Обзор PCI DSS

Защищаемые активы

Вид информации	Обозначение	Определение
Номер платёжной карты	PAN	Номер, идентифицирующий платёжную карту. Наносится на лицевую или оборотную сторону физической платёжной карты, а также может отображаться в личном кабинете приложения компании-эмитента.
Имя держателя платёжной карты	CH.NAME	Имя и фамилия человека, которому банк предоставил право распоряжения платёжной картой. Наносится на лицевую или оборотную сторону физической платёжной карты.
Дата окончания действия платёжной карты	EXP.DATE	Дата, после которой платёжная карта становится недействительной. Наносится на лицевую или заднюю сторону физической платёжной карты, а также может отображаться в личном кабинете приложения компании-эмитента.

Защищаемые активы *(продолжение)*

Вид информации	Обозначение	Определение
Сервисный код	SERVICE CODE	Служебное значение, содержащееся на магнитной полосе и (или) чипе платёжной карты.
Содержимое магнитной полосы платёжной карты	TRACK, TRACK2	Вся информация, содержащаяся на магнитной полосе платёжной карты.
Содержимое чипа платёжной карты	Chip equivalent data	Вся информация, содержащаяся на чипе платёжной карты.

Защищаемые активы *(продолжение)*

Вид информации	Обозначение	Определение
Проверочное значение платёжной карты	CVV2, CVC2, CVP2, ППК2	Значение, используемое для авторизации платёжной транзакции в электронной коммерции. Наносится на оборотную сторону физической платёжной карты, а также может отображаться в личном кабинете приложения компании-эмитента.
ПИН-код	PIN	Значение, вводимое держателем карты на банкоматах или POS-терминалах для авторизации транзакции.
ПИН-блок	PIN-Block	Значение, используемое для авторизации транзакции на банкоматах и POS-терминалах. Получается из обычного PIN путем преобразования в один из общепринятых форматов.

Защищаемые активы *(продолжение)*

Актив	Категория	Вид информации	Правила хранения
Данные платёжной карты (ДПК)	**Данные о держателе карты (ДДК)**	PAN	При хранении следует применять один из методов защиты согласно требованию 3.5 стандарта PCI DSS. При хранении следует применять один из методов защиты согласно требованию 3.5 стандарта PCI DSS.
		CH.NAME	Разрешается хранить.
		EXP.DATE	
		SERVICE CODE	
	Критичные аутентификационные данные (КАД)	TRACK, TRACK2	Запрещается хранить после авторизации транзакции. Даже в зашифрованном виде. Исключением являются эмиссионные бизнес-процессы, в рамках которых для хранения КАД есть явное обоснование. КАД при этом необходимо защищать с использованием стойкой криптографии.
		Chip equivalent data	
		CVV2, CVC2, CVP2, ППК2	
		PIN	
		PIN-Block	

Область применимости требований PCI DSS

Компонент информационной инфраструктуры – любая система, работающая в информационной инфраструктуре Компании. Например, сервер, сетевое устройство, виртуальная машина, средство защиты информации, гипервизор, промежуточное ПО, СУБД, бизнес-приложение.

Область применимости требований PCI DSS – совокупность компонентов информационной инфраструктуры, работников, документации и локаций компании, к которым применимы требования стандарта PCI DSS.

Область применимости требований PCI DSS

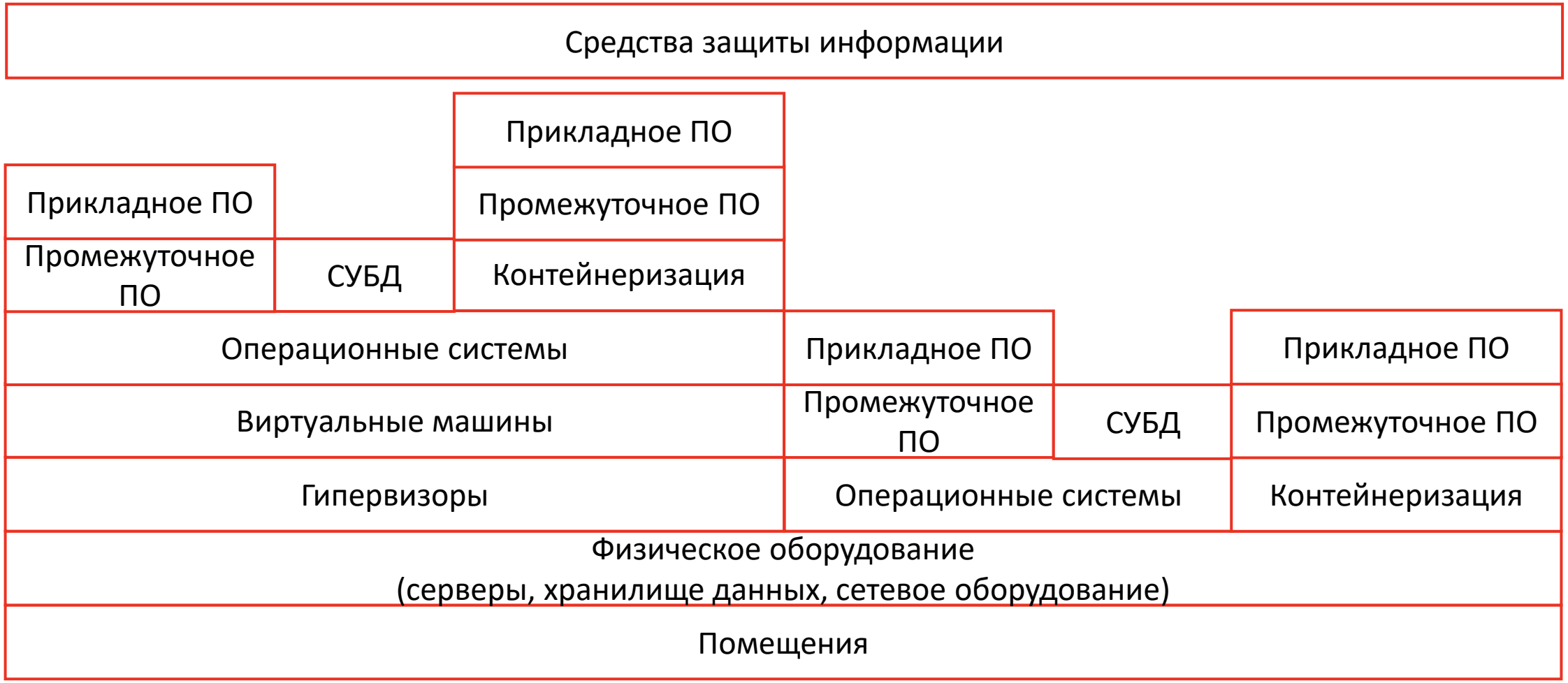
(продолжение)

Состав области применимости требований PCI DSS:

- Среда обработки данных платежных карт (Cardholder Data Environment, CDE):
  a) компонент хранит, обрабатывает или передает данные платежных карт;
  b) компонент находится в одном сегменте сети с компонентами из пункта (a);
- Смежные или влияющие на безопасность компоненты информационной инфраструктуры (Connected-to or Security-impacting Systems):
  a) компоненты, необходимые для выполнения требований самого стандарта;
  b) компоненты, влияющие на конфигурацию или безопасность CDE;
  c) компоненты, обеспечивающие сегментацию в области применимости.

Верификация области применимости происходит в рамках тестирования на проникновение и тестирования средств сегментации.

Слои информационной инфраструктуры, входящие в область применимости PCI DSS



Структура PCI DSS

Стандарт PCI DSS v. 4.0 содержит двенадцать основных разделов с требованиями и три приложения для разного типа компаний:

Раздел 1. Защита вычислительной сети.

Раздел 2. Конфигурация компонентов информационной инфраструктуры.

Раздел 3. Защита хранимых данных о держателях карт.

Раздел 4. Защита передаваемых данных о держателях карт.

Раздел 5. Антивирусная защита информационной инфраструктуры.

Раздел 6. Разработка и поддержка информационных систем.

Раздел 7. Управление доступом к данным о держателях карт.

Структура PCI DSS *(продолжение)*

Раздел 8. Механизмы аутентификации.

Раздел 9. Физическая защита информационной инфраструктуры.

Раздел 10. Протоколирование событий и действий.

Раздел 11. Контроль защищенности информационной инфраструктуры.

Раздел 12. Управление информационной безопасностью.

Приложение A1. Требования для поставщиков услуг совместного хостинга.

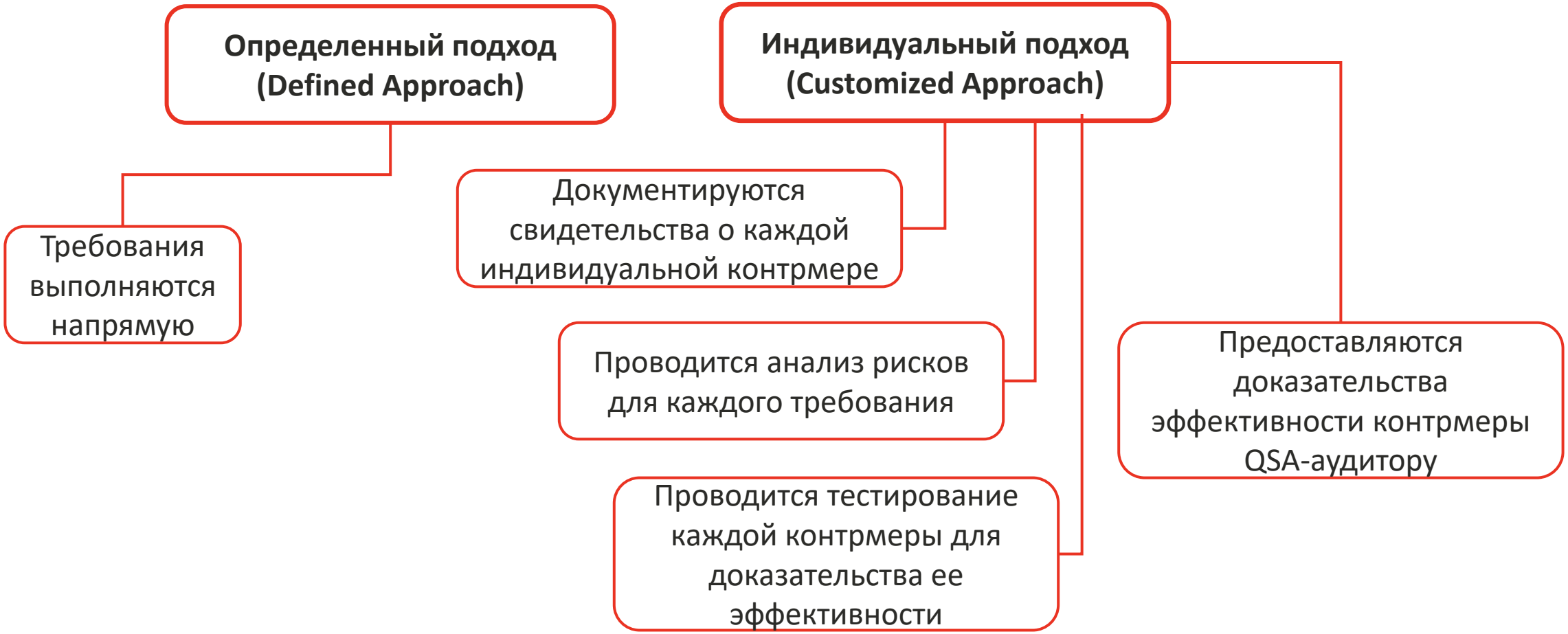
Приложение A2. Требования для компаний, использующих протокол SSL и ранние версии протокола TLS для соединения POS POI устройств с серверной частью.

Приложение A3. Дополнительные требования, для внедрения PCI DSS на Business-as-usual основе.

Способы внедрения PCI DSS *(продолжение)*

	Определенный подход	Компенсационные меры	Индивидуальный подход
В каком случае применяется?	По умолчанию.	Когда для выполнения требования на прямую существует либо техническое ограничение, либо ограничения с точки зрения бизнеса, либо ограничение с точки зрения законодательства.	После анализа рисков компанией.
Что из себя представляет контрмера?	Контрмера, описанная в стандарте для конкретного требования.	Контрмера, спроектированная компанией на основе анализа рисков.	Контрмера, спроектированная компанией на основе анализа рисков.
Для каких требований можно применять?	Для всех.	Для всех.	Для тех, у которых явно обозначена такая возможность.
Какие условия внедрения контрмеры?	Полностью внедрить контрмеру, описанную в стандарте.	Внедрить контрмеру, которая позволит выполнить цель требования и которая по уровню безопасности не ниже, чем контрмера, описанная в стандарте.	Внедрить контрмеру, которая позволит выполнить цель требования и которая по уровню безопасности не ниже, чем контрмера, описанная в стандарте.

Подходы к выполнению требований PCI DSS v. 4.0



Особенности Индивидуального подхода

- Индивидуальные контрмеры должны обеспечивать уровень безопасности не ниже, чем контрмеры, описанные в Определенном подходе (Defined Approach).
- Индивидуальный подход больше всего подходит зрелым компаниям, имеющим выстроенный процесс управления рисками информационной безопасности.
- Почти для каждого отдельно взятого требования можно применять как Определенный, так и Индивидуальный подход.
- Индивидуальный подход требует уровень документирования выше, чем Определенный подход.
- При заполнении листов самооценки любого типа (SAQ) компания не может использовать Индивидуальный подход. Либо SAQ и Определенный подход для него, либо QSA и возможность применять Индивидуальный подход.

Индивидуальный подход не применим

- Запрет на хранение критичных аутентификационных данные после авторизации транзакции (требование 3.3.1).
- Шифрование критичных аутентификационных данных, пока они хранятся до авторизации транзакции (требование 3.3.2).
- Если используется шифрование на уровне диска, то такое шифрование допустимо использовать только на съемных носителях. В остальных случаях требуется применять дополнительные меры для шифрования PAN (требование 3.5.1.2).
- ASV-сканирование (требование 11.3.2).
- Все требования Приложения A2 и A3.

Ответственность Организации при использовании Индивидуального подхода

- Документировать свидетельства о каждой примененной индивидуальной контрмере в виде Матрицы индивидуальных контрмер.
- Проводить таргетированный анализ рисков для каждого требования, выполненного с помощью индивидуального подхода.
- Тестировать каждую индивидуальную контрмеру для доказательства её эффективности.
- Осуществлять мониторинг и поддержку эффективности индивидуальных контрмер.
- Предоставлять QSA-аудитору Матрицу индивидуальных контрмер, Отчет об анализе рисков и свидетельства о проведенных тестированиях.

Ответственность QSA-аудитора при использовании Индивидуального подхода

- Изучить предоставленную документацию.
- Разработать индивидуальные проверочные процедуры для каждого требования, к которому применен Индивидуальный подход.
- Документировать разработанные индивидуальные проверочные процедуры.
- Проверить, что индивидуальные контрмеры внедрены и достигают целей требований, для которых они внедрены.
- Сформировать отчетные документы.

Состав Матрицы индивидуальных контрмер

Название индивидуальной контрмеры	*Формируется организацией*
Номер и цель требования PCI DSS	***Требование**: XXX; **Цель требования**: YYY*
Детали о внедрении индивидуальной меры	
Описание контрмеры	*Организация описывает состав контрмеры.*
Где контрмера внедрена?	*Организация идентифицирует все места, в которых индивидуальная контрмера внедрена.*
Когда выполняется контрмера?	*Организация описывает периодичность выполнения индивидуальной контрмеры.*

Состав Матрицы индивидуальных контрмер

(*продолжение*)

Кто несет ответственность за выполнение контрмеры?	*Организация определяет ответственного за выполнение индивидуальной контрмеры.*
Для каждого требования PCI DSS, в котором используется контрмера, организация описывает следующее	
Как внедренная контрмера позволяет достигнуть цели требования?	*Организация приводит описание, как индивидуальная контрмера позволяет достигнуть цели требования PCI DSS.*
Какие тесты были проведены?	*Организация приводит описание проведенных тестов, демонстрирующих, что индивидуальная контрмера позволяет достигнуть цели требования PCI DSS.*

Состав Матрицы индивидуальных контрмер

(*продолжение*)

Результаты анализа рисков	*Организация приводит краткое описание результатов проведенного анализа рисков с учетом внедрения индивидуальной контрмеры.*
Что выполняется для того, чтобы поддерживать на постоянной основе саму контрмеру, а также ее эффективность?	*Организация приводит описание того, что выполняется, чтобы поддерживать на постоянной основе саму индивидуальную контрмеру и ее эффективность.*

Компенсационные меры

Компенсационные меры – это метод выполнения требований PCI DSS, применяемый, когда организация не может их выполнить в силу обоснованных бизнес- или технических ограничений.

ВАЖНО! Компенсационные меры – это не «лазейка». Это способ обеспечить тот же уровень защиты, вместо получения Not In-Place из-за невыполнения требований напрямую из-за обоснованных ограничений.

Компенсационные меры (*продолжение*)

Компенсационная мера должна:

- обеспечивать достижение цели оригинального требования;
- обеспечивать аналогичный уровень защиты: риск должен быть снижен также эффективно, как если бы требование было выполнено;
- не быть переиспользованием других требований, которые и так должны быть выполнены (например, использование антивируса – это не компенсационная мера, но дополнительный функционал средства антивирусной защиты может быть использован для построения компенсационной меры).

Компенсационные меры (*продолжение*)

Для каждой компенсационной меры необходимо задокументировать:

- **Constraints:** в чем именно заключается бизнес- или техническое ограничение?
- **Objective:** какую цель преследует оригинальное требование?
- **Identified Risk:** какой риск возникает из-за невыполнения требования?
- **Validation:** как проверили, что меры работают?
- **Maintenance:** как поддерживается работоспособность и эффективность меры?

Компенсационные меры валидируются QSA-аудитором и не могут существовать дольше, чем наличие обоснованных ограничений.

Типы организаций

PCI DSS	НСПК (МИР)	VISA	MasterCard	AmEx	JCB	Discover
Merchant	ТСП	Merchant	Merchant	Merchant	Merchant	Merchant
Service Provider	Прямой участник	Issuer	Issuer (Principal or Affiliate)	Issuer (Principal or Affiliate)	Issuer	Issuer
	Косвенный участник	Acquirer	Acquirer (Principal or Affiliate)	Acquirer (Principal or Affiliate)	Acquirer	Acquirer
	Платежный поставщик услуг	VisaNet provider	Member Service Provider	Service Provider	Third Party Provider (TPP)	Service provider
	Расчетный центр	Third Party Agent (TPA)				

Уровни ТСП (Merchants)

Название ПС	Level 1	Level 2	Level 3	Level 4
МИР	обработка > 6 млн. транзакций в год по торговому эквайрингу и электронной коммерции (e-commerce); компрометация ДПК (статус на год); Подтверждение соответствия: • **QSA или ISA ежегодно;** • **отправка AOC ежегодно;** • **ASV ежеквартально.**	обработка от 1 до 6 млн. транзакций в год по торговому эквайрингу и электронной коммерции (e-commerce). Подтверждение соответствия: • **QSA или ISA ежегодно не в полном объеме (1 и 2 шаг приоритетного подхода);** • **отправка AOC ежегодно;** • **ASV ежеквартально.**	обработка от 20 000 до 1 млн. транзакций в год по электронной коммерции (e-commerce). Подтверждение соответствия: • **SAQ ежегодно;** • **ASV ежеквартально.**	обработка до 20 000 транзакций в год по электронной коммерции (e-commerce); до 1 млн. транзакций в год по торговому эквайрингу. Подтверждение соответствия: • **QSA, ISA или SAQ ежегодно (на усмотрение банка-эквайрера);** • **отправка AOC или SAQ ежегодно (на усмотрение банка-эквайрера);** • **ASV ежеквартально (на усмотрение банка-эквайрера).**

Уровни ТСП (Merchants) *(продолжение)*

Название ПС	Level 1	Level 2	Level 3	Level 4
Visa	обработка > 6 млн. транзакций в год; решение Visa о назначении уровня 1. Подтверждение соответствия: • **QSA или ISA ежегодно;** • **отправка AOC ежегодно;** • **ASV ежеквартально.**	обработка от 1 до 6 млн. транзакций в год. Подтверждение соответствия: • **SAQ ежегодно;** • **отправка AOC ежегодно;** • **ASV ежеквартально.**	обработка от 20 000 до 1 млн. транзакций в год по электронной коммерции (e-commerce). Подтверждение соответствия: • **SAQ ежегодно;** • **отправка AOC ежегодно;** • **ASV ежеквартально.**	обработка до 20 000 транзакций в год по электронной коммерции (e-commerce); до 1 млн. транзакций в год любым другим способом. Подтверждение соответствия: • **SAQ ежегодно;** • **отправка AOC ежегодно;** • **ASV ежеквартально (если применимо).**

Уровни ТСП (Merchants) *(продолжение)*

Название ПС	Level 1	Level 2	Level 3	Level 4
MasterCard	обработка > 6 млн. транзакций в год; решение MasterCard о назначении уровня 1; уровень 1 согласно критериям Visa; компрометация ДПК; Подтверждение соответствия: • **QSA или ISA ежегодно;** • **отправка AOC ежегодно;** • **ASV ежеквартально.**	обработка от 1 до 6 млн. транзакций в год; уровень 2 согласно критериям Visa. Подтверждение соответствия: • **SAQ ежегодно;** • **отправка AOC ежегодно;** • **ASV ежеквартально.** В случае заполнения SAQ A, SAQ A-EP или SAQ D мерчант обязан привлечь QSA или ISA для проверки соответствия. По желанию могут проходить QSA или ISA ежегодно вместо SAQ.	обработка от 20 000 до 1 млн. транзакций в год по электронной коммерции (e-commerce); уровень 3 согласно критериям Visa. Подтверждение соответствия: • **SAQ ежегодно;** • **отправка AOC ежегодно;** • **ASV ежеквартально.** По желанию могут проходить QSA или ISA ежегодно вместо SAQ.	все остальные. Подтверждение соответствия: • **SAQ ежегодно;** • **отправка AOC ежегодно;** • **ASV ежеквартально.** По желанию могут проходить QSA или ISA ежегодно вместо SAQ.

Уровни поставщиков услуг

Название ПС	Level 1	Level 2
МИР	Third Party Processors (TPP); обработка > 300 тыс. транзакций в год. Подтверждение соответствия: • **QSA ежегодно;** • **отправка AOC ежегодно;** • **ASV ежеквартально.**	обработка < 300 000 транзакций в год (кроме TPP). Подтверждение соответствия: • **SAQ-D MIR ежегодно;** • **отправка SAQ D AOC ежегодно;** • **ASV ежеквартально.**

Уровни поставщиков услуг *(продолжение)*

Название ПС	Level 1	Level 2
Visa	обработка > 300 тыс. транзакций в год; процессинг, напрямую подключенный к VisaNet (через VisaNet Extended Access Server, VEAS), (Third Party VNP, Visa Client VNP acting as Service Provider), независимо от количества транзакций; Visa Client Acquiring VNP в случае первичного подключения независимо от количества транзакций. Подтверждение соответствия: • **QSA ежегодно или ISA ежегодно (для Visa Client Acquiring VNP, если не первое подключение);** • **отправка AOC ежегодно;** • **ASV ежеквартально.** Visa Client Issuing VNP в случае первичного подключения и по запросу Visa должен предоставить одно из следующего: • QSA или ISA; • SAQ D AOC, подписанный руководством (CISO, Head of IT or Risk и т. д.).	обработка < 300 000 транзакций в год. Подтверждение соответствия: • **SAQ D ежегодно;** • **отправка SAQ D AOC ежегодно;** • **ASV ежеквартально.**

Уровни поставщиков услуг *(продолжение)*

Название ПС	Level 1	Level 2
MasterCard	обработка > 300 000 транзакций в год (для Data Storage Entities (DSEs) and Payment Facilitators (PFs)); все Third Party Processors (TPPs); все Staged Digital Wallet Operators (SDWOs); все Digital Activity Service Providers (DASPs); все Token Service Providers (TSPs); все 3-D Secure Service Providers (3-DSSPs); все AML/Sanctions Service Providers; все Installment Service Providers (ISPs). Подтверждение соответствия: • **QSA ежегодно;** • **отправка AOC ежегодно;** • **ASV ежеквартально.**	обработка < 300 000 транзакций в год (для Data Storage Entities (DSEs) and Payment Facilitators (PFs)); Все Terminal Servicers (TSs). Подтверждение соответствия: • **SAQ ежегодно;** • **отправка SAQ D AOC ежегодно;** • **ASV ежеквартально.** В качестве альтернативы DSE может предоставлять результат QPA раз в два года. В качестве альтернативы TS может предоставлять Terminal Servicer QIR Participation Validation Form (если применимо).

Внешний аудит (QSA)	Внутренний аудит (ISA)	Самооценка (SAQ)
Выполняется внешней аудиторской организацией (Qualified Security Assessor, QSA), сертифицированной Советом PCI SSC.	Выполняется внутренним прошедшим обучение и сертифицированным по программе Совета PCI SSC аудитором (Internal Security Assessor, ISA).	Выполняется самостоятельно путем заполнения листа самооценки (Self-Assessment Questionnaire, SAQ).
В ходе проверки QSA-аудиторы собирают свидетельства выполнения требований стандарта и сохраняют их в течение трех лет.	В ходе проверки ISA-аудиторы собирают свидетельства выполнения требований стандарта и сохраняют их в течение трех лет.	Сбор свидетельств выполнения требований стандарта не требуется.
По результатам QSA подготавливает Отчет о Соответствии (Report on Compliance, ROC).	По результатам ISA подготавливает Отчет о Соответствии (Report on Compliance, ROC).	Отчетным документом является самостоятельно (или с помощью аудитора) заполненный лист самооценки SAQ.
Применим для поставщиков услуг и торгово-сервисных предприятий.	Применим для торгово-сервисных предприятий только после успешного прохождения внешнего QSA-аудита.	Применим для поставщиков услуг и торгово-сервисных предприятий.
Рассматриваются все применимые к организации требования из всего стандарта PCI DSS.	Рассматриваются все применимые к организации требования из всего стандарта PCI DSS.	Рассматриваются все применимые требования к организации из листа самооценки SAQ в зависимости от сертифицируемого бизнес-процесса.

e-Commerce: SAQ A vs. SAQ A-EP

SAQ A:

- применим для iFrame или Redirect на платежную страницу сертифицированного платежного поставщика услуг;
- в этом случае сайт мерчанта вообще не видит ДПК, но влияет на их безопасность;
- небольшой объем требований, которые нужно выполнить.

SAQ A-EP:

- применим для Direct POST или Scripting, когда форма ввода данных ваша, но данные отправляются сертифицированному поставщику услуг;
- в этом случае сайт мерчанта принимает ДПК, а следовательно влияет на их безопасность в большей степени;
- объем требований сильно больше, чем в SAQ A.

POS/POI устройства

SAQ B:

- применим для старых терминалов (dial up) или импринтеров без Интернета и без хранения данных;

SAQ B-IP:

- применим для современных IP-терминалов, подключенных к сети, но изолированных от кассы и офисной сети;
- требует контроль сегментации (пентест);

SAQ P2PE:

- применим там, где мерчант использует сертифицированное P2PE-решение;
- самый короткий и простой лист самооценки;
- применяется не зависимо от количества транзакций (даже свыше 6 миллионов транзакций в год).

Мобильные и виртуальные терминалы

SAQ SPoC:

- Применим там, где используется сертифицированное SoftPOS решение с внешним ридером;

SAQ C-VT:

- применим для ручного ввода ДПК через виртуальный терминал в браузере;
- требует контроль сегментации (пентест);

SAQ C:

- применим для платежных приложений (например, POS-касса с терминалом для считывания карт), подключенных к Интернету;
- данные не должны храниться, но могут проходить через оперативную память кассы.

Для всех остальных

SAQ D:

- применим для всех поставщиков услуг;
- применим для ТСП, которые хранят ДДК;
- для всех, кто не прошли по критериям других листов самооценок.

Алгоритм выбора SAQ

- Вы поставщик услуг? Тогда это сразу SAQ D.
- Вы храните ДДК? Тогда это тоже сразу SAQ D.
- Вы принимаете оплату в Интернете (e-Commerce/card-not-present)?
  - Используете iFrame/Redirect? Тогда для вас SAQ A.
  - Используете Direct POST/Scripting? Тогда для вас SAQ A-EP.
- Вы принимаете оплату лично (retail/card-present)?
  - Используете P2PE решение? Тогда заполняете только P2PE.
  - Используете старые dial up терминалы? Вам нужен SAQ B.
  - У вас современные выделенные IP-терминалы? Заполняем SAQ B-IP.
  - У вас есть виртуальные терминалы? SAQ C-VT ваш выбор.
  - На ваших точках POS-касса с платежным приложением? Выбирайте SAQ C.

А что на счет DESV?

DESV – дополнительный набор требований (Appendix A3), которые идет в дополнение к основным 12 разделам PCI DSS.

Кто получает статус Designated Entities:

- организации, у кого были утечки ДПК;
- организации с огромным объемом транзакций (например, крупные агрегаторы, процессинги, шлюзы);
- те, кого МПС или эквайреры сочли высокорисковыми.
- является обязательным для сертификации бекенда в SPoC, CPoC решениях.

Философия DESV

Business-as-Usual (BAU):

- принцип от «для галочки» к «постоянству»;
- соответствие должно поддерживаться непрерывно, а не раз в год;
- любой сбой средства защиты должен быть мгновенно обнаружен, исправлен, а причина расследована;
- контроли работают 24/7/365.

Ключевые требования DESV

- **Управление:** создание комитета по PCI DSS, ежегодный отчет перед высшим руководством.
- **Область применимости:** валидация скоупа не раз в год, а минимум раз в квартал и при любых изменениях.
- **Контроль логического доступа:** пересмотр прав доступа раз в 6 месяцев, в том числе тестирование средств сегментации.
- **Детектирование:** расширенные требования к выявлению аномалий и подозрительной активности.

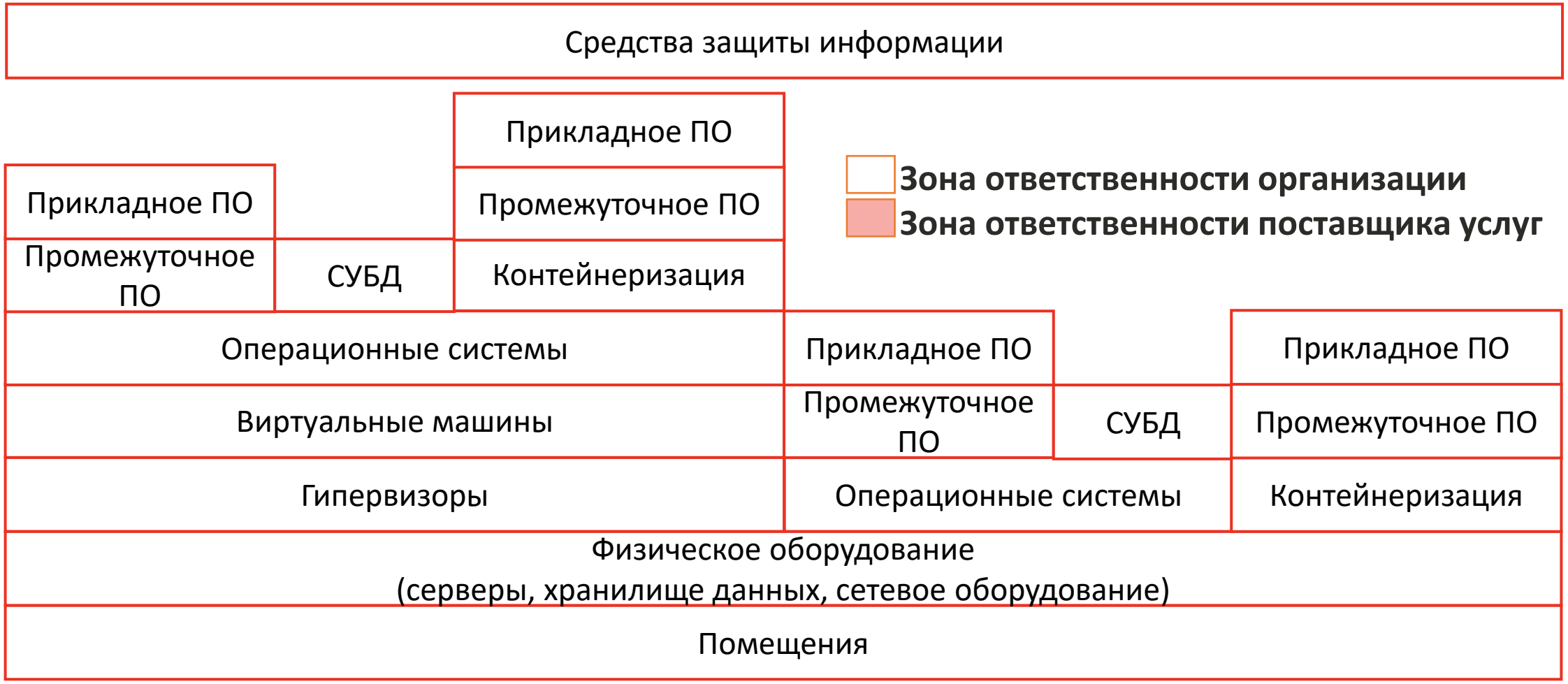
Отчетность DESV

DESV – это дополнительная оценка, соответственно нужен отдельный набор отчетных документов:

- вместе с основным ROC заполняется S-ROC;
- Вместе с основным AOC заполняется и подписывается S-AOC.

Нельзя пройти DESV, если неуспешно пройден основной PCI DSS.

Привлечение поставщиков услуг



Привлечение поставщиков услуг *(продолжение)*

Привлечение поставщиков услуг *(продолжение)*

Привлечение поставщиков услуг *(продолжение)*

Привлечение поставщиков услуг *(продолжение)*

Привлечение поставщиков услуг *(продолжение)*

Part 2. Executive Summary		
Part 2a. Scope Verification		
Services that were INCLUDED in the scope of the PCI DSS Assessment (check all that apply):		
Name of service(s) assessed:		
Type of service(s) assessed:		
Hosting Provider: ☐ Applications / software ☐ Hardware ☐ Infrastructure / Network ☐ Physical space (co-location) ☐ Storage ☐ Web ☐ Security services ☐ 3-D Secure Hosting Provider ☐ Shared Hosting Provider ☐ Other Hosting (specify):	**Managed Services (specify):** ☐ Systems security services ☐ IT support ☐ Physical security ☐ Terminal Management System ☐ Other services (specify):	**Payment Processing:** ☐ POS / card present ☐ Internet / e-commerce ☐ MOTO / Call Center ☐ ATM ☐ Other processing (specify):
☐ Account Management	☐ Fraud and Chargeback	☐ Payment Gateway/Switch
☐ Back-Office Services	☐ Issuer Processing	☐ Prepaid Services
☐ Billing Management	☐ Loyalty Programs	☐ Records Management
☐ Clearing and Settlement	☐ Merchant Services	☐ Tax/Government Payments
☐ Network Provider		
☐ Others (specify):		

***Note**: These categories are provided for assistance only, and are not intended to limit or predetermine an entity's service description. If you feel these categories don't apply to your service, complete "Others." If you're unsure whether a category could apply to your service, consult with the applicable payment brand.*

Part 2a. Scope Verification *(continued)*		
Services that are provided by the service provider but were NOT INCLUDED in the scope of the PCI DSS Assessment (check all that apply):		
Name of service(s) not assessed:		
Type of service(s) not assessed:		
Hosting Provider: ☐ Applications / software ☐ Hardware ☐ Infrastructure / Network ☐ Physical space (co-location) ☐ Storage ☐ Web ☐ Security services ☐ 3-D Secure Hosting Provider ☐ Shared Hosting Provider ☐ Other Hosting (specify):	**Managed Services (specify):** ☐ Systems security services ☐ IT support ☐ Physical security ☐ Terminal Management System ☐ Other services (specify):	**Payment Processing:** ☐ POS / card present ☐ Internet / e-commerce ☐ MOTO / Call Center ☐ ATM ☐ Other processing (specify):
☐ Account Management	☐ Fraud and Chargeback	☐ Payment Gateway/Switch
☐ Back-Office Services	☐ Issuer Processing	☐ Prepaid Services
☐ Billing Management	☐ Loyalty Programs	☐ Records Management
☐ Clearing and Settlement	☐ Merchant Services	☐ Tax/Government Payments
☐ Network Provider		
☐ Others (specify):		
Provide a brief explanation why any checked services were not included in the assessment:		

Перед началом взаимодействия с поставщиком услуг

- проверить благонадежность поставщика услуг;
- запросить Свидетельство о соответствии (Attestation of Compliance, AOC);
- согласовать Матрицу распределения ответственности (Responsibility Matrix);
- проверить наличие пунктов об ответственности за безопасность данных платежных карт в договорах/соглашения/оферте.

Доверяй, но проверяй

- **Оценка рисков:** какую часть бизнеса вы отдаете на аутсорс?
- **Проверка статуса:** есть ли у поставщика AOC?
- **Репутация:** была ли информация об инцидентах у поставщика? Есть ли судебные тяжбы, задолженности и т. п.?
- **Рекурсия:** а кто является поставщиками у этого поставщика?

Матрица ответственности

Однозначно определить:

- Что делаете только вы?
- Что делает только поставщик?
- Что вы делаете совместно, кто в каком объеме?

Соглашения с поставщиком

Поставщик должен письменно подтвердить:

- «да, мы берем ответственность за безопасность передаваемых данных»
- «да, мы соответствуем PCI DSS»

Мониторинг поставщиков

Вы обязаны минимум раз в год запрашивать у всех своих поставщиков актуальное свидетельство о соответствии требованиям PCI DSS - AOC.

Если их AOC истек – это будет ваша проблема на вашем аудите.

Если ваш хостинг, например, нанимает админов на аутсорсе или использует несертифицированного поставщика услуг, влияющего на безопасность ваших данных – это тоже ваши риски.

До заключения договора нужно однозначно определиться с возможными рисками и порядком их обработки в договоре.

Внедрение требований PCI DSS

Приоритетный подход к внедрению PCI DSS

В ответ на закономерный вопрос: «**С выполнения какого требования стандарта лучше начинать его внедрение?**» Советом PCI SSC был разработан документ под названием «Приоритетный подход к выполнению требований стандарта PCI DSS».

Приоритетный подход рекомендует выполнять требования в шесть этапов:

1. Удаление КАД и ограничение хранения ДДК.
2. Защита периметра, внутренних и беспроводных сетей.
3. Обеспечение безопасности приложений, БД и ОС.
4. Мониторинг и контроль доступа.
5. Защита хранимых данных.
6. Внедрение системы менеджмента информационной безопасности.

Этап 1. Удаление КАД и ограничение хранения ДДК

Данные платежных карт являются определяющим фактором применимости требований стандарта PCI DSS к компонентам.

Согласно требованиям раздела 3 стандарта PCI DSS, критичные аутентификационные данные (КАД), к которым относятся **TRACK, ППК2/CVV2/CVC2, PIN/PIN-block/Encrypted PIN-block**, после авторизации транзакции хранить запрещается. Единственным исключением является хранение КАД эмитентом для обеспечения возможности авторизации транзакции.

Номера карт (PAN), относящиеся к данным о держателях карт (ДДК), хранить можно, при этом они должны быть защищены в соответствии с требованием 3.5 стандарта PCI DSS.

Этап 1. Удаление КАД и ограничение хранения ДДК *(продолжение)*

Актив	Категория	Вид информации	Правила хранения
Данные платёжной карты (ДПК)	**Данные о держателе карты (ДДК)**	PAN	При хранении следует применять один из методов защиты согласно требованию 3.5 стандарта PCI DSS. При хранении следует применять один из методов защиты согласно требованию 3.5 стандарта PCI DSS.
		CH.NAME	Разрешается хранить.
		EXP.DATE	
		SERVICE CODE	
	Критичные аутентификационные данные (КАД)	TRACK, TRACK2	Запрещается хранить после авторизации транзакции. Даже в зашифрованном виде. Исключением являются эмиссионные бизнес-процессы, в рамках которых для хранения КАД есть явное обоснование. КАД при этом необходимо защищать с использованием стойкой криптографии.
		Chip equivalent data	
		CVV2, CVC2, CVP2, ППК2	
		PIN	
		PIN-Block и его криптограмма	

“

Если тебе это больше не нужно – не храни это

Золотое правило обеспечения безопасности индустрии платежных карт

Этап 1. Удаление КАД и ограничение хранения ДДК *(продолжение)*

Места хранения ДДК (ДПК для эмиссионных бизнес-процессов)					
Тип места хранения	**Адрес/путь**	**Типы ДДК**	**Применяемый метод защиты**	**Срок хранения**	**…**
Файловая система	…	PAN EXP.DATE CH.NAME	Маскирование Шифрования	1 неделя	…
Таблица БД	…	PAN EXP.DATE CH.NAME	Шифрование	5 лет	…
Электронное хранилище	…	PAN	Шифрование	5 лет	…
Облачное хранилище	…	PAN EXP.DATE CH.NAME	Шифрование	2 года	…
…	…	…	…	…	…

Этап 1. Удаление КАД и ограничение хранения ДДК *(продолжение)*

PAN - обитает практически везде, но особенно предпочитает:

- таблицы баз данных с журналами транзакций;
- файлы протоколирования событий приложений фронт-офиса;
- хранилища данных и журналы, связанные с системами электронной коммерции;
- таблицы баз данных бэк-офиса;
- журналы протоколирования событий на банкоматах (ATM), их контрольная лента;
- в розничных магазинах – системы поддержки программ лояльности и журналы протоколирования операций контрольно-кассовой техники;

Этап 1. Удаление КАД и ограничение хранения ДДК *(продолжение)*

PAN - обитает практически везде, но особенно предпочитает *(продолжение)*:

- служебная почта работников call-центра и технической поддержки;
- АБС банка;
- архивы бумажных документов о выдаче персонализированных карт;
- автоматизированные системы риск-менеджмента и фрод-мониторинга.

ППК2/CVC2/CVV2 - в особенности любит все, что связано с электронной коммерцией:

- хранилища данных и журналы, связанные с платежными системами Интернет-магазина;
- лог-файлы входящих запросов веб-серверов (например, Apache).

Этап 1. Удаление КАД и ограничение хранения ДДК *(продолжение)*

ППК2/CVC2/CVV2 - в особенности любит все, что связано с электронной коммерцией *(продолжение)*:

- таблицы баз данных бэк-офиса.
- Если организация не занимается Интернет-эквайрингом, то найти у неё в информационной инфраструктуре CVV2 почти невозможно.

TRACK - он есть везде, где есть кард-ридер:

- таблицы баз данных с журналами card-present транзакций;
- файлы протоколирования событий приложений фронт-офиса;
- журналы протоколирования событий на банкоматах (ATM), их контрольная лента;

Этап 1. Удаление КАД и ограничение хранения ДДК *(продолжение)*

TRACK - он есть везде, где есть кард-ридер *(продолжение)*:

- в розничных магазинах – в журналах встроенных в кассовое решение POS-приложений;
- системы персонализации карт.

PIN/PIN-блок и его криптограмма - в открытом виде PIN практически не встречается, зато в виде шифрограммы PIN-блока является верным спутником TRACK там, где есть card-present транзакции:

- файлы протоколирования событий старых приложений фронт-офиса;
- таблицы баз данных с журналами card-present транзакций старых приложений.

Этап 1. Удаление КАД и ограничение хранения ДДК *(продолжение)*

Чтобы найти максимум, ответьте на вопросы:

- **Авторизация:** как данные идут от клиента к нам?
- **Клиринг:** как данные идут в конце дня, как обрабатываются реестры?
- **Возврат:** как используются данные при возвратах?
- **Споры:** как используются данные при разборах спорных транзакций?

Этап 1. Удаление КАД и ограничение хранения ДДК *(продолжение)*

Проверьте тех, кто обычно не в фокусе внимания:

- **Бухгалтерия:** получает ли какие-либо реестры от банка с картами? Каким каналом?
- **Колл-центр:** озвучиваются ли ДПК в разговорах? Куда записываются? Как обрабатываются?
- **Маркетинг:** используются ли реальные PAN в аналитике?
- **Разработка:** есть ли у разработчиков практика копирования слепка прода в тест?
- **Претензионка:** есть ли какие-либо формы обратной связи и заявлений, где держатель может написать PAN в открытом виде?

Теперь можем сформировать область применимости

Состав области применимости требований PCI DSS:

- Среда обработки данных платежных карт (Cardholder Data Environment, CDE):
  a) компонент хранит, обрабатывает или передает данные платежных карт;
  b) компонент находится в одном сегменте сети с компонентами из пункта (a);
- Смежные или влияющие на безопасность компоненты информационной инфраструктуры (Connected-to or Security-impacting Systems):
  a) компоненты, необходимые для выполнения требований самого стандарта;
  b) компоненты, влияющие на конфигурацию или безопасность CDE;
  c) компоненты, обеспечивающие сегментацию в области применимости.

Зачем нужна сегментация?

Правило: если нет сегментации – в области применимости стандарта все.

Если корпоративная сеть не отделена в соответствии с требованиями корректно настроенным межсетевым экраном, то вся сеть становится **connected-to** компонентами.

Отсутствие сегментации делает внедрение PCI DSS практически невозможным или очень дорогим.

Какие компоненты нужно рассмотреть для оценки на внесение в область применимости?

- ActiveDirectory/LDAP. Если пользователи скоупа аутентифицируются и авторизовываются через корпоративный AD/LDAP, то весь домен в скоупе.
- Jump Host/Bastion. Сервер для администрирования. Если его взломают, получат доступ к CDE.
- Средства защиты. Серверы антивирусной защиты, SIEM-коллекторы, системы обновлений (pkg-репозитории).

Какие компоненты нужно рассмотреть для оценки на внесение в область применимости?

- Гипервизоры. Если на одном физическом хосте живут виртуалки CDE и не-CDE, и через вторые скомпрометируют гипервизор – считаем, что взломано все.
- Cloud IAM. Консоль управления облаком. Права доступа к ней критичны, особенно, если под одной консолью несколько сред (CDE и не-CDE).
- Оркестраторы. K8S, vCloudDirector и другие. Если их скомпрометируют – получат доступ ко всему.
- ServiceMesh. Компоненты управления трафиком между микросервисами. Их компрометация позволяет скомпрометировать трафик, включая платежный.

Какие компоненты нужно рассмотреть для оценки на внесение в область применимости?

- Code Repositories. GitLab, Gitea, BitBucket и другие. Все, где лежит код, влияющий на безопасность (например, IaaC описания инфраструктуры, код платежного приложения и т. п.).
- CI/CD Tools. Jenkins, TeamCity – серверы сборки и деплоя. Они имеют привилегированные права в продуктовой среде. Их компрометация позволяет добраться до ДПК.
- Container Registry. Хранилища образов контейнеров являются точкой доверия для инфраструктуры.

Какие компоненты нужно рассмотреть для оценки на внесение в область применимости?

- Хосты для редиректа, балансировки. Все они влияют на безопасность, так как могут перенаправлять держателя на вредоносный сайт и через это красть данные. Это основа для применимости SAQ A.

Как можно улучшить?

Постараться уменьшить количество **CDE**:

Компонент хранит, обрабатывает или передает данные платежных карт	• А можем ли мы отказаться от обработки ДПК на компоненте? • Можем ли заменить ДПК на «не-ДПК»?
Компонент не работает с ДПК, но находится в одном сегменте сети	• А можем ли мы выделить такие компоненты в отдельный сегмент сети? • Данный компонент не является смежной системой?

Как можно улучшить?

Постараться уменьшить количество **смежных систем**:

Компоненты, влияющие на конфигурацию или безопасность CDE	• Можем ли мы избавиться от зависимости, если компонент будет скомпрометирован? • Можем ли мы уменьшить количество компонентов, которые отвечают за сегментацию?

Описание области применимости PCI DSS

Для того, чтобы выполнить требования стандарта PCI DSS и упростить работникам исполнение процессов информационной безопасности, область применимости PCI DSS должна быть описана в виде трех документов:

- Схема сети области применимости PCI DSS.
- Схема потоков ДПК.
- Перечень компонентов информационной инфраструктуры, входящих в область применимости PCI DSS.

Схема сети

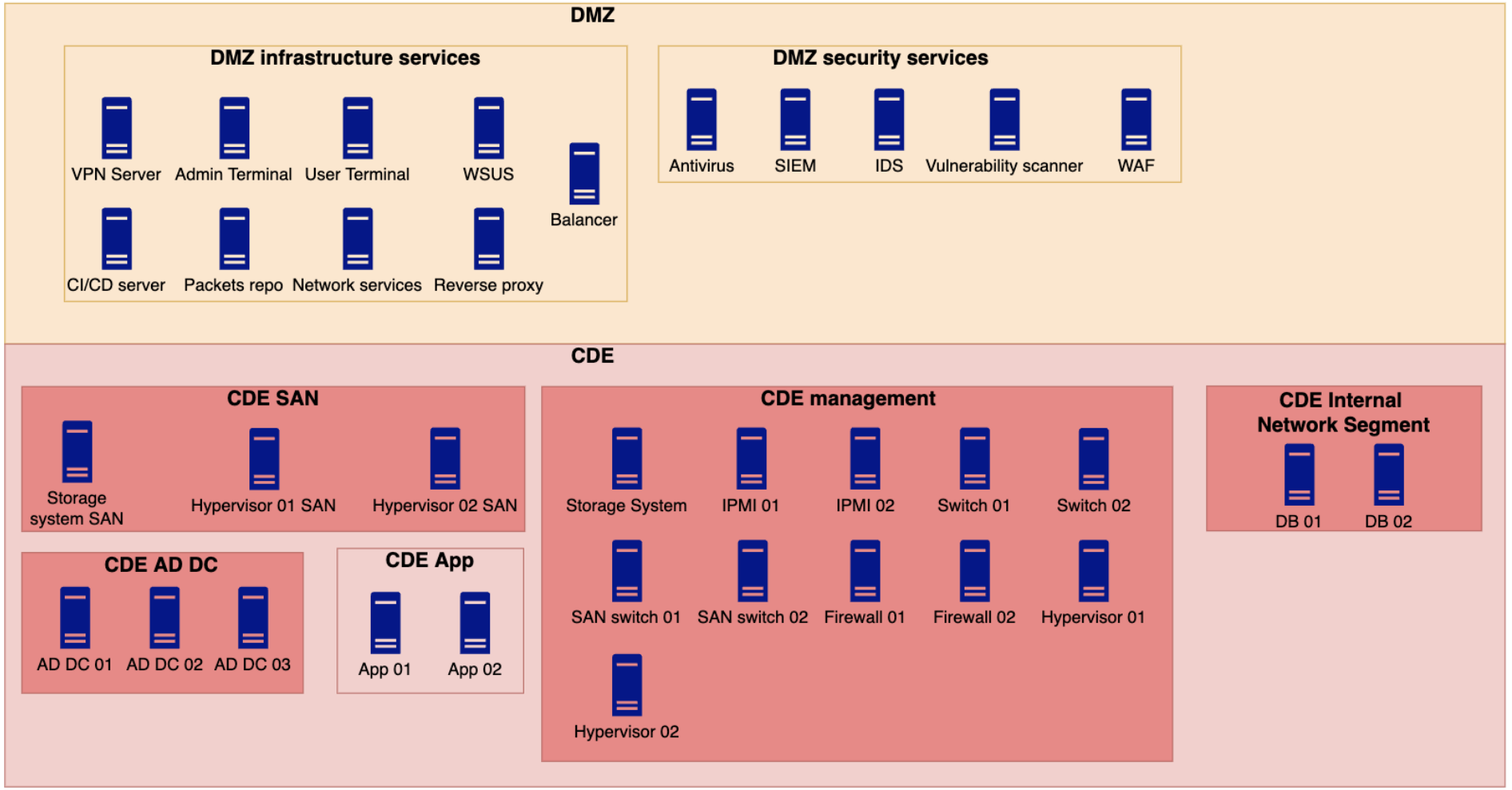


Схема потоков. Электронная коммерция

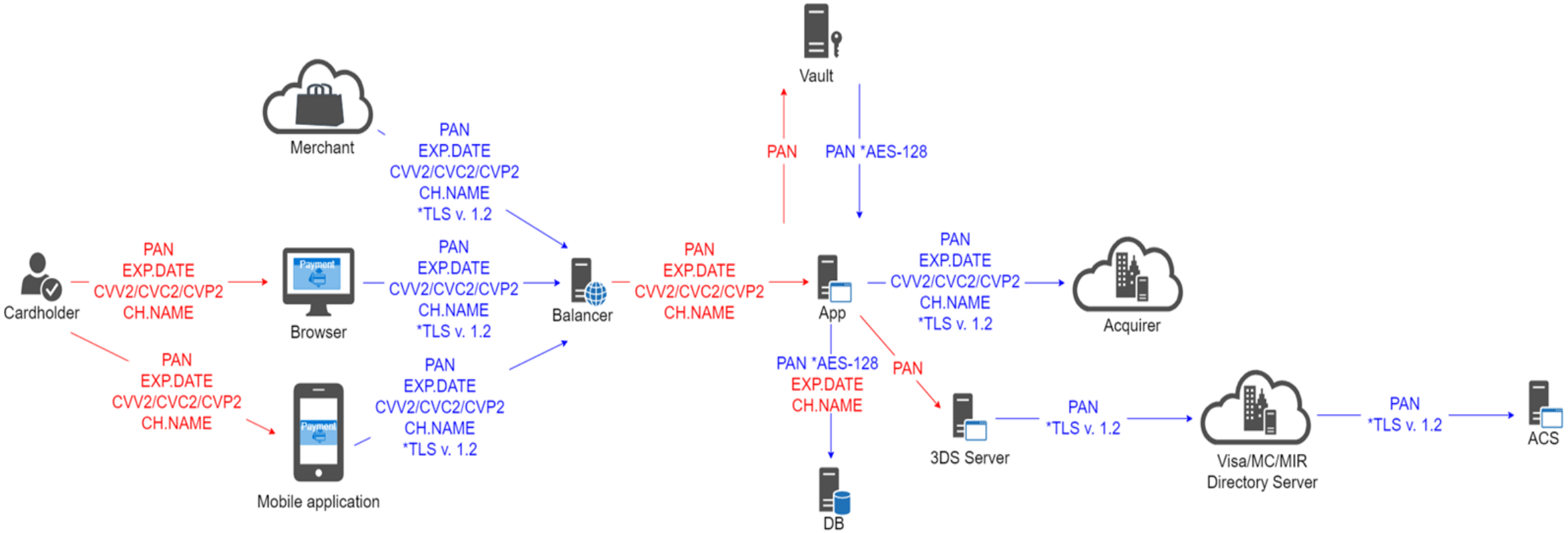


Схема потоков. Наземный эквайринг

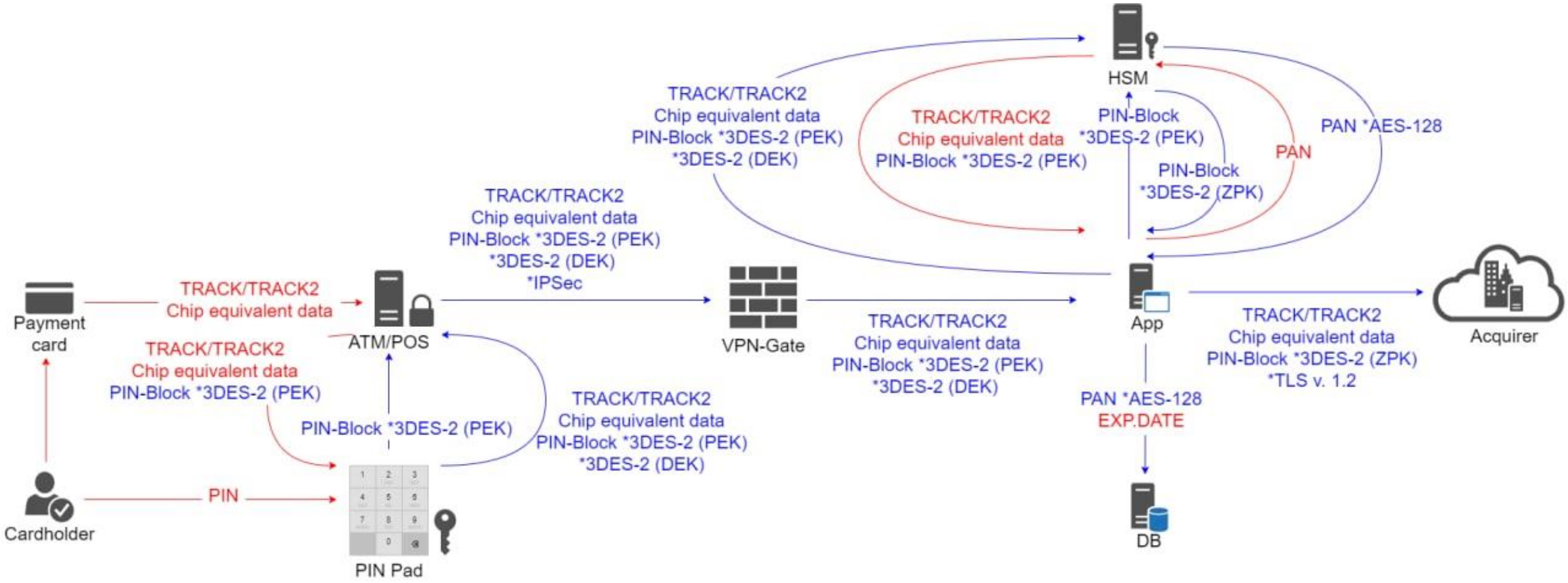


Схема потоков. Персонализация

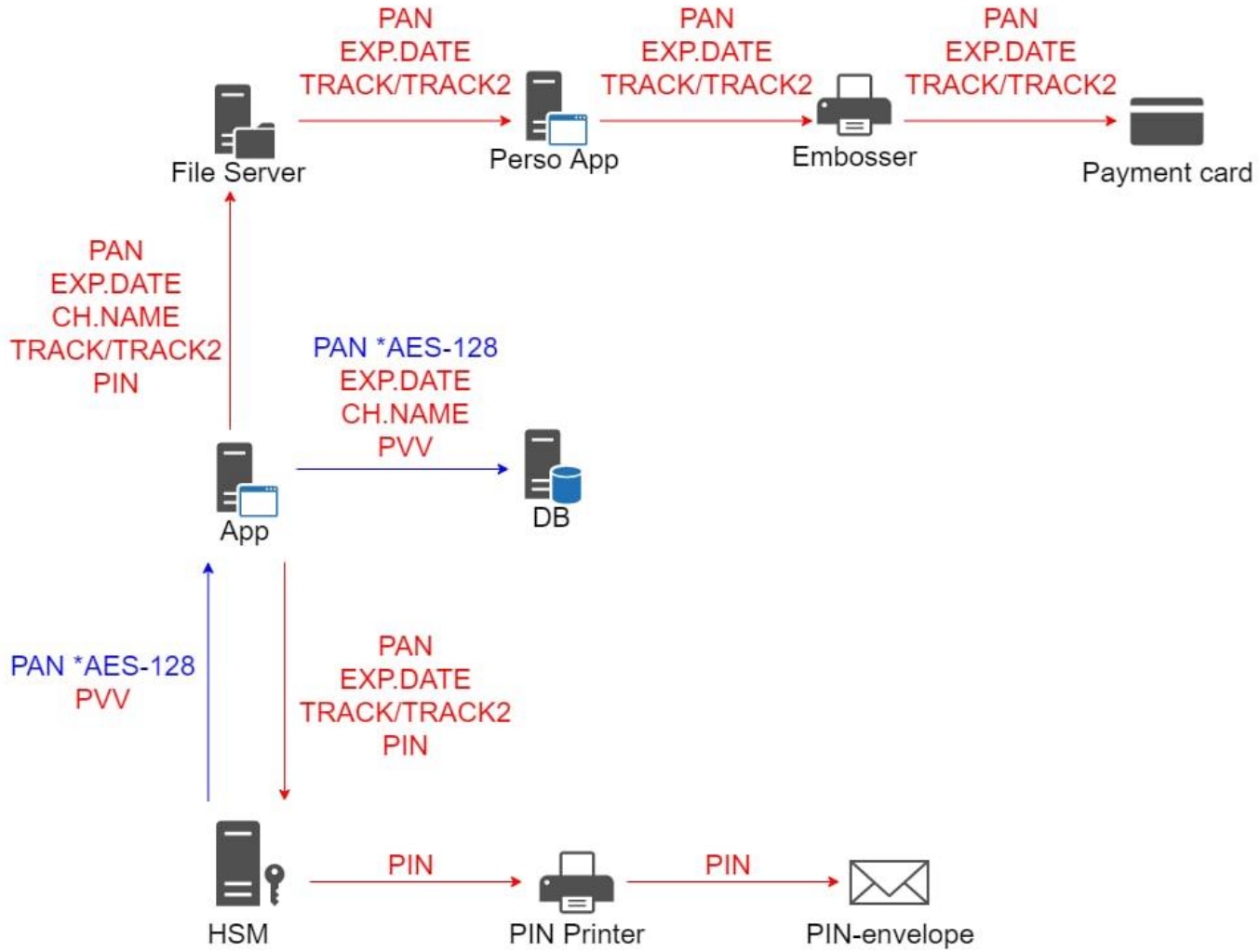
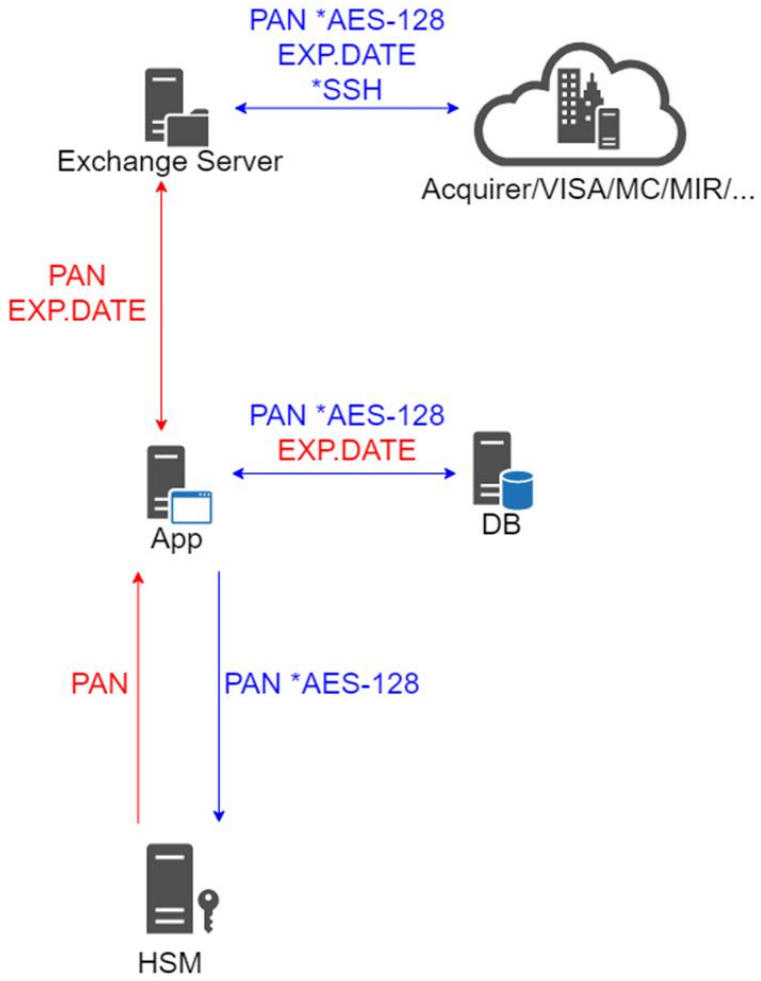


Схема потоков. Клиринг



Перечень компонентов. Приложения

№	Название приложения	Основные функции	Тип приложения	Какие данные обрабатывает	Версия	Какие хранилища использует
1	Card-gateway	Получает ДПК, сохраняет PAN и EXP.DATE в БД и передает эквайреру транзакцию на авторизацию	Монолитное приложение, написанное на C#	PAN, EXP.DATE, CVV2/CVC2, CH.NAME	1.0	БД card_gateway, таблица cards

Перечень компонентов. Хранилища ДПК

№	Название хранилища	Тип хранилища	Места хранения защищаемых данных	Виды хранимых данных	Обоснование хранения	Длительность хранения	Способ защиты хранимых данных	Метод гарантированного удаления
1	DB 01, БД card_gateway	Таблица в реляционной СУБД	БД card_gateway, таблица cards, поле pan_cryptogram	PAN, EXP.DATE	Рекуррентные платежи, оплата клиентами по сохраненной карте	До момента наступления EXP.DATE	Шифрование с помощью AES-128 GCM	SQL-запрос DELETE

Перечень компонентов. Серверы

№	Название компонента	FQDN	IP-адрес	Функция	Тип компонента	ОС	Версия
1	VPN сервер	…	…	VPN-сервер для удаленного подключения к инфраструктуре скоупа PCI DSS.	Виртуальная машина	…	…
2	DB 01	…	…	Сервер базы данных.	Виртуальная машина	…	…
3	Hypervisor 01	…	…	Гипервизор с системой виртуализации.	Физический сервер	…	…

Перечень компонентов. Бизнес-процессы

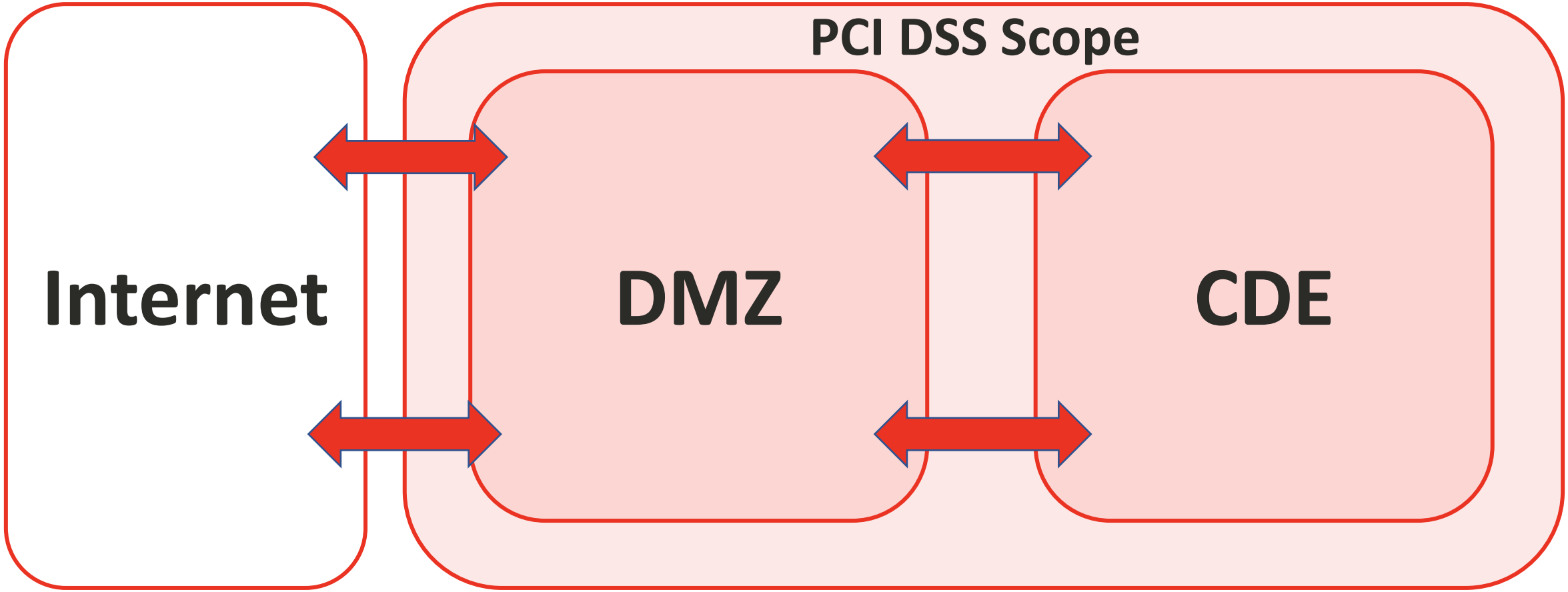
№	Название бизнес-процесса	Какие данные обрабатываются	К какому процессу относится (эмиссия или эквайринг)
1	Авторизация транзакций электронной коммерции	PAN, EXP.DATE, CH.NAME, CVV2/CVC2/CVP2	Эквайринг
2	Перевод с карты на карту	PAN, EXP.DATE, CH.NAME, CVV2/CVC2/CVP2	Эквайринг
3	Клиринг	PAN, EXP.DATE	Эквайринг

Этап 2. Защита периметра, внутренних и беспроводных сетей

На этом этапе следует:

- защитить вычислительную сеть организации путем корректной настройки маршрутизаторов и межсетевых экранов, а также организации выделенного защищенного внутреннего (Internal network segment) и пограничного DMZ-сегментов сети;
- обеспечить учет и контроль конфигураций компонентов информационной инфраструктуры, для этого разработать стандарты конфигурации компонентов информационной инфраструктуры;
- обеспечить безопасность передаваемых ДДК путем шифрования каналов связи, по которым они передаются (можно применять широкий спектр решений от различных VPN до TLS).

Этап 2. Защита периметра, внутренних и беспроводных сетей *(продолжение)*



Этап 2. Защита периметра, внутренних и беспроводных сетей *(продолжение)*

Для тех, кто использует POS POI-устройства с поддержкой SSL и ранних версий TLS, необходимо выполнить требования Приложения A2 стандарта PCI DSS:

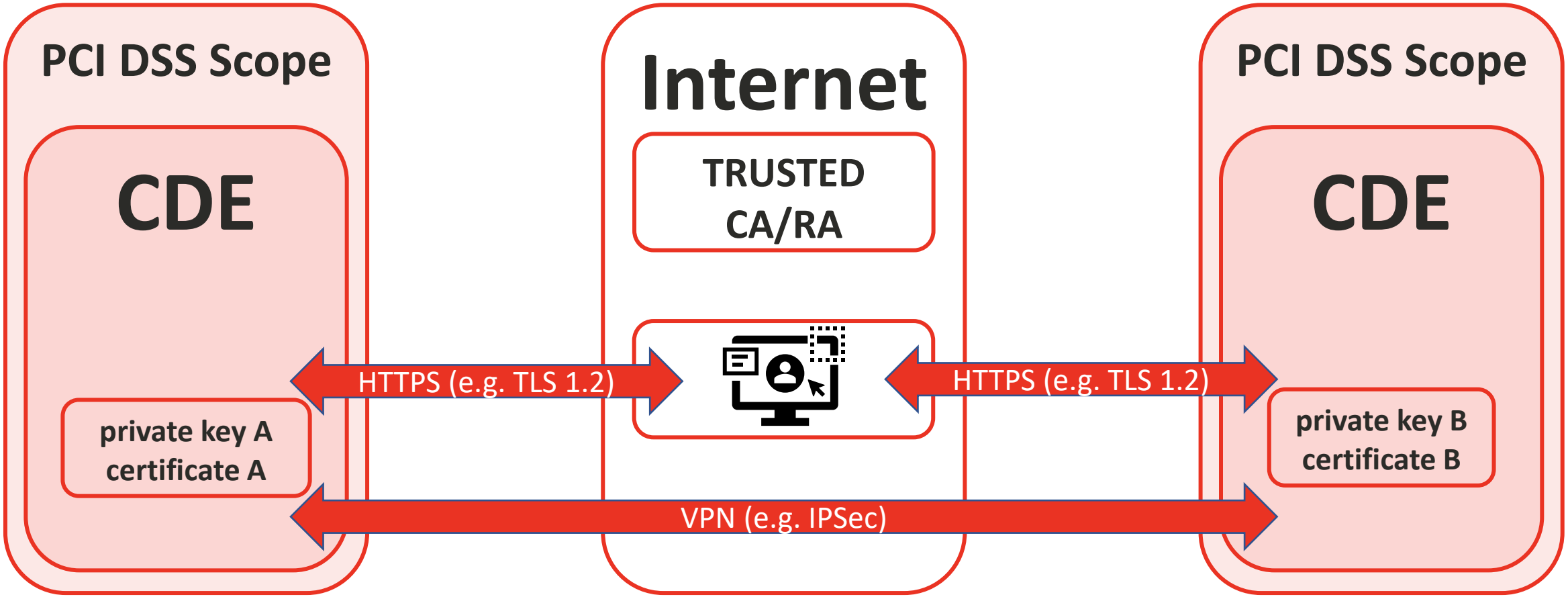
- нужно убедиться, что устройства не подвержены атакам на небезопасные версии SSL и TLS;
- для поставщиков услуг необходимо разработать План миграции и внедрить меры по снижению рисков ИБ, связанных с использованием небезопасных протоколов;
- поставщики услуг должны озаботиться переводом своих клиентов на безопасные версии протоколов.

Этап 2. Защита периметра, внутренних и беспроводных сетей *(продолжение)*

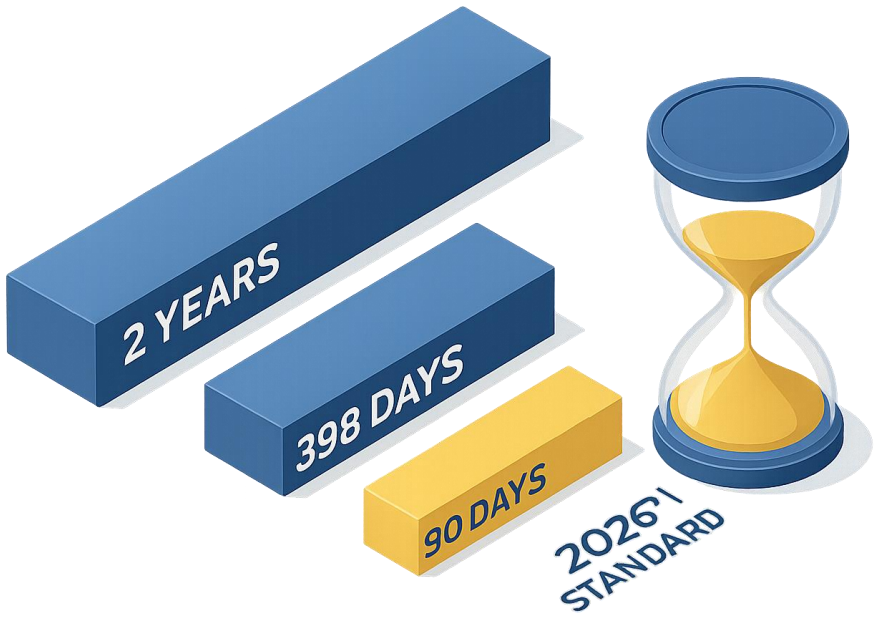
Не все сертификаты одинаковы:

- DV (Domain Validated): проверяется только домен. Дешево, но не подтверждает, что вы – реальная компания. Подходит для блогов, но не очень для коммерческих сервисов. Пример – Let’s Encrypt.
- OV (Organization Validated): центр регистрации и сертификации проверяет документы компании. Выше уровень доверия.
- EV (Extended Validated): самая строгая проверка. Ранее давала «зеленую строку» в браузере. Лучшее решение для крупных брендов.

Этап 2. Защита периметра, внутренних и беспроводных сетей *(продолжение)*



Этап 2. Защита периметра, внутренних и беспроводных сетей *(продолжение)*



Сокращение TTL для TLS-сертификатов до 90 дней. Зачем?

- Минимизация риска: если закрытый ключ украден, он будет валиден не год, а всего несколько недель.
- Позволяет быстрее выводить из обращения старые алгоритмы.
- Короткий TTL делает громоздкие списки CRL/OCSP менее критичными.
- Переход на ACME (Automated Certificate Management Environment).

Этап 3. Обеспечение безопасности приложений, БД и ОС

На этом этапе следует:

- наладить процесс безопасной поддержки информационной инфраструктуры, внедрив процедуры управления изменениями, в том числе на соответствие их требованиям стандарта PCI DSS. Хорошей практикой будет внедрение такого элемента из руководства ITIL-ITSM как база данных управления конфигурациями Configuration Management Database (CMDB);

- каждое изменение следует анализировать на предмет его соответствия требованиям PCI DSS;

- для каждого типа компонентов необходимо разработать и поддерживать в актуальном виде стандарты конфигурации;

Этап 3. Обеспечение безопасности приложений, БД и ОС *(продолжение)*

На этом этапе следует *(продолжение)*:

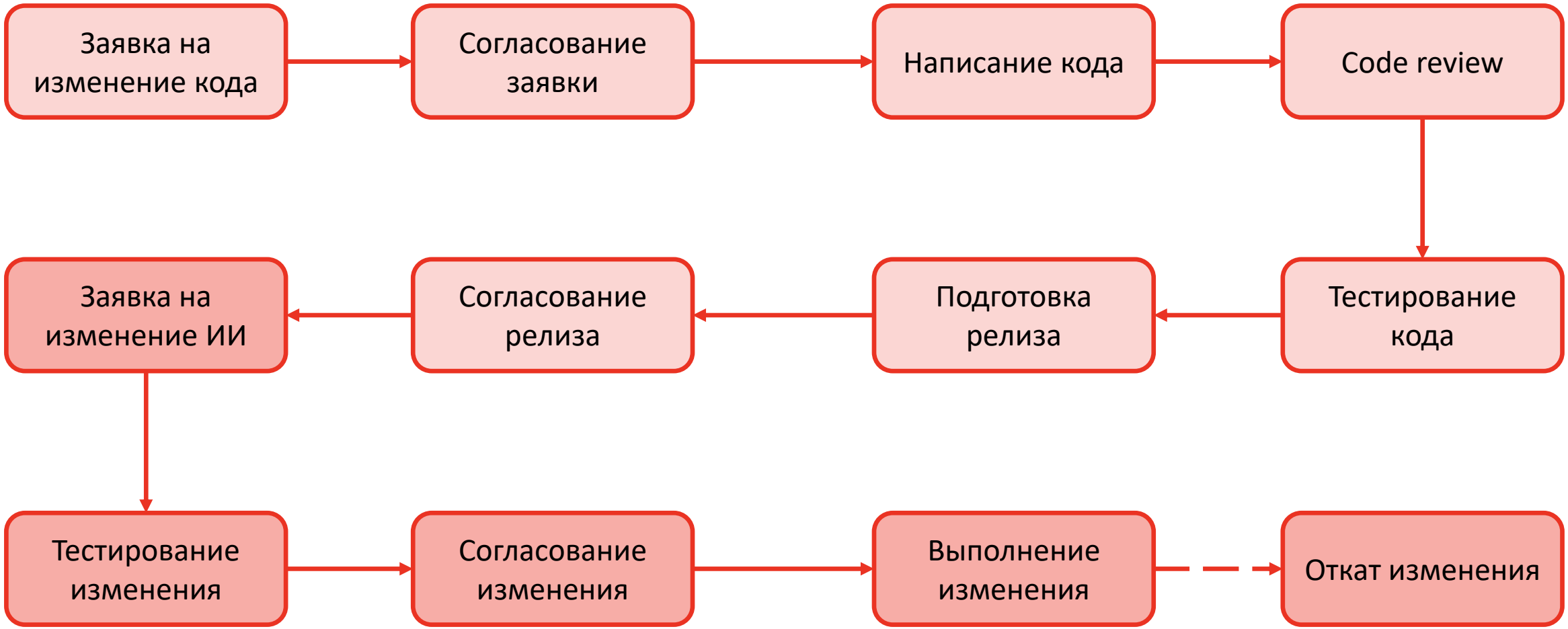
- необходимо обеспечить регулярное обновление программного обеспечения: установку критических патчей в течение месяца и установке остальных патчей не позднее установленного организацией периода;
- если в организации ведется разработка программного обеспечения, следует выделить под неё отдельную среду разработки, не связанную с производственными системами, вести учет всех зависимостей и анализировать их на предмет наличия в них уязвимостей;
- перед переводом в производственный режим обязательно нужно очистить систему от тестовых данных (ключей, аккаунтов и т. п.).

Этап 3. Обеспечение безопасности приложений, БД и ОС *(продолжение)*

На этом этапе следует *(продолжение)*:

- настроить механизмы аутентификации пользователей приложений, баз данных и операционных систем, внедрив строгую парольную политику;
- разработать и внедрить организационные процедуры управления логическим и физическим доступом к данным. Лучшим вариантом будет внедрение метода управления доступом, основанного на ролях пользователей в бизнес-процессах (Role-Based Access Control, RBAC);
- внедрить средства антивирусной защиты информационной инфраструктуры.

Управление изменениями (пример)



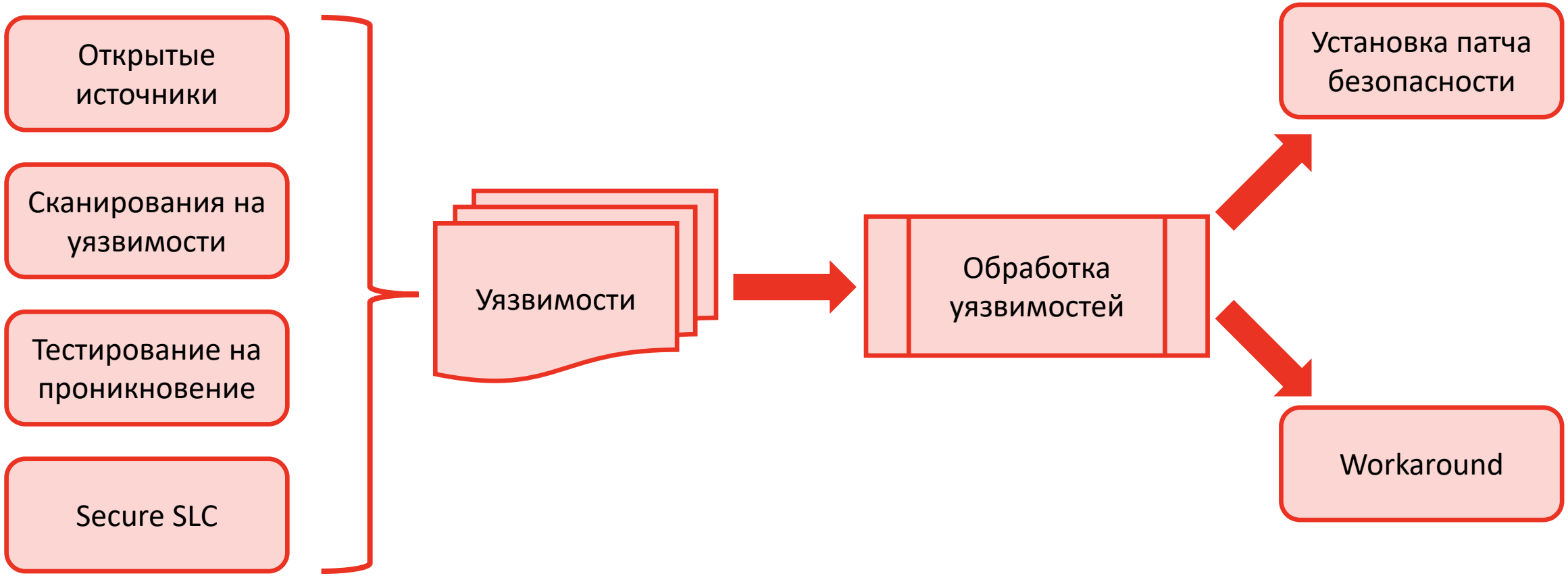
Стандарты конфигурации

Все компоненты информационной инфраструктуры должны быть настроены безопасно и единообразно в соответствии с принятыми в отрасли стандартами безопасности или рекомендациями поставщика.

Стандарт конфигурации может быть составлен на основании рекомендаций:

- Center for Internet Security (CIS);
- International Organization for Standardization (ISO);
- National Institute of Standards and Technology (NIST);
- Cloud Security Alliance;
- производителей компонентов;
- регуляторов отрасли.

Управление уязвимостями



Парольная политика

- длина пароля – минимум 12 символов или максимальную длину, поддерживаемую системой, но не менее 8 символов;
- пароль должен состоять минимум из букв и цифр;
- срок смены пароля – 90 дней или должны быть внедрены методы динамического мониторинга учетной записи (применяется не для CDE компонентов области применимости);
- запрещается использовать четыре последних пароля;
- блокировка на 30 минут после 10 неудачных попыток ввода пароля;
- обязательная смена случайного пароля при первом входе;
- обязательная повторная аутентификация после простоя 15 минут;
- хранение и передача паролей только в защищенном виде.

Учетные записи

Пользовательские:

- учетные записи должны быть индивидуальны;
- стандартные, разделяемые административные записи должны быть запрещены к использованию.

Сервисные:

- не должны поддерживать интерактивный логин, кроме исключительных ситуаций;
- учетные данные должны изменяться на периодической основе;
- не должны использоваться пользователями;
- запрещено хранить учетные данные в коде или конфигах в открытом виде.

Multi-Factor Authentication. Определение

Что я знаю?

Пароль, парольная фраза

Чем я обладаю?

Ключ, устройство, отчуждаемый носитель

Кто я сам?

Биометрические данные

Системы MFA должны быть устойчивы к атакам и строго контролировать любые попытки административного вмешательства.

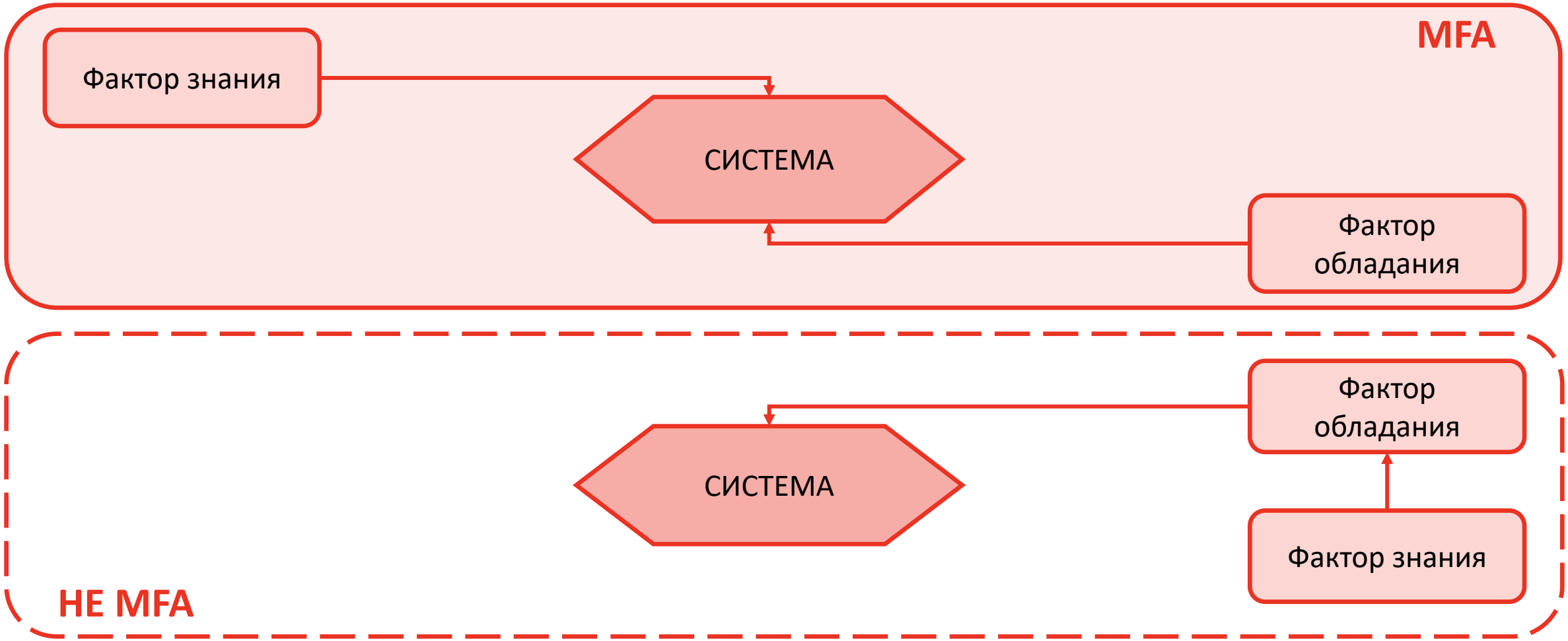
MFA. Лучший выбор факторов

- **Лучше всего:** фишинг-устойчивые методы: FIDO2, WebAuth, аппаратные ключ (секрет никогда не передается по сети).
- **Тоже неплохо:** локальные OTP, биометрий, длинные случайные пароли.
- **Допустимо пока еще:** SMS-коды, пароли, придуманные пользователем.

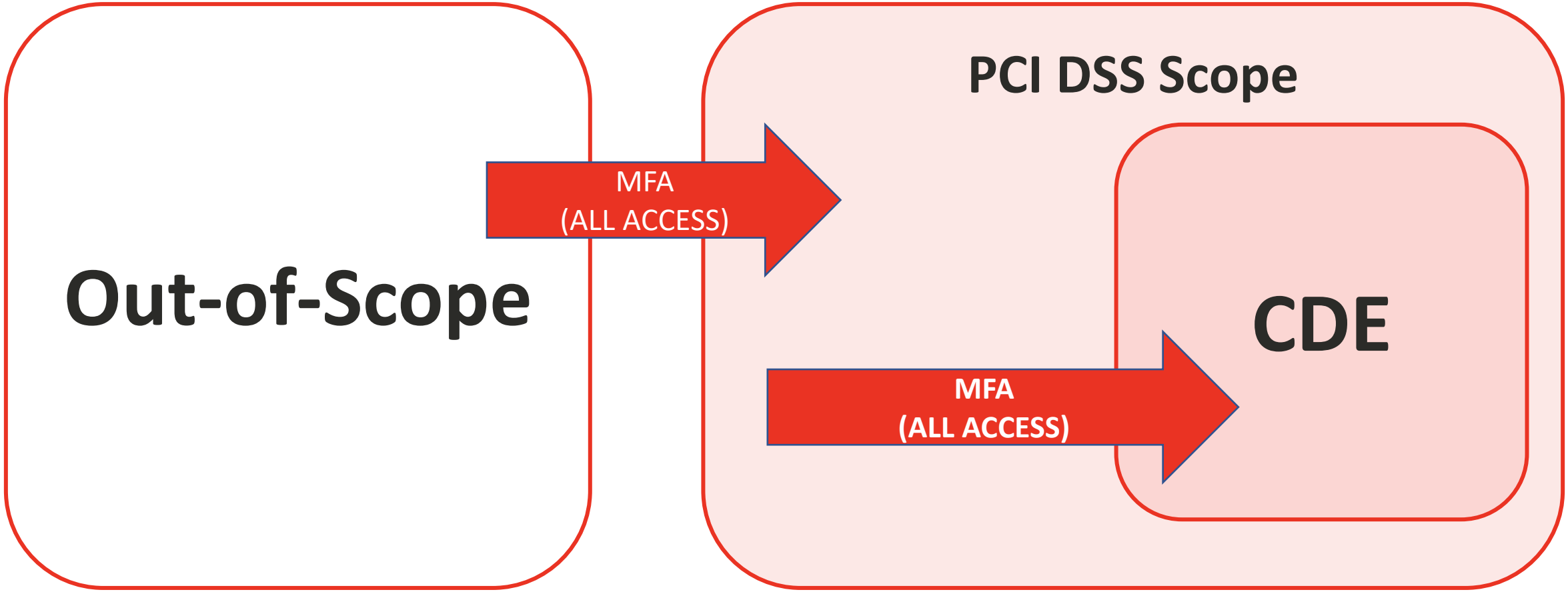
Что не является MFA?

- **Два пароля:** знание + знание = 1 фактор.
- **Пароль + ПИН:** аналогично.
- **Пошаговая аутентификация:** ввод пароля для входа, потом OTP для операции.

MFA. Независимость факторов



MFA



> **Самый стойкий MFA бесполезен, если злоумышленник сможет восстановить доступ на свое устройство.**

Безопасность контейнеров

- Не запускайте контейнеры от root.
- Критичные системы выносите на отдельные ноды или отдельные кластеры.

Помните: побег из контейнера приводит к доступу к ядру хоста и ко всем контейнерам на этом хосте.

Безопасность оркестратора

- Доступ к API K8S должен быть закрыт из недоверенных сетей и ограничен внутри организации.
- Минимизируйте права доступа через RBAC и ServiceAccounts.
- Никогда не храните секреты в открытом виде. Используйте внешние хранилища (например, Vault) или зашифрованные K8S Secrets.

Безопасность образов

- Не качайте образы из недоверенных источников, особенно с тегом latest. Используйте свой приватный Registry.
- Образы должны сканироваться на уязвимости на этапе сборки и в Registry на периодической основе.
- Мы не должны патчить запущенный контейнер. Мы всегда пересобираем образ с патчем и деплоим заново.

Безопасность кластера

- Уделите большое внимание CNI и сетевым политикам.
- Пропишите гранулярные доступы на L3,L4,L7 уровнях.
- По возможности внедрите mesh-сеть с mTLS.

Обеспечение физической безопасности

- изоляция физических компонентов области применимости PCI DSS;
- контрольно-пропускной режим;
- СКУД;
- видеонаблюдение;
- учет физических компонентов области применимости PCI DSS;
- транспортировку физических компонентов области применимости PCI DSS;
- уничтожение носителей информации.

Обеспечение антивирусной защиты

- Все системы, которые считаются подверженными воздействию вредоносного ПО, должны быть защищены с помощью средств антивирусной защиты.
- Для систем, которые считаются не подверженными воздействию вредоносного ПО, необходимо на периодической основе проводить оценку необходимости применения средств антивирусной защиты.
- Средство антивирусной защиты должно противодействовать фишинговым атакам.
- Все извлекаемые носители должны проверяться на угрозы средством АВЗ.

Этап 4. Мониторинг и контроль доступа

На этом этапе следует:

- настроить аудит и протоколирование событий и действий. Это означает, что по возможности все компоненты информационной инфраструктуры должны вести лог-файлы своей активности, связанной с безопасностью информационной инфраструктуры, использованием механизмов аутентификации, использованием административных привилегий, а также доступом к данным о держателях карт. Необходимо обеспечить централизованный сбор копий журналов протоколирования событий на выделенный сервер. Обязательным с 1 апреля 2025 года решением будет внедрение автоматизированной системы управления событиями безопасности (SIEM).

Мониторинг. С чего начать?

- что вам нужно и что вы хотите отслеживать?
- какие компоненты должны быть включены в выборку мониторинга?
- какую информацию можно отнести к событиям безопасности?
- как вы будете собирать и анализировать события?
- как часто необходимо анализировать события?
- как долго необходимо хранить собранные события?

Ответы на эти вопросы в разделе 10 стандарта PCI DSS

Мониторинг. С чего начать? *(продолжение)*

- сформулируйте на высоком уровне, что хотите видеть в мониторинге;
- идентифицируйте и документируйте все источники событий;
- скоррелируйте системные события со своей высокоуровневой моделью;
- приоритезируйте источники событий;
- определите ответственных за реагирование и документируйте эти процессы;
- определитесь с инструментом по сбору и анализу событий безопасности;
- внедрите решение, нормализируйте собираемые события;
- настройте срабатывания на события, их корреляцию и автоматическое уведомление ответственных работников.

Этап 4. Мониторинг и контроль доступа
(продолжение)

На этом этапе следует *(продолжение)*:

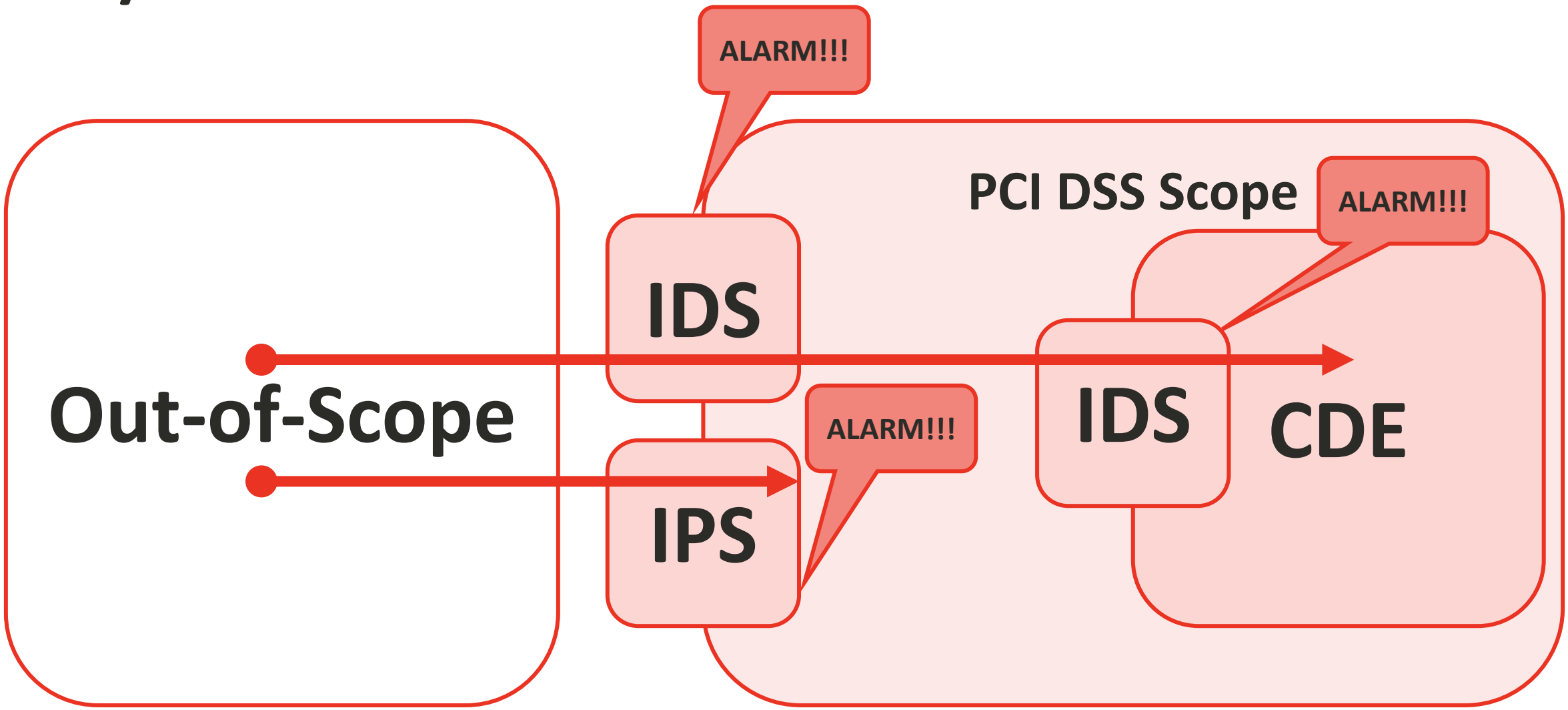
- внедрить средства контроля информационной безопасности – сканеры уязвимостей, системы обнаружения и предотвращения вторжений, системы контроля беспроводных сетей, межсетевые экраны уровня приложений, системы контроля целостности файлов, внутренние аудиты;

- разработать и внедрить регулярные процедуры использования всего вышеперечисленного, определить ответственных лиц и форму регистрации записей о выполнении. Также следует разработать планы реагирования на инциденты и события информационной безопасности, в том числе на события потери доступности систем безопасности.

Сканеры уязвимостей

Внутренний сканер	Внешний сканер	Сканер web-приложений
Сканирует внутренние («серые») IP-адресы	Сканирует внешние («белые») IP-адресы	Сканирует web-приложения по доменным именам
Решение может быть от любого вендора, включая opensource	Решение должно быть только от ASV-компании	Решение может быть от любого вендора, включая opensource
Проводить сканирования на ежеквартальной основе и после внесения значимых изменений	Проводить сканирования на ежеквартальной основе и после внесения значимых изменений	Проводить сканирования на периодической основе и после внесения значимых изменений
Начиная с 01 апреля 2025 года должно поддерживаться сканирование с использованием аутентификации на хостах	Не требует обязательного сканирования с аутентификацией на хостах	Не требует обязательного сканирования с аутентификацией на хостах

IDS/IPS



WAF

- начиная с 1 апреля 2025 года, обязательный для защиты публично доступных web-приложений;
- может быть облачным сервисом, on-premise программно-аппаратным отдельным решением или модулем к web-серверу;
- не является панацеей в части защиты web-приложений, но дает хорошую базовую защиту от атак.

Применение WAF не освобождает от необходимости устранять уязвимости в программном коде!

FIM

Все критичные к несанкционированным изменениям файлы должны быть под наблюдением FIM-системы не реже, чем на еженедельной основе. Например:

- исполняемые файлы;
- конфигурационные файлы;
- криптографические ключи.

Оповещения о срабатываниях FIM должны быть направлены ответственным за реагирование работникам.

Защита от e-commerce skimming

Проблема: современные сайты подгружают десятки скриптов (аналитика, боты, рекламные пиксели).

Атака: если хакер взломает сторонний сервис (например, сервис чат-бота), то вредоносный код прилетит в браузер держателя вместе с легитимным скриптом. Код крадет данные в момент ввода ДО того, как они будут зашифрованы и отправлены в процессинг.

Решение: контролировать все, что исполняется в браузере.

Защита от e-commerce skimming

- О нарушениях CSP можно сообщать с помощью директивы «report-to» CSP.
- Изменения в самой CSP могут свидетельствовать о несанкционированном доступе.
- Внешний мониторинг системами, которые запрашивают и анализируют полученные веб-страницы (также известный как синтетический мониторинг пользователей), может обнаружить изменения JavaScript в платежных страницах.
- Встраивание в платежную страницу скрипта, устойчивого к несанкционированному вскрытию, может предупреждать и блокировать страницу при обнаружении вредоносного поведения скрипта.
- Обратные прокси-серверы и сети доставки контента (CDN) могут также обнаружить изменения в сценариях.

Процесс управления инцидентами

В рамках процесса управления инцидентами информационной безопасности должны выполняться такие активности, как:

- логирование требуемых событий информационной безопасности;
- централизованный сбор событий информационной безопасности;
- автоматизированный анализ событий информационной безопасности;
- мониторинг событий информационной безопасности;
- разработка и (или) доработка планов реагирования на инциденты;
- тестирование планов реагирования на инциденты.

Этап 5. Защита хранимых данных

Актив	Категория	Вид информации	Правила хранения
Данные платёжной карты (ДПК)	**Данные о держателе карты (ДДК)**	PAN	При хранении следует применять один из методов защиты согласно требованию 3.5 стандарта PCI DSS. При хранении следует применять один из методов защиты согласно требованию 3.5 стандарта PCI DSS.
		CH.NAME	Разрешается хранить.
		EXP.DATE	
		SERVICE CODE	
	Критичные аутентификационные данные (КАД)	TRACK, TRACK2	Запрещается хранить после авторизации транзакции. Даже в зашифрованном виде. Исключением являются эмиссионные бизнес-процессы, в рамках которых для хранения КАД есть явное обоснование. КАД при этом необходимо защищать с использованием стойкой криптографии.
		Chip equivalent data	
		CVV2, CVC2, CVP2, ППК2	
		PIN	
		PIN-Block и его криптограмма	

Этап 5. Защита хранимых данных *(продолжение)*

Этап 5. Защита хранимых данных *(продолжение)*

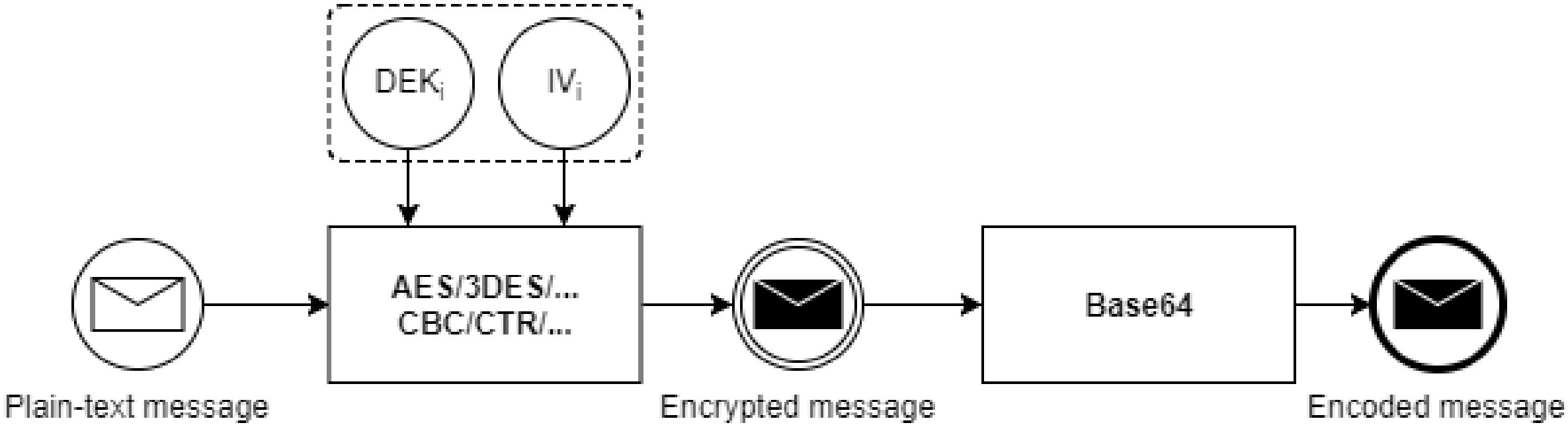
Битовая стойкость	Симметричные алгоритмы шифрования	Ассиметричные алгоритмы шифрования (например, RSA)	Алгоритмы на эллиптических кривых
112	TDEA	2048	224
128	AES-128	3072	256
192	AES-192	7680	384
256	AES-256	15360	512

Этап 5. Защита хранимых данных

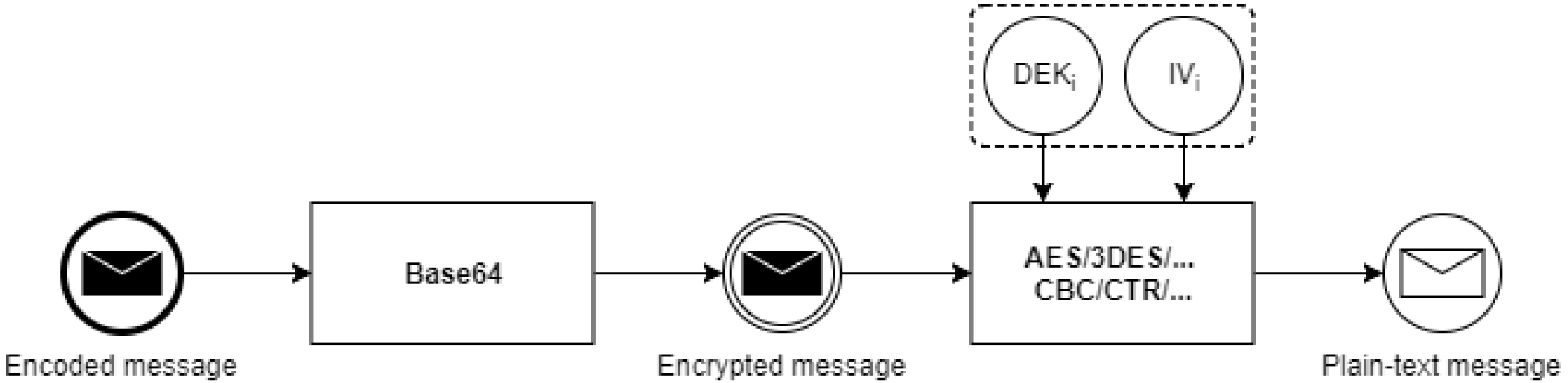
Будьте готовы к изменениям!

- Не зашивайте алгоритмы в код жестко. Архитектура должна позволять сменить алгоритм шифрования без переписывания всего приложения.
- Отслеживайте международные стандарты (например, NIST/FIPS).

Этап 5. Защита хранимых данных *(продолжение)*



Этап 5. Защита хранимых данных *(продолжение)*

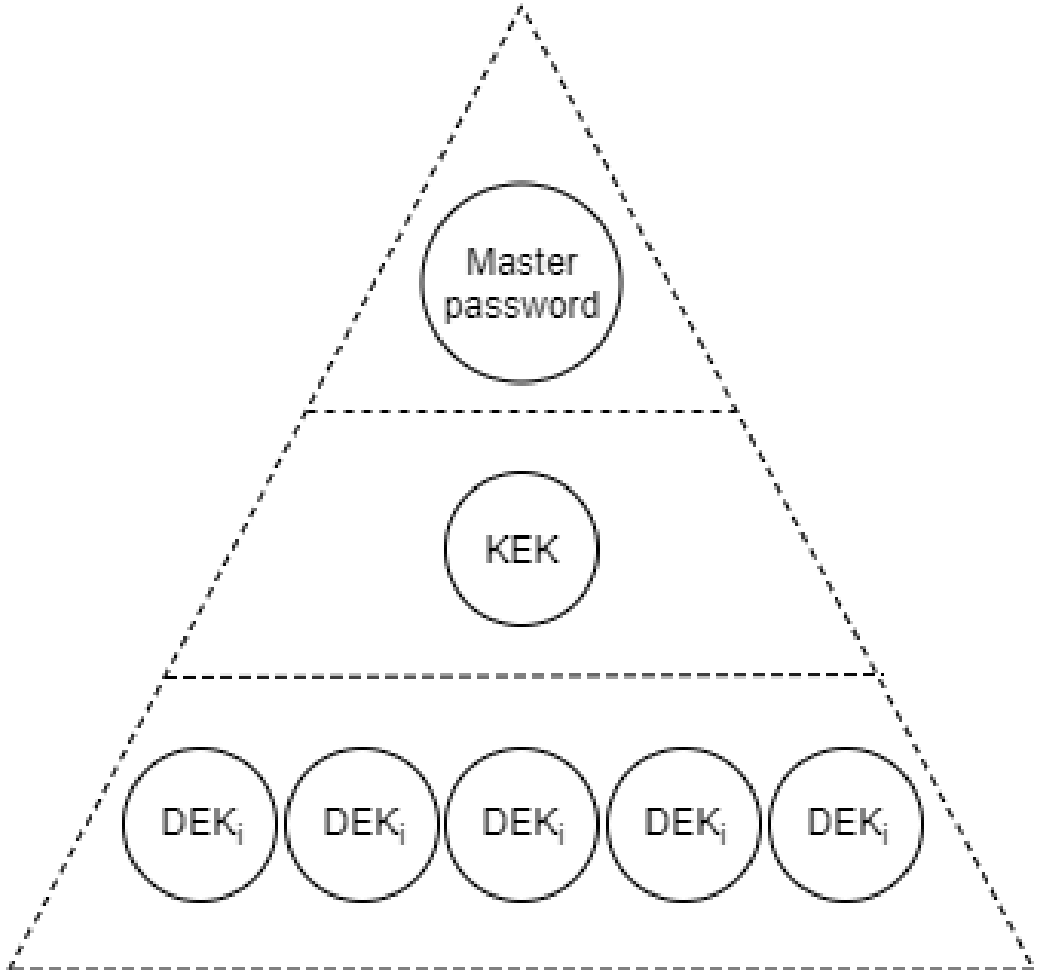


Этап 5. Защита хранимых данных

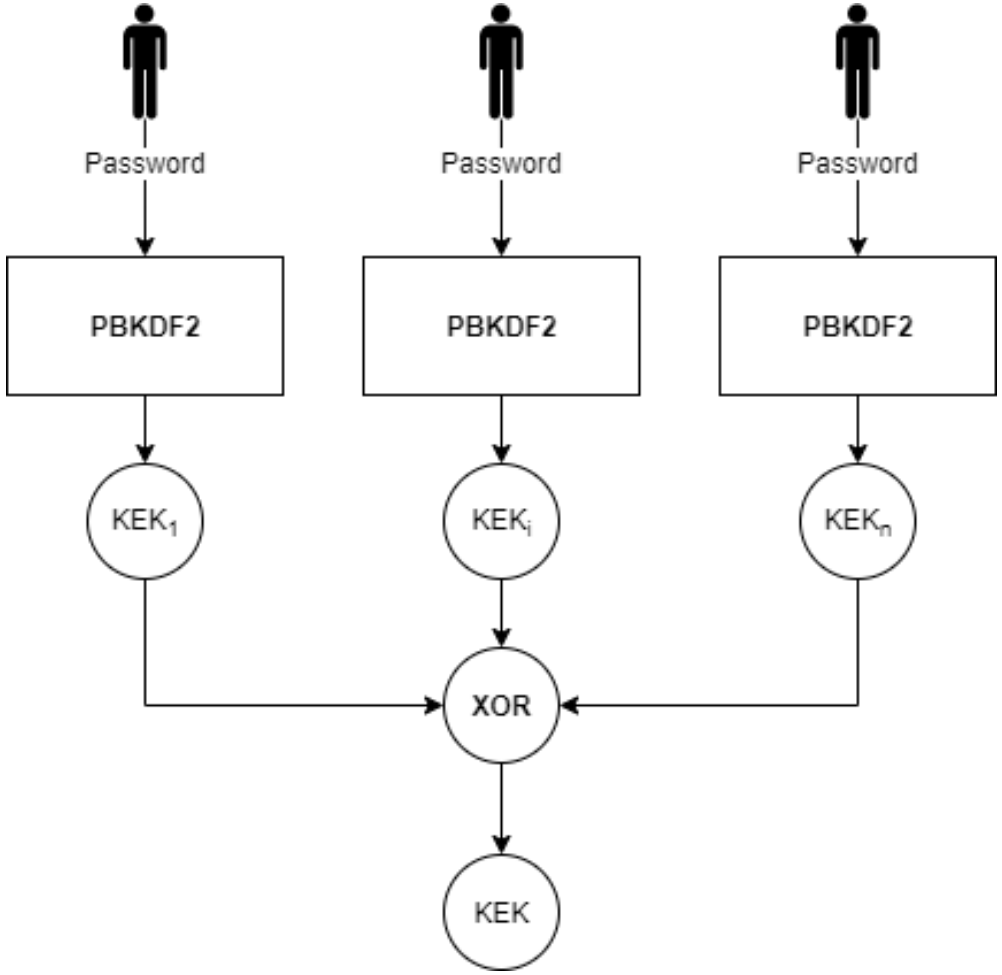
Ошибки внедрения

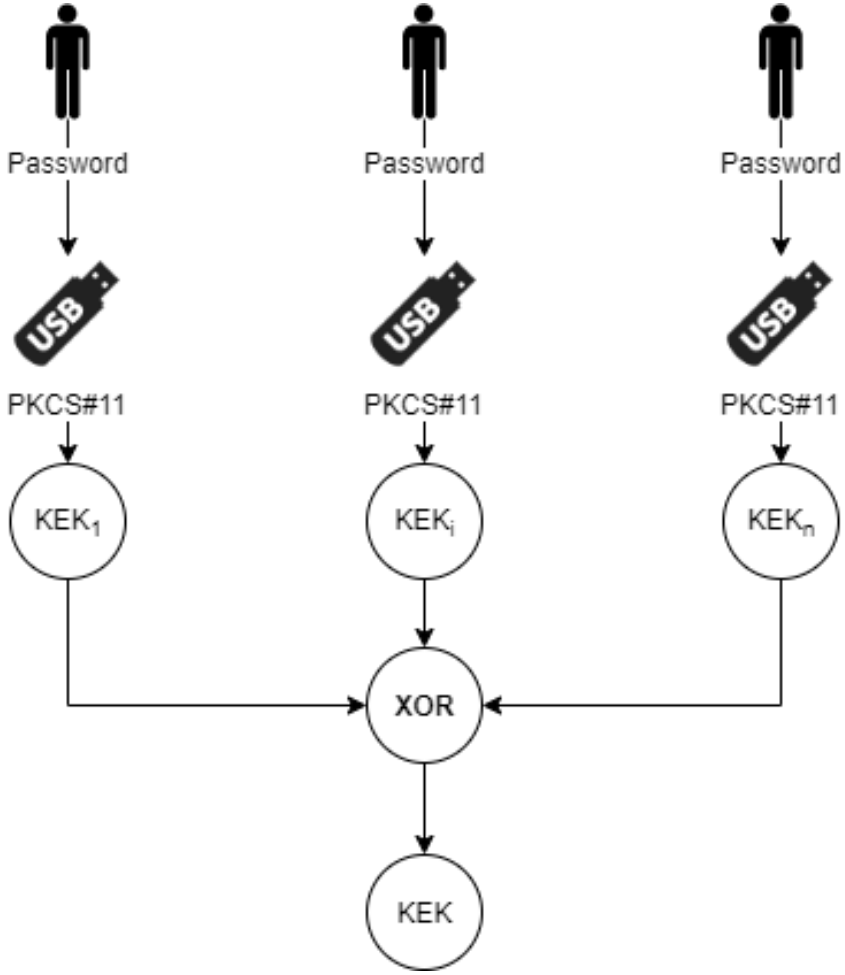
- Не используйте небезопасные режимы (например, ECB).
- Пароль != ключ. Не генерируйте ключи шифрования напрямую из паролей пользователей (энтропия будет недостаточна). Используйте функции деривации PBKDF2/Argon2.
- Никогда не хардкодьте ключи шифрования или другие данные (например IV).
- Не изобретайте свой алгоритм, если не имеете в этом подтвержденного признанного опыта в индустрии.

Этап 5. Защита хранимых данных *(продолжение)*

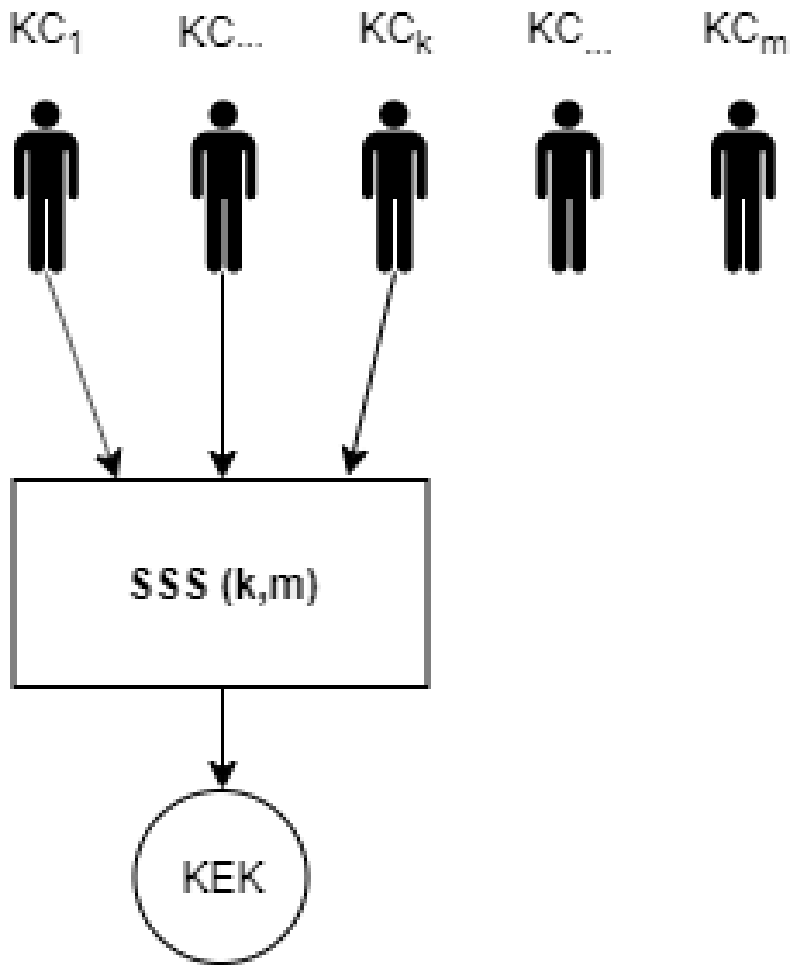


Этап 5. Защита хранимых данных *(продолжение)*





Этап 5. Защита хранимых данных *(продолжение)*



Внедрение системы менеджмента ИБ

- Информационная безопасность – это процесс, который имеет начало, но не имеет конца, и им необходимо управлять. Для закрепления внедренных методов защиты данных о держателях карт следует внедрить процессы информационной безопасности, выполняемые на практике в строгом соответствии с документированными процедурами. Хорошим решением здесь будет следование рекомендациям таких стандартов, как, например, ISO 27001.

- Структура нормативных документов (документированных процедур) по информационной безопасности в первую очередь должна быть адекватной размерам, организационной структуре и бизнес-процессам организации.

Процесс управления рисками

- Общий анализ рисков. Необходим для того, чтобы обнаружить риски, которые не обработаны контрмерами, описанными в стандарте PCI DSS. Должен учитывать:
  - оценку периодичности для контрмер;
  - оценку стойкости криптографических алгоритмов;
  - оценку наличия поддержки и обновлений безопасности для компонентов информационной инфраструктуры.
- Таргетированный анализ рисков. Необходим для того, чтобы в рамках конкретно взятого требования применить Индивидуальный подход.

Взаимодействие с работниками

- кадровые проверки;
- повышение осведомленности в области информационной безопасности:
  - ознакомление с внутренней нормативной документацией, а также процессами и процедурами информационной безопасности;
  - составление и исполнение планов повышения осведомленности, включая обучение противодействию фишингу;
  - выбор подходящего способа повышения осведомленности для работников с определенными ролями;
- распределение ответственности и обязанностей.

Регулярные процедуры ИБ

Ежедневно:

- изучение и анализ журналов протоколирования событий.

Раз в неделю:

- выполнение контроля целостности критичных файлов;
- просмотр публикаций в открытых источниках информации с целью обнаружения актуальных уязвимостей.

Раз в месяц:

- установка критичных обновлений безопасности программного обеспечения.

Регулярные процедуры ИБ *(продолжение)*

Раз в 3 месяца:

- анализ мест хранения PAN и уничтожение данных, хранение которых более не требуется для бизнес-целей Компании (в том числе анализ записей в логах);
- проведение ASV-сканирования на уязвимости;
- проведение внутреннего сканирования на уязвимости;
- проведение внутреннего аудита выполнения работниками Компании требований нормативных документов.

Регулярные процедуры ИБ *(продолжение)*

Раз в 6 месяцев:

- пересмотр правил межсетевого экранирования;
- пересмотр учетных записей и прав доступа в информационных системах;
- тестирование на проникновение.

Регулярные процедуры ИБ *(продолжение)*

Раз в 12 месяцев:

- смена ключей шифрования ДДК;
- анализ рисков информационной безопасности;
- проведение оценки необходимости применения антивирусного ПО для компонентов, которые считаются не подверженными воздействию вредоносного кода;
- пересмотр и обновление внутренних нормативных документов по обеспечению информационной безопасности;

Регулярные процедуры ИБ *(продолжение)*

Раз в 12 месяцев *(продолжение)*:

- ознакомление работников с требованиями внутренних нормативных документов по обеспечению информационной безопасности под роспись;
- проверка статуса соответствия поставщиков услуг требованиям стандарта PCI DSS, актуализация перечня поставщиков услуг;
- разработка годового плана повышения осведомленности работников в области обеспечения информационной безопасности;

Регулярные процедуры ИБ *(продолжение)*

Раз в 12 месяцев *(продолжение)*:

- контроль практических навыков и теоретических знаний пользователей информационной инфраструктуры;
- разработка, пересмотр, тестирование и актуализация планов реагирования на инциденты ИБ;
- проведение сертификационного QSA-аудита.

QSA-аудит

QSA-аудит

Сертификационный QSA-аудит (Qualified Security Assessment) – внешняя независимая аудиторская проверка соответствия организации требованиям стандарта PCI DSS, выполняемая QSA-аудиторами, сертифицированными Советом PCI SSC.

Актуальность статуса аудитора можно проверить на сайте Совета PCI SSC.

Являясь наиболее серьезным вариантом подтверждения соответствия организации требованиям PCI DSS, QSA-аудит дает наиболее объективные результаты и пользуется максимальным уровнем доверия со стороны международных платежных систем, эквайреров и иных участников индустрии платежных карт.

QSA-аудит

1. Согласовать область аудита PCI DSS с QSA-аудитором.
2. Предоставить документацию организации, связанную с областью аудита PCI DSS QSA-аудитору.
3. Определить локации для QSA-аудита.
4. Согласовать план аудита с QSA-аудитором.
4. Пройти очную часть QSA-аудита.
5. Исправить несоответствия, если они были найдены.
6. Ожидать заполнения отчетных документов QSA-аудитором.
7. Подписать PCI DSS AOC.

QSA-аудит

1. Интервью.
2. Наблюдение.
3. Анализ документации, в том числе и записей.
4. Анализ кода.
5. Анализ конфигураций.
6. Сбор свидетельств.

Свидетельства хранятся в QSA-компании не менее 3 лет.

QSA-аудит

Отчетные документы, предоставляемые после QSA-аудита:

- AOC (Attestation Of Compliance) – свидетельство о соответствии. Документ, подтверждающий статус соответствия организации требованиям PCI DSS.
- ROC (Report On Compliance) – отчет о соответствии. Документ, в котором детально описаны наблюдения аудитора в ходе QSA-аудита.

Если проводилась оценка по Приложению A3 (DESV), то предоставляются дополнительно:

- S-AOC
- S-ROC

Результаты QSA-аудита

Итог	Поставщик услуг (в т.ч. банк)	Торгово-сервисное предприятие
Подтверждено 100% соответствие	**QSA предоставляет компании:** • ROC; • AOC; • Сертификат Соответствия. В случае, если поставщик услуг зарегистрирован в МПС, то **QSA предоставляет МПС:** • Свидетельство о Соответствии; • Резюме Отчета о Соответствии; • Отчет о Соответствии (по запросу).	**QSA предоставляет компании:** • ROC; • AOC; • Сертификат Соответствия. ТСП по запросу предоставляет Отчет о Соответствии своему банку-эквайреру.
Выявлены несоответствия	**QSA предоставляет компании:** • ROC*; • AOC.	**QSA предоставляет компании:** • ROC*; • AOC.

* – по желанию компании в случае несоответствия PCI DSS, QSA помогает компании заполнить форму отчетного документа «План действий по устранению несоответствий» для отправки его в МПС или банку-эквайреру.