А. С. Зайцев

ИССЛЕДОВАНИЕ ПРОЦЕССА МОНИТОРИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНИЗАЦИИ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

Введение

В настоящее время в связи с ростом количества технических средств, используемых в организациях, вопрос анализа журналов аудита данных средств для оценки уровня информационной безопасности (ИБ) организации становится все более и более актуальным.

Для решения этой задачи используются средства централизованного сбора журналов аудита (лог-менеджмент) и средства для обработки и анализа полученных данных. Эти средства представляют собой базис для организации процесса мониторинга информационной безопасности.

В данной статье произведено исследование процесса мониторинга ИБ в организации банковской системы Российской Федерации (БС РФ), для которой проблемы адекватной оценки уровня ИБ, реагирования на инциденты ИБ и их расследования крайне важны.

1. Место и роль процесса мониторинга ИБ в организации БС РФ

Мониторинг ИБ – один из основных процессов ИБ в организации БС РФ. Правильно спроектированный, настроенный и отлаженный мониторинг является основным источником информации о реальном уровне ИБ организации.

Стандартом в области ИБ БС РФ является комплекс СТО БР ИББС [1]. Ввиду этого указанная совокупность документов будет чаще всего использоваться в данной статье. Согласно этому стандарту, мониторинг ИБ – постоянное наблюдение за объектами и субъектами, влияющими на ИБ организации банковской системы Российской Федерации, а также сбор, анализ и обобщение результатов наблюдений.

Выделим основные задачи процесса мониторинга:

1. Оперативное выявление инцидентов ИБ;

2. Проверка на выполнение требований регуляторов ИБ;

3. Проверка на отсутствие деградации системы обеспечения информационной безопасности (СОИБ), то есть того, что соблюдаются информационные технологии, заданные в документации;

4. Создание базы данных, которую возможно использовать:

– при расследовании инцидентов ИБ;

– при проведении аудита или самооценки ИБ;

– для корректировки моделей угроз и нарушителя;

– для внесения корректировок в оценку рисков нарушения ИБ.

5. Создание и предоставление отчетов руководству (ввиду необходимости анализа СОИБ со стороны руководства, выраженной в стандартах [1, 2]).

Таким образом, мониторинг ИБ является основным процессом группы процессов «Проверка» цикла Деминга системы управления информационной безопасностью (СУИБ), а также основой для следующих процессов ИБ:

1. Менеджмент инцидентов ИБ (является логическим продолжением процесса мониторинга ИБ);

2. Аудит ИБ (внутренний и внешний);

3. Самооценка ИБ;

4. Прогнозирование (моделирование ИБ);
5. Оценка рисков нарушения ИБ.

2. Существующие исследования в области мониторинга ИБ. Рекомендации в области мониторинга и управления инцидентами в организации БС РФ.

Проблема глубокого исследования процесса мониторинга ИБ встала перед научной общественностью не так давно и получила отражение в комплексе стандартов по управлению информационной безопасностью ISO/IEC 27000, в котором главным документом в области мониторинга и управления инцидентами является [3].

В основополагающем стандарте комплекса ISO/IEC 27000 – ISO/IEC 27001 не дается четкой формулировки процесса мониторинга ИБ, вместо этого требования по мониторингу ИБ разделены между процессами постоянного контроля (что практически идентично понятию мониторинга) и менеджмента инцидентов (процесс, который является логическим продолжением процесса мониторинга ИБ).

Не будем останавливаться подробно на анализе данных стандартов ввиду того, что эти принципы адаптированы с учетом специфики БС РФ в комплексе СТО БР ИББС.

Основные принципы и требования к процессу мониторинга организации БС РФ сформулированы в СТО БР ИББС-1.0-2010. В методике оценки соответствия данным требованиям – СТО БР ИББС-1.2-2010 [4] – в групповом показателе М3 «Обеспечение информационной безопасности при управлении доступом и регистрации» мониторингу ИБ посвящены 6 частных показателей ИБ:

–Определены ли в документах организации, выполняются ли и контролируются ли процедуры регистрации событий и действий?

–Документируются ли результаты контроля процедур регистрации событий и действий?

–Определены ли в документах организации процедуры мониторинга и анализа данных регистрации, действий и операций, позволяющие выявить неправомерные или подозрительные операции и транзакции?

–Используются ли специализированные программные и (или) технические средства для проведения процедур мониторинга и анализа данных регистрации, действия и операций?

–Используют ли процедуры мониторинга и анализа документально определенные критерии выявления неправомерных или подозрительных действий и операций?

–Применяются ли процедуры мониторинга и анализа на регулярной основе (например, ежедневно) ко всем выполненным операциям и транзакциям?

Учтем данные требования в дальнейшем при составлении принципов мониторинга ИБ.

Процесс мониторинга и управления инцидентами ИБ отражен в работе отечественных ученых [5].

Комплекс СТО БР ИББС, согласно Федеральному закону от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании» [6] и в соответствии с лучшими мировыми практиками, носит рекомендательный характер. Но, согласно тому же закону, требования стандарта носят обязательный характер для организаций, которые добровольно приняли решение о внедрении стандарта. Стандарт закладывает принципы построения, эксплуатации и модернизации системы СОИБ организации. Комплекс был создан под руководством Банка России (ЦБ РФ) для объединения российского и международного опыта в ИБ применительно к банковской сфере в условиях отечественной информационной среды.

Ключевым моментом является то, что стандарт ЦБ РФ призван стать единым комплексом документов для удовлетворения требований регуляторов ИБ в БС РФ. Это подтверждает Федеральный закон от 25 июля 2011 г. № 261-ФЗ «О внесении изменений в Федеральный закон “О персональных

данных"» [7], являющийся поправкой к Федеральному закону № 152-ФЗ [8] и наделивший ЦБ РФ правом разработки отраслевых нормативных документов в области обработки персональных данных (ПДн). На сегодняшний день отмечены несколько незначительных несоответствий в текстах СТО БР ИББС и Федерального закона № 152-ФЗ (п. 7.4.2 СТО БР ИББС-1.0-2010 позволяет оператору ПДн использовать несертифицированные средства защиты, получив при этом одобрение руководства организации БС РФ, что неприемлемо, согласно Федеральному закону № 152-ФЗ; п. 7.10.9 СТО БР ИББС-1.0-2010 выводит автоматизированную систему (АС), обрабатывающую платежную банковскую информацию и реализующую банковский платежный технологический процесс, из-под понятия информационной системы персональных данных). Эта проблема освещена в документе «Методические рекомендации по выполнению законодательных требований при обработке персональных данных в организациях банковской системы Российской Федерации» (2010).

Вышеперечисленные причины позволяют использовать комплекс СТО БР ИББС в качестве основной нормативно-методической документации при настройке мониторинга ИБ в организации БС РФ. Также необходимо использовать нормативно-методическую документацию соответствующей организации БС РФ, в которой ведется настройка процесса мониторинга и управления инцидентами ИБ.

При конфигурировании мониторинга ИБ можно будет также опираться на рекомендацию РС БР ИББС-2.5-20ХХ «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Выделение и назначение ролей», находящуюся на момент написания данной статьи в стадии разработки, а также на соответствующую рекомендацию по классификации активов, также находящуюся в стадии разработки.

Резюмируем постулаты и рекомендации, которые дает стандарт СТО БР ИББС-1.0-2010 в отношении мониторинга и управления инцидентами ИБ:

1. Самой критически важной категорией нарушителей ИБ является внутренний нарушитель — нарушитель, действующий с использованием легально предоставленных прав и полномочий. Наряду с угрозой внутреннего нарушителя одной из важнейших угроз является несоответствие требованиям в области ИБ.

2. Мониторинг и менеджмент событий и инцидентов ИБ является оперативной мерой поддержания системы информационной безопасности на должном уровне. Мониторинг ИБ, наряду с самооценкой, аудитом и анализом функционирования СОИБ, является основой стадии «Проверка» цикла Деминга СУИБ. Процедуры мониторинга и менеджмента инцидентов ИБ должны быть документированы и регулярно (например, ежедневно) выполняться. Причем этим должна заниматься служба ИБ или уполномоченное лицо.

3. Ролевая структура АС критична при построении СОИБ. Самую большую опасность ИБ представляет привилегированный пользователь, его контроль обязателен. Не рекомендуется совмещение в одной роли следующих функций: разработки и эксплуатации системы, разработки и сопровождения системы, сопровождения и эксплуатации, администрирования и администрирования ИБ, выполнения операций и контроля над их выполнением.

4. Необходима документированная классификация защищаемых активов АС.

5. Самым критичным информационным активом организации БС РФ является платежная информация. Функция администрирования средств защиты платежной информации входит в роль администратора ИБ. Необходим контроль над доступом к ресурсам банковского платежного технологического процесса, исполнением установленной технологии подготовки, обработки, передачи и хранения платежной информации.

6. Требуется повышенный контроль за информацией, необходимой для регистрации, идентификации, аутентификации и авторизации.

3. Процесс конфигурирования средств мониторинга и менеджмента инцидентов

Предлагается рассматривать процесс настройки мониторинга ИБ на конкретном уровне организации БС РФ (мониторинг конкретного подконтрольного объекта), при этом он должен состоять из следующих последовательных стадий:

1. Создание модели подконтрольного объекта;
2. Создание модели информационных технологий, реализованных на данном подконтрольном объекте;
3. Классификация информационных активов (объектов доступа);
4. Классификация учетных записей (субъектов доступа);
5. Формирование частных моделей угроз и нарушителя ИБ;
6. Составление матрицы доступа и списка разрешенных действий, не описанных матрицей доступа;
7. Составление списка критических событий подконтрольного объекта (инцидентов ИБ) и инструкций, моделей взаимодействия персонала в случае наступления каждого события из списка;
8. Составление политики мониторинга и менеджмента инцидентов ИБ, а также конфигурирование ПО, выполняющего мониторинг ИБ.

Пункт 8 целесообразно осуществлять во время всех стадий конфигурирования мониторинга ИБ.

Процесс настройки ПО, производящего мониторинг ИБ, формирования единого хранилища событий ИБ и управления инцидентами ИБ (SIEM-система — Security Incident and Event Manager) структурно изображен на рис. 1.

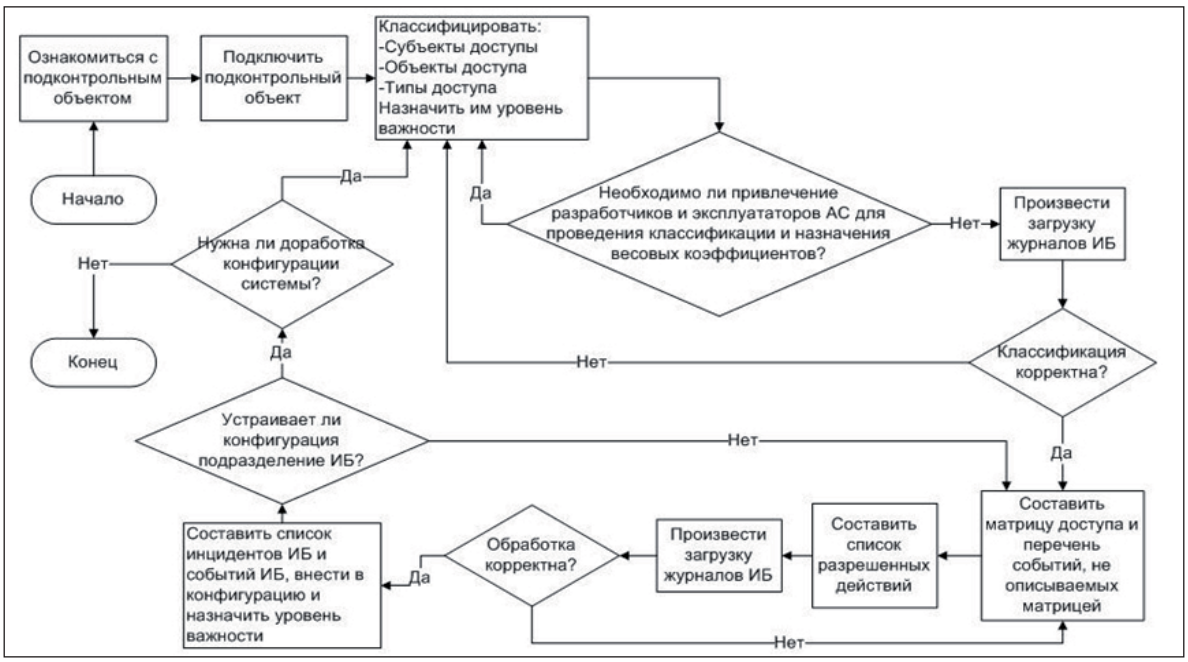

Рис. 1. Настройка SIEM-системы на основе решения IBM TSIEM

Необходимо отметить важность совместной работы специалиста, организующего разделение доступа, и специалиста, организующего мониторинг ИБ. Ведь все модели и матрица доступа могут быть успешно использованы и тем, и другим специалистом, а вместе им необходимо четко осознавать, какая часть угроз нейтрализована при помощи разграничения доступа, а какие угрозы необходимо контролировать при помощи системы мониторинга ИБ, а также как контролировать неизменность настроек разграничения доступа при помощи системы мониторинга.

4. Принципы настройки мониторинга ИБ и придание процессу мониторинга и управления инцидентами ИБ юридической силы

В результате исследования было выявлено три основных способа настройки мониторинга ИБ:

1. Разобрать все события, происходящие в системе в штатном режиме функционирования за продолжительный промежуток времени. Убедиться, что эти события легитимны. Зафиксировать их в системе мониторинга ИБ. Считать любые другие события инцидентами ИБ;

2. На основе построенных моделей, матрицы доступа и списка событий, не описанных матрицей доступа, составить список инцидентов ИБ, указать их в настройке системы мониторинга ИБ;

3. Комбинированный способ.

У первого способа есть существенный недостаток. За время, данное на анализ, могли произойти не все штатные события, возможные в АС. Тем самым оператору системы мониторинга ИБ придется выполнять дополнительную работу по анализу обнаруженных событий ИБ. Основной недостаток второго способа заключается в том, что в случае ошибок, допущенных в модели, система мониторинга не сможет обнаружить события, не описанные моделью. Поэтому желательно использование способа, являющегося комбинацией первого и второго: настроить параметры известных легитимных событий и указать перечень инцидентов ИБ. В данном случае события, не попавшие ни в одну из указанных двух категорий, будут свидетельствовать о необходимости доработки частных моделей.

По сути, данные принципы напоминают принципы противодействия атакам: сигнатурный и эталонный анализ и некий гибридный вариант анализа.

Отметим также, что для придания такой системе юридической силы необходимо обеспечить ее следующими документами:

1. Частная политика ИБ: политика мониторинга и менеджмента инцидентов. Нормативно-методический документ, уточняющий принципы основной политики ИБ организации в области мониторинга менеджмента ИБ;

2. Программа управления инцидентами ИБ (в том числе список инцидентов ИБ и правил реагирования на них, а также взаимодействие персонала в случае возникновения инцидента ИБ);

3. Документация на АС, частью которой является подконтрольный объект;

4. Приказы о назначении сотрудника на конкретную роль;

5. Классификация активов и учетных записей;

6. Частная модель угроз и нарушителей.

Полученные выводы и методики были использованы при отладке Систем обеспечения информационной безопасности Коллективных центров обработки информации Банка России.

СПИСОК ЛИТЕРАТУРЫ:

1. Стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» (СТО БР ИББС-1.0-2010).
2. ISO/IEC 27001:2005 «Information technology. Security techniques. Information security management systems. Requirements».
3. ISO/IEC 27035:2011 «Information technology. Security techniques. Information security incident management».
4. Стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0 - 2010» (СТО БР ИББС-1.2-2010).
5. *Милославская Н. Г., Сенаторов М. Ю., Толстой А. И.* Управление инцидентами информационной безопасности и непрерывностью бизнеса. М.: Горячая линия—Телеком, 2012.
6. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».
7. Федеральный закон от 25 июля 2011 г. № 261-ФЗ «О внесении изменений в Федеральный закон “О персональных данных”».
8. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».