УДК 004.7.056.5 ***DOI: 10.46960/1810-210X_2020_4_16***

Н.Г. Лабутин, П.В. Костин, Н.Ю. Шадрунова

МОДЕЛИРОВАНИЕ ПРОЦЕССОВ ВЫЯВЛЕНИЯ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И РЕАГИРОВАНИЯ НА НИХ

Приволжский институт повышения квалификации федеральной налоговой службы

Проведен анализ действий должностных лиц при выявлении и расследовании инцидентов информационной безопасности, а также реагировании на них. С использованием методологии IDEF0 разработана модель этих действий, позволяющая формализовать и регламентировать процедуры выявления инцидентов информационной безопасности и реагирования на них в любой информационной системе.

Ключевые слова: инцидент информационной безопасности, моделирование процессов, методология IDEF0, выявление инцидентов информационной безопасности, расследование инцидентов информационной безопасности.

Введение

Выявление инцидентов информационной безопасности (ИБ) в процессе ее обеспечения – действие, четко не регламентированное и детерминированное многими факторами. К последним можно отнести назначение и тип информационной системы, ее структуру (распределенная, локальная, корпоративная) и масштабы, вид обработки информации (централизованная, децентрализованная), разграничение прав доступа к ресурсам (одинаковые или различные для разных пользователей), ограничение доступа к обрабатываемой информации и т.д. В информационных системах (ИС) выявление инцидентов ИБ является начальным этапом в процедуре определения и реагирования на них. От того, насколько полно они будут выявлены, зависит надежность защиты информации, уровень которой необходимо обеспечить в конкретной ИС. При этом у специалиста по защите информации или администратора безопасности возникают следующие вопросы. Все ли события, связанные с информационной безопасностью данной ИС, необходимо относить к инцидентам ИБ, или надо выбирать только те события ИБ, которые могут нанести ощутимый ущерб ИС? По каким критериям необходимо классифицировать события ИБ? Какие события необходимо считать инцидентами ИБ для конкретной ИС с определенной архитектурой, видами обработки информации и другими факторами, указанными выше.

Несмотря на то, что инциденты и события ИБ и принципы управления ими представлены в ГОСТ Р ИСО/МЭК ТО 18044-2007 [1], в настоящее время во многих организациях, использующих различные информационные системы, нет четкого понимания того, что необходимо относить к инцидентам ИБ, какие события ИБ могут быть отнесены к инцидентам, как классифицировать события и инциденты ИБ для того, чтобы формализовать и регламентировать порядок их выявления и реагирования на них.

При определении инцидентов ИБ возможны следующие крайности. Если все события, связанные с ИБ, выявленные в данной ИС, отнести к инцидентам ИБ, то на них надо определенным образом реагировать: либо прекращать обработку данных во всей ИС, либо прекращать работу пользователя, связанного с инцидентом, либо выполнять другие действия, которые, в любом случае, приводят к дополнительным временным затратам, простою оборудования и снижению эффективности работы всей ИС в целом. Если относить к инцидентам ИБ только выборочные события без должной их классификации по степени наносимого ущерба ИС, то будет страдать безопасность информации. Также необходимо понимать то, что инциденты ИБ – это неизбежное явление для любой ИС. И какие бы превентивные меры не предпринимались в ИС для их недопущения, избежать всех инцидентов ИБ невозможно, так как в любой, даже самой защищенной ИС могут происходить события,

приводящие к инцидентам ИБ. Поэтому при эксплуатации любой ИС очень важна четкая регламентация действий по определению инцидентов ИБ и реагированию на них.

Авторами проведено моделирование действий по выявлению, анализу и расследованию инцидентов ИБ в ИС с целью их формализации. Разработанная модель призвана помочь специалистам (администраторам) информационной безопасности регламентировать эти действия в любой организации, независимо от типа ИС, ее структуры, принципов обработки информации и т.д. Для моделирования использованы функциональные модели процессов, построенные по методологии IDEF0 [2]. Моделирование различных процессов по методологии IDEF0 производится с помощью диаграмм, которые изображаются в виде функциональных блоков, обозначающих какое-либо действие. Блоки обозначаются в диаграмме прямоугольниками. Каждая сторона прямоугольника играет свою роль: верхняя – управление (управляющее воздействие), нижняя – механизм реализации данной функции, левая – вход, правая – выход. Блоки соединяются линиями в виде стрелок. Каждая стрелка предназначена для отображения элемента системы, который или обрабатывается блоком (вход), или является результатом обработки (выход), или оказывает другое воздействие на функцию, отображенную данным блоком [2].

Анализ действий должностных лиц при выявлении инцидентов ИБ и реагировании на них, разработка модели действий

При моделировании использованы принципы, рассмотренные в [3]. Модель любой системы представляется сначала в виде основной целевой функции, затем с помощью декомпозиций детализируется до состояния, определяемого разработчиком. Целевой функцией в данном случае является последовательность процессов при выявлении инцидентов ИБ и реагировании на них и действий, производимых ответственными за безопасность информации должностными лицами организации. На рис. 1 представлена диаграмма с целевой (контекстной) функцией модели действий по обнаружению и реагированию на инциденты ИБ, т.е., обобщенное представление предметной области данного исследования.

Рис. 1. ДиаграммаА-0. Целевая функция «Выявление инцидентов ИБ и реагирование на них, А0

Декомпозиция целевой функции представляется в виде диаграммы А0, на которой изображены функции А1 «Мониторинг и выявление событий ИБ», А2 «Выявление инцидента ИБ», А3 «Оперативное реагирование на инцидент ИБ», А4 «Расследование и закрытие инцидента ИБ, выработка превентивных мер».

В диаграмме А-0 в качестве входа представлены различные источники обнаружения событий ИБ, в качестве управляющих воздействий – Политика ИБ в организации как основной организационно-распорядительный документ локального уровня, в котором должны быть представлены механизмы и действия должностных лиц при выявлении инцидентов ИБ и реагировании на них. Также управляющими воздействиями можно считать должностные инструкции и различные другие инструкции пользователей ИС, администратора

ИБ, сотрудников организации, входящих в группу реагирования на инциденты ИБ (ГРИИБ) и т.д. ГРИИБ – это коллегиальный орган в любой организации, создаваемый для оперативного реагирования на возникающие инциденты ИБ, их расследования, анализа и выработки мер по недопущению подобных инцидентов в дальнейшем, то есть, для минимизации рисков для активов организации от инцидентов ИБ.

В роли «Механизмов» для выполнения функции А0 выступают должностные лица, задействованные в процессах выявления и расследования инцидентов ИБ: Пользователи ИС, администраторы ИБ, группа РИИБ. На выходе целевой функции в общем виде в качестве желаемого результата представим «поддержание ИБ активов ИС», что означает, недопущение негативных последствий в ИС от инцидента ИБ, определение источников инцидента и недопущение подобных инцидентов ИБ в будущем. На рис. 2 приведена диаграмма с декомпозицией целевой функции А0.

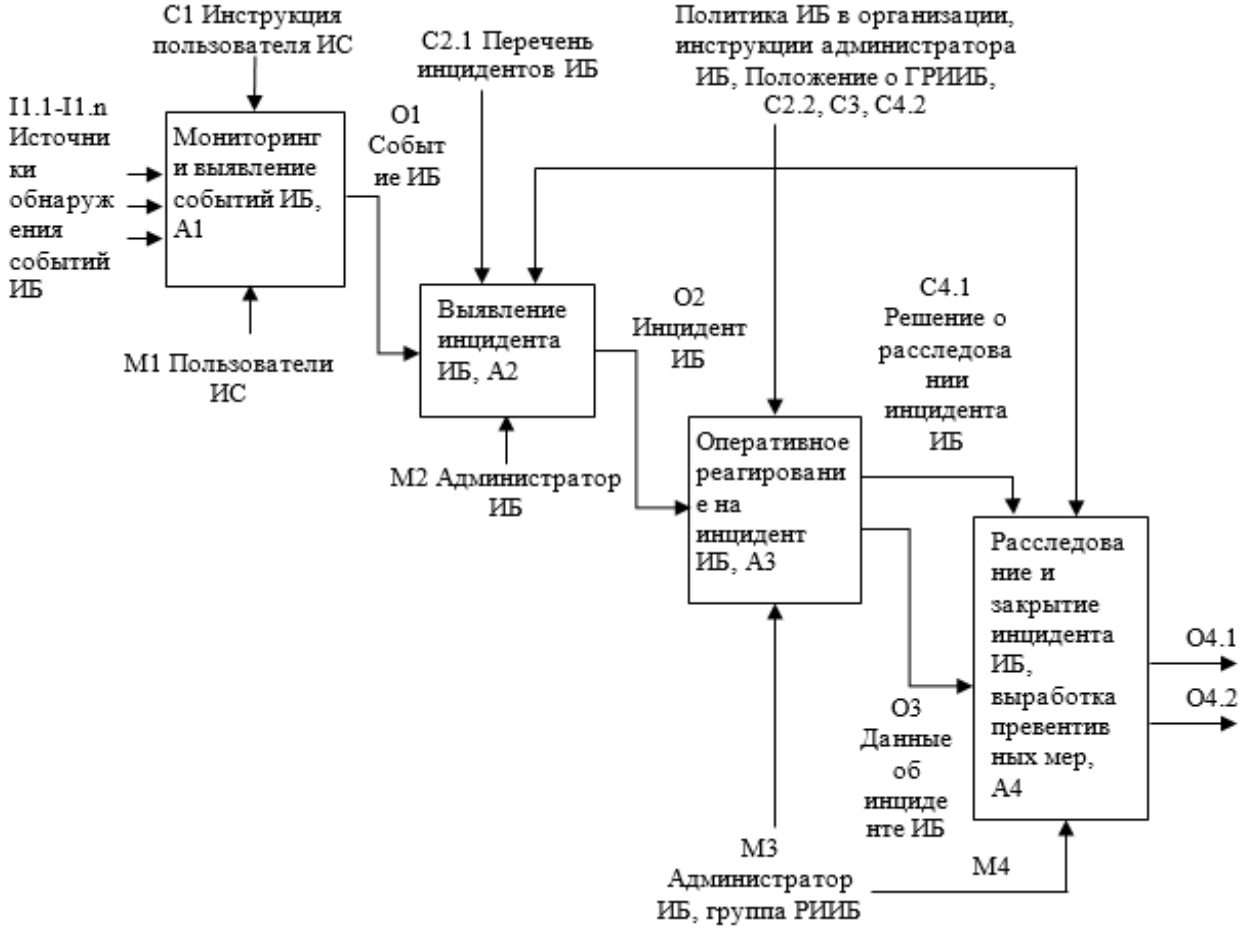

Рис. 2. Декомпозиция целевой функции «Выявление инцидентов ИБ и реагирование на них», А0

Описание диаграммы А0.

I 1.1 – I 1.n – Источники обнаружения событий ИБ.

Функция А1 «Мониторинг и выявление событий ИБ» предполагает применение пользователями ИС таких источников, как:

- автоматизированные системы мониторинга и оповещения, средства сигнализации о системных событиях, ошибках и нарушениях в работе системы;
- средства регистрации событий в системе, прикладных программах и аппаратном обеспечении;
- антивирусное ПО, системы обнаружения вторжений;
- сообщения пользователей и других сотрудников организации, допущенных к инфраструктуре вычислительной системы.

C1 – инструкция пользователя ИС.

M1 – пользователи ИС.

O1 – событие ИБ, является входом I2.

C2.1 – перечень инцидентов ИБ, установленный в организации.

C2.2, C3, C4.2 – политика ИБ в организации, инструкции администратора ИБ, Положение о ГРИИБ.

M2 – администратор ИБ.

O2 – инцидент ИБ, является входом I3.

M3, M4 – администратор ИБ.

O3 – подробные данные об инциденте ИБ – вход I4.

C4.1 – решение о расследовании инцидента ИБ, принимается руководителем группы реагирования на инциденты ИБ.

O4.1 – результаты работы ГРИИБ по расследованию инцидента ИБ с указанием нарушителей, источников и факторов, способствующих возникновению инцидента;

O4.2 – меры по недопущению подобных инцидентов, добавление этого инцидента в Перечень инцидентов ИБ организации.

Вообще все действия при выявлении инцидентов ИБ и реагировании на них можно представить в виде последовательности:

- обнаружение событий ИБ в результате мониторинга всех событий в ИС;
- обработка событий ИБ, то есть, определение того, относится событие к инцидентам или нет; любое событие ИБ может быть результатом преднамеренных или непреднамеренных попыток нарушения конфиденциальности, целостности и (или) доступности информации в ИС в обход защитных мер, но совсем необязательно то, что эта попытка будет отнесена к инцидентам ИБ исходя, в первую очередь, из того, какой ущерб активам ИС она может нанести;
- идентификация инцидента ИБ с целью дальнейшей оценки возможного ущерба от него и дальнейшего реагирования на него;
- оперативное реагирование на выявленный инцидент ИБ с целью минимизации воздействия инцидента на активы ИС;
- расследование инцидента ИБ, определение причин, по которым стал возможен инцидент, выявление «виновника» инцидента, был ли злой умысел и т.д.;
- выводы из расследованного инцидента ИБ и принятие мер для недопущения его в дальнейшем.

Первое действие назовем функцией A1 «Мониторинг и выявление событий ИБ». Действия по обработке и идентификации инцидентов объединим вместе и назовем A2 «Выявление инцидента ИБ». Остальные действия назовем одноименными функциями A3 «Оперативное реагирование на инцидент ИБ» и A4 «Расследование и закрытие инцидента ИБ, выработка превентивных мер».

После обнаружения события ИБ пользователь или иной сотрудник организации обязан оповестить администратора ИБ установленным в данной организации способом или несколькими способами, например, по телефону, электронной почте, или лично. При этом по требованию Администратора ИБ возможно уточнение данных о событии для того, чтобы он смог точно идентифицировать произошедшее событие как инцидент ИБ.

Декомпозиция функции (процесса) A1 «Мониторинг и выявление событий ИБ» приведена на рис. 3. Выходом O14 функции «Регистрация данных о событии в журнале (в электронном/бумажном виде)», A14 будет запись в журнале регистрации данных о событии ИБ, которая используется в качестве входа функции A2 «Выявление инцидента ИБ».

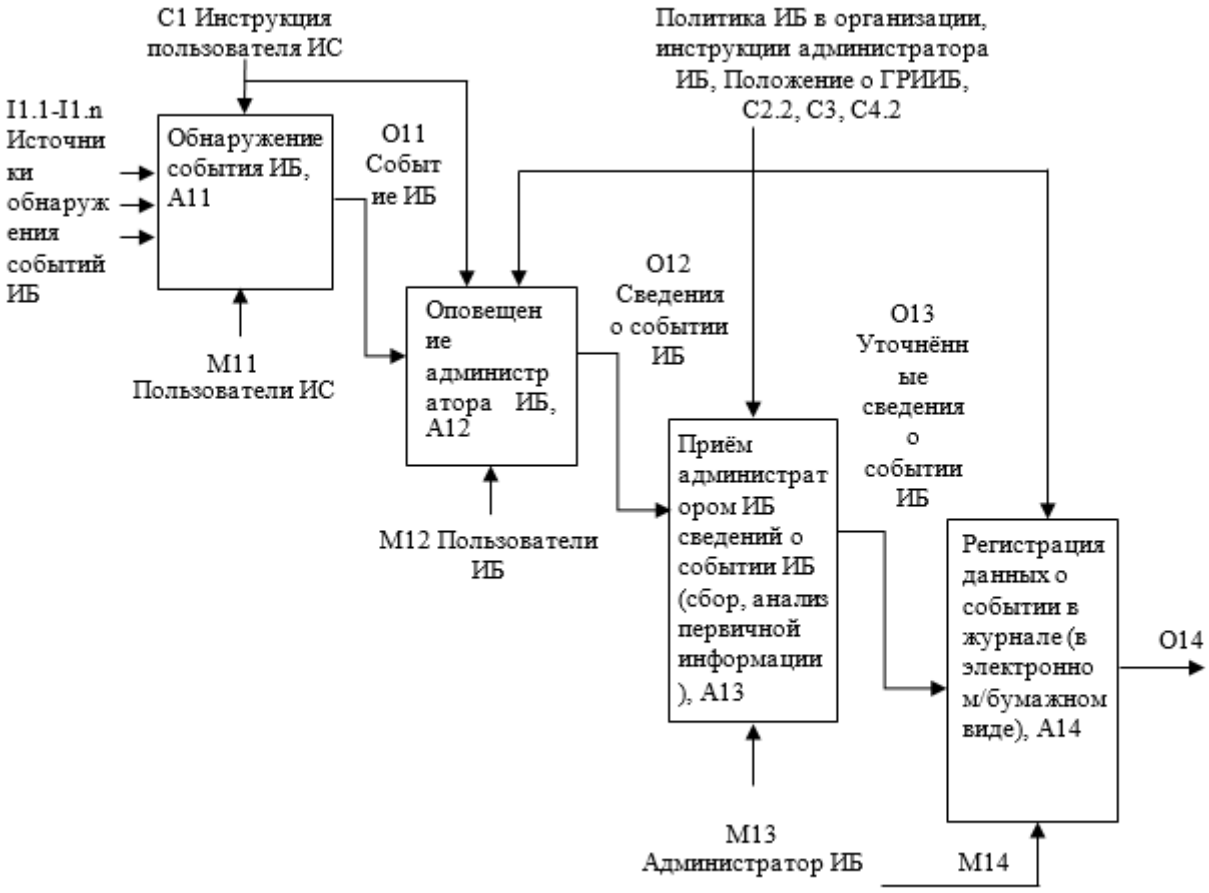

Рис.3. Декомпозиция функции «Мониторинг и выявление событий ИБ», A1

В процессе выявления инцидента из обнаруженных пользователями событий ИБ, администратором ИБ выполняются следующие процедуры:

- прием администратором ИБ сведений о событии ИБ (сбор, анализ первичной информации от пользователей ИС);
- регистрация данных о событии в журнале (в электронном/бумажном виде);
- идентификация Администратором ИБ события ИБ;
- отнесение или не отнесение события к инцидентам ИБ;

Выявление инцидентов ИБ и их идентификация может производится по Перечню инцидентов ИБ, разработанному в данной организации, а также, с использованием методик отнесения событий ИБ к инцидентам, которые в индивидуальном порядке могут быть разработаны для организации в зависимости от используемых информационных систем, вида обрабатываемой информации и прочих факторов.

Администратор ИБ, проведя процедуры выявления инцидента ИБ из обнаруженных событий, в свою очередь, должен сообщить о нем руководителю группы реагирования на инциденты ИБ (ГРИИБ) и передать ему всю собранную об инциденте ИБ информацию. Если событие не отнесено к инцидентам ИБ, тогда администратор ИБ делает запись в журнал регистрации событий и инцидентов ИБ и затем Уведомление заявителю и руководителю ГРИИБ. Декомпозиция функции A2 «Выявление инцидента ИБ» представлена на рис. 4.

В результате выполнения функции «Выявление инцидента ИБ», A2 администратор ИБ сообщает о выявленном инциденте ИБ руководителю ГРИИБ по определенной в данной организации форме, в которой указывается вся имеющаяся информация о данном инциденте, а также делает запись о выявленном инциденте в журнал регистрации инцидентов ИБ. В диаграмме на рис. 4 такая форма обозначена O22. Выход O24 – это уведомление о событии, не признанном инцидентом ИБ.

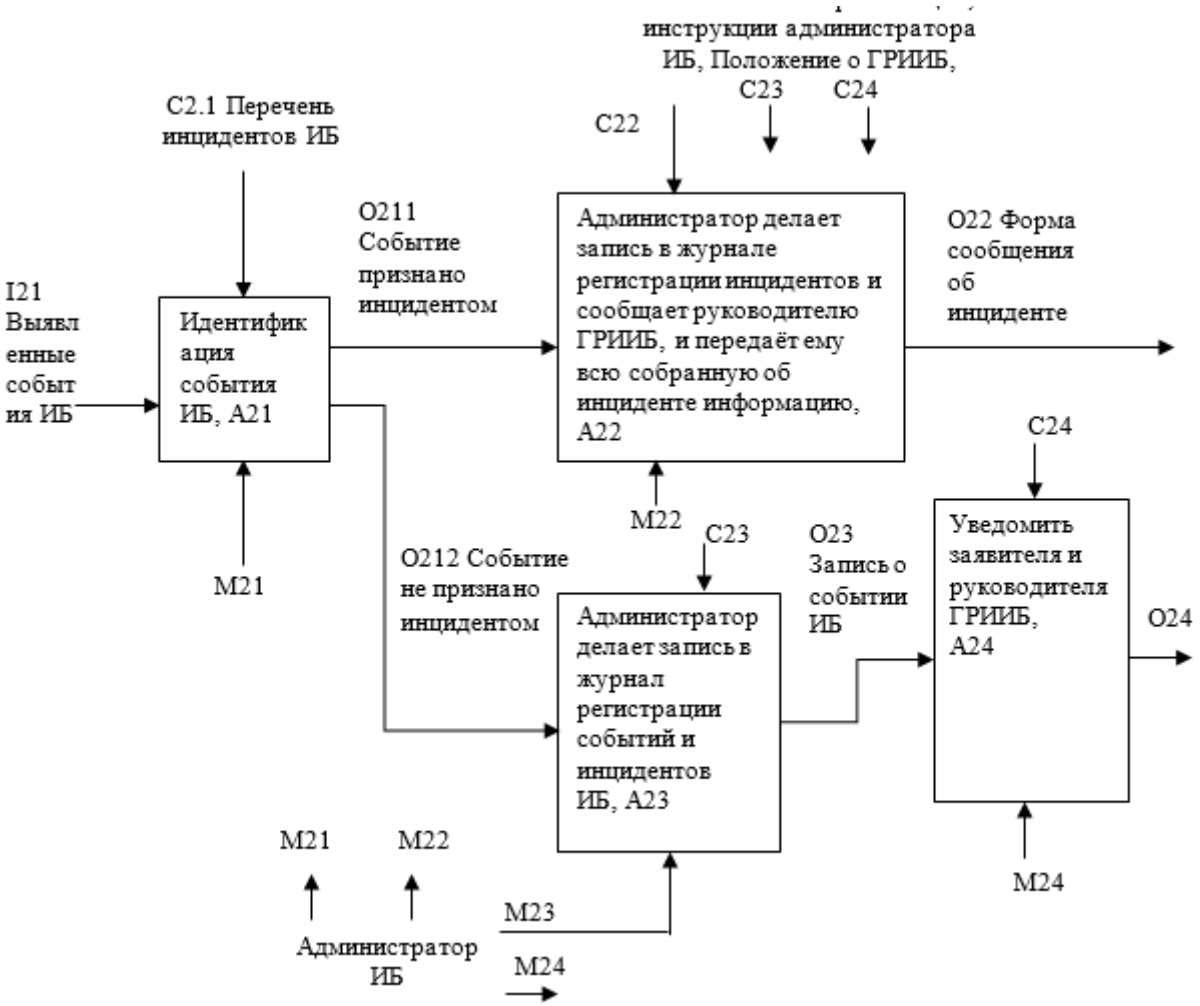

Рис. 4. Декомпозиция функции «Выявление инцидента ИБ», A0

Действия ГРИИБ вместе с администратором ИБ по оперативному реагированию на выявленный инцидент представим в виде одноименной функции «Оперативное реагирование на инциденты ИБ», A3, которая содержит следующую последовательность процедур: Определение факта обработки инцидента ИБ в ИС в настоящее время; Если обрабатывается, то сравнение его и нового инцидента: нет ли общих черт? Если в данный момент в системе уже обрабатываются инциденты ИБ, то вновь поступивший инцидент сопоставляется с обрабатываемыми. Идентичные события по источнику и носителю угрозы обрабатываются в рамках одного зарегистрированного инцидента ИБ.

Руководитель ГРИИБ организует сбор дополнительной информации об инциденте (зона, область, масштаб, длительность и источник воздействия, количество и значимость вовлечённых активов, список вовлеченных лиц, характер причиненного ущерба). На основании этого принимается решение о критичности инцидента, определяется перечень и степень срочности принятия мер по локализации инцидента ИБ.

Администратор ИБ обеспечивает оповещение руководства о регистрации событий и инцидентов ИБ. Затем производится оперативное реагирование на инцидент, включающее локализацию инцидента, отключение АРМов или ресурсов, подверженных негативному воздействию, от общей инфраструктуры, взятие инцидента под оперативный контроль. Для этого руководитель ГРИИБ привлекает любые подразделения и средства, необходимые для эффективного реагирования на произошедший инцидент. После взятия инцидента под оперативный контроль руководитель ГРИИБ определяет необходимость и вероятные способы дальнейшего реагирования на инцидент, включая восстановление повреждённых данных и принятие решения о расследовании инцидента ИБ.

Члены ГРИИБ, в том числе, администратор ИБ, по команде руководителя предпринимают меры по сохранности собранных сведений об инциденте; носители информации сохраняются в сейфе у Администратора ИБ, электронные документы об инциденте (например, журналы безопасности ИС) копируются на машинный носитель и сохраняется в сейфе Администратора ИБ. В дальнейшем, доступ к этим документам предоставляется уполномоченным сотрудникам только для чтения. Таким образом, декомпозиция функции А3 «Оперативное реагирование на инциденты» будет выглядеть в виде диаграммы, представленной на рис. 5.

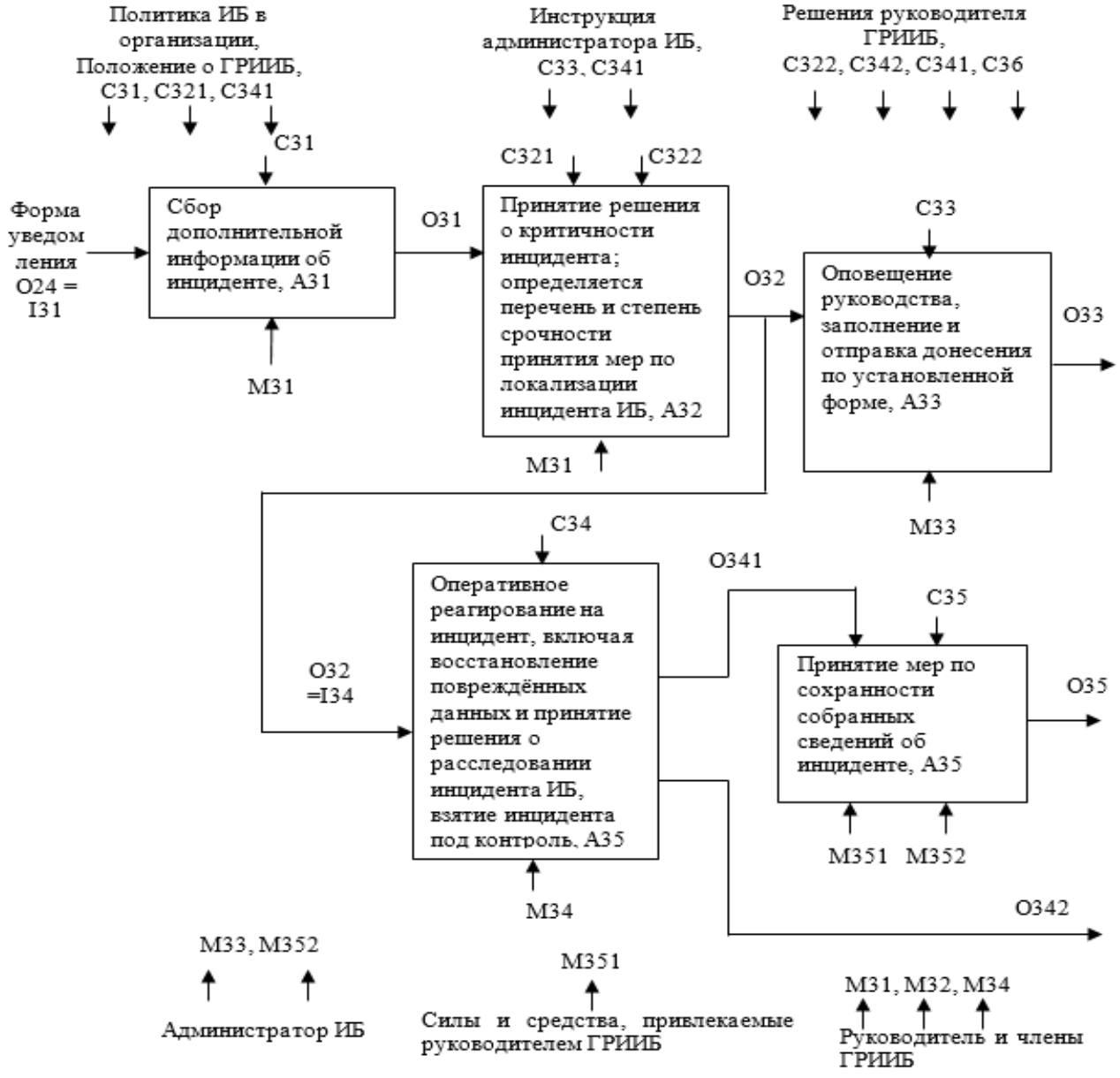

Рис. 5. Декомпозиция функции «Оперативное реагирование на инциденты ИБ», А3

Описание функции «Оперативное реагирование на инциденты ИБ», А3:

I31 – это уведомление заявителя и руководителя ГРИИБ о событии, которое не признано инцидентом ИБ, которое является выходом О24 функции «Уведомить заявителя и руководителя ГРИИБ», А24.

О31 – это информация, необходимая для принятия руководителем ГРИИБ решения о критичности инцидента и для определения перечня и степени срочности принятия мер по локализации инцидента ИБ.

О32 – решение руководителя ГРИИБ о критичности инцидента; перечень мер по локализации инцидента ИБ и очередность их принятия.

О33 – донесение руководителю организации по установленной форме о произошедшем инциденте ИБ.

О341 – задания (инструкции), выработанные группой реагирования на инциденты ИБ во главе с ее руководителем, которые необходимо выполнить администратору ИБ и всем задействованным сотрудникам организации.

О342 – решение о расследовании инцидента ИБ.

О35 – скомпилированные у ГРИИБ все сведения о произошедшем инциденте ИБ, может быть применена форма документа, разработанная для каждой организации индивидуально.

Декомпозиция функции А4 «Расследование и закрытие инцидента, выработка превентивных мер» представлена на диаграмме (рис. 6).

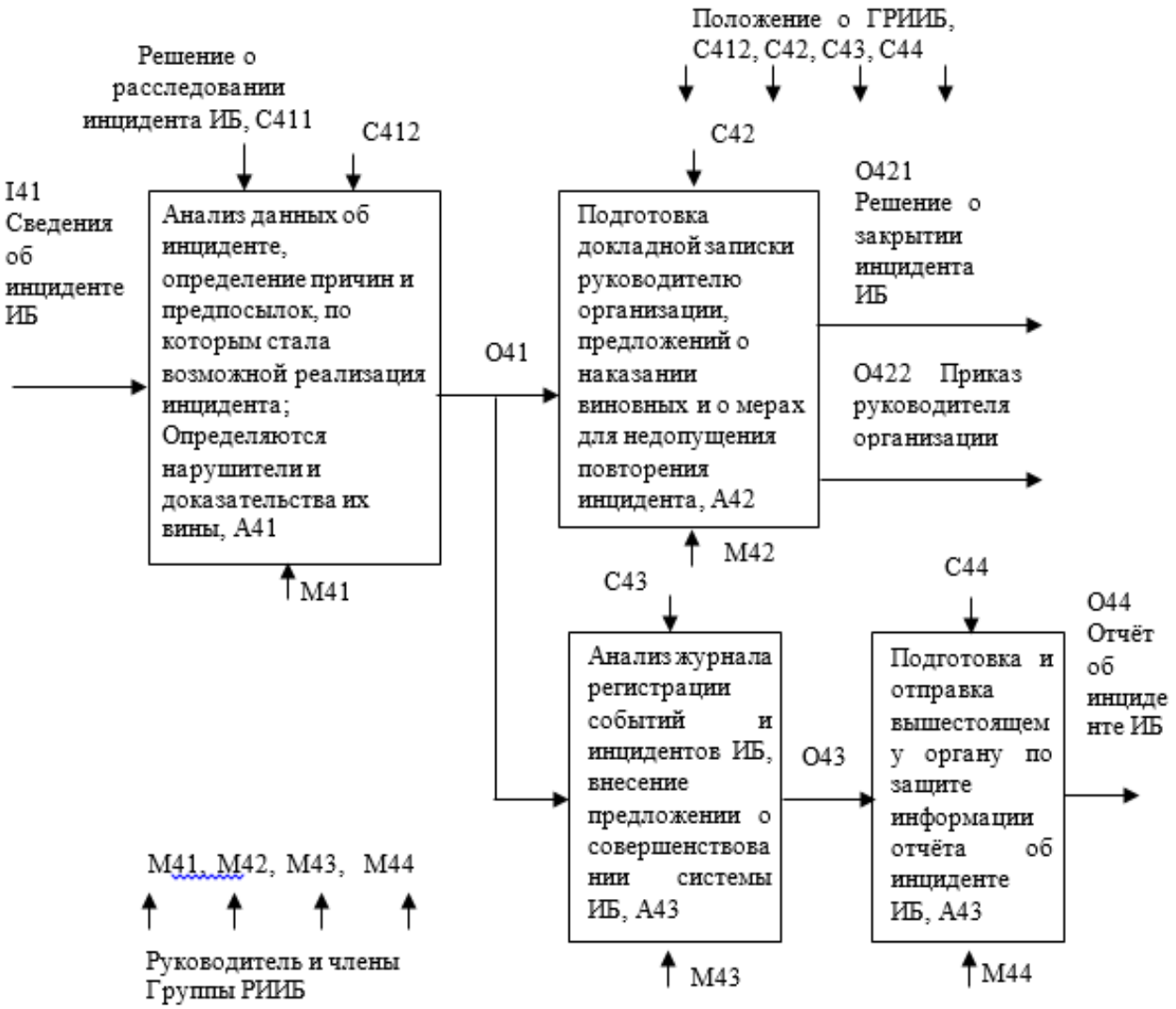

Рис. 6. Декомпозиция функции «Расследование и закрытие инцидента ИБ, выработка превентивных мер», А3

Описание диаграммы, представленной на рис. 6.

А41 – Проводится анализ данных об инциденте; определяются причины и предпосылки, по которым стала возможной реализация инцидента. Определяются нарушители (злоумышленники) и доказательства их деятельности в рамках инцидента ИБ.

А42 – Готовится докладная записка на имя руководителя организации, включающая собранную в рамках расследования информацию, а также, предложения о принятии дисциплинарных и организационных мер в отношении нарушителей и мер для недопущения повторения инцидента ИБ.

А43 – Анализ журнала регистрации событий и инцидентов ИБ; выявление тенденций и закономерностей возникновения инцидентов. Принятие решений о внесение изменений в перечень инцидентов, о совершенствовании системы управления инцидентами и системой ИБ организации.

А44 – На основе проведенного анализа ГРИИБ формирует и отправляет вышестоящему органу по защите информации отчет об инциденте ИБ, содержащий всю собранную информацию.

Выходами диаграммы декомпозиции функции А3, представленной на рис. 6, являются:

О421 – решение о закрытии инцидента ИБ;

О422 – приказ руководителя организации о наказании виновных в произошедшем инциденте ИБ и о принятии превентивных мер, направленных на предотвращение подобных инцидентов в будущем;

О44 – отчет об инциденте ИБ в вышестоящую организацию.

Отчет об инциденте ИБ может представляться в подразделение по защите информации или другое подразделение вышестоящей организации по установленной форме.

Заключение

Разработана модель процессов и действий, производимых должностными лицами при выявлении и расследовании инцидентов ИБ в любой организации, эксплуатирующей информационные системы. Моделирование произведено по методологии IDEF0, которая в настоящее время пользуется популярностью и отличается простотой в восприятии, понятностью и наглядностью моделируемых процессов.

Авторы статьи надеются на то, что представленная модель поможет специалистам по защите информации и их руководителям формализовать процессы по выявлению и расследованию инцидентов ИБ в их организации, а также будет способствовать разработке собственного регламента действий.

Библиографический список

1. ГОСТ Р ИСО/МЭК ТО 18044-2007 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности.
2. Integration DEFinition for function modeling (IDEF0). Draft Federal Information Processing Standards Publication 183, 1993 December 21. URL: http://idef.com/wp-content/uploads/2016/02/idef0.pdf. (дата обращения 19.09.2020 г.)
3. **Карпычев, В.Ю.** Функциональное моделирование (IDEF0) как метод исследования блокчейн-технологии // Труды НГТУ им. Р.Е. Алексеева. – № 4 (123). – 2018.

Дата поступления
в редакцию: 03.10.2020

N.G. Labutin. P.V. Kostin, N.U. Shadrunova

SIMULATING INFORMATION SECURITY INCIDENT DETECTION AND RESPONSE PROCESSES

Federal State Institution of Advanced finance Professional Training
Federal Tax Service Training Institute

Purpose: development of a model designed to help information security specialists (administrators) regulate the detection and investigation of information security incidents in any organization, regardless of the type of information system, its structure, information processing principles.
Methodology: functional modeling of processes and actions of specialists when identifying and investigating information security incidents using the methodology of SADT/IDEF0
Value: the model of information security incident detection and investigation processes developed by the authors of the article can be used to develop the rules of these processes in any information system.
Research implications: modeling of actions of officials in the detection and investigation of information security incidents can be continued with more detail and specificity.

Key words: information security incident, process modeling, IDEF0 methodology, information security incident detection, information security incident investigation.