АССОЦИАЦИЯ РЕГИОНАЛЬНЫХ БАНКОВ РОССИИ
(АССОЦИАЦИЯ "РОССИЯ")

109074, г.Москва,
Славянская площадь, д. 2/5/4, стр.3
тел./факс: (495) 785-29-90
e-mail: asros@asros.ru
http://www.asros.ru

18.12.14 № 06/259
На № _____ от _____

Заместителю начальника
Главного управления безопасности
и защиты информации Банка России

СЫЧЕВУ А.М.

Уважаемый Артем Михайлович,

На основании Вашего письма от 17.11.2014 № 23-5-2-4/3643 Ассоциация «Россия» провела опрос среди кредитных организаций-членов Ассоциации по проекту указания Банка России «Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных» (далее – проект Указания).

Кредитные организации положительно оценивают разработку и принятие нормативного акта Банка России, регулирующего угрозы, нейтрализацию которых необходимо обеспечивать при обработке персональных данных в банковских информационных системах и отмечают, что проект Указания определяет достаточный перечень актуальных угроз безопасности персональных данных.

При этом **53,3%** опрошенных считают *нецелесообразным* в качестве угроз безопасности персональных данных, актуальных при обработке в информационных системах персональных данных (далее – ИСПД), угроз 1-го типа и 2-го типа в соответствии с терминологией, установленной Постановлением Правительства Российской Федерации от 01.11.2012 г. № 1119 (далее - Правительства РФ № 1119). *Поддерживают* установление в проекте Указания угроз 1-го типа и 2-го типа в соответствии с терминологией, установленной Постановлением Правительства РФ № 1119, **26,7%**. При этом было высказано предложение дополнить п. 2 проекта Указания определениями типов угроз в соответствии с терминологией, установленной Постановлением Правительства РФ № 1119. При разбивке угроз на «угрозы 1-го типа», «угрозы 2-го типа», а так же «угрозы 3-го типа» (угрозы, устанавливаемые проектом Указания), проект будет более информативен и будет соответствовать практическим нуждам о*тделов информационной безопасности* кредитных организаций.

Соответственно, предлагается внести уточнения в проект Указания, в частности в п. 5, п. 5.1, п.5.2, п. 5.3 заменить фразу «не могут быть вызваны наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе персональных

данных» на «*не могут быть отнесены к угрозам 1-го или 2-го типа*». Например, предлагается изложить п. 5 Проекта в следующей формулировке: «5. Угрозы безопасности персональных данных, указанные в пункте 4 настоящего Указания не могут быть отнесены к угрозам 1-го или 2-го типа за исключением угроз: ...далее по тексту...».

Отмечается, что предложенная редакция п. 4 и 5 проекта Указания затруднительна для восприятия, ввиду использования громоздких определений и сложной структуры пунктов. Предлагается следующий вариант редакции данных пунктов проекта Указания:

«4. Актуальными угрозами безопасности персональных данных при их обработке в информационных персональных данных, которые ***не могут*** *быть вызваны наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе персональных данных, являются:*

- нарушение конфиденциальности, доступности и (или) целостности персональных данных, в результате несанкционированного доступа к персональным данным, лицами обладающими полномочиями в информационной системе персональных данных;

- нарушение конфиденциальности, доступности и (или) целостности персональных данных, в результате несанкционированного доступа к персональным данным в ходе создания, эксплуатации (использования по назначению, технического обслуживания и (или) ремонта), модернизации, снятия с эксплуатации информационной системы персональных данных;

- нарушение конфиденциальности, доступности и (или) целостности персональных данных, в результате использования методов социального инжиниринга к лицам, имеющим доступ к информационной системе персональных данных;

- нарушение конфиденциальности персональных данных, в результате несанкционированного доступа к носителям персональных данных, утраты (потере) носителей персональных данных, включая переносные персональные компьютеры пользователей информационной системы персональных данных;

- нарушение конфиденциальности, доступности и (или) целостности персональных данных, в результате несанкционированного доступа к персональным данным с использованием уязвимостей в организации и контроле доступа к информационной системе персональных данных;

- нарушение конфиденциальности, доступности и (или) целостности персональных данных, в результате несанкционированного доступа к персональным данным с использованием уязвимостей при эксплуатации средств криптографической защиты информации.

5. Актуальными угрозами безопасности персональных данных при их обработке в информационных персональных данных, которые ***могут*** *быть вызваны наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе персональных данных, являются:*

- нарушение конфиденциальности, доступности и (или) целостности персональных данных, в результате воздействия вредоносного кода, внешнего по отношению к информационной системе персональных данных;

- нарушение конфиденциальности, доступности и (или) целостности персональных данных, в результате несанкционированного доступа к персональным данным с использованием уязвимостей в программном обеспечении информационной системы персональных данных;

- нарушение конфиденциальности, доступности и (или) целостности персональных данных, в результате несанкционированного доступа к персональным данным с использованием уязвимостей в организации защиты персональных данных при информационном взаимодействии со смежными информационными системами и информационно-телекоммуникационной сетью Интернет;

- нарушение конфиденциальности, доступности и (или) целостности персональных данных, в результате несанкционированного доступа к персональным данным с использованием уязвимостей в обеспечении защиты сетевого взаимодействия и каналов передачи данных;

- нарушение конфиденциальности, доступности и (или) целостности персональных данных, в результате несанкционированного доступа к персональным данным с использованием уязвимостей в обеспечении защиты вычислительных сетей информационной системы персональных данных.»

В п. 4 Указания определена такая актуальная угроза, как «нарушение конфиденциальности <...> в результате несанкционированного доступа к персональным данным лицами, обладающими полномочиями в информационной системе персональных данных». Кредитные организации отмечают отсутствие четкого понимания, кто относится к «лицам, обладающим полномочиями» и каким образом ими может быть осуществлен «несанкционированный доступ» (за пределами полномочий или др.). Предлагается внести соответствующие уточнения в формулировки пункта.

Некоторыми кредитными организациями было высказано мнение, что угрозы безопасности персональных данных, перечисленные в п. 5 проекта Указания, необоснованно причислены к угрозам, вызванным исключительно наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении (ПО). В частности, кредитные организации считают, что:

– угрозы, обусловленные воздействием вредоносного кода, внешнего по отношению к ИСПД, не могут относиться к недокументированным (недекларированным) возможностям в системном и прикладном ПО ИСПД. По определению ИСПД - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств, включает системное и прикладное ПО. Таким образом, внешний по отношению к ИСПД вредоносный код не может входить в состав системного и прикладного ПО ИСПД и составлять их недокументированные (недекларированные) возможности;

– уязвимости в программном обеспечении ИСПД, уязвимости в организации защиты персональных данных при информационном взаимодействии со смежными информационными системами и сетью Интернет, уязвимости в обеспечении защиты сетевого взаимодействия и каналов передачи данных, уязвимости в обеспечении защиты вычислительных сетей ИСПД не могут относиться к недокументированным (недекларированным) возможностям в системном и прикладном ПО ИСПД. *Недокументированные (недекларированные) возможности* ПО представляют собой *специально заложенные разработчиком* и недокументированные (недекларированные,

скрытые от пользователей) возможности или функции ПО (программные закладки). В отличие от недокументированных (недекларированных) возможностей, *уязвимости ПО* и систем защиты это слабые места, недостатки, причем *исходно неизвестные как разработчику, так и пользователям* и выявляемые в процессе эксплуатации соответствующих ПО и систем. Выявленные уязвимости декларируются разработчиком и принимаются меры для их устранения или блокирования их влияния. В связи с этим, отождествление уязвимостей с недекларированными возможностями представляется некорректным.

Кредитные организации считают, что предложенные в пп.5.1-5.3 проекта Указания варианты действий для признания угроз, вызванных исключительно наличием недокументированных (недекларированных) возможностей ПО ИСПД, не учитывают следующее:

До принятия предложенных в проекте мер, угрозы 1-го и 2-го типа для ИСПД вынужденно считаются актуальными, что приводит в необходимости обеспечения 1-го уровня защищенности персональных данных для ИСПД банковских организаций и реализации соответствующего перечня мер защиты. Кроме того, для реализуемости предложенных вариантов применяемые меры защиты должны соответствовать документам Банка России, разработанных в рамках законодательства о техническом регулировании (являться техническими регламентами, обязательными для выполнения). В настоящее время такие документы отсутствуют и момент их принятия неизвестен. В их отсутствие банки вынуждены реализовывать весь перечень мер, требуемых для обеспечения 1-го уровня защищенности персональных данных.

В пунктах 5.2 и 5.3 проекта Указания фактически устанавливается обязательность применения СТО БР ИББС по 5 уровню соответствия как способа нейтрализации угроз 1-го и 2-го типов при защите персональных данных. Малые и средние кредитные организации отметили, что возможность реализации ими данного требования на практике вызовет затруднения, ввиду того, что материальные затраты на обеспечение мер по нейтрализации угрозы, в том числе привлечение испытательных лабораторий в целях анализа уязвимостей ПО, существенно превышают возможный ущерб от реализации угрозы. При этом, актуальность угроз 1-го типа и 2-го типов для кредитных организаций сомнительна, так как большинство банков не являются лицензированными разработчиками ПО или компаниями, лицензированными в области технической защиты информации, следовательно, у них отсутствует возможность самостоятельно выявлять уязвимости в ПО. Более того, декомпиляция и прочие действия с поставляемым вендорами ПО являются нарушением лицензионных соглашений в соответствии с российским законодательством.

Представляется целесообразным определить в проекте Указания источники угроз безопасности персональных данных и способы реализации угроз безопасности персональных. Также предлагается предусмотреть в проекте Указания описание возможных компенсирующих мер кредитных организаций по обеспечению информационной безопасности.

Предлагается распространить действие проекта Указания на персональные данные, относящихся к специальным, биометрическим персональным данным и персональным данным, полученным из общедоступных источников.

В соответствии с пресс - релизом Банка России от 30.05.2014 «О вводе в действие документов Комплекса документов в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации» были утверждены документы Комплекса БР ИББС, *рекомендованные для выполнения* организациями банковской системы Российской Федерации требований законодательства Российской Федерации в области персональных данных. Кроме того, на текущий момент действует Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утв. ФСТЭК РФ 14.02.2008). С учетом изложенного, возникает возможность *возникновения противоречий*, в отношении того, является ли проект Указания Банка России обязательным либо имеет рекомендательный характер, и каким образом соотносится с ранее утвержденными документами. Данные противоречия могут быть исключены, в случае придания Указанию *рекомендательного характера, и (или) приведения в соответствие проекта Указания с ранее утвержденными документами*.

С уважением,

Вице-президент Ассоциации «Россия» А.В. Ветрова

Исп.: Зотова М.,
(495) 785 29 91