9.7. Все действия по определению, обработке и принятию рисков, обмену информацией относительно рисков, мониторингу рисков, должны выполняться в соответствии со стандартом **O'z DSt ISO/IEC 27005:2013**.

II.Угрозы информационной безопасности

9.8. Под угрозами ИБ понимается совокупность условий и факторов, создающих предпосылки к возникновению инцидента информационной безопасности.

9.9. Угрозы ИБ подразделяются на:

1) случайные - стихийные бедствия (природные источники угроз - землетрясение, пожары, осадки, наводнения и т.д.), непреднамеренные ошибочные действия со стороны работников Платежной организации, ошибки аппаратных и программных средств и т.д.;

2) преднамеренные, т.е. умышленная фальсификация или уничтожение данных, неправомерное использование данных, компьютерные преступления и т.д.

31. К числу угроз ИБ относятся (но не ограничены ими):

1) утрата информации, составляющей тайну организации, коммерческую тайну Платежной организации и иную охраняемую законом информацию;

2) искажение (несанкционированная модификация, подделка) защищаемой информации;

3) утечка - несанкционированное ознакомление с защищаемой информацией посторонних лиц (несанкционированный доступ, копирование, хищение и т.д.);

4) несанкционированное использование информационных ресурсов (злоупотребления, мошенничества и т.п.);

5) недоступность информации в результате ее блокирования, отказа и сбоя оборудования или программ, дезорганизации функционирования

операционных систем рабочих станций, серверов, активного сетевого оборудования, систем управления баз данных, распределенных вычислительных сетей, воздействия вирусов, стихийных бедствий и иных форс-мажорных обстоятельств, и злонамеренных действий.

9.10. В результате воздействия указанных угроз могут возникнуть следующие негативные последствия, влияющие на состояние ИБ Платежной организации и его нормальное функционирование:

1) финансовые потери, связанные с утечкой, разглашением, или модификацией защищаемой информации;

2) финансовые потери, связанные с уничтожением и последующим восстановлением утраченной информации;

3) финансовые потери, связанные с несанкционированными действиями в информационных ресурсах Платежной организации;

4) ущерб от дезорганизации деятельности Платежной организации, финансовые и репутационные потери, связанные с невозможностью выполнения им своих обязательств;

5) ущерб от принятия управленческих решений на основе необъективной информации;

6) ущерб от отсутствия у руководства Платежной организации объективной информации;

7) ущерб, нанесенный репутации Платежной организации;

8) иной вид ущерба.

Глава 10. Модель нарушителя информационной безопасности

10.1. Нарушители ИБ классифицируются следующим образом:

1) внутренние нарушители - работники Платежной организации, неосознанно либо злонамеренно нарушающие режим ИБ;

2) внешние нарушители - лица, не связанные с Платежной организации трудовыми отношениями (в том числе стажеры и практиканты), из хулиганских или корыстных побуждений предпринимающие действия, способные нанести ущерб информационным ресурсам Платежной организации.

10.2. Опасность нарушителя во многом определяется количеством и степенью важности доступных ему информационных ресурсов. Исходя из этого, наиболее рисковыми категориями следует считать менеджеров высшего и

среднего звена, администраторов информационных ресурсов и лиц, работающих с большими объемами клиентской и финансовой информации.

10.3. Основные типы внутренних нарушителей:

1) «необученный/халатный работник» - работник Платежной организации, по незнанию или по собственной халатности допускающий нарушение, не несущее в себе злого умысла;

2) «конкурирующий работник» - работник Платежной организации, по личной неприязни либо по иным причинам пытающийся нанести ущерб другому работнику. В результате его действий может пострадать не только его «цель», но и в целом Платежной организации;

3) «заинтересованный нарушитель» - работник Платежной организации, который заинтересован в неправомерных действиях по отношению к Платежной организацию третьей стороной либо собственной выгодой. Как правило, заинтересован в дальнейшем сохранении с Платежной организации трудовых отношений и не будет предпринимать действий, прямо его компрометирующих. Наиболее вероятное нарушение - утечка информации (в случае заинтересованности собственной выгодой - финансовые мошенничества);

4) «внедренный злоумышленник» - работник Платежной организации, поступивший на работу с целью совершения противоправных действий в интересах третьих лиц. Практически не заинтересован в дальнейших трудовых отношениях с Платежной организации;

5) «увольняющийся работник» - работник, прекращающий с Платежной организации трудовые отношения без взаимных претензий. Наиболее вероятна утечка информации, к которой он имел непосредственный доступ;

6) «обиженный работник» - работник Платежной организации, неудовлетворенный условиями трудовой деятельности, либо, как вариант, руководство Платежной организации явно недовольно деятельностью работника. Возможны любые, даже самые нелогичные нарушения, особенно в момент расторжения трудовых отношений.

10.4. Основные типы внешних нарушителей (в данном разделе используется терминология, принятая на настоящий момент в сообществе специалистов по ИБ):

1) «Script Kiddie», или «Начинающий» - лицо, интересующееся взломом любого информационного ресурса, имеющего общеизвестные уязвимости. Не нацелен на взлом информационных ресурсов именно Платежной организациа, легко прекращает атаку в случае обнаружения серьезных

средств защиты. Как правило, использует широко распространенные методы взлома, не разрабатывает собственных средств;

2) «Black hat» - «Черный хакер» - в отличие от «Script Kiddie» более упорен во взломе конкретного ресурса, обход систем защиты считает «делом чести», может разрабатывать простые атакующие средства. Действует с целью самоутверждения или для извлечения личной выгоды, может продавать свои услуги криминальным структурам;

3) «Elite hacker», или «Гуру» - высококлассный специалист по взлому информационных систем. Как правило, работает «под заказ» криминальных структур либо конкурирующих организаций. В первом случае будет нацелен на проведение финансового мошенничества, во втором - либо на утечку информации, либо на недоступность серверов и компрометацию Платежной организации в глазах клиентов. В арсенале имеет полный спектр специального программного - технического обеспечения, а также использует методы социальной инженерии;

4) «Партнер» - работник организации-партнера, имеющих доступ к информационным системам Платежной организации. Можно определить любым типом внутреннего нарушителя, но он, как правило, менее управляем и менее осведомлен о требованиях ИБ, принятых в Платежной организацией;

5) «Консультант» - работник сервисной компании, который имеет доступ к информационным ресурсам. Возможны разные сценарии проявления несанкционированной деятельности, как правило, в рамках обслуживаемой информационной системы;

6) «Стажер/практикант» - как правило, ограничен в доступе к информации

и информационным системам, однако постоянно находится на территории Платежной организацию и может получать информацию косвенно либо методами социальной инженерии. Может нанести серьезный ущерб только при халатном отношении к своим обязанностям работника Платежной организации, курирующего данного стажера/практиканта;

7) «Клиент» - клиент Платежной организации, имеющий доступ к его сервисам дистанционного обслуживания. Может нанести урон при неправильном использовании данных сервисов, утере идентификационных данных либо действовать как первые три типа внешних нарушителей, имея - пусть и ограниченный - доступ к информационным ресурсам организации.

Глава 11. Меры информационной безопасности

11.1. Основными мерами по обеспечению ИБ Платежной организации являются:

1) административно-правовые и организационные меры;

2) меры физической безопасности;

3) программно-технические меры.

11.2. Административно-правовые и организационные меры включают (но не ограничены ими):

1) контроль исполнения требований законодательства РУз и внутренних документов;

2) разработку, внедрение и контроль исполнения правил, методик и инструкций, поддерживающих Политику;

3) контроль соответствия бизнес-процессов требованиям Политики;

4) информирование и обучение работников Платежной организации работе с информационными ресурсами и требованиям ИБ;

5) реагирование на инциденты, локализацию и минимизацию последствий;

6) анализ новых рисков ИБ;

7) отслеживание и улучшение морально-делового климата в коллективе;

8) определение действий при возникновении чрезвычайных ситуаций;

9) проведение профилактических мер при приеме на работу и увольнении работников Платежной организации;

10) организация и обеспечение системой поддержания заданных параметров температуры и влажности;

11) обеспечение системой видеонаблюдения;

12) морально-этические (психологические) меры.

39. Меры физической безопасности включают (но не ограничены ими):

1) организацию пропускного и внутри объектового режимов;

2) построение периметра безопасности защищаемых объектов;

3) организацию круглосуточной охраны режимных объектов, в том числе с использованием технических средств безопасности;

4) организацию противопожарной безопасности охраняемых объектов;

5) контроль доступа работников Платежной организации в помещения ограниченного доступа.

11.3. Программно-технические меры включают (но не ограничены ими):

1) использование лицензионного программного обеспечения и сертифицированных средств защиты информации;

2) использование средств защиты периметра (firewall, Intrusion Prevention System (IPS) и т.п.);

3) применение комплексной антивирусной защиты;

4) использование средств ИБ, встроенных в информационные системы;

5) использование специальных комплексов ИБ (как защита электронных информационных ресурсов, так и защита от утечки по электромагнитным и акустическим каналам);

6) обеспечение регулярного резервного копирования информации;

7) контроль за правами и действиями пользователей, в первую очередь привилегированных;

8) применение систем криптографической защиты информации;

9) обеспечение безотказной работы аппаратных средств;

10) мониторинг состояния критичных элементов информационной системы.

Глава 12. Защита информации о платежах

12.1. Операторами платежных систем и поставщиками платежных услуг, исходя из свойств собственных информационных систем, разрабатывается политика информационной безопасности.

12.2. Операторами платежных систем и поставщиками платежных услуг, в целях непрерывной защиты платежных сведений, на всех этапах формирования, передачи, хранения и обработки платежей предпринимаются следующие меры:

внедрение систем идентификации, аутентификации и авторизации;

применение методов (логин, пароль и т.д.) предупреждения входа в систему без разрешения;

защита от фальсификации платежного документа и идентификационных сведений, изменения их без разрешения и передачи третьим лицам;

обеспечение и осуществление контроля над формированием платежных данных, проверкой подлинности платежного документа, их обработкой, а также внесения обоснованных изменений;

при передачи платежных документов - обеспечение доставки настоящего документа его истинному владельцу и предупреждения его отправки другим лицам;

меры по предотвращению несанкционированной записи, изменения, удаления и отправки третьим лицам сведений по произведенным платежам;

обеспечение хранения в сейфе (железном шкафу) платежных сведений, перезаписанных на внешний носитель, а также назначение ответственного за хранение данных работника (работников);

осуществление контроля и ведение учета ПО в информационных системах, а также обеспечение бесперебойной работы версий ПО, аппаратно-программных устройств и программных средств в информационных системах

обеспечение актуальности (применение новой/свежей версии) информационных систем, при внедрении новой версии ПО в информационную систему осуществлять только после ее проверки;

автоматическое формирование процессов обработки, передачи и хранения платежных данных в электронных протоколах и обеспечение их хранения;

создание службы информационной безопасности (назначение ответственного работника по информационной безопасности) и осуществление контроля над выполняемыми работами по информационной безопасности;

обеспечение сетевой и криптографической защиты, защиты от компьютерных вирусов, управление входом в информационные системы, настройка технических средств и принятие других мер;

обеспечение оборудованием и устройствами защиты информации, определение порядка их использования, предупреждение пользования техническими устройствами не по назначению во время их технического обслуживания, ремонта, а также в других случаях;

защита от несанкционированного доступа к используемым техническим средствам со всех телекоммуникационных сетей, а также от изменения, удаления, перезаписи находящихся в них сведений;

Предупреждение несанкционированного распространения данных.

12.3. В целях предупреждения вредоносных кодов (компьютерных вирусов) и их отрицательного воздействия на программы и операционные системы, операторами платежных систем и поставщиками платежных услуг осуществляются следующие меры:

выявление вредоносных для работы устройств вычислительной техники (серверов, компьютеров и т.д.), банкоматов, эмбоссеров и платежных терминалов (исходя из технических возможностей) кодов (компьютерных вирусов) и принятие мер по предупреждению их отрицательного влияния;

применение в информационных системах исключительно лицензированной антивирусной программы, обеспечение актуальности их версий и ежедневное обновление их баз;

обеспечение автоматического обновления антивирусных программ;

осуществление проверки всех электронных сведений антивирусной программой, пришедшей по Интернет сети и электронной почте.

12.4. В платежных системах необходимо использовать криптографические методы защиты информации, при этом в правилах платежной системы определить:

порядок подключения средств криптографической защиты к автоматизированным системам, их запуска, пользования и вывода из обращения;

порядок восстановления средств криптографической защиты в случае сбоя, выхода из строя, а также в других чрезвычайных случаях;

порядок внесения изменений в программы криптографической защиты и их технические документы;

порядок управления криптографическими ключами;

порядок применения организационных, технических методов по использованию, хранению, изменению устройств, носящих криптографические ключи.

При обмене информацией между операторами платежных систем, поставщиками платежных услуг и Центральным банком Республики Узбекистан, обеспечение информационной безопасности и обмен информацией осуществляется на основании двухстороннего соглашения.

12.5. В целях ограничения несанкционированного использования и доступа в информационные объекты операторов платежных систем и поставщиков платежных услуг необходимо принять следующие меры:

установить контроль над оказанием физического воздействия на информационные объекты, включая банкоматы, платежные терминалы и электронные устройства проведения платежей, а также входом в здания и помещения, в котором находится техническое оборудование;

обеспечивать физическую защиту (режим безопасности) технических средств, которая включает в себя параметры и структуры автоматизированных систем, программ, вычислительных техник, телекоммуникационных устройств, используемых при осуществлении платежей, а также сведения (пароли, биометрические и другие данные), позволяющие работать в платежной системе, и предупреждать несанкционированное воздействие;

внедрить системы по контролю доступа в объекты информатизации операторами платежных систем и работниками поставщиков платежных услуг и защите от несанкционированного распространения данных;

с помощью систем видеонаблюдения осуществлять контроль рабочих процессов в помещениях с серверами и телекоммуникационными устройствами.

12.6. Операторы платежных систем и поставщики платежных услуг обязаны обеспечить информационную защиту информационных систем, включающие в себя следующие данные:

сведения об остатках денежных средств на банковском счете (на карте);

сведения об остатках электронных денег;

сведения о выполненных платежах;

сведения, включающие в себя безналичные расчеты;

платежные сведения межбанковских платежей и клиринговых систем;

криптографические ключи, применяемые для обеспечения криптографической защиты;

сведения, составляющие банковскую тайну, персональные данные и прочие сведения, охраняемые законом и подлежащие обработке при осуществлении платежей.

12.7. Операторы платежных систем либо поставщики платежных услуг при предоставлении программ клиентам, осуществляющим платежи и внесении изменений в них обязаны обеспечить:

разработку инструкции по применению программ и предоставление клиентам с обеспечением их актуальности;

внесение изменений в целях устранения выявленных уязвимостей;

контроль над актуальностью используемых клиентами программ.

12.8. Операторы платежных систем и поставщики платежных услуг для осуществления взаимообмена посредством телекоммуникационных сетей

платежными данными и сведениями, касающихся платежных данных, исходя из свойств информационных объектов сторон, обязаны разработать правила обеспечения информационной безопасности, включающие в себя также их обязанности, ответственность и требования настоящего Положения.

12.9. Агентским договором на оказание платежных услуг, составленным между платежным агентом и банком, либо платежной организацией, определятся ответственность сторон по информационной безопасности.

12.10. Поставщики платежных услуг обязаны вести перечень сомнительных (фродовых) операций, связанных с переводом денежных средств.

12.11. При переводе денежных средств пользователя платежной услуги поставщики платежных услуг, в случае, если данный платеж включен в перечень сомнительных (фродовых) операций, обязаны сообщить об этом пользователю (по СМС, мессенджеру или с помощью иных информационных систем), получить повторное подтверждение (пин код либо другие сведения), и при не получении данного подтверждения в течении определенного промежутка времени, отменить данную платежную операцию.

12.12. Операторы платежных систем и поставщики платежных услуг обязаны создать возможность приостановления (блокировки) пользователем платежных операций, касающихся его лицевых счетов.

Глава 13. Конфиденциальность платежных сведений и защита персональных данных

13.1. Операторами платежных систем и поставщиками платежных систем, с целью обеспечения конфиденциальности и целостности сведений, в том числе во время защиты персональных данных пользователей платежных услуг, а также обеспечения надлежащей защиты, предпринимаются следующие меры:

защита целостности и неприкосновенности конфиденциальных и персональных данных, обрабатываемых в платежных системах, и разработка порядка их использования;

разработка правил и мер обеспечения безопасности и конфиденциальности во время работы с защищаемыми данными, регулируемых внутренними документами;

максимальное уменьшение количества сотрудников, работающих с конфиденциальными и персональными данными, заключение с сотрудниками обязательств (договоров) по предупреждению разглашения

конфиденциальных и персональных данных, и определение прав пользования настоящими данными исходя из должностных обязанностей сотрудников;

определение порядка использования ключей электронной цифровой подписи и хранения зашифрованных сведений в целях обеспечения целостности и безопасности сведений;

обеспечение идентификации, аутентификации и авторизации при входе в ресурсы с конфиденциальными и персональными данными;

предупреждение несанкционированной выдачи прав на работу с конфиденциальными и персональными данными;

фиксирование в электронных протоколах действий, выполненных в процессе входа, обработки, хранения и предоставления защищенных данных пользователей в информационных системах;

предупреждение выноса из здания и кражи внешних устройств хранения информации и технических средств;

установление контроля над обеспечением предупредительных мер по несанкционированной передаче, хранению, удалению, обработки и выноса данных.

Глава 14. Служба информационной безопасности

14.1. Операторами платежных систем и поставщиками платежных услуг в целях обеспечения защиты информации в информационных системах в список задач службы информационной безопасности (ответственного за информационную безопасность работника) относятся:

проверка соответствия информационной безопасности информационных систем требованиям настоящего Положения;

оценка обеспеченности мерами по информационной безопасности, повышение уровня информационной безопасности, а также снижение потерь в результате аварий и ошибок работников и предупреждение их происхождения;

осуществление контроля целостности и безопасности информационной инфраструктуры;

защита программных обеспечений в серверах;

ведение перечня электронных протоколов действий работников во всех технологических процессах, а также, действий пользователей платежных услуг, выполняемых в информационных системах;

принятие мер по кибербезопасности и предупреждению присвоения средств незаконными действиями;

принятие предупредительных мер по разглашению сведений третьим лицам;

изучение один раз в квартал соответствия требованиям настоящего Положения и требованиям информационной безопасности, внутренним положениям и порядку информационной безопасности платежной системы, при этом результаты изучения оформляются актом.

Глава 15. Ограничение полномочий сотрудников в информационных системах

15.1. Операторы платежных систем и поставщики платежных услуг с целью ограничения полномочий сотрудников в процессе работы в информационных системах, включая в процессах производства и тестирования, обязаны принять следующие меры:

разработать порядок и правила, определяющие право работать в информационных системах и обозначить их в должностных инструкциях, а также обеспечить порядок пользования системой на основании соответствующего документа (заявление, запрос или иная форма);

формировать перечень ответственных работников, имеющих право работать в информационных системах;

регистрировать действия, связанные с определением и распределением прав работать в информационных системах;

периодически (не менее двух раз в год) проверять логичность, правильность определения прав работать в информационных системах исходя из рабочих задач;

обеспечивать информационную безопасность в период функционирования и тестирования информационных систем, а также контролировать правильность прав работы в данных информационных системах;

предупреждать возможность изменения пользователями информационных систем предоставленных им информационной системой прав работы, а также предоставления доступа чужими лицами.

15.2. Операторы платежных систем и поставщики платежных услуг при привлечении сторонних организаций для внесения изменений в свои информационные системы обязаны:

заключить договор о неразглашении конфиденциальных и персональных данных;

осуществлять работы с платежными и прочими защищаемыми данными в информационных системах после выдачи разрешений в установленном порядке;

привлекать организации, имеющие соответствующие лицензии и (или) другие разрешения (в случае, если настоящая деятельность осуществляется на основании лицензии или соответствующего разрешения);

разработать меры по обеспечению конфиденциальности данных на этапе проектирования информационных систем;

оформить выполняемые по информационной безопасности процедуры (выполняемые работы, устанавливаемые программы, устройства и т.д.), техническое задание, документы по приемке (план проведения тестовых испытаний) и другие соответствующие документы;

составить перечень программного обеспечения и организаций, разработавших его и внесших (вносящих) в него изменения;

определить ориентировочные сроки и условия разработки и внедрения информационных систем;

обеспечить осуществление контроля службой информационной безопасности (ответственным работником по информационной безопасности) и ответственным работником по информатизации на предмет обоснованности вносимых сотрудниками привлеченных организаций изменений в информационные системы, а также их соответствия имеющимся техническим поручениям, отсутствия инородных информационной системе программ (системных функций), положительность результатов тестовых испытаний.

После выполнения организацией, вносившей изменения в автоматизированные системы, своих обязанностей, службой информационной безопасности (работником, ответственным за информационную безопасность) все известные ей конфиденциальные сведения (идентификаторы, пароли и т.д.) подлежат изменению.

Глава 16. Защита информационных сетей от атак

16.1. Операторы платежных систем и поставщики платежных услуг в целях защиты информационной сети и всемирной информационной сети Интернет, а также серверов и каналов связи от возможных атак, обязаны принять необходимые меры, которые включают в себя:

сегментирование компьютерных сетей и использование межсетевого экрана;

принятие технических (криптографических и других) и/или организационных мер по предупреждению несанкционированного доступа к получаемым и отправляемым через информационные сети, в том числе всемирную информационную сеть Интернет, данным, а также обеспечение фильтрации сетевых данных (применение межсетевых экранов);

идентификация, многофакторная аутентификация и авторизация при осуществлении платежей через информационные сети и веб-сайты (многофакторная аутентификация не применяется при осуществлении мобильных и оффлайн (в условиях отсутствия связи) платежей);

идентификация пользователей информационных сетей и всемирной информационной сети Интернет, а также серверов и каналов связи;

организация использования сотрудниками ресурсов всемирной информационной сети Интернет через прокси-сервер, ограничение доступа к веб-сайтам, неиспользуемым в рабочей деятельности и фиксация посещаемых веб-сайтов;

обеспечение информационных систем основными и запасными каналами связи;

защита сети серверов (создание демилитаризационных зон (DMZ);

закрытие ненужных в рабочей деятельности портов в серверах и прекращение услуг;

ведение учета объектов и ресурсов доступа к информационной системе;

многофакторная аутентификация пользователей во время осуществления мобильных платежей (определение с помощью SMS, QR-кода, NFC, отпечатков пальцев, радужной оболочки глаз, либо применение подобных способов подтверждения);

обеспечение информационной безопасности платежных сведений и информационных систем (баз данных) при дистанционном доступе через мобильные устройства;

определение порядка применения паролей, применяемых с целью дистанционного обслуживания и аутентификации клиента в других информационных системах (разовых или многоразовых), применение подтверждающих кодов, освещение времени активации кода и др.

предупреждение мошеннических действий;

регистрация идентификационных данных (IP-адрес, MAC-адрес и другие идентификаторы) о примененном устройстве во время входа в автоматизированную систему;

выявление атак и применение систем предупреждения атак.

16.2. Операторы платежных систем и поставщики платежных услуг вправе применять оборудование информационной защиты иностранных организаций.

16.3. Операторы платежных систем обязаны устанавливать технические и организационные меры, режим работы, применяемые для обмена информацией, обеспечение исполнения которых осуществляется поставщиками платежных услуг.

16.4. В целях усиления защиты информации может применяться протокол изменения сетевых адресов (NAT), позволяющий изменить IP адреса сетевых транзитных пакетов в сетевом протоколе (TCP/IP). При этом электронные журналы всех сетевых подключений подлежат ведению с указанием настоящих IP адресов и электронному архивированию в установленном порядке.

16.5. Операторы платежных систем и поставщики платежных услуг в своих внутренних документах обязаны определить:

порядок обеспечения информационных сетей безопасными и надежными каналами связи;

порядок процесса входа и выхода из платежной системы;

порядок обеспечения информационной безопасности при присоединении пользователя к платежной системе;

порядок и требования информационной безопасности в процессинговых и клиринговых процессах (в случае осуществления данной услуги);

меры и методы управления рисками;

порядок создания единого идентификатора пользователей в автоматизированной системе, информационных программах;

перечень регистрируемых действий;

порядок регистрации и хранения сведений.

Глава 17. Мониторинг информационных ресурсов

17.1 Операторы платежных систем и поставщики платежных услуг осуществляют мониторинг использования конфиденциальных сведений и

важнейших логических и физических ресурсов по платежам (информационных сетей, информационных систем, баз данных, модулей защиты информации). При этом во время мониторинга устанавливаются:

ведение учета программ и устройств информационной инфраструктуры, применяемых для обработки, хранения и передачи информации;

внедрение систем, позволяющих анализировать нежелательные случаи информационной безопасности, осуществлять мониторинг состояния информационной безопасности, а также предупреждать (Security information and event management (SIEM) или др.);

принятие мер по проведению анализа системных данных, осуществляющих мониторинг состояния информационной безопасности, устранению выявленных случаев (таких как несанкционированный доступ и попытки доступа к информационной сети, сбои в системе, нехватка информационных ресурсов, сбои в сети, ограничения в обеспечении информационной безопасности и прочие нежелательные случаи) и (или) их предупреждению.

принятие мер по предупреждению несанкционированного использования конфиденциальных сведений и важнейших логических и физических ресурсов (информационных сетей, информационных систем, баз данных, модулей защиты информации);

фиксирование таких данных, как дата (день, месяц, год) и время (час, минута, секунда) выполнения пользователем операции, идентификационного номера, присваиваемого в автоматизированных системах и информационных программах пользователю во время выполнения им операции, идентификационных сведений, имеющихся во время доступа к системам (IP-адрес, MAC-адрес, номер SIM-карты, IMEI-код, номер телефона и/или иной идентификатор устройства, исходя из технических возможностей), действий, связанных с предоставлением пользователю информационными системами прав;

фиксирование действий (операций) пользователей, связанных с использованием информационных программ, автоматизированных систем.

Глава 18. Выявление нежелательных случаев, связанных с нарушением требований информационной безопасности

18.1. Операторы платежных систем и поставщики платежных услуг в целях выявления нежелательных случаев, связанных с нарушением требований по обеспечению защиты информации во время осуществления платежей и перевода денежных средств, при принятии организационных мер

защиты информации и применении технических средств обязаны организовать работы по:

определению необходимых организационных мер по информационной безопасности;

назначению ответственных работников по эксплуатации, настройки имеющихся технических устройств и регистрации их данных;

принятию мер по выявлению нежелательных случаев, связанных с нарушением требований информационной безопасности, а также, в случае выявления сотрудниками таких случаев, уведомлению об этом службы информационной безопасности (ответственного работника по информационной безопасности);

устранению нежелательных случаев, связанных с нарушением информационной безопасности в случае их возникновения, выявлению причин их возникновения, произведения их анализа и принятию мер для недопущения их возникновения;

регистрации (ведению реестра) выявленных нежелательных случаев и предупреждению клиентов путем размещения сведений по этим случаям на официальном веб-сайте (либо оповещению другими способами);

определению порядка хранения сведений о выявленных нежелательных случаях;

принятие иных мер по обеспечению информационной безопасности.

Операторы платежных систем и поставщики платежных услуг обязаны сообщить о нежелательных случаях, связанных с нарушением требований информационной безопасности Центральному банку в незамедлительном порядке.

18.2. Операторы платежных систем в целях предупреждения нежелательных случаев, связанных с нарушением требований информационной безопасности обязаны установить:

для других участников платежной системы - требования к информационной безопасности в отношении технических и программных средств, необходимых для осуществления платежей;

требования к форме и порядку уведомления о нежелательных случаях, связанных с платежной системой и платежами;

порядок управления рисками информационной безопасности в платежной системе и критерии их оценки;

порядок обеспечения безопасного функционирования средств обработки платежных данных;

порядок взаимодействия при возникновении нежелательных случаев в платежной системе.

18.3. Поставщики платежных услуг в целях предупреждения нежелательных случаев, связанных с нарушением требований информационной безопасности обязаны установить следующие требования:

принятие мер по предупреждению рисков, связанных с доставкой клиенту платежных устройств;

уведомление операторов платежных систем при выявлении таких случаев, как утеря, кража, присвоение посторонними лицами платежного оборудования;

18.4. Операторы платежных систем обязаны уведомлять поставщиков платежных услуг о выявленных нежелательных случаях, связанных с нарушением требований информационной безопасности в платежной системе и предоставить им методическое пособие по проведению анализа и устранению данного случая.

Глава 19. Меры воздействия на нежелательные случаи, связанные с нарушением требований информационной безопасности

19.1. Операторы платежных систем и поставщики платежных услуг обязаны принять следующие меры воздействия на выявленные нежелательные случаи, связанные с нарушением требований информационной безопасности:

прогнозирование необходимых действий по принятию мер воздействия на возможные нежелательные случаи и определение перечня действий, которые надлежит выполнить;

принятие мер воздействия в отношении возникших нежелательных случаев в короткие сроки;

обеспечение непрерывности работы при возникновении нежелательных случаев, предупреждение несанкционированного изменения незаконных платежей и остаточных средств на счетах, восстановление информации и устранение прочих нежелательных случаев;

обеспечение соблюдения работниками требований информационной безопасности во время работы в имеющихся информационных системах;

в целях выявления факторов происхождения возникших нежелательных случаев необходимо произвести оформление, сбор, анализ

электронных протоколов сетевых устройств и информационных систем, и на их основании разработать соответствующие указания;

Глава 20. Проведение анализа причин нежелательных случаев, связанных с нарушением информационной безопасности

20.1. Операторы платежных систем и поставщики платежных услуг обязаны производить анализ причин выявленных нежелательных случаев, связанных с нарушением требований, касающихся обеспечения защиты информации и производить оценку результатов их воздействия. При этом система анализа причин выявленных нежелательных случаев и оценки результатов их воздействия должна включать в себя:

порядок проведения службой информационной безопасности (ответственным работником по информационной безопасности) совместно с соответствующими подразделениями анализа причин происхождения нежелательных случаев после принятия мер воздействия в их отношении;

изучение соответствующих электронных протоколов информационных систем и получение объяснений от работников, являющихся виновниками возникновения выявленного нежелательного случая;

выяснение причин происхождения нежелательных случаев и разработка мероприятий, исключающих возможность возникновения таких случаев, либо снижающих возможность нанесения вреда при их возникновении (в том числе, с привлечением соответствующих специалистов);

классификация нежелательных случаев в зависимости от уровня их отрицательного влияния, и произведение их оценки на основании оценочных критериев.

Выявленные нежелательные случаи, связанные с нарушением требований информационной безопасности, принятые в их отношении меры воздействия, результаты их оценки и прочие дополнительные сведения подлежат распечатке и хранению в отдельной папке.

Глава 21. Обеспечение бесперебойного функционирования платежной системы и ведение электронного архива

21.1. В целях обеспечения бесперебойного функционирования и стабильности платежных систем необходимо принять следующие меры:

обеспечение привидения в рабочее состояние сети и других устройств, связанных с системой платежа, при неполадках, а также обеспечение их бесперебойного функционирования;

разработка порядка (механизма) резервирования копий (backup) данных (баз данных, параметров, электронных протоколов) операционных систем, программного обеспечения, программ информационных систем, хранения их в архиве, их восстановления, ведения их учета и осуществления контроля;

иметь резервные технические устройства и оборудование;

разработать план восстановления зарезервированных (backup) копий сведений при технических неполадках и чрезвычайных ситуациях и периодическое восстановление информационной системы (один раз в год);

осуществлять проверку вносящихся изменений в программы на серверах, предназначенных для тестирования;

осуществлять контроль над функционированием устройств и оборудования в системе;

предупреждение возможных случаев отрицательного влияния на бесперебойное функционирование платежной системы и обеспечение информационной безопасности;

использование дизельной электростанции и/или других средств обеспечения бесперебойного электроснабжения (UPS и т.д.);

обеспечение хранения обработанных данных и ведения их в электронных архивах;

обеспечение хранения данных, касающихся действий клиентов в течение не менее пяти лет;

иметь резервные сети передачи информации.

21.2. Операторы платежных систем и поставщики платежных услуг, не являющихся важными, обязаны организовать основные информационные системы обработки данных, а также создать резервные информационные системы на расстоянии не менее чем в 5 километрах от места их нахождения. При этом основные и резервные информационные системы создаются на территории Республики Узбекистан.

Данные в информационных системах (электронные протоколы и прочие данные, связанные с платежами) подлежат хранению в электронном архиве в количестве не менее двух копий (в частности, по одной копии в основной и резервной информационных системах).

21.3. При прекращении деятельности операторами платежных систем и поставщиками платежных услуг имеющиеся у них информационные ресурсы электронного архива передаются в государственные архивы.

При прекращении деятельности операторами платежных систем и поставщиками платежных услуг и их присоединении к другой организации, данные электронного архива передаются в электронный архив присоединяемой организации.

Глава 22. Режим безопасности

22.1. Операторы платежных систем и поставщики платежных услуг должны быть снабжены помещениями для хранения и обработки платежных сведений. Данные помещения должны отвечать следующим требованиям:

должны быть защищены от несанкционированного физического доступа;

в случае расположения на первом этаже окна должны быть оснащены металлической решеткой;

оснащены охранными и пожарными защитно-ограждающими из вещателей в количестве двух штук;

оснащены ночными охранно-из вещательными устройствами;

установление контроля с помощью видеонаблюдения.

Операторы платежных систем и поставщики платежных услуг могут принять и другие меры защиты помещений, предназначенных для хранения и обработки платежных сведений, отличающиеся от установленных настоящим пунктом.

22.2. Срок хранения всех данных видеонаблюдения, определенных настоящим Положением, должен составлять не менее одного месяца.

22.3. Для защиты зданий операторами платежных систем и поставщиками платежных услуг должны быть оснащены необходимым оборудованием, организационно-техническими средствами и применяться соответствующие программные обеспечения.

Глава 23. Контроль над процессом осуществления платежей

23.1. Операторы платежных систем при принятии мер информационной безопасности в своих платежных системах обязаны выполнять работы по контролю и мониторингу.

23.2. Операторы платежных систем и поставщики платежных услуг обязаны осуществлять анализ уязвимости информационной безопасности автоматизированных систем, приложений, а также объектов информационной инфраструктуры, и не менее одного раза в год осуществлять проверку на предмет несанкционированного доступа и производить контроль над отсутствием не задокументированных возможностей.

23.3. Операторами платежных систем и поставщиками платежных услуг, ежегодно, не позднее первого апреля следующего года, предоставляется отчет в Центральный банк о состоянии обеспеченности безопасности.

Глава 24. Защита от несанкционированного доступа и контроль целостности

24.1 Методы защиты информации

1. *Технические средства* – устройства для аутентификации, электронные ключи и пр.).
2. *Программное обеспечение* – доступ с помощью пароля, блокировка экрана и клавиатуры и пр.).
3. *Криптографическую защиту (шифрование),* включая крипто провайдеры (программные компоненты шифрования), средства удостоверения, организации VPN, а также формирования и проверки ключей и электронной цифровой подписи.

Защита от несанкционированного доступа должна обеспечиваться с помощью целого комплекса мероприятий.

24.2. Цифровая защита данных

К защите от несанкционированного доступа относят шифрование, а также аппаратные и программные средства, которые позволяют предотвратить попытки незаконного доступа к информации.

24.3. Защита компьютерных систем от несанкционированного доступа

Играет ключевую роль в предотвращении утечки данных. Надежная программа безопасности должна использовать комплексную многоуровневую защиту. Дополнительные уровни безопасности включают защиту данных, конечных точек и сети.

Отсутствие же защиты может привести:

- к изменению информации;
- к утечкам конфиденциальной информации;
- к непреднамеренному изменению информации.

24.4. Необходимость контроля целостности

Контроль целостности выполняет следующие задачи:

1. Следит за целостностью обрабатываемой информации и гарантирует её неизменность.
2. Обеспечивает доверенный доступ к конфиденциальным данным, системам управления и инфраструктуре.
3. Защищает от утечек конфиденциальной информации.

24.5. Организация системы защиты данных

Основные действия по предотвращению несанкционированного доступа:

1. Двухфакторную аутентификацию. Один из лучших способов предотвратить несанкционированный доступ – это дополнить методы аутентификации.
2. Политику надежных паролей. Передовые методы для паролей пользователей (без повторных вариантов для доступа к разным системам).
3. Мониторьте активность пользователей. Следите за ее аномальными проявлениями с помощью изучения журналов и поведенческой аналитики.
4. Защита конечных точек. Корпоративный антивирус и обеспечат видимость и защитные меры на самих конечных точках при атаках на устройства.

24.6. Использование DLP системы.

ООО «RAQAMLI BIZNES AGREGATOR» внедряет системное решения от корпорации **Kaspersky Lab DLP**.

24.7 Использование Firewalla в системе.

ООО «RAQAMLI BIZNES AGREGATOR» использовано решения от Mikrotik Router OS - Mikrotik RB3011UIAS-RM

Глава 25. Заключительные положения

25.1. Лица, виновные в нарушении требований настоящего Положения, несут ответственность в установленном законодательством порядке.

25.2. Каждый календарный год обновляется политика информационной безопасности ООО «RAQAMLI BIZNES AGREGATOR»