А. Б. Костина, Н. Г. Милославская (к. т. н., доцент)
Московский инженерно-физический институт (государственный университет)

РАЗРАБОТКА ПРОЦЕССА УПРАВЛЕНИЯ ИНЦИДЕНТАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СООТВЕТСТВИИ С ТРЕБОВАНИЯМИ МЕЖДУНАРОДНЫХ СТАНДАРТОВ

Введение

Ни одна самая совершенная мера по снижению рисков информационной безопасности (ИБ), будь это досконально проработанная политика или самый современный межсетевой экран, не может полностью предотвратить возникновение в информационной среде событий, потенциально несущих угрозу бизнесу организации [1]. Сложность и разнообразие среды деятельности современного бизнеса предопределяют наличие остаточных рисков в независимости от качества подготовки и внедрения мер противодействия. Также, всегда существует вероятность реализации новых, не известных до настоящего времени, угроз информационной безопасности. Неготовность организации к обработке подобного рода ситуаций может существенно затруднить восстановление нормального функционирования организации и потенциально усилить нанесенный ущерб. Таким образом, любой организации, серьезно относящейся к вопросам обеспечения ИБ, необходимо реализовать комплексный подход для решения следующих задач [1]:

· обнаружения, информирования и учета инцидентов ИБ;

· реагирования на инциденты ИБ, включая применение необходимых средств для предотвращения, уменьшения и восстановления нанесенного ущерба;

· анализа и расследования произошедших инцидентов с целью планирования превентивных мер защиты и улучшения процесса обеспечения ИБ целом.

Решение всех этих задач можно получить, разработав и реализовав эффективный процесс управления инцидентами ИБ.

Тема управления инцидентами ИБ является сегодня одновременно и популярной, и актуальной. Именно во время работы разных этапов процесса управления инцидентами ИБ проявляются конкретные уязвимости активов организации, обнаруживаются следы атак и вторжений, проверяется работа защитных механизмов, эффективность работы процессов обеспечения ИБ и управления ею.

Создание эффективного процесса управления инцидентами ИБ помогает решить проблемы, с которыми сталкиваются динамично развивающиеся компании: увеличение ущерба от инцидентов ИБ, факт которых в большинстве случае даже не известен, а также выбор и принятие адекватных решений, минимизирующих проблемы ИБ.

Разработка и внедрение процесса управления инцидентами ИБ важны еще и потому, что процесс управления инцидентами ИБ является одной из основополагающих частей общей системы управления ИБ (СУИБ) [1]. Данные, аккумулируемые в рамках данного процесса, являются необходимыми для работы достаточно большого количества других процессов управления ИБ, например, для корректного проведения анализа рисков ИБ или для оценки эффективности существующих мер по обеспечению ИБ и процессов управления ею.

Основной целью разработки процесса управления инцидентами ИБ является повышение уровня защищенности ресурсов организации и повышение готовности организации к разрешению нештатных ситуаций, связанных с ИБ, за счет эффективного управления инцидентами ИБ.

Для достижения поставленных целей прежде всего необходимо решить следующие задачи:

· изучение рекомендаций и лучших практик в области построения процессов управления инцидентами ИБ;

· проведение анализа понятия «инцидента ИБ»;

· определение подхода к разработке процесса управления инцидентами ИБ.

1. Российские и международные документы, регламентирующие аспекты управления инцидентами информационной безопасности

На данный момент существует достаточное количество международных документов, регламентирующих аспекты управления инцидентами ИБ. Как правило, все документы рассматривают последовательно все этапы процесса управления инцидентами ИБ: от планирования процесса управления инцидентами ИБ до улучшения данного процесса после анализа результатов работы самого процесса. Что касается российской нормативной базы, то на текущий момент эта сфера только начинает прорабатываться.

1.1. ISO/IEC 27001:2005 «Information security management system. Requirements» и ГОСТ Р ИСО/МЭК 27001-2006 «Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности»

Международный стандарт управления безопасностью ISO/IEC 27001 предназначен для разработки СУИБ организации вне зависимости от ее сферы деятельности. В рамках данного стандарта выдвигаются общие требования к построению СУИБ, относящиеся, в том числе, и к процессам управления инцидентами ИБ.

Стандарт ISO/IEC 27001 накладывает ряд общих требований по построению процессов управления ИБ, в состав которых входит и процесс управления инцидентами. К числу таких требований относятся [1]:

· использование модели PDCA [1, 4] для обеспечения планирования процессов, внедрения процессов, контроля и анализа процессов, улучшения процессов;

· надлежащее документирование процессов и процедур;

· должна быть обеспечена поддержка руководством организации всех процессов управления ИБ;

· процессы управления ИБ должны непрерывно анализироваться и улучшаться.

Дополнительно к перечисленным требованиям стандарт выдвигает следующие требования к процессу управления инцидентами ИБ.

Согласно разделу 4.2.3 «Мониторинг и анализ СУИБ» в организации должны быть выполнены следующие требования [1]:

· необходимо своевременно идентифицировать неудавшиеся и успешные нарушения безопасности и инциденты безопасности;

· необходимо помочь в выявлении событий безопасности и, таким образом, предотвратить инциденты безопасности путем использования индикаторов;

· необходимо определить, эффективны ли действия, предпринятые для устранения нарушения безопасности;

· необходимо предоставить руководству возможность определять, выполняются ли надлежащим образом действия по обеспечению безопасности, порученные людям или реализованные средствами информационных технологий.

В Приложении А «Цели управления и средства управления» в раздел А.13 «Управление инцидентами ИБ» включен также определенный набор требований [1]. Эти требования уже более конкретны и предъявляются к отдельным этапам работы процесса управления инцидентами ИБ.

Национальный стандарт Российской Федерации ГОСТ Р ИСО/МЭК 27001-2006 «Методы и средства обеспечения безопасности. Системы менеджмента ИБ» идентичен рассмотренному выше международному стандарту [2] и предъявляет к процессу управления ИБ аналогичные требования.

1.2. ISO/IEC TR 18044 «Information security incident management»

Международный стандарт ISO/IEC TR 18044 по управлению инцидентами ИБ определяет формальную модель процессов управления инцидентами ИБ. В данном стандарте описание процессов управления инцидентами ИБ, как и в стандарте ISO/IEC 27001, основано на использовании циклической модели Деминга (цикле PDCA) [1, 4]. Документ подробно описывает стадии планирования

и подготовки, эксплуатации, анализа и улучшения процесса реагирования на инциденты ИБ. Также рассматриваются вопросы разработки и обеспечения нормативной документации. Даются рекомендации по необходимым ресурсам и процедурам.

Целями следования этой модели является уверенность в том, что:

· события и инциденты ИБ выявляются и обрабатываются эффективным образом, в особенности в части классификации событий;

· выявленные инциденты ИБ в организации учитываются и обрабатываются наиболее подходящим и эффективным образом;

· последствия инцидентов ИБ могут быть минимизированы в процессе реагирования на инциденты, возможно с привлечением процессов восстановления после сбоев и аварий;

· за счет анализа инцидентов и событий ИБ повышается вероятность предотвращения инцидентов в будущем, улучшаются механизмы и процессы обеспечения ИБ.

В России уже существует проект данного адаптированного стандарта, пока еще не введенного в действие.

Стандарт является очень емким и содержит все необходимые сведения для разработки полноценного процесса управления инцидентами ИБ и поддерживающей его документации. Поскольку в основе формальной модели управления инцидентами ИБ, представленной в данном стандарте, также как и в стандарте ISO/IEC 27001, лежит модель PDCA, то в процессе разработки процесса управления инцидентами ИБ возможно связать требования ISO/IEC 27001 и модель управления инцидентами ИБ, предоставляемую стандартом ISO/IEC 18044, и создать процесс, полностью удовлетворяющий требованиям ISO/IEC 27001.

1.3. NIST SP 800-61 «Computer security incident handling guide»

Данный документ («Руководство по реагированию на инциденты компьютерной безопасности») представляет собой сборник «лучших практик» по построению процессов реагирования на инциденты компьютерной безопасности. В данном документе процесс реагирования на инциденты компьютерной безопасности рассматривается, начиная с первоначальных приготовлений и заканчивая разбором инцидента после окончания процесса реагирования на него. Подробно разбираются вопросы реагирования на разные типы инцидентов компьютерной безопасности.

Использование данного документа может помочь при разработке процесса управления инцидентами компьютерной безопасности «с нуля» или при доработке существующего процесса с учетом лучших практик.

Следует еще раз подчеркнуть, что данный документ рассматривает аспекты реагирования на инциденты именно компьютерной безопасности [5], однако в данной работе под инцидентом ИБ рассматривается более широкое понятие. Группа программно-технических инцидентов, в которую включаются инциденты компьютерной безопасности, является лишь его составной частью. Следовательно, можно сделать вывод, что классификация, предлагаемая документом NIST SP 800-61, не может быть полностью перенята при разработке классификации инцидентов ИБ для целей данной работы. Однако положения и рекомендации, изложенные в данном документе, могут быть использованы при разработке процедур реагирования на программно-технические инциденты, частью которых, безусловно, являются инциденты компьютерной безопасности.

1.4. CMU/SEI-2004-TR-015 Defining incident management processes for CSIRT

В данном документе («Определение процессов управления инцидентами для Группы реагирования на компьютерные инциденты») описана методика планирования, внедрения, оценки и улучшения процессов реагирования на инциденты. Создатели данного документа заявляют о том, что представленная концепция поможет в построении эффективного процесса управления инцидентами ИБ.

Как видно из названия, основное внимание в данном документе уделяется организации работы группы реагирования на инциденты ИБ. В данном документе учитывается то, что не все организации

имеют возможность содержать отдельный орган под названием Группа реагирования на инциденты. В документе определяется порядок взаимодействия различных ролей участников процессов управления инцидентами. Использование ролевого принципа позволяет наделять сотрудников организации дополнительными обязанностями в рамках процесса управления инцидентами без привязки к их должностям и служебным обязанностям [1, 6].

Помимо этого в документе вводится ряд критериев, на основании которых организация может оценивать эффективность предотвращения, обработки и реагирования на инциденты ИБ, приводятся подробные описания этих процессов.

Положения данного документа разрабатывались на основе существующего опыта по разработке и внедрению процесса управления инцидентами ИБ в различных организациях, а также на основе лучших практик в этой и смежных областях. Положения документа могут быть использованы в качестве основы для построения процесса управления инцидентами ИБ в различных организациях. Это возможно, так как даже в самом документе говорится о том, что процесс управления инцидентами ИБ может иметь множество вариантов реализации в зависимости от условий, в которых он будет реализован.

Данный документ можно использовать не только при построении процесса управления инцидентами ИБ, но и для анализа уже существующего в организации процесса. Это тоже важно, особенно в свете того, что сейчас во многих организациях задача формализации существующих процессов управления ИБ и построения СУИБ становится все популярнее.

Следует также отметить, что данный документ рассматривает аспекты, которые должны быть реализованы в рамках процесса управления инцидентами ИБ, но не касается того, как именно могут быть реализованы те или иные положения. Можно сделать вывод, что данный документ не является пошаговой инструкцией по разработке, внедрению и совершенствованию процесса управления инцидентами ИБ.

1.5. СТО БР ИББС-1.0-2006 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения»

В стандарте Банка России также используется понятие «инцидент ИБ». Использование этого понятия и внимание, которое ему уделяется, можно объяснить тем, что особенности банковских систем таковы, что негативные последствия сбоев в работе отдельных организаций могут привести к быстрому развитию системного кризиса платежной системы РФ, нанести ущерб интересам собственников и клиентов. В случаях наступления инцидентов ИБ значительно возрастают результирующий риск и возможность нанесения ущерба организациям банковской системы РФ. Поэтому для организаций БС РФ угрозы ИБ информационным активам представляют реальную опасность.

В текущей версии стандарта подчеркивается необходимость разработки процессов обнаружения и реагирования на инциденты ИБ. Реализация процесса обнаружения и реагирования на инциденты ИБ в соответствии с рассматриваемым стандартом должна обеспечиваться с учетом требований раздела 13 международного стандарта ISO/IEC IS 17799-2005 и технического отчета ISO/IEC TR 18044 [7]. Данные требования вводятся в рамках раздела «Реализация и эксплуатация системы менеджмента ИБ банковской системы РФ».

2. Анализ понятия «инцидент информационной безопасности»

Для наиболее эффективной разработки процесса управления инцидентами ИБ было принято решение руководствоваться требованиями международных стандартов ISO/IEC 27001:2005 и ISO/IEC TR 18044. Эти стандарты был выбраны потому, что они устанавливают требования к СУИБ в целом, а также к отдельным ее процессам. В частности, как говорилось выше, данные стандарты обращают особое внимание на необходимость создания процесса управления инцидентами ИБ и поддерживающей его работу документации, необходимой для регулирования и управления работой в рамках разработанного процесса и определения обязанностей и необходимых действий сотрудников.

Но прежде чем приступать к определению целей процесса управления инцидентами и задач, которые необходимо решить для достижения этих целей, необходимо было проанализировать понятия, предлагаемые стандартами — «событие ИБ» и «инцидент ИБ».

Обобщенно рассматриваемые стандарты вводят следующее определение:

· **событие ИБ:** идентифицированный случай состояния системы или сети, указывающий на возможное нарушение политики ИБ или отказ средств защиты, либо ранее неизвестная ситуация, которая может быть существенной для безопасности [1, 3].

Существует несколько аспектов касательно данного определения, которые необходимо выделить. Во-первых, для того чтобы событие имело место, необходимо, чтобы было совершено какое-то действие, направленное на какой-либо объект (рис. 1). Действие должно быть совершено субъектом. Действие, направленное на объект, имеет определенный результат. Но нужно понимать, что это действие не обязательно должно изменить состояние объекта, на который оно направлено. Например, если пользователь неверно вводит имя пользователя или пароль, то имеет место событие, но оно заключается в том, что проверка того, имеет ли пользователь право доступа к данной учетной записи, завершилась неудачей. Событие представляет собой логическую связь между действием и объектом, на который направлено данное действие, и результатом этого действия.

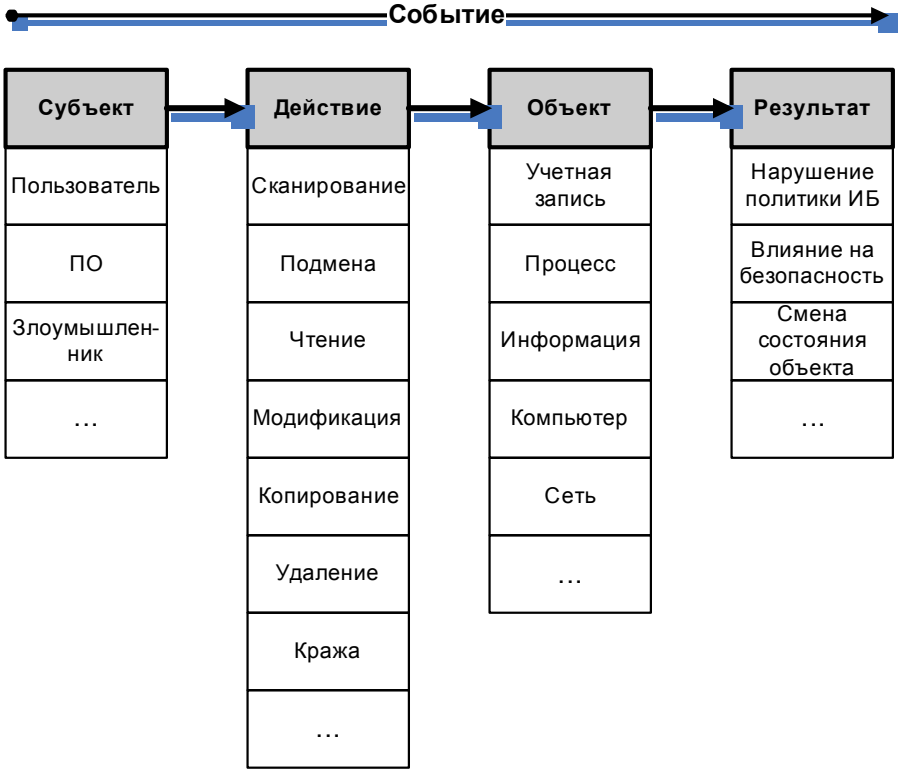

Рис. 1. Событие ИБ

Во-вторых, данное определение события не делает различия между авторизованными и неавторизованными действиями. Иногда обнаруживаемые события могут быть частью инцидента ИБ или просто иметь отношение к безопасности. Данное определение события рассматривает как авторизованные, так и неавторизованные действия. Например, если пользователь верно вводит имя пользователя и пароль, тогда ему дается доступ к данной учетной записи. Но может оказаться, что в данном случае произошла подмена пользователя. В-третьих, на рисунке 1 представлены не все возможные события.

Иногда события, которые возникают, являются частью шагов, предпринимаемых злоумышленником, для получения какого-то несанкционированного результата. Эти события можно рассматривать как часть инцидента ИБ:

· **инцидент ИБ:** единичное событие или ряд нежелательных и непредвиденных событий ИБ, из-за которых велика вероятность компрометации информации и угрозы ИБ [1, 3].

Инциденты ИБ могут быть преднамеренными или случайными (например, являться следствием ошибки или природных явлений) и могут вызываться как техническими, так и физическими средствами. Их последствиями могут быть такие события, как несанкционированные изменения информации, ее уничтожения или другие события, которые делают ее недоступной, а также нанесение ущерба активам организации или их хищение. Примерами инцидентов ИБ являются отказ в обслуживании, сбор информации, несанкционированный доступ [3].

Прежде всего злоумышленник руководствуется некими целями, на достижение которых направлены все его действия. В ходе инцидента злоумышленник совершает несколько шагов. В рамках этих шагов злоумышленник использует определенные методы и средства, которые позволяют ему совершить некоторые несанкционированные действия, направленные на интересующие его объекты. Успешное выполнение этих действий позволяет злоумышленнику добиться желаемых результатов, а в итоге и поставленных целей.

На рис. 2 представлена схема, на которой показано, что инцидент включает в себя такие элементы как: злоумышленник(-и), цели, на достижение которых направлена его деятельность, используемые методы и средства, действия и объекты, на которые направлены эти действия, и показана их взаимосвязь. Данная схема действительна, если рассматривать инцидент как совокупность событий ИБ, которые происходят из-за действий злоумышленника.

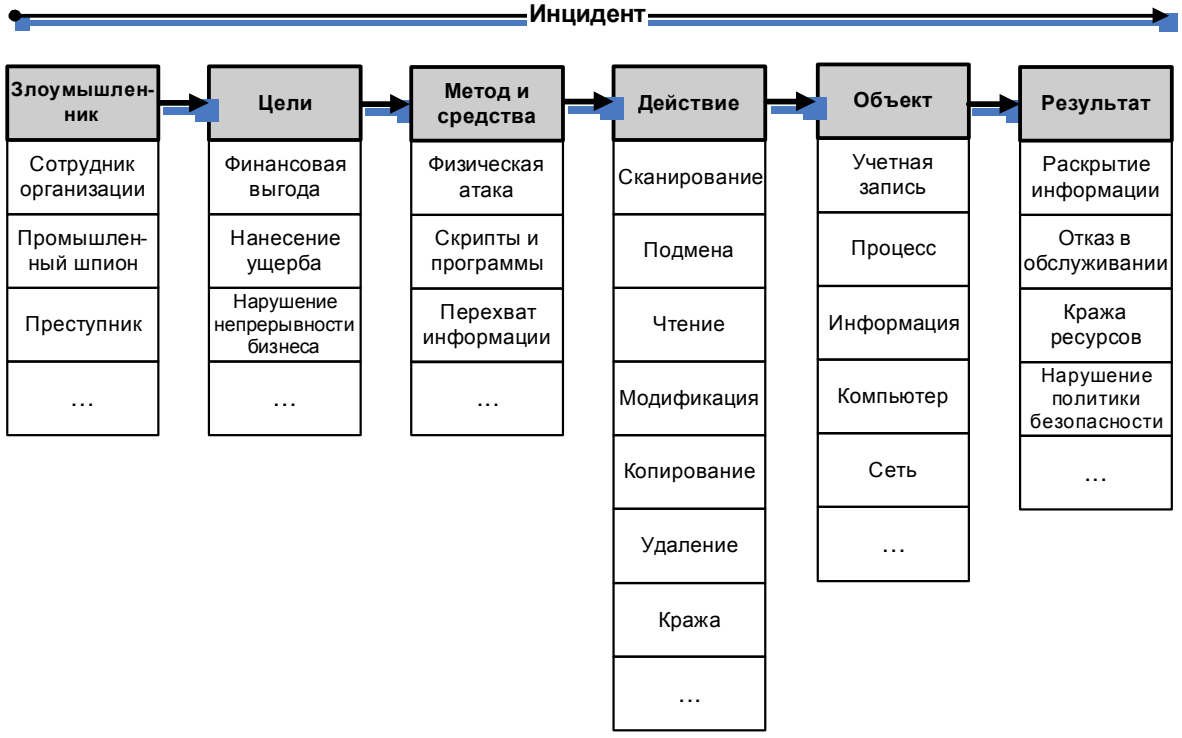

Рис. 2. Инцидент ИБ

Однако не стоит ограничиваться приведенной схемой. Агентами реализации инцидента могут быть не только люди, но и процессы, сбои ПО и оборудования и т. д., тогда инцидент можно рассматривать как совокупность событий ИБ. Помимо этого инциденты могут происходить по вине

нарушителей, которые в отличие от злоумышленников не имеют целей получения несанкционированных результатов, а становятся виновниками инцидентов, например, вследствие недостатка знаний по ИБ и принятым в организации порядкам в отношении обеспечения ИБ.

Таким образом, можно сделать вывод, что инцидент ИБ — весьма гибкое и многогранное понятие. Необходимо четкое понимание этого понятия для проведения классификации инцидентов, на основе которой будет проводиться реагирование на инциденты ИБ.

3. Подход к разработке процесса управления инцидентами информационной безопасности

В настоящей работе за основу предполагается принять процессный подход к планированию и подготовке, разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию управления инцидентами ИБ.

В организации должна быть разработана и внедрена политика менеджмента инцидентами ИБ [3]. В ней отражаются, в частности, значимость менеджмента инцидентов ИБ для организации и обязательств высшего руководства относительно поддержки менеджмента и его системы, обзор процедур обнаружения событий ИБ, оповещения и сбора соответствующей информации, и то, как эта информация должна использоваться для определения инцидентов ИБ; обзор оценки инцидентов ИБ; краткое изложение видов деятельности, следующих за подтверждением того, что некоторое событие ИБ является инцидентом ИБ; ссылки на необходимость правильной регистрации всех видов деятельности для последующего анализа и ведение непрерывного мониторинга для обеспечения безопасного хранения свидетельств в электронном виде на случай их востребования для судебного или дисциплинарного взыскания внутри организации; деятельность после разрешения инцидента ИБ, включая извлечение уроков и улучшение процесса, следующего за инцидентами ИБ; подробности хранения документации о системе, включая процедуры; структура менеджмента инцидентов ИБ в организации; положения о менеджменте; обзор программы обеспечения осведомленности и обучения менеджменту инцидентов ИБ; перечень правовых и нормативных аспектов, предполагаемых к рассмотрению.

В рамках управления инцидентами ИБ организация должна идентифицировать и управлять различными действиями. Любое действие, использующее ресурсы и управляемое с целью преобразования входных данных в выходные, может рассматриваться как процесс [1]. Часто выходные данные одного процесса непосредственно представляют входные данные для следующего процесса. Например, данные, полученные в результате реагирования на инцидент ИБ, являются входными для процесса расследования данного инцидента.

Применение системы процессов в организации, в частности к управлению инцидентами ИБ, вместе с идентификацией и взаимодействием этих процессов, а также управлением этими процессами может быть названо «процессным подходом» [1].

В рамках процессного подхода к управлению инцидентами ИБ, выбранного для разработки процесса, особое значение придается следующему:

· пониманию требований ИБ организации и необходимости определить цели управления инцидентами ИБ;

· внедрению и использованию процесса управления инцидентами ИБ в рамках общей системы обеспечения и управления ИБ в организации;

· мониторингу и анализу производительности и эффективности процессов управления инцидентами ИБ;

· постоянному совершенствованию процессов управления инцидентами ИБ, основанному на объективных показателях.

За основу предполагается принять циклическую модель Деминга, которая применяется для структурирования всех процессов СУИБ [1, 4]. Такой подход акцентирует внимание на достижении поставленных целей, а также на ресурсах, затраченных на достижения целей.

4. Заключение

Таким образом, на текущий момент проанализированы требования, рекомендации и лучшие практики в области построения процессов управления инцидентами ИБ, представленные как в российских, так и международных документах.

Для того чтобы получить правильное понимание базовых понятий «событие ИБ» и «инцидент ИБ» был проведен их анализ. Понимание этих понятий чрезвычайно важно для успешного выполнения дальнейших работ по разработке процесса управления инцидентами ИБ.

Помимо этого был определен подход к разработке процесса управления инцидентами ИБ.

Дальнейшие исследования проводятся в направлении решения следующих задач:

· анализ этапов работы процесса управления инцидентами ИБ;

· анализ требований, предъявляемых к процессу управления инцидентами ИБ стандартом ISO/IEC 27001:2005;

· выделение подпроцессов, входящих в состав процесса управления инцидентами ИБ;

· непосредственная разработка и формализация подпроцессов, входящих в состав процесса управления инцидентами ИБ;

· разработка документации, регламентирующей и поддерживающей работу процесса в целом;

· разработка способов оценки эффективности процесса в целом и отдельных его подпроцессов.

СПИСОК ЛИТЕРАТУРЫ:

1. ISO/IEC 27001:2005 Information security management system. Requirements. Введ. 2005-15-10;
2. ГОСТ Р ИСО/МЭК 27001-2006 Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Введ. 2006-27-12;
3. ISO/IEC TR 18044:2004 Information security incident management. Введ. 2004-15-10;
4. *Деминг Э.* Выход из кризиса: новая парадигма управления людьми, системами и процессами. Пер. с англ. М., 2007. — 370 с.;
5. NIST SP 800-61 Computer security incident handling guide;
6. CMU/SEI-2004-TR-015 Defining incident management processes for CSIRT;
7. СТО БР ИББС-1.0-2006 Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения. Введ. 2006-01-01.