АКЦИОНЕРНОЕ ОБЩЕСТВО
«Единый общереспубликанский
процессинговый центр»

Приложение №2
к Правилам платежной системы «UZCARD»

СТАНДАРТ ПЛАТЁЖНОЙ СИСТЕМЫ UZCARD

Требования информационной безопасности Платежной системы «UZCARD»

(Версия 3.1)

ТАШКЕНТ - 2025

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ.

Для целей Стандарта термины и определения применяются в значениях, установленных Законом Республики Узбекистан от 01.11.2019 года №ЗРУ-578 «О платежах и платежных системах», Законом Республики Узбекистан от 05.11.2019 года №ЗРУ-580 «О банках и банковской деятельности», нормативными документами Центрального банка Республики Узбекистан, Правилами Платежной системы «UZCARD», а также иными актами законодательства Республики Узбекистан.

В Стандарте, если контекст не предусматривает иного, слова, употребляемые в единственном числе, могут подразумевают и множественное число и наоборот, а слова, употребляемые в мужском роде, могут подразумевать также женский и средний род и наоборот.

2. ОБЩИЕ СВЕДЕНИЯ

2.1. Настоящий Стандарт разработан в целях повышения уровня безопасности данных держателей банковских карт, обрабатываемых Участниками и поставщиками платёжных услуг (далее – Партнёры), осуществляющих деятельность в Республике Узбекистан.

Оператор осуществляет контроль за соблюдением Партнёрами требований информационной безопасности и мер непрерывности функционирования ПС.

2.2. Настоящий Стандарт является неотъемлемой частью Правил ПС «UZCARD», адресован и обязателен для исполнения всеми Партнёрами

2.3. Порядок присоединения Субъектов ИКТВ к настоящему Стандарту:

- Участник ПС «UZCARD» - на основании действующего договора с ЕОПЦ на обслуживание в процессинговой центре и при наличии действующего договора с ЕОПЦ на оказание автоматизированных услуг по обработке данных посредством API ПО «SV-Gate»;
- ПО – путём акцептования Оферты о взаимодействии с ПС «UZCARD».

2.4. Присоединение к настоящему Стандарту означает принятие Партнёрами полностью всех условий настоящего Стандарта, Правил ПС «UZCARD» без каких-либо изъятий или ограничений.

2.5. Настоящий Стандарт содержит требования информационной безопасности к Партнёрам для их дальнейшего подключения и работы с ПС и ПО «SV-GATE», являющимся единым платежным шлюзом для обработки онлайн Операций по банковской карте.

2.6. Нормативно-правовые акты и стандарты, использованные в создании документа:

- Закон Республики Узбекистан «О платежах и платежных системах» №ЗРУ-578 от 01.11.2019 г.;
- Закон Республики Узбекистан №547 «О Персональных данных» №ЗРУ-547 от 02.07.2019 г.;

- Стандарт Безопасности Данных Индустрии Платежных Карт «PCI DSS Requirements and Testing Procedures» 4.0.

2.7. Настоящий Стандарт устанавливает требования к Партнёрам для обеспечения базового уровня информационной безопасности, применяемых для платежных инструментов, которые хранят, обрабатывают и передают данные банковских карт, полученные из единого платежного шлюза «SV-GATE». Также, документ содержит рекомендации по усовершенствованию систем информационной безопасности Партнёров для достижения более высокого уровня информационной безопасности.

2.8. Требования информационной безопасности, применяемые для Партнёров в ходе проведения технической проверки, приведены в Приложении 1 настоящего Стандарта.

Приложение 1
к Стандарту платежной системы «UZCARD»
«Требования информационной безопасности
Платежной системы «UZCARD»

№	ТРЕБОВАНИЯ	ПРОВЕРОЧНЫЕ ПРОЦЕДУРЫ
1	**ДОКУМЕНТАЦИЯ ИБ** **Внедрить и поддерживать нормативно-распорядительные документы по информационной безопасности**	
1.1.	Разработать, опубликовать, поддерживать в актуальном состоянии и распространять политику информационной безопасности. 1.1.1. Пересматривать политику информационной безопасности не реже раза в год и обновлять ее в случае изменения среды Партнера. 1.1.2. Вести журнал ознакомления с Политикой ИБ и поддерживать ее в актуальном состоянии	Проверить актуальную версию политики информационной безопасности. Просмотреть лист изменений политики для удостоверения наличия цикла пересмотра. Проверить журнал ознакомления с политикой информационной безопасности и убедиться в том, что все сотрудники, взаимодействующие со средой ИСП ознакомлены
1.2.	Политика информационной безопасности должна поддерживаться локальными нормативными документами с целью дальнейшего управления и внедрения мер защиты информационной безопасности у Партнера. Данные локально-нормативные документы должны соответствовать требованиям Политики информационной безопасности и дополнять ее в управлении отдельными доменами мер защиты информационной безопасности. Примерами данных локально-нормативных документов могут быть: - Регламент обеспечения антивирусной защиты (защиты систем от вредоносного ПО) - Регламент разработки и	Проверить реестр документов, чтобы удостовериться в наличии локально-нормативных документов, поддерживающие политику информационной безопасности. Документы второго уровня также могут быть прописаны в основной Политике ИБ как отдельные Приложения к Политике

	тестирования ПО - Положение аутентификации и управления паролями учетных записей - Положение регистрации и мониторинга событий информационной безопасности	
1.3.	Внедрить процесс оценки рисков, который осуществляется не реже, чем раз в год и после значительного изменения среды в структуре Партнера, выявляет критичные активы, угрозы и уязвимости, и завершается официальным оформленным анализом рисков.	Проверить наличие актуального документа с надлежащими процессами по оценки рисков
1.4.	Внедрить официальную программу повышения осведомленности сотрудников Партнера об информационной безопасности, целью которой является информирование сотрудников Компании о политиках и процедурах обеспечения безопасности. 1.4.1. Проводить обучение сотрудников Партнера при приеме на работу, а также не реже одного раза в год. 1.4.2. Требовать, чтобы персонал Партнера не реже одного раза в год подтверждал свое знание и понимание политик и процедур обеспечения информационной безопасности Партнера.	Проверить наличие данного пункта в Политике ИБ или других документах, получить последние данные по проведению обучения ИБ сотрудников Партнера. По крайней мере ответственные сотрудники, взаимодействующие со средой проверяемой ИСП, должны пройти обучение. Проверить наличие фактов о прохождении сотрудниками Партнера ежегодных тестов на проверку знаний по ИБ
1.5.	Разработать план реагирования на инциденты, применяемый в случае взлома системы. Быть готовым немедленно отреагировать на взлом информационной системы. 1.5.1. Анализировать и тестировать план по реагированию на инциденты не реже одного раза в год 1.5.2. Включить в план процедуры реагирования на оповещения систем мониторинга информационной безопасности, включая, без ограничения, системы	Запросить план реагирования на инциденты и убедиться, что план актуален, пресматирвается и тестируется регулярно.

	обнаружения и предупреждения вторжений, межсетевые экраны, а также системы мониторинга целостности файлов.	
1.6.	Гарантировать, что политики безопасности и рабочие процедуры управления межсетевыми экранами задокументированы, используются и известны всем вовлеченным сотрудникам Партнера.	Проверить наличие актуального документа по управлению межсетевых экранов
1.7.	Разработать стандарты конфигурирования для всех системных компонентов среды ИСП. Убедиться, что стандарты учитывают все известные уязвимости безопасности, а также положения общепринятых отраслевых стандартов безопасной конфигурирования. К примерам источников общепринятых отраслевых стандартов безопасной конфигурирования относятся: - Центр Интернет-безопасности (CIS Benchmark); - Международная организация по стандартизации (ISO); - Институт системного администрирования, аудита, сетевых технологий и проблем безопасности (SANS); - Национальный институт стандартов и технологий (NIST).	Выборочно проверить утвержденные актуальные стандарты конфигурирования

1.8.	Внедрить процедуры управления идентификацией пользователей на всех системных компонентах среды ИСП, регламентирующих следующие требования: - Немедленно отзывать доступ у учетных записей уволенных сотрудников Партнера. - Удалять/блокировать неактивные учетные записи не реже одного раза в 90 календарных дней - Ограничивать попытки получить доступ путем блокировки идентификатора пользователя после шести неудачных попыток входа в учетную запись подряд. - Устанавливать время блокировки учетной записи равным 30 минутам, либо до момента, пока администратор не снимет блокировку. - Если сеанс работы пользователя находится в режиме ожидания свыше 15 минут, требовать от пользователей пройти повторную аутентификацию, чтобы возобновить работу терминала или сессии.	Проверить наличие процедур управления идентификацией пользователей
2	**ФИЗИЧЕСКАЯ БЕЗОПАСНОСТЬ** **Обеспечить физическую безопасность сегмента ИСП, которая получает, обрабатывает и хранит данные платежных карт.** **Ограничить физический доступ к среде ИСП**	
2.1.	Использовать надлежащие средства контроля доступа в помещение, чтобы ограничивать и отслеживать физический доступ к системам в среде ИСП. 2.1.1. Использовать систему видеонаблюдения (СВН) для контроля физического доступа в критичное помещение среды ИСП. 2.1.2. Использовать систему или механизмы контроля и управления доступом (СКУД) для контроля физического доступа в критичное помещение среды ИСП. 2.1.3. Проводить анализ данных, собранных системами и механизмами контроля доступа.	В случае, если серверная инфраструктура ИСП находится в здании Партнера, где ответственность за физическую защиту несет непосредственно Партнер, проверить использование средств контроля доступа в помещение (ЦОД). В случае, если серверная инфраструктура ИСП была арендована у сервис провайдера на основании договора (среда виртуальных машин, колокейшн), проверить наличие

	Хранить такие данные не менее трех месяцев. 2.1.4. Ограничивать доступ к беспроводным точкам доступа, шлюзам, портативным устройствам, сетевому/коммуникационному оборудованию и каналам связи.	надлежащего пункта договоре об ответственности за физическую защиту оборудований сервис провайдером
2.2.	Разработать процедуры, позволяющие легко различать сотрудников Партнера, имеющих доступ к среде ИСП, включающие: - Идентификацию сотрудников Партнера. - Внесение изменений в права доступа. - Процедуры отзыва или отключения средств идентификации уволенных сотрудников Партнера. Гарантировать, что политики безопасности и процедуры ограничения физического доступа к сегменту ИСП одобрены руководством, используются и известны всем заинтересованным сотрудникам Партнера.	Запросить список ответственных сотрудников Партнера, имеющих доступ в серверное помещение
2.3.	Контролировать физический доступ сотрудников к критичным помещениям следующим образом: - Доступ должен быть разрешен на основании должностных обязанностей - Доступ сотрудника Партнера моментально отзывается после увольнения, а также ими возвращаются и отключаются все устройства физического доступа (например, ключи, карты доступа, биометрические данные и т. д.).	Запросить заявления на предоставление доступа в серверное помещение
3	**СЕТЕВАЯ БЕЗОПАСНОСТЬ Установить и поддерживать конфигурацию межсетевых экранов для защиты данных в среде ИСП**	
3.1.	Разработать и реализовывать стандарты конфигурирования межсетевых экранов и маршрутизаторов 3.1.1. Разработать формальный процесс утверждения и тестирования всех сетевых	Убедиться, что была внедрена актуальная схема сети и схема потоков данных платежных карт сегмента ИСП. Изучить актуальную схему сети и схему потоков данных платежных карт UZCARD.

	подключений и изменений в конфигурациях межсетевых экранов и маршрутизаторов. 3.1.2. Внедрить актуальную схему сети с указанием всех подключений к среде ИСП из других сетей, включая все беспроводные сети. 3.1.3. Внедрить актуальную схему, отображающая все потоки данных платежных карт в среде ИСП, полученных из ПО SVGATE в системах и сетях.	Удостовериться, что был создан формальный процесс утверждения и тестирования всех сетевых подключений и изменений в конфигурациях МЭ.
3.2.	Ограничивать входящий и исходящий трафик только соединениями, необходимыми для среды ИСП, запрещать весь остальной трафик. 3.2.1. Настраивать ограничения соединений на межсетевых экранах и маршрутизаторах между другими сетями и любыми системными компонентами, находящимися в среде ИСП. 3.2.2. Пересматривать наборы правил межсетевых экранов и маршрутизаторов не реже одного раза в полгода.	Проверить правила межсетевого экрана на отсутствие правил по умолчанию и общедоступных правил (any-any). Убедиться, что была проведена настройка ограничения соединений в среде ИСП. Обеспечить проведение пересмотра наборов правил межсетевых экранов и маршрутизаторов не реже одного раза в полгода.
3.3.	Запрещать прямой публичный доступ между Интернетом и любыми системными компонентами в среде ИСП. 3.3.1. Внедрить демилитаризованную зону (DMZ), чтобы ограничить входящий трафик только теми системными компонентами, которые предоставляют авторизованный доступ к общедоступным службам, протоколам и портам. 3.3.2. Ограничивать входящие Интернет-соединения только адресами, находящимися в DMZ. 3.3.3. Запрещать неавторизованный исходящий трафик из среды ИСП в Интернет. 3.3.4. Размещать системные компоненты (например, базы данных), в которых хранятся данные держателей карт, во внутреннем	Удостовериться, что основные системные компоненты ИСП не имеют прямой доступ в Интернет, равно также, как и отсутствует прямой доступ к основным системным компонентам ИСП из Интернета. Проверить, что интернет-соединение в сегменте ИСП осуществляется через зону DMZ. Удостовериться, что системные компоненты, которые хранят карточные данные размещены во внутреннем сегменте сети, отдельный от DMZ.

	сегменте сети, отделенном от DMZ и иных недоверенных сетей. 3.3.5. Не раскрывать частные IP-адреса и данные о маршрутах третьим сторонам, не имеющим санкционированного доступа к такой информации. Примечание: Методы сокрытия IP-адресации включают, но не ограничиваются: - технология Network Address Translation (NAT); - расположение серверов, содержащих данные держателей карт за прокси-серверами/ межсетевой экранами	
3.4.	Использовать механизмы обнаружения и/или предотвращения вторжений для обнаружения и/или предотвращения вторжения в сеть. 3.4.1. Осуществлять мониторинг сетевого трафика по периметру среды ИСП и в критичных точках внутри среды ИСП, и оповещать сотрудников Партнера о подозрительных действиях. 3.4.2. Поддерживать системы обнаружения и предотвращения вторжений и их сигнатуры в актуальном состоянии.	Проверить настройки межсетевого экрана на наличие включенных модулей обнаружения и/или предотвращения вторжений в сеть. Данные механизмы так же могут быть развернуты отдельно от основного межсетевого экрана.
3.5.	Контролировать и отслеживать любой доступ к сетевым ресурсам. 3.5.1. Внедрить журнал регистрации событий, связывающий любой доступ к системным компонентам с конкретным пользователем. 3.5.2. Настроить журналы регистрации событий на отправку событий в централизованную систему сбора событий (SIEM).	Проверить события с централизованной системы сбора событий на наличие событий входа/выхода из межсетевых экранов. Проверить внедрение журнала регистрации событий. Удостовериться в настройке журнала регистрации событий на отправку событий в SIEM. Проверить внедрение журнала регистрации событий. Удостовериться в настройке журнала регистрации событий на отправку событий в SIEM.

4	**БЕЗОПАСНОСТЬ СЕРВЕРОВ И СИСТЕМНЫХ КОМПОНЕНТ** **Обеспечить безопасность серверов и системных компонент среды ИСП**	
4.1.	Настроить все системные компоненты среды ИСП на основе формально утвержденных стандартов конфигурирования. 4.1.1. Не использовать пароли и другие системные параметры безопасности, заданные производителем по умолчанию 4.1.2. Включать только необходимые службы, протоколы, демоны и т. д., требующиеся для функционирования системы.	Выборочно проверить системные компоненты ИСП на обновленные настройки безопасности. Убедиться, что системные настройки не являются по умолчанию и были настроены в соответствии с утвержденным стандартом конфигурирования.
4.2.	При использовании неконсольного административного доступа к системе шифровать канал с использованием стойких криптографических алгоритмов.	Проверить настройки удаленного доступа к серверам ИСП, такие как настройки SSH и убедиться, что используются стойкие методы шифрования для удаленного доступа к серверам ИСП
4.3.	Вести журнал учета системных компонентов, которые входят в область технической проверки.	Проверить наличие данного журнала. Журналом учета системных компонентов может быть документ с таблицей всех системных компонентов среды ИСП.
4.4.	Защищать все системы от вредоносного ПО и регулярно обновлять антивирусное ПО или программы - Разворачивать антивирусное программное обеспечение на всех системах, подверженных воздействию вредоносного ПО (особенно на рабочих станциях и серверах). - Гарантировать, что антивирусное программное обеспечение способно обнаруживать и удалять все известные виды вредоносного программного обеспечения, а также обеспечивать защиту от всех известных видов вредоносного программного обеспечения. Гарантировать, что все	Проверить актуальную лицензию антивирусного ПО и дату последнего обновления в выборочном устройстве

	антивирусные механизмы: - Поддерживаются в актуальном состоянии. - Выполняют периодическое сканирование. - Включен модуль файловой защиты - Создают журналы регистрации событий и направляют события в централизованную систему сбора событий.	
4.5.	Разрабатывать и поддерживать безопасные системы и ПО 4.5.1. Наладить процесс выявления уязвимостей с помощью авторитетных внешних источников информации об уязвимостях, а также управлению риска (например, «высокий», «средний» или «низкий») недавно обнаруженных уязвимостей. 4.5.2. Гарантировать, что все компоненты систем и ПО защищены от известных уязвимостей при помощи установки патчей безопасности, выпускаемых производителем. Устанавливать критичные исправления безопасности в течение месяца с даты их выпуска. Примечание. Какие из исправлений безопасности считаются критичными, должно быть установлено исходя из анализа рисков" 4.5.3. Удалять учетные записи разработчиков, тестовые и (или) пользовательские учетные записи, идентификаторы пользователей и пароли перед переводом приложений в производственный режим или их доступностью клиентам.	Выборочно проверить сервера приложения на историю обновления и установки патчей безопасности. Убедиться в установке патчей безопасности и в своевременной установке критичных исправлений. Запросить последний отчет о выполненной работе по выявлению и устранению уязвимостей путем установки патчей безопасности. Убедиться, что был налажен процесс выявления уязвимостей с помощью авторитарных внешних источников.

4.6.	Проверять написанный программный код (автоматически или вручную) на наличие потенциальных уязвимостей до запуска в производственный режим или доступностью клиентам и убеждаться, что: · Изменения в коде проверяются другими сотрудниками, которые не являются авторами кода, а также сотрудниками, знакомыми с методиками code review и принципами безопасного программирования. · Код разработан в соответствии с принципами безопасного программирования. · Необходимые корректировки вносятся до выпуска ПО. · Результаты code review рассматриваются и согласовываются с руководством до выпуска ПО. Примечание. Данное требование к code review применимо ко всему написанному коду (как внутренним, так и общедоступным системам) в рамках жизненного цикла разработки системы. Code review могут проводиться компетентным внутренним персоналом или третьими сторонами. 4.6.1. Соблюдать процессы и процедуры управления изменениями системных компонентов. 4.6.2. Предотвращать распространенные уязвимости программного кода в процессе разработки ПО следующим образом: - Не реже раза в год обучать разработчиков актуальным методикам безопасного программирования, включая обучение тому, как избежать распространенных программных уязвимостей.	Получить сведения на тему какие работы ведутся по проверке программного кода и работе над выявленными уязвимостями в коде и в использованных библиотеках. Убедиться в соблюдении процессов и процедур управления изменениями системных компонентов. Примечание. Следует использовать актуальную версию таких требований, например, OWASP, SANS CWE Top 25, CERT Secure Coding и т.д.

	- Разрабатывать приложения в соответствии с основными принципами безопасного программирования. Примечание. Следует использовать актуальную версию таких требований, например, OWASP, SANS CWE Top 25, CERT Secure Coding и т.д. 4.6.3. Изучать на постоянной основе новые угрозы и уязвимости общедоступных веб-приложений и гарантировать, что эти приложения защищаются от известных атак при помощи следующих методов: - Проверка общедоступных веб-приложений на наличие уязвимостей с использованием методов, средств ручного или автоматического анализа защищенности не реже одного раза в год, а также после внесения любых изменений. - Установка перед общедоступными веб-приложениями технического средства для постоянной проверки всего трафика (например, межсетевой экран уровня приложений) с целью обнаружения и предупреждения веб-атак.	
4.7.	Отделить среды разработки/тестирования от производственных сред, а также внедрить механизмы разграничения доступа.	Проверить наличие разделенных сегментов под производственные и тестовые среды. Удостовериться, что между сегментами нет какого либо доступа.
4.8.	Разделять обязанности между сотрудниками, выполняющими обязанности разработки/тестирования, и сотрудниками, работающими в производственной среде.	Удостовериться, что сотрудники, работающие в тестовой среде, не имеют доступа к производственной среде. Работа с производственной средой может быть осуществляться только отдельными ответственными сотрудниками, назначенные

		приказом или иным подтверждающим документом
4.9.	Не использовать производственные данные (действующие основные номера держателей карт) для тестирования и разработки.	Запросить выборку (select) из базы данных тестовой среды с наличием данных платежных карт и проверить их реальность и актуальность
4.10.	Удалять все тестовые данные и учетные записи из системы перед переводом такой системы в эксплуатацию / производственный режим.	Интервьюировать персонал Партнера на метод перевода тестовой среды в производственный. Проверить производственную среду на отсутствие тестовых данных
4.11.	Синхронизировать все системные часы и системное время на критичных системах и обеспечивать выполнение следующих требований для получения, распространения и хранения данных о времени: - Устанавливать точное и согласованное время на критичных системах. - Получать настройки времени из общепризнанных отраслевых источников.	Запросить данные о наличии централизованной системы синхронизации системных часов. Убедиться, что сервера ИСП настроены на синхронизации системных часов
5	**БЕЗОПАСНОСТЬ ДАННЫХ ПЛАТЕЖНЫХ КАРТ ПРИ ИХ ХРАНЕНИИ И ОБРАБОТКЕ. 5. Обеспечить защиту данных платежных карт, полученные из ПО SV-Gate при их хранении и обработке в системах управления базами данных (СУБД)**	
5.1.	Огранивать хранение данных только необходимым минимумом.	Запросить информацию о том, в каких целях и процессах используются данные платежных карт "UZCARD".
5.2.	Маскировать основной номер держателя карты (PAN) при его отображении (SELECT), где максимально возможное количество цифр для отображения - первые шесть и последние четыре. Пример: 8600 00xx xxxx 1234	Запросить выборку (SELECT) из базы данных производственной среды с наличием данных платежных карт. Убедиться, что номера карт отображаются в маскированном виде.

5.3.	Применить механизмы шифрования с использованием стойких криптографических алгоритмов для шифрования полного номера карт PAN UZCARD.	Запросить и проверить настройки СУБД или настройки приложения, где применены механизмы шифрования нолного номера PAN Также, запросить выборку (select) из базы данных производственной среды с наличием данных платежных карт чтобы удостовериться что PAN зашифрованы.
5.4.	Ограничить доступ к криптографическим ключам. Разрешать доступ к таким ключам наименьшему возможному числу сотрудников, ответственных за криптографические ключи. - Документировать в полной мере и применять все процессы и процедуры управления криптографическими ключами для шифрования ИСП - Генерировать стойкие криптографические ключи. - Безопасно распространять ключи шифрования. - Безопасно хранить ключи шифрования - Исключить несанкционированную замену криптографического ключа.	Запросить документ по управлению криптографическими ключами и удостовериться в том, что криптографические ключи хранятся надежно и доступ к ним ограничен в соответствии с внутренним приказом. Проверить чтобы документация выполнялась в полной мере, проверить стойкость криптографических ключей, проверить безопасность распространения ключей шифрования, проверить безопасность хранения ключей шифрования.
5.5.	Шифровать данные держателей карт при их передаче в открытых общедоступных сетях 5.5.1. Использовать стойкую криптографию и протоколы безопасности для защиты конфиденциальных ИСП при их передаче в открытых общедоступных сетях, с учетом следующего: · Принимаются только доверенные ключи и сертификаты. · Используемый протокол поддерживает только безопасные версии и конфигурации. Стойкость шифрования	Проверить конфигурацию приложения для того, чтобы удостовериться, что используется шифрование данных при их передаче через интернет. Убедиться в использовании стойкой криптографии и протоколов безопасности для защиты конфиденциальных ИСП при их передаче в открытых общедоступных сетях.

	соответствует используемой методологии шифрования. 5.5.2. Запретить пересылать незащищенный PAN при помощи пользовательских технологий передачи сообщений (например, электронная почта, системы мгновенного обмена сообщениями, СМС-сообщения, чаты и т.д.).	
6	**ВНЕДРЕНИЕ СРЕДСТВ ОБЕСПЕЧЕНИЯ ИБ. 6. Внедрить общеизвестные средства обеспечения информационной безопасности в среде ИСП**	
6.1.	Внедрить средства сбора и анализа журналов протоколирования событий, а также средства оповещения, системы сбора и корреляции событий (SIEM) 6.1.1. Выполнять автоматизированную регистрацию событий всех системных компонентов: - Регистрировать все факты доступа пользователя к данным держателей карт; - Регистрировать все действия пользователя с неограниченными правами доступа (root) и пользователя с административными привилегиями; - Регистрировать доступ ко всем записям о событиях в системе; - Регистрировать все неуспешные попытки логического доступа; - Регистрировать факты использования и изменения механизмов идентификации и аутентификации включая, помимо прочего, факты создания новых учетных записей, расширения привилегий — а также все изменения, добавления, удаления учетных записей пользователя с неограниченными правами доступа (root) или пользователя с административными привилегиями; - Регистрировать запуски, остановки или приостановки ведения журналов регистрации событий.	Проверить наличие рабочей системы SIEM. Удостовериться, что все сервера сегмента ИСП настроены на отсылку событий безопасности в SIEM. Проверить настройки аудита в системных компонентах информационной системы партнера на наличие настроек по автоматическому регистрированию событий безопасности. Удостовериться что доступ к просмотру журналов регистрации событий имеют только сотрудники, которым такой доступ необходим в соответствии с их должностными обязанностями. Проверить что журналы регистрации событий хранятся не менее одного года, и в оперативном доступе не менее трех месяцев.

	6.1.2. Регистрировать как минимум следующие параметры в журналах регистрации событий в отношении каждого события каждого системного компонента: Идентификатор пользователя, Тип события, Дата и время, Каким было событие - успешным или неуспешным, Источник события, Идентификатор или название данных, системного компонента или ресурса, затронутых событием. 6.1.3. Ограничивать доступ к просмотру журналов регистрации событий только теми сотрудниками, которым такой доступ необходим в соответствии с их должностными обязанностями. 6.1.4. Защищать журналы регистрации событий от неавторизованного изменения. 6.1.5. Просматривать журналы регистрации событий и события безопасности всех системных компонентов с целью обнаружения аномалий или подозрительной активности. Не реже одного раза в день проверять: - Все события безопасности - Журналы всех системных компонентов, осуществляющих хранение, обработку или передачу ИСП и/или критичных аутентификационных данных - Журналы всех критичных системных компонентов - Журналы всех серверов и системных компонентов, выполняющих функции защиты (например, межсетевых экранов, систем обнаружения и предотвращения вторжений, серверов аутентификации, и т.д.). 6.1.6. Хранить журналы регистрации событий не менее одного года, и в оперативном доступе не менее трех месяцев (например, они могут	

	находиться в прямом доступе, либо архивированы, либо могут быть оперативно восстановлены с носителя резервной копии).	
6.2.	Установить систему контроля доступа к системным компонентам, которая ограничивает доступ в соответствии со служебной необходимостью пользователя и которая настроена запрещать все, что заранее не разрешено. Внедрить систему управления привилегированным доступом (PAM) для контроля доступов к среде ИСП 6.2.1. Открывать доступ к среде ИСП отдельной учетной записью для каждого пользователя с разными уровнями доступов согласно внутренней матрицей доступов 6.2.2. Включить в системе журнал генерации событий при эксплуатации PAM с протоколированием каждые действия всех пользователей 6.2.3. Настроить систему на отсылку	Проверить актуальную систему PAM. Удостовериться, что доступ к серверам сегмента ИСП осуществляется через систему PAM. Убедиться, что доступ к среде ИСП открывается отдельной учетной записью для каждого пользователя с разными уровнями доступов согласно внутренней матрицей доступов. Убедиться во включении в системе журнала генерации событий при эксплуатации PAM с протоколированием каждого действия всех пользователей. Проверить что систему настроена на отсылку всех событий в централизованную

	всех событий в централизованную систему сбора и корреляции событий (SIEM)	систему сбора и корреляции событий (SIEM)
6.3.	Внедрить систему предотвращения утечек данных (DLP) для защиты от утечек конфиденциальной информации в среде ИСП 6.3.1. Обеспечить полное покрытие агентов в устройствах пользователей, взаимодействующих со средой ИСП 6.3.2. Ежедневно проверять активность агентов, а также оповещения от системы DLP по предустановленным критериям 6.3.3. Включить в системе журнал генерации событий при появлении оповещений (Alerts) в системе DLP 6.3.4. Настроить систему на отсылку всех событий в централизованную систему сбора и корреляции событий (SIEM)	Проверить актуальную систему DLP. Удостовериться, что обеспечено полное покрытие агентов в устройствах пользователей, взаимодействующих со средой ИСП. Проверить что обеспечено полное покрытие агентов в устройтсвах пользователей, взаимодействующих со средой ИСП.
6.4.	Внедрить механизм обнаружения изменений (например, мониторинг целостности файлов FIM) таким образом, чтобы оповещать сотрудников о неавторизованных модификациях (включая изменения, добавления и удаления) критичных системных файлов, файлов конфигурации и файлов данных; сконфигурировать ПО таким образом, чтобы проводить сравнение критичных файлов не реже одного раза в неделю. Примечание. В контексте обнаружения изменений критичные файлы — это файлы, изменение которых происходит редко, но факт изменения которых может служить признаком компрометации системы или риска компрометации системы. Механизмы обнаружения	Запросить наличие систем, механизмов обнаружения изменений в информационных системах среды ИСП. Проверить актуальность данных в системе и отчет по последнему реагированию на изменения

	изменений (такие как средства мониторинга целостности файлов) обычно содержат предустановленный перечень критичных файлов в используемой операционной системе. Внедрить процесс реагирования на любое срабатывание решения для обнаружения изменений.	
6.5.	Внедрить систему мониторинга и отслеживания статусов серверов и сервисов ИСП. Обеспечить полное покрытие агентов на серверах ИСП	Проверить актуальную систему отслеживания и мониторнига статусов серверов сегмента ИСП. Удостовериться, что обеспечено полное покрытие агентов системы мониторинга и отслеживания статусов на серверах ИСП. Проверить полное покрытие агентов на серверах ИСП
7	**ОРГАНИЗАЦИЯ РАБОТ ПО ОБЕСПЕЧЕНИЮ ИБ. 7. Организовать физические, логические, методологические работы по обеспечению ИБ у Партнера включительно для среды ИСП**	
7.1.	Ограничить доступ к данным держателей карт в соответствии со служебной необходимостью 7.1.1. Ограничивать доступ к системным компонентам и данным держателей карт только для тех лиц, которым такой доступ требуется в соответствии с их должностными обязанностями. 7.1.2. Назначать права доступа на основании классификации должностей и должностных обязанностей. 7.1.3. Требовать формального утверждения доступа уполномоченными сторонами с указанием требуемых привилегий. 7.1.4. По умолчанию должен быть запрещен любой доступ (установлен параметр «запрещено все, что явно не разрешено» («deny all»)).	Удостовериться в наличии документа или процесса по управлению данными платежных карт. Запросить подтверждающие данные по ограничениям доступа к данным платежных карт. Удостовериться в установке процесса по ограничению доступа к системным компонентам и данным держателей карт только для тех лиц, которым такой доступ требуется в соответствии с их должностными обязанностями.

7.2.	Обеспечить парольную политику при эксплуатации среды ИСП 7.2.1. Использовать стойкую криптографию для шифрования учетных данных для проверки подлинности (например, паролей/парольных фраз) при их передаче и хранении во всех системных компонентах. 7.2.2. Обеспечить соответствия паролей/парольных фраз следующим требованиям: - наличие в пароле не менее двенадцати символов; - наличие в пароле и цифр, и букв. 7.2.3. Менять пароли/парольные фразы не реже одного раза в 90 дней. 7.2.4. Запретить смену пользователем пароля/парольной фразы на какие-либо из четырех последних паролей/парольных фраз данного пользователя, использованных ранее. 7.2.5. Устанавливать уникальные первоначальные пароли/парольные фразы для каждого пользователя и требовать их немедленной смены при первом входе пользователя в систему.	Удостовериться в наличии документа или процесса по управлению паролей в среде ИСП. Убедиться, что используемая криптография для шифрования учетных данных для проверки подлинности при из передаче и хранении во всех системных компонентах, является стойкой. Проверить соответствие паролей/парольных фраз по следующим параметрам: - наличие в пароле не менее двенадцати символов; - наличие в пароле и цифр, и букв. - пароли/парольные фразы менялись не реже одного раза в 90 дней. - установлены уникальные первоначальные пароли/парольные фразы для каждого пользователя и убедиться в их немедленной смене при первом входе пользователя в систему
7.3.	Предусмотреть многофакторную аутентификацию (MFA) для всех случаев неконсольного доступа в среду ИСП для сотрудников с правами администратора. Предусмотреть многофакторную аутентификацию для всех случаев удаленного сетевого доступа (пользователей и администраторов, включая доступ любых третьих лиц для поддержки или техобслуживания), исходящего извне сети Партнера.	Убедиться в настройке многофакторной аутентификации для всех случаев удаленного сетевого доступа, исходящего извне сети Партнера.

7.4.	Выполнять ограничение доступа к любой базе данных, содержащей данные держателей карт (включая доступ со стороны приложений, администраторов и любых других пользователей), следующим образом: - Все доступы, запросы и операции с базами данных должны осуществляться только программными методами. - Только администраторам баз данных разрешено направлять запросы и запрашивать прямой доступ к базам данных. - Использование идентификаторов приложений разрешено только приложениям (а не отдельным пользователям или иным процессам, не относящимся к приложениям).	Удостовериться в наличии документа или процесса по управлению доступов к информационным системам сегмента ИСП. Запросить подтверждающие данные по предоставлению и ограничению доступа к базам данных, содержащие данные платежных карт
7.5.	Внедрить процессы для проведения ежеквартальной проверки наличия беспроводных точек и для обнаружения всех авторизованных и неавторизованных беспроводных точек доступа. 7.5.1. Вести список авторизованных беспроводных точек доступа с указанием обоснования их необходимости. 7.5.2. Внедрить процедуры реагирования в случае, если обнаружены неавторизованные беспроводные точки доступа.	Удостовериться в наличии документа или процесса по управлению беспроводными сетями. Запросить последний отчет по проведению сканирования беспроводных точек и обнаружения неавторизованных беспроводных точек. Проверить что ведется список авторизованных беспроводных точек доступа с указанием обоснования их необходимости. Убедиться во внедрении процедуры реагирования в случае, если обнаружены неавторизованные беспроводные точки доступа.
7.6.	Выполнять внешнее и внутреннее сканирование сети на наличие уязвимостей не реже одного раза в квартал, а также после внесения значительных изменений в сеть. 7.6.1. Проводить ежеквартальное внутреннее сканирование на наличие уязвимостей. Устранять уязвимости и проводить повторные	Удостовериться в наличии документа или процесса по выполнению сканирований сегмента ИСП на наличие уязвимостей. Запросить последний отчет (страницы, где указаны дата и время выполнения сканирования, статус отчета) по

	сканирования, пока не будут устранены все уязвимости, представляющие «высокий» уровень риска. Сканирования должны выполняться квалифицированными специалистами. 7.6.2. Проводить ежеквартальное внешнее сканирование на наличие уязвимостей посредством соответственного ПО для проведения внешнего сканирования на уязвимости. Проводить повторные сканирования до достижения удовлетворительного результата. Сканирования должны выполняться квалифицированными специалистами.	проведенному внутреннему сканированию на наличие уязвимостей в сегменте ИСП. Запросить последний отчет (страницы, где указаны дата и время выполнения сканирования, статус отчета) по проведенному внешнему сканированию на наличие уязвимостей в сегменте ИСП
7.7.	Внедрить методологию проведения тестирования на проникновение, которая: - Основана на общепринятых отраслевых подходах к проведению тестирования на проникновение - Покрывает весь периметр среды ИСП - Предусматривает тестирование внутри и снаружи сети - Предусматривает анализ и оценку угроз и уязвимостей, найденных за последние 12 месяцев - Регламентирует хранение результатов тестов на проникновение и результатов действий, выполненных для устранения уязвимостей. 7.7.1. Проводить внешний тест на проникновение не реже одного раза в год, а также после любой значительной модификации или обновления инфраструктуры среды ИСП. 7.7.2. Проводить внутренний тест на проникновение не реже одного раза в год, а также после любой значительной модификации или обновления инфраструктуры среды ИСП. 7.7.3. Устранять эксплуатируемые	Удостовериться во внедрении методологии проведения тестирования на проникновение, которая: - Основана на общепринятых отраслевых подходах к проведению тестирования на проникновение - Покрывает весь периметр среды ИСП - Предусматривает тестирование внутри и снаружи сети - Предусматривает анализ и оценку угроз и уязвимостей, найденных за последние 12 месяцев - Регламентирует хранение результатов тестов на проникновение и результатов действий, выполненных для устранения уязвимостей.

	уязвимости, обнаруженные во время теста на проникновение, и проводить повторное тестирование для проверки их устранения.	
7.8.	Внедрить процедуру своевременного выявления отказов и уведомления об отказах критических систем контроля безопасности, включающих отказы: - Межсетевых экранов - Систем обнаружения и предотвращения вторжений (IDS/IPS) - Мониторинга целостности файлов (FIM) - Антивирусного ПО - Средств физического контроля доступа - Средств логического контроля доступа - Механизмов ведения журналов аудита - Средств контроля сегментации (если применимо)	Запросить наличие систем, механизмов и процедуру своевременного выявления отказов и уведомления об отказах критических систем контроля безопасности. Удостовериться в актуальности систем и агентов по выявлению отказов в информационных системах сегмента ИСП
7.9.	Выполнять своевременное реагирование на любые отказы критичных средств контроля безопасности. Процедуры для реагирования на отказы механизмов обеспечения безопасности должны включать: - Восстановление функций систем безопасности - Идентификацию и регистрацию длительности (даты и времени от начала до конца) отказа систем безопасности - Идентификацию и регистрацию причины (причин) отказа, включая	Удостовериться в наличии документа или процесса по реагированию на отказы систем и серверов сегмента ИСП.

	основную причину, и регистрацию исправлений, требуемых для устранения основной причины - Выявление и устранение любых проблем безопасности, возникающих в ходе отказа - Выполнение оценки рисков с целью определения необходимости выполнения дальнейших действий в результате отказа механизмов защиты - Осуществление контроля для предотвращения повторного возникновения причины отказа - Возобновление мониторинга контроля безопасности	