

Актуальные и перспективные направления работы комитета по банковской безопасности АРБ

Велигура Александр Николаевич

председатель комитета по
банковской безопасности АРБ

Практические вопросы взаимодействия с создаваемым центром мониторинга и предупреждения компьютерных атак

Для эффективной работы должны сложиться система, включающая создаваемый центр, ЦБ, банки и другие организации, функции которой не должны сводиться только к сбору и обобщению информации об инцидентах.

Ее работа должна быть динамичной и автоматизированной. В её становлении необходимо взаимодействие всех заинтересованных сторон.

Какие данные и как будут использоваться?

Для автоматизации использования данных и оптимизации процедур их использования они должны быть формализованы.

Практические вопросы взаимодействия с создаваемым центром мониторинга и предупреждения компьютерных атак

В каких системах они будут использоваться?

Какие требования следует к ним предъявить?

И другие вопросы.

Разработка форматов данных информационного обмена:

- для обозначения/индикации/описания угроз и уязвимостей
- для формирования записей об инцидентах
- для обмена информацией с другими системами (с системами защиты, с аналитическими системами)
- И.т.д.....

Практические вопросы взаимодействия с создаваемым центром мониторинга и предупреждения компьютерных атак

Кроме того, требуется определить:

- протоколы обмена данными между составными частями системы;
- вопросы обеспечения ИБ данных;
- жизненный цикл данных;
- режимы обращения с данными;
- требования к аналитической части – какие результаты, кому и в каком виде она должна выдавать;
- И.т.д.....

Обеспечение доверия к качеству определенных видов работ, связанных с ИБ

Постоянно имеют место

- недостаточное взаимопонимание между ИБ банков и разработчиками/поставщиками ПО;
- претензии к качеству разработки;
- разнобой в трактовке положений стандартов ЦБ и нормативных документов организациями, проводящими оценку соответствия.

Обеспечение доверия к качеству определенных видов работ, связанных с ИБ

Периодически поднимаются вопросы

- сертификации банковского ПО;
- установления неких общих требований к организациям, проводящим оценку соответствия требованиям к обеспечению ИБ (попытка – создание ABISS)

Обеспечение доверия к качеству определенных видов работ, связанных с ИБ

В последнее время, в т.ч. на прошлом форуме, выдвигалась идея использовать для решения этих задач форму СРО.

Представляется, что существующий Федеральный закон от 1 декабря 2007 года N 315-ФЗ «О саморегулируемых организациях»

(с изменениями, внесенными Федеральными законами: от 22 июля 2008 года N 148-ФЗ; от 23 июля 2008 года N 160-ФЗ, от 28 апреля 2009 года N 62-ФЗ; от 27 декабря 2009 года N 374-ФЗ; от 27 июля 2010 года N 240-ФЗ; от 1 июля 2011 года N 169-ФЗ; от 21 ноября 2011 года N 327-ФЗ; от 3 декабря 2011 года N 383-ФЗ; от 25 июня 2012 года N 93-ФЗ; от 7 июня 2013 года N 113-ФЗ; от 24 ноября 2014 года N 359-ФЗ)

дает необходимые возможности

Обеспечение доверия к качеству определенных видов работ, связанных с ИБ

Кого могли бы объединить саморегулируемые организации?

Организации, проводящие оценку соответствия требованиям
к обеспечению ИБ («аудиторы»)

Разработчиков банковского ПО

Интеграторов

Обеспечение доверия к качеству определенных видов работ, связанных с ИБ

Кому и зачем это нужно?

Кредитным организациям – это уменьшит их риски, т.к.

315-ФЗ требует наличие стандартов и правил деятельности, обязательных для выполнения всеми членами СРО+ имущественную ответственность членов СРО перед потребителями

А что это даст участникам (членам) СРО?

Обеспечивать и аргументировать уровень работ (услуг), ссылаясь на стандарты и правила деятельности, соблюдение которых контролируется СРО.

Пример АБИСС

Спасибо за внимание!

Велигура Александр Николаевич



Председатель комитета
по банковской безопасности
Ассоциации российских банков



Заместитель генерального директора
ООО Андэк Консалтинг

Москва, ул.Серпуховской Вал,19-8

Телефон:+7 (495) 984-60-40

E-mail: a.veligura@andekconsult.ru

