ВЕРИФИКАЦИЯ ТРЕБОВАНИЙ СТАНДАРТА PCI DSS 3.1 НА СООТВЕТСТВИЕ ТРЕБОВАНИЯМ ЗАКОНОДАТЕЛЬСТВА РФ

Борхаленко В.А.[1]

В статье приводится обоснование необходимости проверки предприятия на соответствие его систем обеспечения информационной безопасности стандарту безопасности индустрии платежных карт, вызванной наличием различного типа уязвимостей в банковских информационных системах, а также информационных системах торгово–сервисных компаний, участвующих в системах обслуживания электронных платежей. Наибольшие финансовые риски связаны с вероятностью возникновения точек массовой компрометации данных держателей платежных карт с последующим использованием полученной информации для совершения мошенничества. Основной задачей, решаемой стандартом PCI DSS (Payment Card Industry Data Security Standard) является предотвращение указанных точек массовой компрометации. В статье приводится анализ стандарта индустрии платежных карт PCI DSS 3.1 на соответствие требованиям безопасности персональных данных, содержащимся в законодательстве РФ, в частности требованиям, определенным в Приказе №21 ФСТЭК от 18 февраля 2013 г. «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и Постановлении Правительства РФ «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 01 ноября 2012 г. № 1119.

На основании выявленных несоответствий разработаны рекомендации по доработке организационно–распорядительной документации, регламентирующей процессы обеспечения информационной безопасности компаний, сертифицированных по стандарту PCI DSS, в целях приведения указанных процессов в соответствие с требованиями российских регуляторов в области защиты персональных данных.

***Ключевые слова**: PCI DSS, персональные данные, политика безопасности, процедура идентификации, обеспечение безопасности, безопасность платежных карт, электронная коммерция, меры безопасности*

Стандарт PCI DSS и проблема компрометации данных держателей платежных карт

Проблема наличия рисков безопасности банковских информационных систем (ИС), а также ИС торгово-сервисных компаний, участвующих в процессах обслуживания электронных платежей, влекущих массовую компрометацию данных держателей платежных карт с последующим использованием полученной информации для совершения мошенничества, стала одной из главных причин, побудившей международные платежные системы объединить свои усилия и принять дополнительные меры для защиты своих клиентов.

С этой целью в 2004г. был разработан единый набор требований к безопасности данных – PCI DSS [1-7], объединивший в себе требования ряда программ по безопасности таких платежных систем как Visa, MasterCard, American Express, Discover Card и JCB. Последней версией стандарта на данный момент является версия PCI DSS 3.1[2].

Законодательство в области защиты персональных данных в РФ

Федеральным законом «О персональных данных» от 27 июля 2006 г. № 152-ФЗ[3], главой 14 Трудового Кодекса Российской Федерации от 30 декабря 2001 г. № 197-ФЗ[4], Постановлением Правительства РФ «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 01 ноября 2012 г. № 1119[5] были установлены

1 Борхаленко Вадим Анатольевич, Национальный исследовательский университет «МЭИ», г.Москва, email: vadikhide@yandex.ru

2 Стандарт безопасности данных индустрии платежных карт PCI DSS 3.1 [Электронный ресурс]. Режим доступа: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf (дата обращения 11.09.2015).

3 Федеральный закон «О персональных данных» от 27 июля 2006 г. № 152 [Электронный ресурс]. - Режим доступа: http://www.rg.ru/2006/07/29/personaljnye-dannye-dok.html (дата обращения 11.09.2015)

4 Трудовой кодекс Российской Федерации от 30 декабря 2001 г. N 197-ФЗ [Электронный ресурс]. - Режим доступа: http://www.rg.ru/2001/12/31/trud-dok.html (дата обращения 11.09.2015)

5 Постановление Правительства РФ «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 01 ноября 2012 г. № 1119 [Электронный ресурс]. - Режим доступа: http://www.rg.ru/2012/11/07/pers-dannye-dok.html (дата обращения 11.09.2015).

правила и требования в отношении порядка обработки и обеспечения безопасности персональных данных (ПДн), как собственных работников, так и сторонних физических лиц, ПДн которых обрабатываются в организации. На основании вышеуказанных правил регуляторами (ФСТЭК России, ФСБ России и Банком России) разработаны руководящие и нормативно-методические документы по защите ПДн, одним из них является приказ ФСТЭК «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» от 18 февраля 2013 г. №21[6].

Невыполнение требований указанных правовых актов, а также нормативных документов регуляторов по вопросам обработки и защиты ПДн может привести к гражданским искам со стороны субъектов ПДн, приостановлению или прекращению обработки ПДн в ходе выполнения перевода денежных средств и выполнения платежей с использованием пластиковых карт, привлечению руководителей и должностных лиц к административной, уголовной, гражданской, дисциплинарной и иным видам ответственности (в соответствии с КоАП и УК РФ), приостановлению действия или аннулированию лицензий на деятельность, иным репутационным рискам и рискам недобросовестной конкуренции.

Исследуем на предмет возможности использования имеющегося у компании сертификата [8,9] на соответствие требованиям PCI DSS в качестве гарантии выполнения компанией требований российского законодательства [10] в области защиты ПДн, в частности требованиям, определенным в документе Приказа №21 ФСТЭК от 18 февраля 2013 г.. В случае выявленной неполноты требований PCI DSS относительно российских требований, предполагается разработка рекомендаций по приведению организационно-распорядительной документации компании – оператора ПДн в соответствие с требованиями российских регуляторов. А также предложим рекомендации для внесения в комплект типовых организационно-распорядительных документов по ИБ организации.

Сравнение мер по обеспечению безопасности

При сравнении мер по обеспечению безопасности ПДн, необходимых для обеспечения каждого из уровней защищенности ПДн, описанных в постановлении Правительства РФ № 1119 от 01 ноября 2012 г. с PCI DSS 3.1 было выявлено отсутствие соответствия требований стандарта PCI DSS 3.1, следующим необходимым мерам обеспечения безопасности ПДн, описанных в приказе ФСТЭК №21 и предложены следующие рекомендации:

1. **УПД.7:**

В политике ИБ (либо иной другой политике, определяющей требования по обеспечению доступа к информационным ресурсам (ИР)) указать требование разместить на рабочих местах, с которых возможна обработка ПДн, памятки содержащей правила, установленные оператором. Так же в политике должно быть указано должностное лицо, ответственное за актуализацию указанной памятки и ее наличие на рабочих местах.

2. **УПД.8:**

Для соответствующего уровня защиты ИС обеспечить в ИС после успешного завершения процесса аутентификации пользователя в ИС оповещение этого пользователя о дате и времени предыдущего входа в ИС от имени этого пользователя. Данные рекомендации можно реализовать в политике доступа к ИР или правилах работы с автоматизированной системой.

3. **УПД.9:**

Включить в политику доступа к ИР ограничения на число параллельных сеансов доступа или правилах работы с автоматизированной системой.

4. **УПД.11:**

Оператором ИС должен быть установлен перечень действий пользователей, разрешенных до прохождения ими процедур идентификации и аутентификации, и запрет действий пользователей, не включенных в перечень разрешенных действий, до прохождения ими процедур идентификации и аутентификации. Внести список действий пользователей, разрешенных до прохождения ими процедур идентификации и аутентификации в список в общую политику ИБ, либо в Политику (правила) доступа к ИР.

5. **УПД.16:**

Внедрить в политику обеспечения ИБ при взаимодействии с третьими сторонами следующие положения:

1) Определение типов прикладного программного обеспечения (ПО) ИС, к которым разрешен доступ авторизованным пользователям из внешних ИС.
2) Определение системных учетных записей, используемых в рамках данного взаимодействия.

6 Приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 18 февраля 2013 г. N 21 [Электронный ресурс]. - Режим доступа: http://www.rg.ru/2013/05/22/soderjanie-dok.html (дата обращения 11.09.2015).

3) Определение порядка предоставления доступа к ИС авторизованными пользователями из внешних ИС.
4) Определение порядка обработки, хранения и передачи информации с использованием внешних ИС.

6. **УПД.17:**

Разработать в политике ИБ правила и процедуры обеспечения доверенной загрузки средств вычислительной техники (СВТ).

1) Доверенная загрузка должна обеспечивать:
2) Блокирование попыток несанкционированной загрузки нештатной операционной системы (среды) или недоступность ИР для чтения или модификации в случае загрузки нештатной операционной системы;
3) Контроль целостности ПО и аппаратных компонентов СВТ.

7. **ОПС.4:**

В политике ИБ организации должны быть определены принципы использования временных файлов. В правилах настройки системного ПО должны быть указаны, там где это возможно, опции, обеспечивающие управление временными файлами, которое должно обеспечивать перехват записи временной информации в файлы на системном (загрузочном) разделе машинного носителя информации (МНИ) СВТ и ее перенаправление в оперативную память и (или) в другой раздел МНИ с последующей очисткой, В случае отсутствия возможности обеспечения указанных условий штатными средствами используемого системного ПО, должно быть предусмотрено использование дополнительного ПО.

8. **СОВ.2:**

Оператором должно быть задокументировано в политике установки обновлений ПО обновление базы решающих правил системы обнаружения вторжений, применяемой в ИС.

9. **ОЦЛ.7:**

Должен использоваться форматно-логический контроль вводимых данных, обеспечивающий возможность установления и проверки соблюдения форматов ввода данных, синтаксических, семантических и (или) иных правил ввода информации в ИС. Кроме того, вводимые данные должны проверяться на наличие конструкций, которые могут быть интерпретированы программно-техническими средствами ИС как исполняемые команды.

10. **ОДТ.1:**

В плане обеспечения непрерывности бизнеса с использованием аварийных процедур должно быть предусмотрено использование отказоустойчивых технических средств.

Оператором должно быть обеспечено определение требуемых характеристик (коэффициентов) надежности и готовности в соответствии с национальными стандартами.

11. **ОДТ.5:**

Оператором ИС должны быть записаны правила и процедуры восстановления информации с резервных МНИ в политике резервного копирования и восстановления данных. Включить следующие меры по восстановлению информации с резервных МНИ (резервных копий):

Определение времени, в течение которого должно быть обеспечено восстановление информации и обеспечивающего требуемые условия непрерывности функционирования ИС и доступности информации;

Восстановление информации с резервных МНИ (резервных копий) в течение установленного оператором временного интервала.

12. **ЗСВ.5:**

Включить в политику ИБ положения, включающие обеспечение доверенной загрузки серверов виртуализации, виртуальных машин (контейнеров) и серверов управления виртуализацией в соответствии с рекомендациями, предложенными к УПД.17

Предусмотреть использование технических решений, обеспечивающих доверенную загрузку.

13. **ЗСВ.6:**

Включить в политику ИБ меры и положения, обеспечивающие управление перемещением компонентов среды виртуализации.

14. **ЗСВ.10:**

В ИС должно обеспечиваться разбиение виртуальной инфраструктуры, где допустимо, на сегменты для обработки информации отдельным пользователем и (или) группой пользователей в соответствии с ЗИС.17.

15. **ЗТС.1:**

Внедрить в политику предотвращения утечки информации по каналам связи (УИКС) требования к защите информации от утечки по техническим каналам. Защита информации должна осуществляться в соответствии со специальными требованиями и рекомендациями по технической защите конфиденциальной информации (СТР-К), утвержденными приказом Гостехкомиссии России от 30 августа 2002 г. № 282, а также иными методическими документами ФСТЭК России по защите информации ограниченного доступа.

16. **ЗИС.2:**

Ввести в политику ИБ набор правил, регламентирующих настройки программно-аппаратного комплекса, обеспечивающие предотвращение задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов (служб, сервисов) с низким приоритетом.

17. **ЗИС.4:**

Оператором ИС должен быть определен перечень целей (функций) передачи данных, для которых требуется доверенный канал (маршрут).

Данную рекомендацию можно включить в политику обеспечения безопасности удаленного доступа, так как доверенный канал между пользователем и СЗИ должен обеспечиваться при удаленном и локальном доступе в ИС.

18. **ЗИС.5:**

В политике предотвращения утечки информации по побочным каналам передачи информации должен быть прописан запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств, в том числе путем сигнализации, индикации.

19. **ЗИС.8:**

В политике предотвращения УИКС должны осуществляться контроль санкционированного и исключение несанкционированного использования технологий передачи речи в ИС, в том числе регистрация событий, связанных с использованием технологий передачи речи, их анализ и реагирование на нарушения, связанные с использованием технологий передачи речи. Правила и процедуры контроля использования технологий передачи речи регламентируются в организационно-распорядительных документах оператора по защите информации.

20. **ЗИС.16:**

Включить в политику предотвращения УИКС мероприятия по выявлению и анализу скрытых каналов передачи информации для определения параметров передачи информации, которые могут использоваться для скрытого хранения информации и скрытой передачи информации за пределы ИС.

21. **ЗИС.18:**

Ввести в политику использования съемных носителей следующие меры, обеспечивающиеся в ИС:

1) Выделение в составе операционной системы и прикладного ПО частей, немодифицируемых в процессе загрузки и выполнения, и размещение их на МНИ, доступных только для чтения;
2) Загрузка и выполнение на СВТ, определяемых оператором, операционной системы с МНИ, доступных только для чтения;
3) Загрузка и выполнение на СВТ прикладного ПО, определяемого оператором, с МНИ, доступных только для чтения.

Также рекомендуется ввести в политику безопасности организации классификацию угроз безопасности, соответствующую классификации, утвержденной в постановлении № 1119 и используемой в приказе № 21 ФСТЭК.

Заключение

Исходя из приведенных выше несоответствий стандарта PCI DSS 3.1 можно сделать вывод, что соблюдение требований, выдвигаемым данным стандартом не является достаточным для обеспечения мер по обеспечению безопасности ПДн при их обработке в ИС ПДн, предполагаемых законодательством РФ и может повлечь за собой серьезные убытки вплоть до аннулирования лицензии на деятельность организации.

В соответствии с выявленными несоответствиями разработан ряд рекомендаций по их устранению, путем внесения в коллекцию типовых организационно-распорядительных документов по ИБ организации, необходимых мер по обеспечению безопасности ПДн.

Научный руководитель: кандидат технических наук, доцент, Хорев Павел Борисович, pbkh@yandex.ru

Литература:

1. Алексанов А.К., Демчев И.А. Безопасность карточного бизнеса : бизнес-энциклопедия, М.: МФПА, 2012. – 277 с.
2. Косенко М.А., Миронова В.Г. Особе нности стандарта безопасности данных индустрии платежных карт PCI DSS // Решетневские чтения. - 2012. - Т. 2. № 16. - С. 662-663.
3. Козлова Н.Ш. Актуальность обеспечения информационной безопасности в банковской системе // Актуальные проблемы технических наук Сборник статей Международной научно-практической конференции.- Уфа, 2015. - С. 105-108.
4. Bonner E., O' Raw J.Implementing the payment card industry (PCI) data security standard (DSS) // Telkomnika. -2011. - V. 9. - № 2, pp. 365-376.
5. Балийон Й. Современные тенденции в области информационной безопасности банков // Банковское дело. - 2014. - № 10. - С. 60-62.

6. Ивлев А. Соответствие стандарту PCI DSS: кому доверить аудит // Банковские технологии. - 2008. - № 8. - С. 82-86.
7. Кузин М.В. PCI DSS: Стандарт безопасности и реальная безопасность // Безопасность информационных технологий. - 2011. - № 4. - С. 120-125.
8. Эмм М. Требования стандарта PCI DSS обязательны для всех компаний, обрабатывающих или хранящих номера платежных карточек // Банковские технологии. - 2008. - № 12. - С. 32-36.
9. Давидич В. Особенности подготовки и прохождения аудита соответствия стандарту PCI DSS 2.0. взгляд изнутри // Защита информации. Инсайд. - 2011. - № 6 (42). - С. 47-51
10. Журавлева В.В., Целых А.Н. Особенности информационной безопасности банковских систем и меры по ее обеспечению // Альманах современной науки и образования. - 2015. - № 9 (99). - С. 67-71.

VERIFICATION OF THE PCI DSS 3.1 REQUIREMENTS FOR COMPLIANCE OF RUSSIAN FEDERATION LEGISLATION

Borkhalenko V.A.[7]

The article provides a justification of the enterprise's information security system testing for the payment card industry standard (PCI DSS) compliance, caused by the presence of various types of vulnerabilities in banking information systems, information systems of trade and service companies, which are participating in the electronic payment service systems. The greatest financial risks associated with the probability of occurrence of points of mass cardholders data compromitation with subsequent usage of the obtained information to commit fraud. The main object of the PCI DSS standard is to prevent these points the mass compromitation. The article provides an analysis of the payment card industry data security standard PCI DSS 3.1 for the compliance of personal data security requirements, governed by the Russian Federation legislation.

Also we give some recommendations according to the identified discrepancies to improve the organizational and administrative documents that are regulating the information security provision processes in companies that are certified according to PCI DSS in order to bring these processes into compliance with Russian regulators in the field of personal data security.

Keywords*: PCI DSS, personal data, security policy, identification procedure, information security, security of payment cards, e-commerce, security controls*

References:

1. Aleksanov A.K., Demchev I.A. Bezopasnost' kartochnogo biznesa : biznes-jenciklopedija, - M.:MFPA, 2012. – pp. 277.
2. Kosenko M.A., Mironova V.G. Osobennosti standarta bezopasnosti dannyh industrii platezhnyh kart PCI DSS // Reshetnevskie chtenija. - 2012. - T. 2. # 16. - pp. 662-663.
3. Kozlova N.Sh. Aktual'nost' obespechenija informacionnoj bezopasnosti v bankovskoj sisteme // Aktual'nye problemy tehnicheskih nauk Sbornik statej Mezhdunarodnoj nauchno-prakticheskoj konferencii. – Ufa. - 2015. - pp 105-108.
4. Bonner E., O' Raw J., Curran K. Implementing the payment card industry (pci) data security standard (dss) // Telkomnika. - 2011. - T. 9. - # 2. - pp. 365-376.
5. Balijon J. Sovremennye tendencii v oblasti informacionnoj bezopasnosti bankov // Bankovskoe delo. - 2014. - # 10. - pp. 60-62.
6. Ivlev A. Cootvetstvie standartu PCI DSS: komu doverit' audit // Bankovskie tehnologii. - 2008. - # 8. - pp. 82-86.
7. Kuzin M.V. PCI DSS: Ctandart bezopasnosti i real'naja bezopasnost' // Bezopasnost' informacionnyh tehnologij. - 2011. - # 4. - pp. 120-125.
8. Jemm M. Trebovanija standarta PCI DSS objazatel'ny dlja vseh kompanij, obrabatyvajushhih ili hranjashhih nomera platezhnyh kartochek // Bankovskie tehnologii. - 2008. - # 12. - pp. 32-36.
9. Davidich V. Osobennosti podgotovki i prohozhdenija audita sootvetstvija standartu PCI DSS 2.0. vzgljad iznutri // Zashhita informacii. Insajd. - 2011. - # 6 (42). - pp. 47-51
10. Zhuravleva V.V., Celyh A.N. Osobennosti informacionnoj bezopasnosti bankovskih sistem i mery po ee obespecheniju // Al'manah sovremennoj nauki i obrazovanija. - 2015. - # 9 (99). - pp. 67-71.

7 Vadim Borhalenko, Moscow Power Engineering Institute (National Research University), Moscow, vadikhide@yandex.ru.