ComTRUST

ComTRUST CyberSecurity, LLC
US, 90013, California, Los Angeles, S. Hill Street, 448, office 235
+13232325390
WEB: comtrust.by

ComTRUST

ООО «КомТРАСТ КиберСекьюрити»
США, 90013, Калифорния, Лос Анджелес, С. Хилл Стрит, офис 235
+13232325390
WEB: comtrust.by

Единые стандарты для платежных систем (SSPS)

Версия: **1.0**

Дата вступления в силу: **11.08.2024**

1. Содержание

2. Основные понятия

Сервис — веб-программа или платформа, размещённая в сети Интернет, к которой применяются настоящие стандарты безопасности SSPS.
Веб-сайт — интернет-ресурс, который может включать в себя один или несколько Сервисов.
Пользователь — лицо, посетившее Сервис и прошедшее в нём регистрацию (при наличии такой возможности).
Разработчик — физическое или юридическое лицо, отвечающее за техническую реализацию и функционирование Сервиса.
Владелец сервиса — физическое или юридическое лицо, обладающее правами собственности на Сервис и несущее ответственность за его работу и соответствие стандартам SSPS.
Администрация сервиса — группа лиц, занимающаяся управлением и курированием работы сервиса.
Техническая поддержка сервиса — группа лиц, оказывающая Пользователю поддержку по всем вопросам, возникшим у него при работе с Сервисом.
Юридическое лицо — тоже самое, что и Разработчик.
Хостинг-провайдер — физическое или юридическое лицо, оказывающее Разработчику услуги по размещению Сервиса на серверах.
Персональные данные — любая информация, относящаяся к прямо или косвенно определенному или определяемому Пользователю.
Платежная информация — данные, связанные с финансовыми транзакциями Пользователя, включая, но не ограничиваясь, номера банковских карт, данные счетов и истории платежей.
Аккредитация — процесс проверки Сервиса Аккредитованным проверяющим или Уполномоченными организациями на соответствие стандартам безопасности SSPS.
Аккредитованный проверяющий — лицо, оказывающее услуги Аккредитации Сервиса.
Уполномоченные организации (Аккредитованного проверяющего) — лица, уполномоченные Аккредитованным проверяющим на оказание услуг Аккредитации Сервиса.
Процесс деаккредитации — процесс обнуления Аккредитации Сервиса на соответствие настоящим стандартам безопасности вследствие их несоблюдения Разработчиком. Данный процесс проводится Аккредитованным проверяющим.

Дополнительные технические понятия доступны в Глоссарии технических терминов (см. Приложение).

3. Предисловие

Стремительное развитие цифровых технологий и электронной коммерции привело к значительному росту онлайн-платежей. Вместе с этим возросли риски, связанные с кибербезопасностью и защитой данных пользователей. В ответ на эти вызовы компания ComTRUST разработала **Единые стандарты для платежных систем (SSPS)**.

SSPS представляет собой комплексный набор требований и рекомендаций, направленных на обеспечение высокого уровня безопасности и надежности платежных систем. Эти стандарты учитывают лучшие мировые практики и соответствуют актуальным угрозам в сфере кибербезопасности.

Цель **SSPS** — предоставить четкие и измеримые критерии для оценки безопасности платежных систем, а также способствовать повышению доверия пользователей к онлайн-транзакциям. Соответствие требованиям **SSPS** подтверждает, что веб-сайт или платежная система отвечает высоким стандартам защиты данных и финансовой информации.

Данный документ предназначен для разработчиков платежных систем, специалистов по информационной безопасности, аудиторов и всех заинтересованных сторон в сфере электронных платежей. Мы призываем к активному применению этих стандартов для создания более безопасной и надежной среды онлайн-платежей.

ComTRUST обязуется регулярно обновлять **SSPS**, чтобы стандарты оставались актуальными и эффективными в противодействии новым угрозам кибербезопасности.

4. Введение

4.1. Цель документа

Целью данного документа является установление единых стандартов безопасности для платежных систем (SSPS), обеспечивающих высокий уровень защиты пользователей и их данных при осуществлении онлайн-платежей.

4.2. Область применения

Настоящие стандарты применяются ко всем Сервисам, прошедшим Аккредитацию.

4.3. Нормативные ссылки

При разработке данных стандартов учтены требования следующих нормативных правовых актов Республики Беларусь:

- Закон Республики Беларусь от 10 ноября 2008 г. № 455-З "Об информации, информатизации и защите информации"
- Закон Республики Беларусь от 7 мая 2021 г. № 99-З "О защите персональных данных"
- Закон Республики Беларусь от 28 июля 2003 г. № 231-З "О торговле"
- Постановление Совета Министров Республики Беларусь от 18 мая 2019 г. № 311 "Об утверждении Концепции информационной безопасности Республики Беларусь"
- Указ Президента Республики Беларусь от 1 февраля 2010 г. № 60 "О мерах по совершенствованию использования национального сегмента сети Интернет"
- Постановление Правления Национального банка Республики Беларусь от 18 мая 2020 г. № 155 "Об утверждении Инструкции о порядке функционирования единого расчетного и информационного пространства Республики Беларусь"

Стандарты SSPS разработаны в соответствии с этими нормативными актами и дополняют их требования в части обеспечения безопасности онлайн-платежей и защиты данных пользователей.

5. Общие положения

5.1. Принципы безопасности SSPS

Стандарты SSPS основаны на следующих ключевых принципах:

1. **Конфиденциальность**: Обеспечение защиты персональных данных и платежной информации пользователей от несанкционированного доступа.

2. **Целостность**: Гарантия неизменности данных при их хранении и передаче.

3. **Доступность**: Обеспечение бесперебойного функционирования платежных систем и доступа пользователей к своим данным.

4. **Аутентичность**: Подтверждение подлинности пользователей и транзакций.

5. **Прозрачность**: Предоставление пользователям полной информации о мерах безопасности и обработке их данных.

6. **Масштабируемость**: Возможность применения стандартов к платежным системам различного масштаба и сложности.

7. **Актуальность**: Регулярное обновление стандартов в соответствии с развитием технологий и появлением новых угроз.

5.2. Структура стандартов

Стандарты SSPS включают следующие основные разделы:

1. Защита персональных данных пользователей
   - Методы сбора и хранения данных
   - Правила обработки и передачи информации
   - Механизмы удаления данных по запросу пользователя

2. Безопасность финансовых транзакций
   - Протоколы безопасной передачи финансовой информации
   - Методы верификации транзакций
   - Системы предотвращения мошенничества

3. Аутентификация и авторизация пользователей
   - Требования к паролям и другим методам аутентификации
   - Многофакторная аутентификация
   - Управление сессиями пользователей

4. Шифрование данных
   - Стандарты шифрования при передаче данных
   - Требования к хранению зашифрованных данных
   - Управление ключами шифрования

5. Мониторинг и предотвращение мошенничества
   - Системы обнаружения аномалий
   - Процедуры реагирования на инциденты
   - Анализ и отчетность по безопасности

6. Обеспечение целостности и доступности систем
   - Требования к отказоустойчивости инфраструктуры
   - Планы аварийного восстановления
   - Регулярное резервное копирование данных

7. Процедуры аккредитации и аудита
   - Методология проведения аккредитации
   - Периодичность проверок
   - Требования к аккредитованным проверяющим
   - Официальная регистрация платёжного сервиса

Каждый раздел содержит конкретные требования, рекомендации по внедрению и критерии оценки соответствия. Соблюдение всех разделов стандартов SSPS обеспечивает комплексную защиту платежных систем и данных пользователей.

6. Требования безопасности

6.1. Управление информационной безопасностью

- Разработка и внедрение политики информационной безопасности
  • Создание комплексного документа, охватывающего все аспекты ИБ
  • Согласование политики с руководством и юридическим отделом
  • Регулярное обновление (минимум раз в год)

- Назначение ответственных лиц за информационную безопасность
  • Создание должности CISO (Chief Information Security Officer)
  • Формирование отдела информационной безопасности
  • Четкое определение ролей и обязанностей в области ИБ

- Регулярный пересмотр и обновление политик безопасности
  • Ежеквартальный анализ эффективности существующих политик
  • Учет новых угроз и изменений в законодательстве
  • Внесение корректировок на основе результатов аудитов и инцидентов

- Обучение персонала основам информационной безопасности
  • Разработка программы обучения для разных категорий сотрудников
  • Проведение регулярных тренингов (минимум раз в полгода)
  • Тестирование знаний сотрудников и проведение учебных фишинг-кампаний

6.2. Безопасность сетевой инфраструктуры

- Использование межсетевых экранов нового поколения
  • Внедрение NGFW с функциями IPS, антивирус, антиспам
  • Настройка правил фильтрации на основе приложений и пользователей
  • Регулярное обновление сигнатур и правил

- Сегментация сети для изоляции критичных систем
  • Разделение сети на VLAN'ы по функциональному признаку
  • Изоляция систем обработки платежей в отдельный сегмент
  • Использование технологий микросегментации для контейнеров и виртуальных машин

- Защита от DDoS-атак
  • Использование специализированных решений для защиты от DDoS
  • Настройка фильтрации трафика на уровне провайдера
  • Разработка плана реагирования на DDoS-атаки

- Регулярное сканирование сети на уязвимости
  • Еженедельное сканирование внешнего периметра
  • Ежемесячное полное сканирование внутренней сети

  • Оперативное устранение обнаруженных уязвимостей

- Безопасная конфигурация сетевого оборудования
  • Использование шаблонов безопасной конфигурации
  • Отключение неиспользуемых портов и сервисов
  • Регулярный аудит конфигураций

6.3. Контроль доступа

- Внедрение принципа наименьших привилегий
  • Предоставление пользователям только необходимых для работы прав
  • Регулярный пересмотр и корректировка прав доступа
  • Использование ролевой модели доступа (RBAC)

- Использование многофакторной аутентификации для критичных систем
  • Обязательное использование MFA для административного доступа
  • Внедрение MFA для пользователей при работе с чувствительными данными
  • Поддержка различных методов второго фактора (SMS, токены, биометрия)

- Регулярный аудит прав доступа
  • Ежеквартальный пересмотр прав доступа всех пользователей
  • Автоматизация процесса аудита с использованием специализированных решений
  • Немедленное удаление прав доступа при увольнении сотрудника

- Автоматическое блокирование неактивных учетных записей
  • Настройка автоблокировки учетных записей после 30 дней неактивности
  • Уведомление администраторов о заблокированных учетных записях
  • Процедура проверки и реактивации или удаления неактивных учетных записей

- Сложные требования к паролям и их регулярная смена
  • Минимальная длина пароля - 12 символов
  • Использование комбинации букв, цифр и специальных символов
  • Принудительная смена паролей каждые 90 дней
  • Запрет на повторное использование последних 10 паролей

6.4. Шифрование данных

- Использование современных алгоритмов шифрования
  • Применение AES-256 для симметричного шифрования
  • Использование RSA-4096 или ECC для асимметричного шифрования
  • Регулярный пересмотр используемых алгоритмов (минимум раз в год)

- Шифрование данных при передаче

• Обязательное использование TLS 1.3 для всех внешних соединений
• Отключение поддержки устаревших протоколов (SSL, TLS 1.0/1.1)
• Настройка HSTS для принудительного использования HTTPS

- Шифрование данных в состоянии покоя
• Шифрование всех носителей информации, содержащих чувствительные данные
• Использование аппаратного шифрования для мобильных устройств
• Шифрование баз данных на уровне столбцов с чувствительной информацией

- Безопасное управление ключами шифрования
• Использование специализированных систем управления ключами (KMS)
• Регулярная ротация ключей шифрования (минимум раз в год)
• Строгий контроль доступа к ключам шифрования

- Регулярное обновление криптографических протоколов
• Мониторинг новостей и рекомендаций в области криптографии
• Своевременное обновление библиотек и компонентов, отвечающих за шифрование
• Планирование перехода на постквантовую криптографию

6.5. Безопасность приложений

- Проведение анализа безопасности кода
• Использование автоматизированных инструментов статического анализа кода
• Проведение ручного анализа кода для критичных компонентов
• Интеграция проверок безопасности в процесс CI/CD

- Защита от OWASP TOP-10 уязвимостей
• Разработка и внедрение чек-листов для защиты от каждой уязвимости из OWASP TOP-10
• Регулярное обучение разработчиков по вопросам безопасной разработки
• Использование WAF для дополнительной защиты от распространенных атак

- Регулярное обновление и патчинг приложений
• Установка критических обновлений безопасности в течение 24 часов
• Ежемесячное обновление всех компонентов системы
• Автоматизация процесса отслеживания и установки обновлений

- Использование безопасных методов разработки (SDL)
• Внедрение практик безопасной разработки на всех этапах жизненного цикла ПО
• Проведение анализа угроз на этапе проектирования

• Обязательное проведение тестирования на проникновение перед релизом

- Проведение регулярного пентестинга
  • Ежегодное проведение полного пентеста внешнего периметра
  • Ежеквартальное проведение пентеста критичных приложений
  • Привлечение внешних экспертов для проведения пентестов

6.6. Мониторинг и аудит

- Внедрение системы SIEM для сбора и анализа логов
  • Централизованный сбор логов со всех критичных систем
  • Настройка корреляционных правил для выявления инцидентов
  • Хранение логов не менее 1 года

- Мониторинг аномальной активности в режиме реального времени
  • Использование систем обнаружения и предотвращения вторжений (IDS/IPS)
  • Внедрение систем поведенческого анализа (UEBA)
  • Настройка оповещений о подозрительной активности

- Регулярные внутренние и внешние аудиты безопасности
  • Проведение внутреннего аудита безопасности раз в квартал
  • Ежегодный внешний аудит на соответствие стандартам (PCI DSS, ISO 27001)
  • Разработка и выполнение плана по устранению выявленных недостатков

- Ведение журналов доступа и изменений в критичных системах
  • Логирование всех действий привилегированных пользователей
  • Отслеживание изменений в конфигурациях критичных систем
  • Обеспечение целостности и неизменности журналов аудита

- Анализ и реагирование на инциденты безопасности
  • Создание процедур для различных типов инцидентов
  • Определение метрик и KPI для оценки эффективности реагирования
  • Регулярный анализ инцидентов для улучшения процессов безопасности

6.7. Управление инцидентами

- Разработка плана реагирования на инциденты
  • Создание детального документа с описанием процедур реагирования
  • Определение ролей и ответственностей в процессе реагирования
  • Регулярное обновление плана (минимум раз в год)

- Создание команды реагирования на инциденты (CERT)
  • Формирование междисциплинарной команды специалистов
  • Обеспечение 24/7 доступности команды

• Проведение регулярных тренингов для членов команды

- Регулярные тренировки по реагированию на инциденты
• Проведение симуляций различных типов инцидентов
• Отработка взаимодействия между различными отделами
• Анализ результатов тренировок и внесение улучшений в процессы

- Анализ инцидентов и извлечение уроков
• Проведение постмортемов после каждого серьезного инцидента
• Документирование извлеченных уроков и рекомендаций
• Внедрение улучшений на основе анализа инцидентов

- Своевременное информирование пользователей о серьезных инцидентах
• Разработка шаблонов уведомлений для различных типов инцидентов
• Определение критериев для обязательного информирования пользователей
• Обеспечение прозрачности и честности в коммуникации с пользователями

6.8. Непрерывность бизнеса

- Разработка и тестирование плана обеспечения непрерывности бизнеса
• Проведение анализа влияния на бизнес (BIA)
• Определение критичных бизнес-процессов и систем
• Ежегодное полное тестирование плана непрерывности бизнеса

- Создание и поддержание резервных копий данных
• Внедрение стратегии резервного копирования 3-2-1
• Ежедневное инкрементное и еженедельное полное резервное копирование
• Регулярное тестирование восстановления из резервных копий

- Обеспечение отказоустойчивости критичных систем
• Внедрение кластерных решений для ключевых сервисов
• Использование балансировщиков нагрузки и географически распределенных ЦОДов
• Автоматическое переключение на резервные системы при сбоях

- Регулярное тестирование процедур восстановления
• Ежеквартальное тестирование восстановления отдельных систем
• Ежегодное полное тестирование аварийного восстановления
• Документирование и анализ результатов тестирований

- Наличие альтернативных каналов связи и обработки платежей
• Обеспечение резервных каналов связи (спутниковая связь, резервные провайдеры)

- Наличие договоренностей с альтернативными платежными провайдерами
- Разработка процедур перехода на альтернативные каналы в случае сбоев

Данные требования могут быть дополнены или улучшены на усмотрение Разработчика или Владельца веб-сайта.

7. Процедура оценки соответствия

7.1. Методология оценки

- Комплексный анализ веб-сайта:
  • Проверка безопасности Frontend и Backend компонентов
  • Анализ обработки и хранения пользовательских данных
  • Оценка защиты API и интеграций с внешними сервисами

- Техническое тестирование:
  • Автоматизированное сканирование на уязвимости
  • Ручное тестирование критических функций
  • Проверка безопасности мобильных версий (если применимо)

- Оценка процессов:
  • Анализ процедур обновления и патч-менеджмента
  • Проверка процессов реагирования на инциденты
  • Оценка практик разработки и тестирования

- Периодичность оценки:
  • Первичная полная оценка
  • Ежегодная переоценка
  • Внеплановые проверки при существенных изменениях на сайте

7.2. Критерии соответствия

- Ключевые области оценки веб-сайта:
  • Защита от распространенных веб-уязвимостей (OWASP TOP-10)
  • Безопасность аутентификации и управления сессиями
  • Шифрование данных в transit и at rest
  • Безопасность обработки платежной информации
  • Защита от DDoS-атак и других внешних угроз

- Количественные метрики:
  • Количество критических, высоких и средних уязвимостей
  • Время устранения выявленных уязвимостей
  • Процент успешно отраженных тестовых атак

- Качественные критерии:
  • Наличие и качество документации по безопасности
  • Регулярность обновлений системы безопасности
  • Прозрачность в коммуникации с пользователями о вопросах безопасности

7.3. Процесс сертификации

- Этапы сертификации веб-сайта:
  1. Подача заявки владельцем сайта
  2. Предварительная самооценка с использованием предоставленных инструментов
  3. Удаленный аудит веб-сайта аккредитованным проверяющим
  4. Устранение выявленных несоответствий (если необходимо)
  5. Финальная проверка и принятие решения о сертификации
  6. Выдача цифрового значка SSPS для размещения на сайте

- Требования к владельцам сайтов:
  • Предоставление полного доступа к тестовой версии сайта
  • Своевременное устранение выявленных уязвимостей
  • Информирование о существенных изменениях в структуре или функционале сайта

- Срок действия сертификации:
  • 1 год с возможностью продления

- Поддержание сертификации:
  • Ежеквартальное автоматизированное сканирование
  • Обязательное информирование о серьезных инцидентах безопасности

- Отзыв сертификации:
  • Критерии: серьезные нарушения безопасности, отказ от устранения критических уязвимостей
  • Процедура апелляции для владельцев сайтов
  • Публичное уведомление об отзыве сертификации

Приложение

Приложение А. Контрольный список для самооценки

Этот контрольный список предназначен для помощи организациям в самостоятельной оценке соответствия стандартам SSPS. Используя этот список, компании могут убедиться, что их системы и процессы соответствуют установленным требованиям безопасности.

1. Защита персональных данных пользователей:

- Определены методы безопасного сбора и хранения персональных данных.
- Реализованы правила обработки и передачи информации в соответствии с требованиями SSPS.
- Внедрены механизмы, позволяющие пользователю запрашивать удаление своих данных.

2. Безопасность финансовых транзакций:

- Применяются протоколы для безопасной передачи финансовой информации.
- Внедрены надежные методы верификации транзакций.
- Действуют системы предотвращения и выявления мошеннических действий.

3. Аутентификация и авторизация пользователей:

- Установлены требования к паролям и другим методам аутентификации.
- Используются многофакторные методы аутентификации (MFA).
- Организовано управление сессиями пользователей с учетом безопасности.

4. Шифрование данных:

- Применяются стандарты шифрования для передачи данных.
- Соблюдаются требования к хранению зашифрованных данных.
- Управление ключами шифрования проводится в соответствии с установленными правилами.

5. Мониторинг и предотвращение мошенничества:

- Внедрены системы обнаружения аномалий в работе сервисов.

- Описаны и задокументированы процедуры реагирования на инциденты безопасности.
- Проводится регулярный анализ и составление отчетности по вопросам безопасности.

6. Обеспечение целостности и доступности систем:

- Система соответствует требованиям к отказоустойчивости инфраструктуры.
- Разработаны и тестируются планы аварийного восстановления.
- Внедрены регулярные процедуры резервного копирования данных.

7. Процедуры аккредитации и аудита:

- Определена методология проведения аккредитации.
- Установлена периодичность проверок на соответствие стандартам SSPS.
- Соблюдаются требования к аккредитованным проверяющим и ведется регистрация платёжных сервисов.

Приложение В. Глоссарий технических терминов

Этот глоссарий содержит определения ключевых технических терминов, используемых в стандартах SSPS, для обеспечения единого понимания их значений.

- **Аутентификация** — процесс проверки подлинности пользователя или системы. Включает в себя подтверждение личности с использованием пароля, биометрических данных, токенов или других методов.
- **Многофакторная аутентификация (MFA)** — метод защиты, требующий от пользователя предоставления двух или более подтверждающих факторов для доступа к системе. MFA повышает уровень безопасности по сравнению с одной только аутентификацией с паролем.
- **Авторизация** — процесс предоставления пользователю или системе прав на выполнение определённых действий или доступ к определённым ресурсам после успешной аутентификации.
- **Шифрование** — процесс преобразования данных в зашифрованный формат, который недоступен для неавторизованных пользователей. Шифрование может применяться как при передаче данных (например, через интернет), так и при их хранении.
- **Протокол** — набор правил и стандартов, определяющих обмен данными между системами или устройствами. В контексте SSPS протоколы безопасной передачи данных обеспечивают защиту финансовой информации.
- **Ключ шифрования** — секретная информация, используемая в криптографических алгоритмах для шифрования и расшифровки

данных. Без правильного ключа доступ к зашифрованным данным невозможен.

- **Резервное копирование данных** — процесс создания копий данных, которые могут быть использованы для восстановления информации в случае её утраты или повреждения.
- **Отказоустойчивость** — способность системы продолжать работу в случае сбоя или неисправности её компонентов. Отказоустойчивость достигается за счёт дублирования ключевых элементов системы.
- **Аварийное восстановление** — процесс восстановления работы системы после серьёзного сбоя или катастрофы. Включает планы по восстановлению данных и инфраструктуры.
- **Мониторинг безопасности** — процесс непрерывного отслеживания активности в системе для выявления подозрительных действий или попыток несанкционированного доступа.
- **Управление инцидентами безопасности** — набор процедур и действий, которые выполняются при обнаружении инцидента безопасности, с целью минимизации ущерба и восстановления нормальной работы системы.
- **Обнаружение аномалий** — процессы и технологии, которые выявляют отклонения от нормального поведения системы, что может указывать на попытки взлома или мошенничества.
- **Платёжная информация** — данные, связанные с финансовыми транзакциями, такие как номера банковских карт, счета, история платежей. Эти данные подлежат шифрованию и защите в соответствии с требованиями SSPS.
- **Аккредитация** — процесс формального подтверждения соответствия системы или сервиса требованиям безопасности SSPS. Аккредитация проводится уполномоченными проверяющими.
- **Сертификация** — документальное подтверждение соответствия сервиса установленным стандартам и требованиям безопасности.
- **Фишинг** — тип кибератаки, при котором злоумышленники пытаются получить конфиденциальную информацию, выдавая себя за доверенные источники.
- **Мошенничество с финансовыми транзакциями** — любые действия, направленные на обман платёжной системы с целью получения финансовой выгоды, такие как использование украденных данных банковских карт.
- **Криптография** — наука и практика защиты информации с помощью методов шифрования, которая позволяет обеспечить конфиденциальность, целостность и подлинность данных.
- **Персональные данные** — информация, которая позволяет прямо или косвенно идентифицировать личность. Включает имя, адрес, контактные данные, а также уникальные идентификаторы.
- **Сервер** — компьютер или система, которая предоставляет ресурсы, данные, услуги или программы другим компьютерам, известным как клиенты, через сеть.

Приложение C. Примеры успешного внедрения SSPS

Этот раздел может содержать кейсы и примеры успешного внедрения стандартов SSPS в различных компаниях. Описания конкретных решений и достигнутых результатов помогут новым пользователям лучше понять ценность этих стандартов.

Пример содержания:

1. **Кейс 1: Внедрение SSPS в крупном интернет-магазине**
    - Описание проблемы: частые мошеннические транзакции
    - Реализованные решения: интеграция многофакторной аутентификации и системы мониторинга
    - Результаты: снижение уровня мошенничества на 80%
2. **Кейс 2: Обеспечение безопасности в банковской системе**
    - Описание проблемы: утечка персональных данных клиентов
    - Реализованные решения: усиление шифрования данных и разработка новых правил хранения данных
    - Результаты: полное устранение инцидентов утечки данных за год
3. **Кейс 3: Внедрение стандартов безопасности в стартапе**
    - Описание проблемы: отсутствие структурированной системы безопасности
    - Реализованные решения: создание комплексной системы безопасности на базе SSPS
    - Результаты: успешное прохождение аккредитации и повышение доверия клиентов

История изменений документа

- Версия 1.0 (от 11.08.2024)

Последняя версия данного документа доступна на официальном сайте SSPS (https://spss.comtrust.by).

Информация об авторском праве