УТВЕРЖДАЮ
Сандыбаев Д.Р.
Директор

_____

«____» _____ 2022г.

ТОО “KHANPAY”

ПОЛИТИКА

Обеспечения Информационной безопасности в Информационной инфраструктуре обработки данных платежных карт

СОДЕРЖАНИЕ

1 ОСНОВНЫЕ ПОНЯТИЯ И ОПРЕДЕЛЕНИЯ

Для целей настоящей ***Политики обеспечения информационной безопасности в информационной инфраструктуре обработки данных платежных карт*** (далее – Политика или настоящий документ) используются следующие понятия, определения и сокращения:

Компания – ТОО "KHANPAY"

Банковская карта – расчетная платежная карта с магнитной полосой или чипом, являющаяся инструментом безналичных расчетов и предназначенная для совершения Держателем операций по счету, расчеты с использованием которой осуществляются в соответствии с действующим законодательством Российской Федерации и.

Бизнес-процесс – набор связанных бизнес-функций, выполняемых последовательно и нацеленных на достижение одной цели.

Данные платежных карт - данные, полученные в результате транзакций, включая следующие:

- Номер карты (PAN)
- Имя держателя карты (Cardholder Name)
- Дата истечения срока действия (Expiration Date)
- Сервисный код (Service Code)

Критичные данные авторизации (Критичные данные платежных карт) - Полное содержание магнитной полосы (Full Magnetic Stripe Data), CAV2/CVC2/CVV2/CID, PIN-код/PIN-блок.

Среда данных платежных карт – часть сети, в которой обрабатываются данные платежных карт или критичные данные авторизации, включая сетевые компоненты, серверы и приложения (см. также ***Информационная инфраструктура***).

Системные компоненты - любой сетевой компонент, сервер или приложение, которое содержится или подключено к среде данных платежных карт.

Информационные активы, содержащие данные платежных карт (далее – Информационные активы) – различные виды информации (платежной, финансово-аналитической, служебной, управляющей и пр.), содержащей данные платежных карт, на следующих фазах их жизненного цикла: генерация (создание), обработка, хранение, передача, уничтожение.

Информационная безопасность – состояние защищенности интересов (целей) Компании в условиях угроз Информационных активов, Информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение, хранение и использование информации, а также системы регулирования возникающих при этом отношений. При этом защищенность достигается обеспечением совокупности свойств безопасности Информационных активов и Информационной инфраструктуры.

Информационная инфраструктура обработки данных платежных карт (далее – Информационная инфраструктура) – комплекс систем и процессов Компании, обеспечивающий реализацию технологий обработки данных платежных карт и представленный в виде иерархии следующих основных уровней:

- физического (линии связи, аппаратные средства и пр.);
- сетевого (сетевые аппаратные средства: маршрутизаторы, коммутаторы, концентраторы и пр.);
- сетевых приложений и сервисов;
- операционных систем;
- систем управления базами данных;
- технологических процессов и приложений;
- бизнес-процессов.

Инцидент Информационной безопасности – событие(я), вызывающее(ие) действительное, предпринимаемое или вероятное нарушение Информационной

безопасности.

Система информационной безопасности – совокупность защитных мер (технических и организационных) и процессов их эксплуатации, скоординированное и управляемое выполнение которых реализует состояние Информационной безопасности Компании.

Система менеджмента информационной безопасности – часть общей системы менеджмента Компании, основывающаяся на оценке рисков, предназначенная для создания, реализации, эксплуатации, мониторинга, анализа, поддержки и совершенствования составляющих Системы информационной безопасности защитных мер и процессов их эксплуатации

Система обеспечения информационной безопасности – совокупность Системы менеджмента информационной безопасности и Системы информационной безопасности.

Стойкий криптографический алгоритм – алгоритм, который для успешной атаки требует от злоумышленника недостижимых вычислительных ресурсов, недостижимого объёма перехваченных открытых и зашифрованных сообщений или же такого времени раскрытия, что по его истечению защищенная информация будет уже не актуальна.

DMZ (демилитаризованная зона) - технология обеспечения защиты информационного периметра, при которой серверы, отвечающие на запросы из внешней сети, находятся в особом сегменте сети и ограничены в доступе к основным сегментам сети с помощью межсетевого экрана.

2 ОБЩИЕ ПОЛОЖЕНИЯ

2.1 Настоящий документ является внутренним нормативным документом Компании и определяет общую стратегию обеспечения Информационной безопасности в Информационной инфраструктуре обработки данных платежных карт, в том числе:

- основные цели и принципы обеспечения информационной безопасности;
- процессы и меры обеспечения информационной безопасности
- роли, полномочия и зоны ответственности в рамках обеспечения Информационной безопасности, в том числе, деятельности по поддержке процессов менеджмента информационной безопасности

2.2 Деятельность Компании в области Информационной безопасности регламентируется комплексом внутренних нормативных документов Компании, позволяющих определить и довести до каждого работника Компании правила и требования по обеспечению Информационной безопасности, которыми он должен руководствоваться в своей производственной деятельности.

- Для достижения целей, определенных настоящей Политикой, должны быть разработаны внутренние нормативные документы, либо внесены изменения в действующие документы по всем направлениям деятельности, в части выполнения требований стандарта безопасности данных индустрии платежных карт (Payment Card Industry Data Security Standard) – далее PCI DSS.

2.3 Политика разработана с учетом требований следующих нормативных документов:

- Стандарт безопасности данных индустрии платежных карт (PCI DSS).

2.4 Положения настоящего документа обязательны для исполнения работниками Компании, работниками сторонних организаций и частными лицами, имеющими доступ к Информационным активам и Информационной инфраструктуре обработки данных платежных карт Компании.

2.5 Сторонние организации и физические лица, имеющие доступ к Информационным активам и Информационной инфраструктуре Компании, должны осуществлять свою

деятельность на основании договоров, соглашений, обязательств или иных документов, в обязательном порядке и в необходимом объеме учитывающих требования и ответственность по обеспечению Информационной безопасности Компании.

2.6 Подразделения, инициирующие заключение договоров, исполнение которых предусматривает доступ к Информационным активам и Информационной инфраструктуре сторонних организаций и физических лиц, обеспечивают включение соответствующих положений в условия договоров.

2.7 Действие Системы обеспечения информационной безопасности распространяется на все Информационные активы и компоненты Информационной инфраструктуры Компании, а также на все реализуемые с их помощью технологические процессы.

2.8 Все документы Компании, регламентирующие вопросы обеспечения Информационной безопасности Компании, должны соответствовать требованиям Политики и не противоречить ее положениям.

2.9 Документы Компании, регламентирующие вопросы обеспечения Информационной безопасности Компании, включая настоящую Политику, подлежат обязательному пересмотру при внедрении новых и изменении существующих бизнес-процессов, изменении информационной инфраструктуры, изменении требований законодательства и нормативных документов, регулирующих вопросы в области информационной безопасности, но не реже одного раза в год.

3 ЦЕЛИ И ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЧАСТИ ТРЕБОВАНИЙ СТАНДАРТА PCI DSS

3.1 Основной целью обеспечения информационной безопасности в части требований Стандарта PCI DSS является защита данных платежных карт от возможного ущерба посредством случайного или преднамеренного несанкционированного вмешательства в процесс функционирования информационной инфраструктуры обработки данных платежных карт или несанкционированного доступа к циркулирующей в ней информации и ее незаконного использования.

3.2 Защитные меры создаются на основе требований Информационной безопасности, определенных, в том числе для отдельных типов Информационных активов, компонентов Информационной инфраструктуры и реализуемых с их помощью технологических процессов.

3.3 Базовый набор требований Информационной безопасности вырабатывается на основании положений Стандарта PCI DSS, который может быть расширен на основе анализа и оценки рисков нарушений Информационной безопасности.

3.4 Защитные меры и процессы их реализации должны быть адекватными с точки зрения затрат, возможных потерь от выполнения угроз, а также с точки зрения их эффективности и возможности оценки их эффективности.

4 ПРОЦЕССЫ И МЕРЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Для достижения основной цели обеспечения информационной безопасности в части требований Стандарта PCI DSS реализуются следующие процессы и меры:

4.1 Процесс управления безопасностью сети, управления конфигурацией активного сетевого оборудования, обеспечивающий:

- регламентирование процедур утверждения и тестирования всех подключений к внешним сетям, а также изменений, вносимых в конфигурацию межсетевых экранов и маршрутизаторов;
- документирование схемы сети с указанием всех подключений (включая беспроводные сети) к сегментам с данными платежных карт. Схема поддерживается в актуальном состоянии с учетом вносимых изменений в инфраструктуру;
- документирование и обоснование применения для всех использующихся сервисов, протоколов и портов, включая документирование реализованных механизмов защиты для небезопасных протоколов;
- периодический пересмотр наборов правил межсетевых экранов и списков доступов маршрутизаторов (не реже чем через каждые 6 месяцев);
- реализацию процедур синхронизации и защиты активных и резервных конфигурационных файлов маршрутизаторов.

4.2 Реализуются следующие принципы построения организации сетевой сегментации, межсетевого экранирования и организации внешних подключений:

4.2.1 для снижения рисков несанкционированного доступа к данным платежных карт, как из сети Интернет, так и внутренних сетей Компании, организуются зоны DMZ и защищенные сегменты внутри локальной сети;

4.2.2 для ограничения входящего и исходящего трафика информационной инфраструктуры обработки данных платежных карт только теми протоколами и адресами, которые необходимы для среды данных платежных карт устанавливаются межсетевые экраны:

- на каждом канале подключения информационной инфраструктуры обработки данных платежных карт к сети Интернет и другим внешним сетям, не контролируемым Компанией;
- на каждом канале подключения информационной инфраструктуры обработки данных платежных карт к беспроводным сетям;
- между любым сегментом локальной сети Компании, являющимся DMZ, и остальными сегментами информационной инфраструктуры обработки данных платежных карт;
- между любым сегментом локальной сети, в котором установлено оборудование, отвечающее за хранение и обработку данных систем платежных карт, и иными сегментами локальной сети Компании или внешними сетями;
- на всех персональных и мобильных компьютерах (ноутбуках), которые подключаются к информационной инфраструктуре обработки данных платежных карт, имеют прямое подключение к Интернет и не защищены корпоративным межсетевым экраном.

4.2.3 межсетевые экраны настраиваются следующим образом:

- запрещается любой трафик, явно не разрешенный;
- разрешающие правила накладывают максимальные ограничения на перечень разрешенных портов/протоколов и адресов, как источника, так и назначения, за исключением ситуаций, где невозможно определить такие ограничения;
- любой входящий интернет-трафик ограничивается только IP-адресами внутри DMZ;
- любой входящий и исходящий трафик из/в сегментов локальной сети, где хранятся данные платежных карт, ограничивается только IP-адресами внутри DMZ или других внутренних сегментов локальной сети.

4.2.4 Запрещается передача трафика с адресами отправителя внутренней сети (RFC 1918), поступающего в DMZ из сети Интернет;

4.2.5 На внешних межсетевых экранах и маршрутизаторах реализуется фильтрация трафика с учетом состояния соединений (stateful inspection), также известной как динамическая фильтрация пакетов (когда доступ в сеть разрешается только для «установленных» соединений);

4.2.6 Базы данных, содержащие данные платежных карт, размещаются во внутренних сегментах сети, отделенных от DMZ межсетевыми экранами.

4.2.7 Для предотвращения трансляции и раскрытия внутренней адресации в сети Интернет осуществляется IP-маскарадинг, использующий адресное пространство частных сетей (RFC 1918), на основе технологий преобразования сетевых адресов (NAT) и переназначения портов и адресов (PAT).

4.3 Для мониторинга всего сетевого трафика в сегментах обработки данных платежных карт и предупреждения персонала о возможных компрометациях используются системы обнаружения вторжений и/или системы предотвращения вторжений.

4.4 Разрабатываются корпоративные стандарты по конфигурированию оборудования и программного обеспечения (далее ПО), определяющие единые требования по настройке параметров безопасности, используемых в Компании операционных систем(далее ОС), оборудования, прикладного ПО, участвующих в обработке данных платежных карт и учитывающие отраслевые практики и рекомендации по обеспечению безопасности систем.

4.5 Подключение оборудования к информационной инфраструктуре обработки данных платежных карт допускается только после выполнения требований корпоративных стандартов по конфигурированию оборудования и ПО.

4.6 Для выявления попыток несанкционированного внесения изменений в критичные системные и конфигурационные файлы на всех системных компонентах, обрабатывающих данные платежных карт, обеспечивается контроль целостности файлов и уведомление персонала о несанкционированных изменениях.

4.7 Разрабатывается политика хранения и уничтожения данных платежных карт, регламентирующая места, объем хранимой информации и период хранения так, как это необходимо исходя из требований бизнеса, правовых и/или нормативных актов;

4.8 При хранении, обработке и передаче данных платежных карт реализуются следующие меры:

4.8.1 запрещается хранить критичные данные платежных карт (sensitive authentication data), полученные в процессе авторизации после прохождения процедуры авторизации (даже в зашифрованном виде);

4.8.2 запрещается передача незашифрованных номеров PAN с помощью технологий обмена сообщениями между конечными пользователями (например, электронной почты, мгновенного обмена сообщениями, чата)

4.8.3 реализуются процедуры удаления данных по истечению разрешенного срока хранения;

4.8.4 реализуются меры по обеспечению защиты данных платежных карт вне зависимости от места хранения (включая данные на портативных носителях, резервных копиях, в журналах)

4.8.5 используются стойкие криптографические алгоритмы и протоколы для защиты данных платежных карт во время передачи их через общедоступные сети;

4.8.6 обеспечивается физическая безопасность всех бумажных и электронных средств (включая компьютеры, электронные носители информации, сетевое оборудование, линии телекоммуникаций, бумажные отчеты, чеки и факсимильные сообщения), содержащие данные платежных карт;

4.8.7 реализуются процедуры уничтожения носителей, содержащих данные платежных, после истечения срока их хранения, методами, гарантирующими невозможность восстановления информации.

4.9 Реализуются процессы и процедуры управления криптографическими ключами для ключей, использующихся при шифровании данных платежных карт, обеспечивающие:

- генерацию стойких криптографических ключей;
- безопасное распределение криптографических ключей;
- безопасное хранение криптографических ключей;
- периодическую замену криптографических ключей;
- отмену или замену старых или заподозренных в компрометации криптографических ключей;
- разделение информации о криптографическом ключе между несколькими лицами и удвоенный контроль над ключами;
- предотвращение несанкционированной подмены криптографических ключей;
- подписание соглашения сотрудниками, ответственными за хранение и использование криптографических ключей, в котором подтверждается, что они понимают и принимают ответственность по обеспечению защищенности ключей;

4.10 Реализуется процесс защиты от вредоносного программного обеспечения, включающий следующие меры:

4.10.1 антивирусное программное обеспечение устанавливается на всех системах, подверженных воздействию вирусов (особенно рабочих станциях и серверах);

4.10.2 обеспечивается регулярное обновление антивирусного ПО и баз сигнатур;

4.10.3 антивирусные механизмы постоянно поддерживаются включенными;

4.10.4 обеспечивается регулярное полное сканирование;

4.10.5 ведется протоколирование работы антивирусного ПО;

4.10.6 обеспечивается централизованный сбор зарегистрированных событий и их хранение не менее 1 года.

4.11 Реализуется процесс своевременной установки обновлений безопасности, для используемых в Компании ОС, оборудования и прикладного ПО, а также внесение изменений в конфигурацию используемого ПО, обеспечивающий:

- мониторинг внешних источников информации для контроля и отслеживания технических уязвимостей;
- своевременную установку на все системные компоненты и программное обеспечение, выпущенных производителями обновлений безопасности. Критичные обновления устанавливаются в течение 1 месяца с момента их выпуска;
- тестирование всех обновлений безопасности и изменений в конфигурации перед внедрением на производственных системах;
- поддержку в актуальном состоянии корпоративных стандартов конфигурирования параметров безопасности систем, с учетом полученного опыта и информации об известных уязвимостях систем.

4.12 Процесс управления изменениями на производственных системах, обеспечивающий:

- документирование любых планируемых изменений, включая оценку оказываемого влияния на бизнес процессы Компании и согласование с заинтересованными подразделениями
- тестирование работоспособности изменений перед внесением в производственные системы
- подготовку процедур возврата в исходное состояние (отката) в случае неуспешного внесения изменений на производственных системах
- согласование и утверждение плана внесения изменений сотрудниками, уполномоченными на принятие решений по изменению соответствующих производственных систем.

4.13 Процессы разработки программного обеспечения, обрабатывающего данные платежных карт, построенные на основе и с применением международных отраслевых рекомендаций и лучших практик по безопасной разработке приложений, обеспечивающие:

4.13.1 тестирование всех обновлений, а также изменений в конфигурации систем и программного обеспечения до внедрения в среду эксплуатации, включая (но не ограничиваясь) следующее:

- проверку всех входных данных (для предотвращения межсайтового выполнения сценариев, угроз инъекций кода, исполнения вредоносных файлов и т. д.)
- проверку правильности обработки ошибок
- проверку защиты хранимых криптографических материалов
- проверку защиты коммуникаций
- проверку правильности управления доступом на основе ролей

4.13.2 разделение среды разработки, тестирования и эксплуатации

4.13.3 разделение обязанностей в средах разработки, тестирования и эксплуатации

4.13.4 подготовку специальных тестовых наборов данных для тестирования или разработки (не должны использоваться данные из среды эксплуатации, реальные номера PAN)

4.13.5 удаление тестовых учетных записей и данных до внедрения в среду эксплуатации

4.13.6 выполнение анализа кода разработанного программного обеспечения перед запуском этого ПО в эксплуатацию

4.13.7 выполнение ежегодного анализа защищенности публичных приложений для идентификации потенциальных уязвимостей

4.14 Реализуется процесс управления и контроля над предоставлением доступа к системам Информационной инфраструктуры обработки данных платежных карт, обеспечивающий:

- предоставление доступа к системным компонентам и данным платежных карт только тем сотрудникам, которым такой доступ необходим в соответствии с их должностными обязанностями;
- назначение полномочий сотрудникам в системах в соответствии с должностью и выполняемыми функциями и ограничивается минимально достаточными полномочиями, необходимыми для выполнения их должностных обязанностей;
- назначение полномочий сотрудникам в системах на основе ролевого доступа – для каждой системы документируется и утверждается карта доступа, содержащая перечень выполняемых в системе ролей (функций) и соответствующего этой роли набора необходимых полномочий;
- предоставление доступа и назначение полномочий в системах на основе заявки с перечнем запрашиваемых прав (роли), утвержденной руководством;
- реализацию для всех многопользовательских систем автоматизированных механизмов разграничения и контроля доступа, основанных на факторе знания, и применяющих принцип «запрещено всё, что явно не разрешено». По умолчанию запрещаются любые виды доступа;
- для доступа к системным компонентам и данным платежных карт каждому пользователю назначается уникальный идентификатор/имя учетной записи. Помимо идентификатора, применяется один из следующих методов для аутентификации пользователей: пароль, ключи (например, SecureID, сертификаты, открытый ключ), биометрические параметры;
- запрещается предоставление групповых учетных записей, не позволяющих однозначно идентифицировать сотрудника, осуществляющего доступ;
- для предоставления удаленного доступа (доступа сетевого уровня, осуществляемого из-за пределов внутренней сети) в сеть сотрудникам Компании или третьим лицам реализуется двухфакторная аутентификация;
- учетные записи, использующиеся сотрудниками сторонних организаций для осуществления удаленной поддержки, активируются только на период оказания поддержки;
- для обеспечения надежной аутентификации и контроля над учетными записями на всех системных компонентах реализуются механизмы управления учетными записями и паролями, обеспечивающие:
  - присвоение уникальных первоначальных паролей для каждого пользователя и его изменение сразу же после первого использования;
  - немедленное аннулирование доступ для каждого сотрудника при его увольнении;
  - удаление/отключение неиспользуемых учетных записей пользователей по крайней мере каждые 90 дней;
  - контроль соответствия используемых паролей критериям криптостойкости (длина, сложность, частота смены, повторное использование и т.п.);
  - ограничение неудачных попыток получения доступа к системе и блокировку учетной записи после превышения заданного количества попыток;
  - разрыв пользовательского сеанса при отсутствии активности более чем 15

минут;

- проведение процедуры проверки подлинности пользователей перед сбросом их паролей или разблокированием учетных записей;
- доведение до всех пользователей, обладающих возможностью доступа к данным платежных карт, парольной политики и процедур.

4.15 Реализуются процессы ограничения и отслеживания физического доступа к системам, в которых хранятся, обрабатываются или передаются данные платежных карт, обеспечивающие:

- использование системы видеонаблюдения для наблюдения за критичными помещениями. Обеспечивается хранение данных видеонаблюдения по крайней мере в течение 3 месяцев;
- использование системы контроля доступа в помещения, в которых хранятся, обрабатываются или передаются данные платежных карт, и реализацию процедур обеспечивающих:
  - выдачу физического средства идентификации (например, пропуска или устройства доступа) с ограниченным сроком действия, отличающего посетителей от сотрудников Компании;
  - авторизацию до входа в помещения, в которых обрабатываются данные платежных карт;
  - изъятие физического средства идентификации перед уходом или по истечении срока действия;
  - ведение журнала регистрации посетителей в котором отражаются имя посетителя, название компании, которую он представляет, и имя сотрудника, разрешившего физический доступ. Обеспечивается хранение журнал регистрации по крайней мере в течение 3 месяцев;
- меры по ограничению физического доступа к оборудованию и сетевым разъемам, расположенным в публично доступных метах;
- реализацию процедур, позволяющих персоналу легко отличать сотрудников Компании от посетителей, особенно в тех помещениях, в которых существует возможность получения доступа к данным.

4.16 Реализуются процессы контроля над хранением и доступностью носителей, содержащих данные платежных карт, обеспечивающие:

- физическую защиту всех бумажных и электронных носителей, содержащих данные платежных карт, включая носители с резервными копиями;
- маркировку носителей, чтобы они могли быть идентифицированы как содержащие конфиденциальную информацию;
- ведение учета всех носителей, а также выполнение периодической инвентаризации носителей не реже 1 раза в год;
- строгий контроль за внутренним или внешним перемещением носителей всех видов, содержащих данные платежных карт, включая:
  - отправку носителей с доверенным курьером или с помощью другого способа доставки, который можно проконтролировать;
  - утверждение руководством перемещения всех носителей, содержащих данные платежных карт, за пределы защищенной территории;
  - уничтожение бумажных и электронных носителей, содержащие критичные данные, методами, гарантирующими невозможность восстановление данных.

4.17 В целях обеспечения контроля и отслеживания доступа к данным платежных карт, действий персонала и пользователей в системах Компании и возможности расследования инцидентов реализуются следующие меры:

- для всех системных компонентов ведется регистрация следующих типов событий:
  - Любого доступа пользователей к данным платежных карт;
  - Всех действий, выполненных с использованием административных привилегий;
  - Доступа ко всем журналам регистрации событий;
  - Неудачных попыток логического доступа;
  - Использования механизмов идентификации и аутентификации;
  - Инициализации файлов аудита;
  - Создания и удаления системных объектов;
- в регистрируемых событиях для каждого системного компонента обеспечивается регистрация, по крайней мере, следующих элементов:
  - Идентификатор пользователя;
  - Тип события;
  - Дата и время;
  - Индикатор успеха или отказа;
  - Источник события;
  - Идентификатор или название задействованных данных, системного компонента или ресурса;
- обеспечивается защита журналов регистрации событий от несанкционированных изменений, включая:
  - Просмотр журналов регистрации событий предоставляется только тем сотрудникам, кому это необходимо для выполнения должностных обязанностей
  - Файлы журналов аудита на локальных системах защищаются от несанкционированных изменений с помощью разграничения прав доступа
  - Со всех системных компонентов, в том числе публично доступных, выполняется сбор зарегистрированных событий ИБ на централизованный log-сервер, расположенный во внутренней сети
  - На централизованном log-сервере обеспечивается защита зарегистрированных событий от несанкционированных изменений
- обеспечивается хранение зарегистрированных событий ИБ на централизованном log-сервере по крайней мере в течение 1 года

4.18 Реализуются процессы, обеспечивающие готовность немедленного реагирования на инциденты ИБ и нарушение информационной безопасности какой-либо системы, обрабатывающей данные платежных карт:

4.18.1 Разрабатывается план реагирования на инциденты ИБ, выполняемый при компрометации системы, включающий следующее:
- описание ролей и обязанностей, а также стратегии уведомления при инциденте
- конкретные процедуры реагирования на инциденты ИБ
- процедуры восстановления и обеспечения непрерывности бизнеса
- процедуры резервирования данных
- анализ правовых требований по отчетности при компрометациях
- покрытие и реагирование для всех критичных системных компонентов
- ссылки на процедуры реагирования на инциденты от платежных систем или сами процедуры

4.18.2 обеспечивается соответствующее обучение персонала, ответственного за реагирование на инциденты ИБ

4.18.3 выполняется по крайней мере ежедневный просмотр зарегистрированных событий ИБ для всех системных компонентов, включая системы, выполняющие функции обеспечения безопасности: систем обнаружения вторжений (IDS), серверов аутентификации, антивирусного ПО, систем контроля целостности

4.18.4 обеспечивается реагирование на наиболее критичные инциденты ИБ в режиме 7 дней в неделю 24 часа в сутки.

4.18.5 проводиться периодическое тестирование плана реагирования, по крайней мере ежегодное

4.18.6 Реализуется процесс изменения и развития плана реагирования на инциденты ИБ в соответствии с приобретенным опытом и с учетом развития отрасли ИБ

4.19 Реализуются процессы, нацеленные на регулярную проверку систем и процессов обеспечения безопасности, обеспечивающие:

- ежеквартальное, а также после любых значительных модернизаций или модификаций инфраструктуры или приложений, проведение внешнего и внутреннего инструментального сканирования сети на наличие технических уязвимостей;
- ежеквартальное тестирование наличия несанкционированных устройств беспроводного доступа в местах обработки данных платёжных карт корпоративной информационной системы;
- ежегодное, а также после любых значительных модернизаций или модификаций инфраструктуры или приложений, проведение теста на проникновение с целью выявления возможности получения несанкционированного доступа к критически важной информации и системным компонентам;
- ежегодный, а также после внесения любых изменений, анализ публичных веб-приложений, обрабатывающих данные платежных карт, с помощью ручных или автоматизированных средств или методов оценки защиты приложений от уязвимостей.

4.20 Реализуются процессы управления персоналом и повышения уровня осведомленности сотрудников Компании в вопросах обеспечения информационной безопасности, обеспечивающие:

- однозначное определение обязанностей всех сотрудников, относящихся к информационной безопасности;
- регламентирование правил эксплуатации и допустимого использования персональных устройств и технологий, которые могут быть использованы сотрудниками (например, технологии удаленного доступа, технологии беспроводного доступа, съемные носители, портативные компьютеры, персональные цифровые секретари (PDA), электронная почта и Интернет;
- разработку и реализацию программы обучения и повышения осведомленности сотрудников в вопросах ИБ при найме на работу и по крайней мере ежегодно для обеспечения понимания сотрудниками важности защиты данных платежных карт;
- письменное подтверждение сотрудниками прочтения и понимания политики и процедур ИБ;
- проверку кандидатов при приеме на работу, для минимизации риска внутренних атак;

4.21 Реализуются процессы управления поставщиками услуг, которым предоставляется доступ к данным платежных карт, обеспечивающие:

- однозначное определение обязанностей всех поставщиками услуг, относящихся к информационной безопасности;

- составление соглашения, подтверждающего признание поставщиками услуг обязанностей по обеспечению безопасности данных платежных карт, к которым они получают доступ
- регламентирование и выполнение процедур подключения/отключения для поставщиков услуг, включая проведение необходимых проверок до предоставления доступа
- выполнение процедур отслеживания статуса соответствия поставщиков услуг стандарту PCI DSS

5 ОЦЕНКА РИСКОВ НАРУШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

5.1 Оценка рисков нарушения Информационной безопасности проводится для всех Информационных активов (типов Информационных активов) области действия Системы обеспечения информационной безопасности.

5.2 Оценка рисков проводится при внедрении новых и изменении существующих бизнес-процессов, изменении информационной инфраструктуры, изменении требований законодательства и нормативных документов, регулирующих вопросы в области информационной безопасности, но не реже одного раза в год.

6 ПОЛНОМОЧИЯ И ОБЯЗАННОСТИ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

6.1 На указанные ниже подразделения Компании возлагаются следующие полномочия и обязанности в рамках деятельности по обеспечению Информационной безопасности в инфраструктуре обработки карточных данных Компании:

6.1.1 Служба информационной безопасности

- Процесс управления безопасностью сети, управления конфигурации межсетевых экранов и маршрутизаторов;
- Построение сетевой сегментации, межсетевого экранирования и организации внешних подключений к информационной инфраструктуре обработки данных платежных карт;
- Разработка корпоративных стандартов по конфигурированию оборудования и ПО, определяющие единые требования по настройке параметров безопасности, используемых в Компании ОС, оборудования, прикладного ПО, участвующих в обработке данных платежных карт;
- Своевременная установка обновлений безопасности, для используемых в Компании ОС, оборудования и прикладного ПО, а также внесение изменений в конфигурацию используемого ПО;
- Управление изменениями на производственных системах Компании;
- Управление и контроль над предоставление доступа к системам Компании(на уровне Домена)
- Разработка и соблюдение мер по хранению, обработке и передаче данных платежных карт в соответствии со Стандартом PCI DSS;
- Процесс управления изменениями на производственных системах обработки данных платежных карт;
- Контроль процесса разработки программного обеспечения, обрабатывающего данные платежных карт;
- Реализация процесса контроля над хранением и доступностью носителей, содержащих данные платежных карт;
- Контроль политики хранения и уничтожения данных платежных карт;

- Реализация процессов и процедур управления криптографическими ключами для ключей, использующихся при шифровании данных платежных карт;
- Реализация процесса управления и контроля над предоставлением доступа к системам Компании;
- Реализация процесса ограничения и отслеживания физического доступа к системам, в которых хранятся, обрабатываются или передаются данные платежных карт;
- Реализация процесса управления поставщиками услуг, которым предоставляется доступ к данным платежных карт.
- Мониторинг всего сетевого трафика в сегментах обработки данных платежных карт и предупреждения персонала о возможных компрометациях используются системы обнаружения вторжений и/или системы предотвращения вторжений;
- Разработка корпоративных стандартов по конфигурированию оборудования и ПО, определяющие единые требования по настройке параметров безопасности, используемых в Компании ОС, оборудования, прикладного ПО, участвующих в обработке данных платежных карт;
- Выявление попыток несанкционированного внесения изменений в критичные системные и конфигурационные файлы на всех системных компонентах, обрабатывающих данные платежных карт;
- Защита от вредоносного программного обеспечения;
- Процесс своевременной установки обновлений безопасности, а также внесение изменений в конфигурацию ПО, участвующего в обработке данных платежных карт;
- Контроль и отслеживание доступа к данным платежных карт;
- Реализация процессов, обеспечивающих готовность немедленного реагирования на инциденты ИБ и нарушение информационной безопасности какой-либо системы, обрабатывающей данные платежных карт;
- Реализация процессов, нацеленных на регулярную проверку систем и процессов обеспечения безопасности;
- Реализация процессов управления персоналом и повышения уровня осведомленности сотрудников Компании в вопросах обеспечения информационной безопасности.