Соответствие требованиям PCI DSS

29 июня 2012 г.

Содержание

Solidex

- Соответствие требованиям PCI DSS
- Соотношение формальных требований PCI DSS и состояния информационной безопасности

Какова важность соответствия PCI DSS?

Solidex

- Для организации, обрабатывающей информацию, включающую данные о держателях карт, соответствие требованиям PCI DSS является входным билетом для занятия данным видом деятельности
- По нашим наблюдениям, для большинства предприятий РБ формальное соответствие требованиям стандартов имеет большее значение, чем фактическое состояние информационной безопасности

Соответствие требованиям на текущий момент

Solidex

Часть требований, связанных с техническими аспектами безопасности, возможно, уже удовлетворена: используются средства защиты информации с функциями Firewall, IPS, Antivirus

Соответствие требованиям PCI DSS: FW, IPS, AV

Solidex

		FW	IPS	AV
1	**Должны быть разработаны стандарты конфигурации межсетевых экранов и маршрутизаторов…**			
1.1	Должны быть разработаны стандарты конфигурации и межсетевых экранов и маршрутизаторов…			
1.2	Должна быть создана конфигурация межсетевых экранов, которая запрещает все соединения между недоверенными сетями…	✔		
1.3	Должна быть запрещена прямая коммуникация между сетью Интернет и любым компонентом среды…	✔		
1.4	Должны быть установлены персональные межсетевые экраны на все мобильные компьютеры...			
2	**Не использовать пароли и другие системные параметры, заданные производителем по умолчанию**			
2.1	Всегда следует менять настройки, установленные производителем по умолчанию…			
2.2	Должны быть разработаны стандарты конфигурации для всех системных компонентов…			
2.3	При использовании неконсольного административного доступа к системе, следует всегда шифровать канал с использованием стойких криптографических алгоритмов...			
2.4	Хостинг-провайдеры должны обеспечивать безопасность сред и данных…			
3	**Обеспечить безопасное хранение данных о держателях карт**			
3.1	Хранение данных о держателях карт должно быть ограничено только необходимым минимумом…			
3.2	Запрещается хранить критичные аутентификационные данные после авторизации (даже в зашифрованном виде).			
3.3	Следует маскировать PAN при его отображении (максимально возможное количество знаков PAN …)	✔		
3.4	PAN должен быть представлен в нечитаемом виде во всех местах хранения…			
3.5	Следует обеспечить защиту всех ключей шифрования данных…			
3.6	Должны быть полностью документированы и внедрены все процессы и процедуры управления ключами шифрования данных…			

Соответствие требованиям PCI DSS: FW, IPS, AV (2)

Solidex

		FW	IPS	AV
4	**Обеспечить шифрование данных о держателях карт при их передаче через сети общего пользования**			
4.1	Для защиты данных о держателях карт во время передачи их через общедоступные сети следует использовать стойкие криптографические алгоритмы и безопасные протоколы…	✓		
4.2	Никогда не следует пересылать незащищенный PAN при помощи пользовательских технологий передачи сообщ.		✓	
5	**Использовать и регулярно обновлять антивирусное программное обеспечение**			
5.1	Антивирусное программное обеспечение должно быть развернуто на всех системах, подверженных воздействию вирусов (особенно рабочих станциях и серверах).			✓
5.2	Антивирусные механизмы должны быть актуальными, постоянно включенными и … вести журналы событий.			✓
6	**Разрабатывать и поддерживать безопасные системы и приложения**			
6.1	На все системные компоненты и программное обеспечение должны быть установлены самые свежие обновления безопасности, выпущенные производителем…			
6.2	Должен быть внедрен процесс выявления и определения вновь обнаруженных уязвимостей по уровню риска.			
6.3	Приложения … должны разрабатываться в соответствии с требованиями PCI DSS…			
6.4	Должны быть разработаны и внедрены процедуры управления изменениями системных компонентов…			
6.5	Процесс разработки приложений должен предупреждать возникновение общеизвестных уязвимостей .. кода …			
6.6	Следует обеспечить защиту общедоступных веб-приложений от известных атак…			
7	**Ограничить доступ к данным платежных карт в соответствии со служебной необходимостью**			
7.1	Доступом к вычислительным ресурсам и информации о держателях карт должны обладать только те сотрудники, которым такой доступ необходим в соответствии с их должностными обязанностями.			
7.2	Для многопользовательских систем следует установить механизм разграничения доступа, основанный на факторе знания и применяющий принцип «запрещено все, что явно не разрешено»…			

Соответствие требованиям PCI DSS: FW, IPS, AV (3)

Solidex

		FW	IPS	AV
8	**Назначить уникальный идентификатор каждому лицу, имеющему доступ к информационной инфраструктуре**			
8.1	Каждому пользователю должно быть назначено уникальное имя учетной записи до предоставления ему доступа к компонентам системы и данным о держателях карт.			
8.2	Помимо идентификатора, должен применяться хотя бы один из следующих методов для аутентификации всех пользователей…			
8.3	Для средств удаленного доступа сотрудников, администраторов и третьих лиц к компьютерной сети (на сетевом уровне извне сети) должен быть реализован механизм двухфакторной аутентификации…			
8.4	Все пароли должны храниться и передаваться только в зашифрованном виде…			
8.5	Должен быть установлен контроль над выполнением процедур идентификации и аутентификации пользователей и управления паролями учетных записей…			
9	**Ограничить физический доступ к данным платежных карт**			
10	**Контролировать и отслеживать любой доступ к сетевым ресурсам и данным о держателях карт**			
10.1	Должен быть разработан процесс мониторинга доступа к компонентам системы…			
10.2	Для каждого системного компонента должен быть включен механизм протоколирования … событий…			
10.3	Для каждого события каждого системного компонента должны быть записаны … следующие параметры…			
10.4	Необходимо использовать технологию синхронизации времени…			
10.5	Журналы протоколирования событий должны быть защищены от изменений.			
10.6	Следует просматривать журналы протоколирования событий не реже одного раза в день…			
10.7	Журналы регистрации событий должны храниться не менее одного года, а также быть в оперативном доступе не менее трех месяцев…			

Соответствие требованиям PCI DSS: FW, IPS, AV (4)

Solidex

		FW	IPS	AV
11	**Регулярно выполнять тестирование систем и процессов обеспечения безопасности**			
11.1	Следует ежеквартально … отслеживать неавторизованные беспроводные точки доступа.			
11.2	Следует проводить внешнее и внутреннее сканирование сети на наличие уязвимостей не реже одного раза в квартал, а также после внесения значительных изменений…			
11.3	Следует проводить внешний и внутренний тест на проникновение не реже одного раза в год…			
11.4	Следует использовать системы обнаружения вторжений и/или системы предотвращения вторжений для контроля сетевого трафика по периметру среды данных…		✓	
11.5	Следует использовать средства контроля целостности файлов для оповещения персонала о несанкционированных изменениях критичных системных файлов, конфигурационных файлов и файлов данных…			
12	**Разработать и поддерживать политику информационной безопасности для всего персонала организации**			
12.1	Должна быть разработана, опубликована и распространена поддерживаемая в актуальном состоянии политика информационной безопасности.			
12.2	Должны быть разработаны ежедневные процедуры безопасности, соответствующие требованиям … стандарта…			
12.3	Должны быть разработаны правила эксплуатации для критичных технологий…			
12.4	Политика и процедуры безопасности должны однозначно определять обязанности всего персонала организации…			
12.5	Определенному сотруднику или группе сотрудников должны быть назначены .. обязанности в области управления информационной безопасностью…			
12.6	Должна быть внедрена … программа повышения осведомленности персонала компании о вопросах безопасности.			
12.7	Следует тщательно проверять кандидатов при приеме на работу, для минимизации риска внутренних атак.			
12.8	В случае, когда данные о держателях карт становятся доступны поставщикам услуг, то должны быть разработаны политики и процедуры взаимодействия с ними…			
12.9	Должен быть внедрен план реагирования на инциденты…			

Соответствие по пунктам: 8 из 52

Соответствие может быть более строгим

Solidex

Соответствие требованиям стандарта может быть более строгим, если усилить систему защиты информации дополнительными средствами:

- SIEM: Security Information and Event Management
- CCM: Configuration Compliance Management
- FIM: File Integrity Monitoring
- VM: Vulnerability Management

Соответствие требованиям PCI DSS: SIEM, CCM, FIM, VM

Solidex

		FW	IPS	AV	SIEM	CCM	FIM	VM
1	**Должны быть разработаны стандарты конфигурации межсетевых экранов и маршрутизаторов…**							
1.1	Должны быть разработаны стандарты конфигурации и межсетевых экранов…					✓		
1.2	Должна быть создана конфигурация межсетевых экранов, которая запрещает все соединения между недоверенными сетями…	✓						
1.3	Должна быть запрещена прямая коммуникация между сетью Интернет и любым компонентом…	✓						
1.4	Должны быть установлены персональные межсетевые экраны на все мобильные компьютеры...					✓		
2	**Не использовать пароли и другие системные параметры, заданные производителем по умолчанию**							
2.1	Всегда следует менять настройки, установленные производителем по умолчанию…					✓		
2.2	Должны быть разработаны стандарты конфигурации для всех системных компонентов…					✓		
2.3	При использовании неконсольного административного доступа к системе, следует всегда шифровать канал с использованием стойких криптографических алгоритмов.					✓		
2.4	Хостинг-провайдеры должны обеспечивать безопасность сред и данных, принадлежащих каждой из обслуживаемых сторон.							
3	**Не использовать пароли и другие системные параметры, заданные производителем по умолчанию**							
3.1	Хранение данных о держателях карт должно быть ограничено только необходимым минимумом.						✓	
3.2	Запрещается хранить критичные аутентификационные данные после авторизации…							
3.3	Следует маскировать PAN при его отображении…	✓						
3.4	PAN должен быть представлен в нечитаемом виде во всех местах хранения…							
3.5	Следует обеспечить защиту всех ключей шифрования данных… (безопасное хранение ключей)						✓	
3.6	Должны быть … внедрены все процессы и процедуры управления ключами шифрования данных.							

Соответствие требованиям PCI DSS: SIEM, CCM, FIM, VM (2)

Solidex

		FW	IPS	AV	SIEM	CCM	FIM	VM
4	**Обеспечить шифрование данных о держателях карт при их передаче через сети общего пользования**							
4.1	Для защиты данных о держателях карт во время передачи их через общедоступные сети следует использовать стойкие криптографические алгоритмы и безопасные протоколы…	✓						
4.2	Никогда не следует пересылать незащищенный PAN при помощи пользовательских технологий...		✓					
5	**Использовать и регулярно обновлять антивирусное программное обеспечение**							
5.1	Антивирусное программное обеспечение должно быть развернуто на всех системах…			✓		✓		
5.2	Антивирусные механизмы должны быть актуальными, постоянно включенными…			✓		✓		
6	**Разрабатывать и поддерживать безопасные системы и приложения**							
6.1	На все системные компоненты и программное обеспечение должны быть установлены самые свежие обновления безопасности, выпущенные производителем…							✓
6.2	Должен быть внедрен процесс выявления и определения вновь обнаруженных уязвимостей…							✓
6.3	Приложения … должны разрабатываться в соответствии с требованиями PCI DSS…							
6.4	Должны быть разработаны и внедрены процедуры управления изменениями системных компонентов…							
6.5	Процесс разработки приложений должен предупреждать возникновение общеизвестных уязвимостей .. кода …							✓
6.6	Следует обеспечить защиту общедоступных веб-приложений от известных атак…							✓
7	**Ограничить доступ к данным платежных карт в соответствии со служебной необходимостью**							
7.1	Доступом к вычислительным ресурсам и информации … должны обладать только те сотрудники, которым такой доступ необходим в соответствии с их должностными обязанностями.							
7.2	Для многопользовательских систем следует установить механизм разграничения доступа…							

Соответствие требованиям PCI DSS: SIEM, CCM, FIM, VM (3)

Solidex

		FW	IPS	AV	SIEM	CCM	FIM	VM
8	**Назначить уникальный идентификатор каждому лицу, имеющему доступ к информационной инфраструктуре**							
8.1	Каждому пользователю должно быть назначено уникальное имя учетной записи до предоставления ему доступа к компонентам системы и данным о держателях карт.							
8.2	Помимо идентификатора, должен применяться хотя бы один из следующих методов для аутентификации всех пользователей…							
8.3	Для средств удаленного доступа сотрудников, администраторов и третьих лиц к компьютерной сети (на сетевом уровне извне сети) должен быть реализован механизм двухфакторной аутентификации…							
8.4	Все пароли должны храниться и передаваться только в зашифрованном виде…							
8.5	Должен быть установлен контроль над выполнением процедур идентификации и аутентификации пользователей и управления паролями учетных записей…							
9	**Ограничить физический доступ к данным платежных карт**							
10	**Контролировать и отслеживать любой доступ к сетевым ресурсам и данным о держателях карт**							
10.1	Должен быть разработан процесс мониторинга доступа к компонентам системы…				✓			
10.2	Для каждого системного компонента должен быть включен механизм протоколирования …							
10.3	Для каждого … должны быть записаны … следующие параметры…							
10.4	Необходимо использовать технологию синхронизации времени…							
10.5	Журналы протоколирования событий должны быть защищены от изменений.				✓			
10.6	Следует просматривать журналы протоколирования событий не реже одного раза в день…				✓			
10.7	Журналы регистрации событий должны храниться не менее одного года, а также быть в оперативном доступе не менее трех месяцев…				✓			

Соответствие требованиям PCI DSS: SIEM, CCM, FIM, VM (4)

Solidex

		FW	IPS	AV	SIEM	CCM	FIM	VM
11	**Регулярно выполнять тестирование систем и процессов обеспечения безопасности**							
11.1	Следует ежеквартально … отслеживать неавторизованные беспроводные точки доступа.							
11.2	Следует проводить внешнее и внутреннее сканирование сети на наличие уязвимостей…							✓
11.3	Следует проводить внешний и внутренний тест на проникновение не реже одного раза в год…							✓
11.4	Следует использовать системы обнаружения вторжений и/или системы предотвращения вторжений для контроля сетевого трафика по периметру среды данных…		✓					
11.5	Следует использовать средства контроля целостности файлов для оповещения персонала о несанкционированных изменениях критичных системных файлов, конфигурационных файлов…						✓	
12	**Разработать и поддерживать политику информационной безопасности для всего персонала организации**							
12.1	Должна быть разработана, … распространена … политика информационной безопасности.							
12.2	Должны быть разработаны ежедневные процедуры безопасности…							
12.3	Должны быть разработаны правила эксплуатации для критичных технологий…							
12.4	Политика и процедуры безопасности должны однозначно определять обязанности всего персонала организации…							
12.5	Определенному сотруднику или группе сотрудников должны быть назначены .. обязанности в области управления информационной безопасностью…							
12.6	Должна быть внедрена … программа повышения осведомленности персонала компании о вопросах безопасности.							
12.7	Следует тщательно проверять кандидатов при приеме на работу…							
12.8	В случае, когда данные о держателях карт становятся доступны поставщикам услуг, то должны быть разработаны политики и процедуры взаимодействия с ними…							
12.9	Должен быть внедрен план реагирования на инциденты…				✓			

Соответствие по пунктам: 27 из 52

Содержание

Solidex

- Соответствие требованиям PCI DSS
- Соотношение формальных требований PCI DSS и состояния информационной безопасности

Соотношение соответствия и безопасности

Solidex

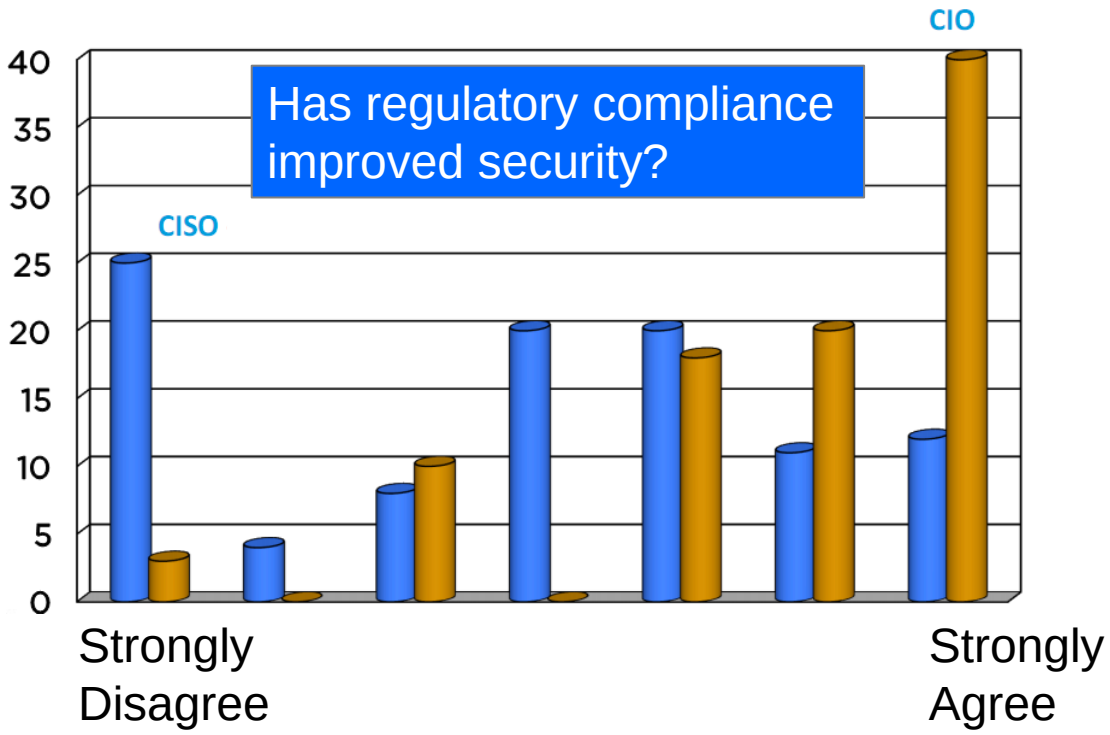
Является ли соответствие стандарту PCI DSS синонимом уровню информационной безопасности?

Безопасность не ограничивается соответствием

Solidex

«Complying with regulations doesn't necessarily make companies more secure»

Robert Frances Group, 2007



Source: NetWitness

Требования стандарта в условиях новых угроз

- Гарантирует ли соответствие требованиям PCI DSS защиту от разработанных под контекст организации атак, сигнатур которых не существует (APT)?
- Традиционные средства защиты оказываются «слепы» в силу используемых против них техник уклонения

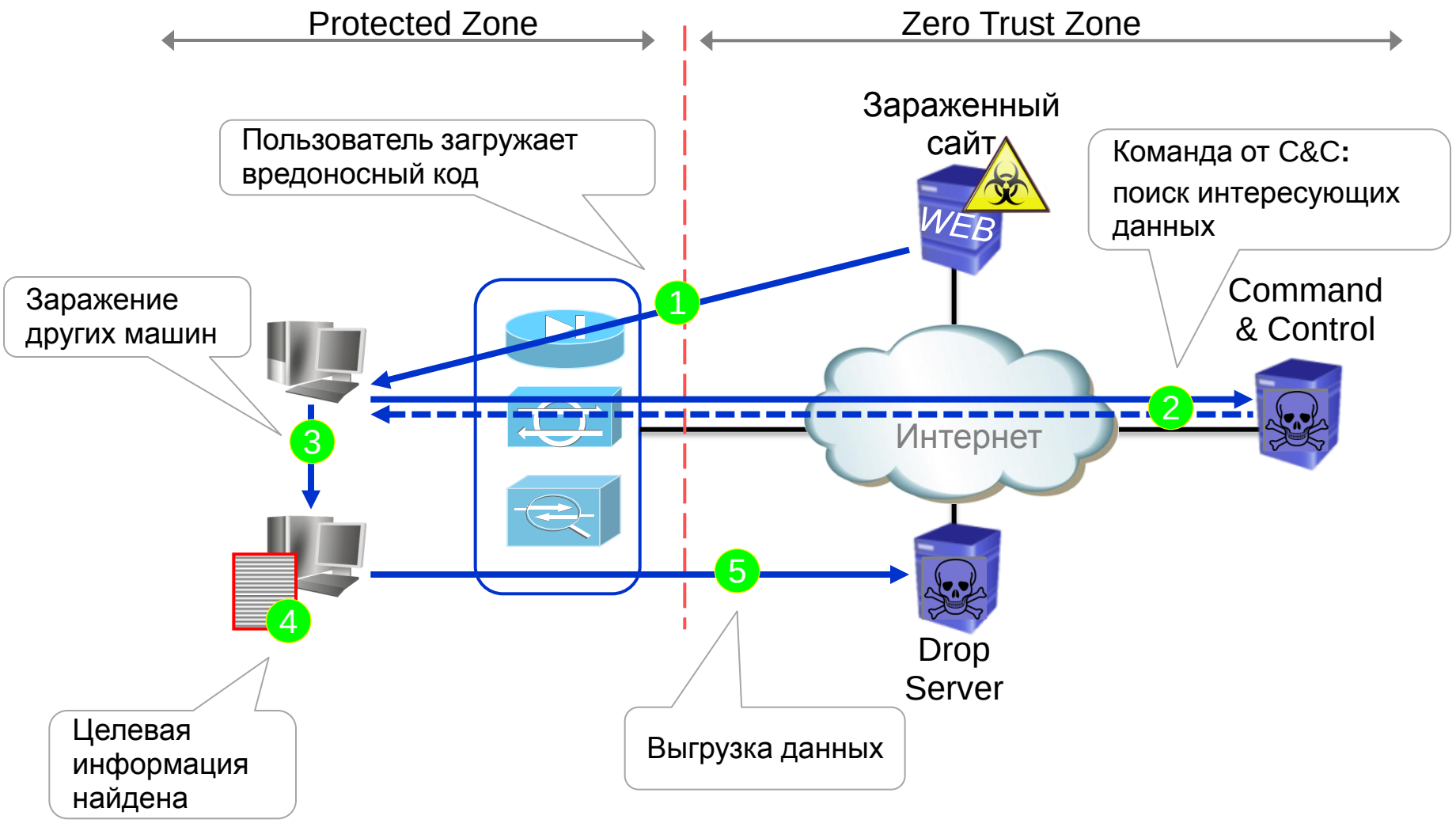
Средство защиты	**Техника уклонения**
Antivirus	полиморфизм, embedded malware, вирусы «Zero day»
Firewall	маскировка в разрешенных каналах
IPS	уязвимости «Zero day»

Противостояние новым угрозам

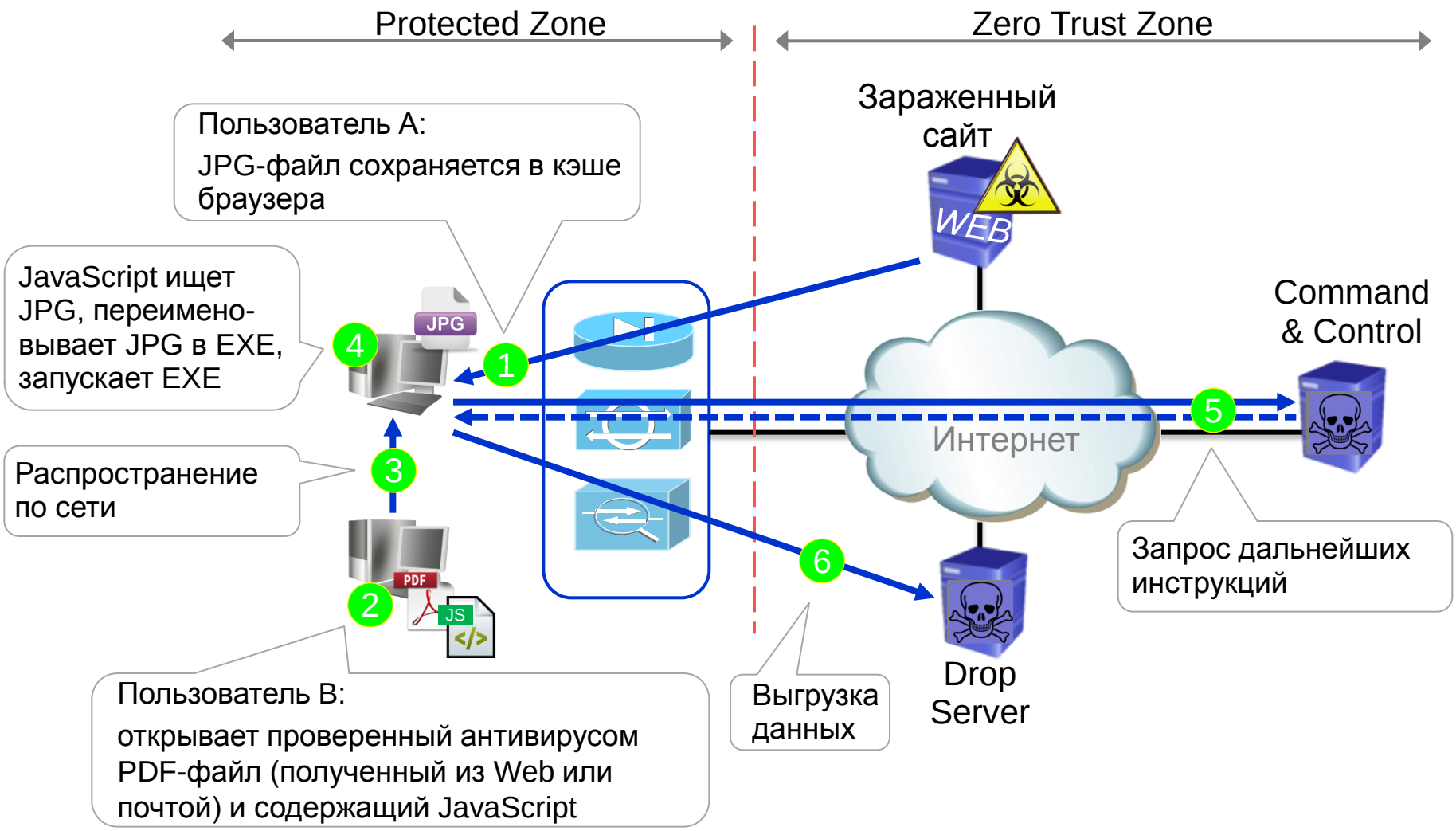
Solidex

- Управление уязвимостями: VM
- Контроль целостности критичных системных файлов, файлов конфигураций, данных: FIM, CCM
- Обнаружение аномальных взаимодействий с учетом контента и контекста: NGIPS
- Корреляция событий: NGSIEM
  - Регистрируемых различными источниками
  - Распределенных во времени
  - С учетом контекста

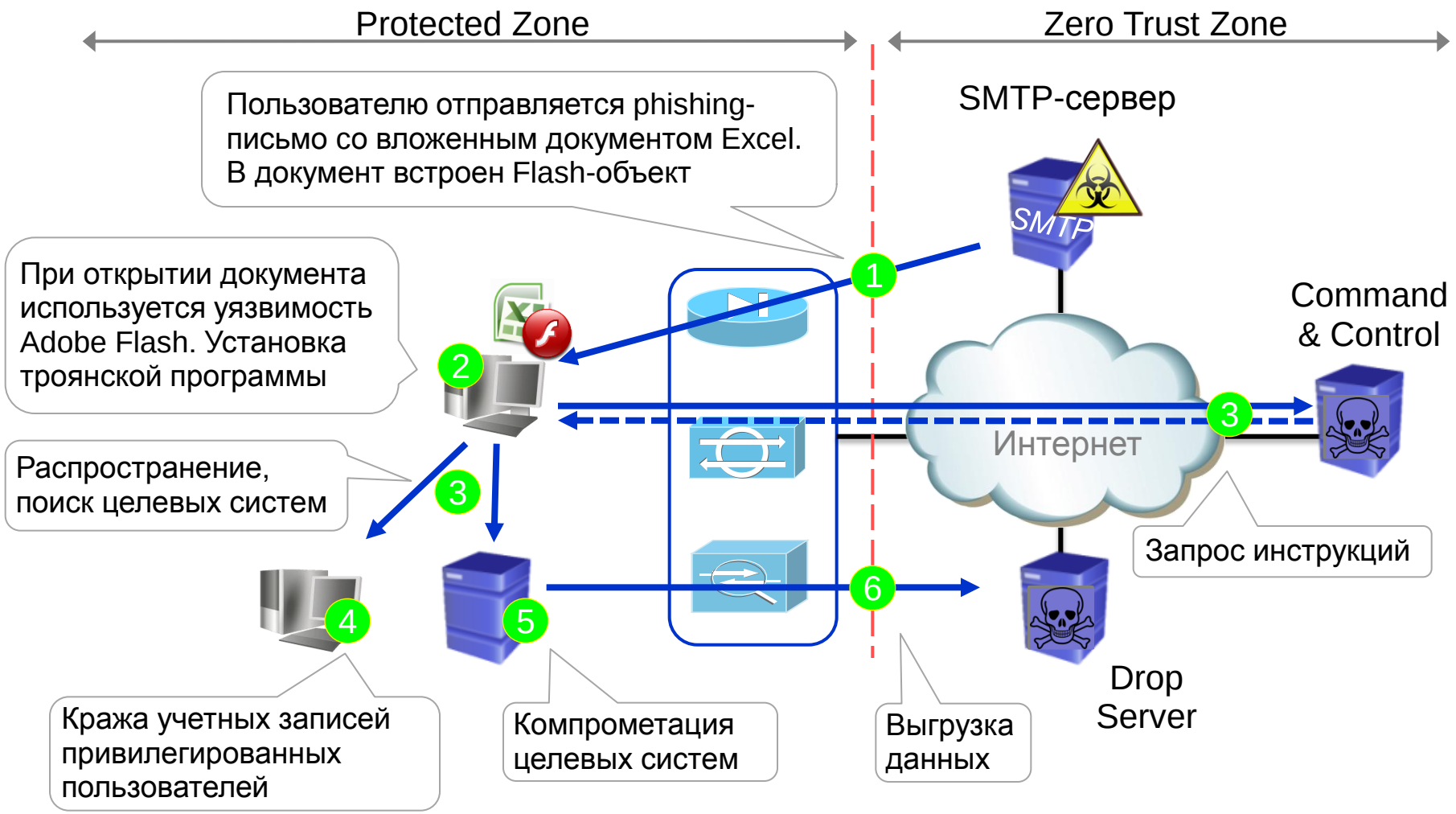
Пример атаки 1



Пример атаки 2



Пример атаки 3 (атака RSA)



Краткое резюме

- Соответствие требованиям PCI DSS само по себе не является адекватной мерой защиты от разработанных под контекст организации атак, для которых не существует сигнатур (APT)
- Анализ контента и контекста взаимодействий, обнаружение несанкционированных изменений файлов, сбор, корреляция и анализ событий от различных источников в рамках широкого временного окна наряду с применение средств защиты информации - FW, IPS, AV, SIEM, CCM, FIM, VM - поднимают уровень информационной безопасности