УДК 004.7.056.5 ***DOI: 10.46960/1816-210X_2022_3_22***

МОДЕЛИРОВАНИЕ ДЕЙСТВИЙ СПЕЦИАЛИСТА ПРИ ОЦЕНКЕ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ И СЕТЯХ В СООТВЕТСТВИИ С НОВОЙ МЕТОДИКОЙ ФСТЭК РОССИИ

Н.Г. Лабутин
ORCID: **0000-0003-3565-252X** e-mail: **ko_kol1@rambler.ru**
Приволжский институт повышения квалификации ФНС России
Нижний Новгород, Россия

П.В. Костин
ORCID: **0000-0002-5401-6011** e-mail: **expert36@list.ru**
Приволжский институт повышения квалификации ФНС России
Нижний Новгород, Россия

Представлен анализ действий специалиста по защите информации в процессе оценки угроз информационной безопасности на объекте информатизации, которые необходимо осуществить в соответствии с новой методикой ФСТЭК России. На основании анализа положений нового методического документа впервые произведено моделирование всей процедуры действий, производимых при выявлении и оценке угроз безопасности информации. Посредством методологии IDEF0, наиболее прогрессивной и адекватной в рассматриваемой ситуации, разработана модель, которая отражает новый подход к систематизации функциональных действий специалистов по защите информации в процессе выполнения своих должностных обязанностей. Представленная модель призвана формализовать эти действия в любой информационной системе и сети, независимо от их назначения, принципов работы и особенностей функционирования.

Ключевые слова: оценка угроз безопасности информации, моделирование процессов, методология IDEF0, модель угроз безопасности информации, актуальные угрозы безопасности информации.

ДЛЯ ЦИТИРОВАНИЯ: Лабутин, Н.Г. Моделирование действий специалиста при оценке угроз безопасности информации в информационных системах и сетях в соответствии с новой методикой ФСТЭК России / Н.Г. Лабутин, П.В. Костин // Труды НГТУ им. Р.Е. Алексеева. 2022. № 3. С. 22-31.
DOI: 10.46960/1816-210X_2022_3_22

MODELING OF A SPECIALIST'S ACTIONS AT ASSESSMENT OF INFORMATION SECURITY THREATS IN INFORMATION SYSTEMS AND NETWORKS IN ACCORDANCE WITH THE NEW METHODOLOGY OF FSTEC OF RUSSIA

N.G. Labutin
ORCID: **0000-0003-3565-252X** e-mail: **ko_kol1@rambler.ru**
Volga institute of advanced training of FTS of Nizhny Novgorod
Nizhny Novgorod, Russia

P.V. Kostin
ORCID: 0**000-0002-5401-6011** e-mail: **expert36@list.ru**
Volga institute of advanced training of FTS of Nizhny Novgorod
Nizhny Novgorod, Russia

Abstract. Analysis of information security specialist's actions in the process of assessment of threats to information security at an informatization facility which must be carried out in accordance with the new methodology of FSTEC (*Federal Service for Technology and Export Control) of Russia, is presented. Based on the analysis of provisions of the new methodological document of FSTEC of Russia, the modeling of the entire procedure performed at identifying and assessing of threats to information security, was carried out for the first time. As a result, using the IDEF0 methodology, a model of these actions has been developed, which represents a new approach to systematizing of the information security specialists' functional actions in the process of performing of their official duties. The developed model is designed to formalize these actions in any information system and network, regardless of their purpose, principles of operation and features of functioning. To model the actions of a specialist in assessing of threats to information security, the IDEF0 methodology was applied as the most progressive and suitable for the situation under consideration.

Key words: information security threat assessment, process modeling, IDEF0 methodology, information security threat model, current information security threats.

FOR CITATION: N.G. Labutin, P.V. Kostin. Modeling of a specialist's actions at assessment of information security threats in information systems and networks in accordance with the new methodology of FSTEC of Russia. Transactions of NNSTU n.a. R.E. Alekseev. 2022. № 3. Pp. 22-31. DOI: 10.46960/1816-210X_2022_3_22

Введение

Для каждого специалиста по защите информации (ЗИ) одним из значимых и ответственных направлений профессиональной деятельности является разработка организационно-распорядительных документов (ОРД) локального уровня. Согласно требованиям государственных регуляторов в сфере защиты информации – ФСТЭК и ФСБ России, наряду с другими ОРД, в каждой организации должен быть подготовлен и поддерживаться в актуальном состоянии локальный документ «Модель угроз безопасности информации (БИ)». При его разработке у многих специалистов по ЗИ возникают некоторые закономерные затруднения, связанные, в первую очередь, с формированием регуляторами новых требований и методик создания модели угроз БИ. Помимо этого, речь идет о растущем числе новых угроз, и, соответственно, о сложностях определения всех актуальных для данной информационной системы (ИС) угроз БИ.

В 2021 г. ФСТЭК России разработала документ «Методика оценки угроз безопасности информации», утвержденный 5 февраля 2021 г. [1]. В связи с этим ранее принятый документ «Методика определения актуальных угроз персональных данных при их обработке в информационных системах персональных данных» от 2008 г. утратил силу. В методике 2021 г. есть ряд нововведений, которые необходимо учитывать каждому специалисту по информационной безопасности, ответственному за «Модель угроз БИ» объекта защиты.

Данная статья предназначена для специалистов по защите информации для правильной оценки угроз БИ и, на основании этого, разработки Модели угроз БИ защищаемых ИС, определяемой методикой оценки угроз БИ ФСТЭК России от 5 февраля 2021 г. Представлен процесс формализации действий по оценке угроз БИ на защищаемом объекте при помощи функционального моделирования IDEF0 [2], рассмотренного в [3, 4].

Анализ действий специалиста при определении степени угроз безопасности информации и построение модели

IDEF0 позволяет производить функциональное моделирование процессов и действий в системах любой сложности, при этом наглядно и достаточно просто отображая их в виде диаграмм с прямоугольниками и соединительными стрелками. Прямоугольниками отображаются функциональные блоки, описанные как действия, представленные глаголами. При этом верхняя сторона прямоугольника используется для обозначения управляющего воздействия на данную функцию (процесс), нижняя – для описания инструментария выполнения данной функции, левая сторона – для задания входных воздействий, правая – для определе-

ния выходных функций. Стрелки на диаграмме предназначены для указания входящих воздействий, которые обрабатываются блоком. Они могут также использоваться для указания результатов предыдущих действий или иных воздействий на функцию, реализуемую данным блоком [2].

Моделирование IDEF0 заключается в представлении моделируемой системы в виде основной целевой функции с дальнейшей ее детализацией; при этом используются декомпозиции, проводимые последовательно. Конечное состояние моделируемой системы, до которого осуществляется детализация, определяется разработчиком [2]. Диаграмма, демонстрирующая в целом действия специалиста по ЗИ при определении степени угроз безопасности информации в системах и сетях организации, представлена на рис. 1.

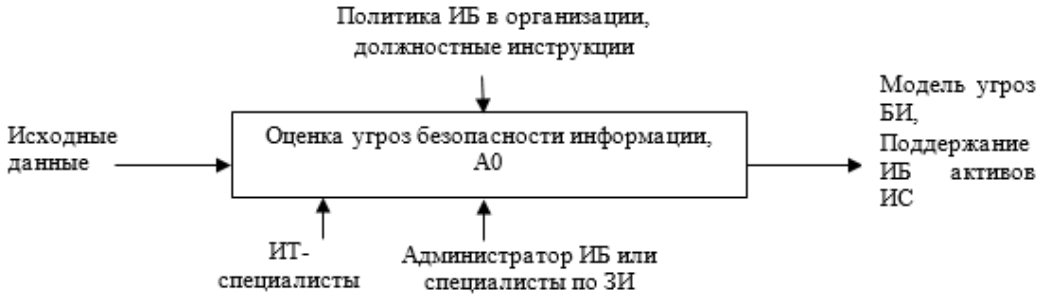

Рис. 1. Диаграмма А-0. Целевая (контекстная) функция «Оценка угроз безопасности информации», А0

Fig. 1. Diagram A-0. «Information security threat assessment» target (contextual) function, A0

Конечной целью оценки угроз БИ на защищаемом объекте является модель угроз безопасности информации, актуальных для этого объекта. В целом это служит достижению единой основной цели – обеспечению достойного уровня безопасности информации (активов) ИС.

Исходные данные для оценки угроз БИ на объекте информатизации [1] (рис. 1):

1) банк данных угроз (БДУ) безопасности информации ФСТЭК России (bdu.fstec.ru), в котором представлены существующие угрозы БИ;

2) модели угроз безопасности информации, если они были разработаны на более высоком уровне организации (например, в ведомстве, отрасли и т.д.);

3) сигнатуры известных компьютерных атак из соответствующих ресурсов сети Интернет (например, STIX, CAPEC, ATT&CK, OWASP и т.д.);

4) сведения из конструкторской и эксплуатационной документации об имеющихся способах и системах защиты информации в эксплуатируемой ИС, такие как: назначение, технические характеристики, структура ИС, имеющиеся группы безопасности пользователей, назначенные им типовые разрешения на доступ и привилегии, а также другие подобные сведения;

5) правила доступа к центру обработки данных или облачного хранилища информации, если таковые предусмотрены в защищаемой ИС;

6) нормативные документы, вводящие в эксплуатацию информационные системы, с указанными в них сведениями о назначении, задачах и функциях систем и сетей, о правовом режиме обрабатываемой информации;

7) технологические или производственные документы (карты) на информационные системы, сети, в которых представлены основные критические процессы для владельца информации или оператора ИС;

8) результаты оценки возможного ущерба от реализованных угроз, проведенной владельцем информации или оператором ИС.

Чтобы не загромождать диаграмму излишними подробностями, на рис. 1 все указанные выше исходные данные для оценки угроз БИ на объекте информатизации подписаны просто: «исходные данные», как входные воздействия для целевой функции А0. Процедура оценки угроз БИ в ИС (понимая ИС как непосредственно информационные системы, так и системы АСУ, информационно-телекоммуникационные сети, информационные инфраструктуры центров обработки данных, а также и облачные сервисы), как определено в «Методике оценки угроз безопасности информации», утвержденной ФСТЭК России 5 февраля 2021 г., может представляться этапами работы, которые в нашей модели обозначаются как следующие процессы:

- «Определение негативных последствий вследствие возникновения и (или) реализации угроз безопасности информации» А1.
- «Установление вероятных объектов, подвергаемых воздействию угроз безопасности информации» А2.
- «Оценка вероятности возникновения и (или) реализации угроз безопасности информации с определением актуальности таковых» А3.

На рис. 2 приведена диаграмма с декомпозицией целевой функции А0.

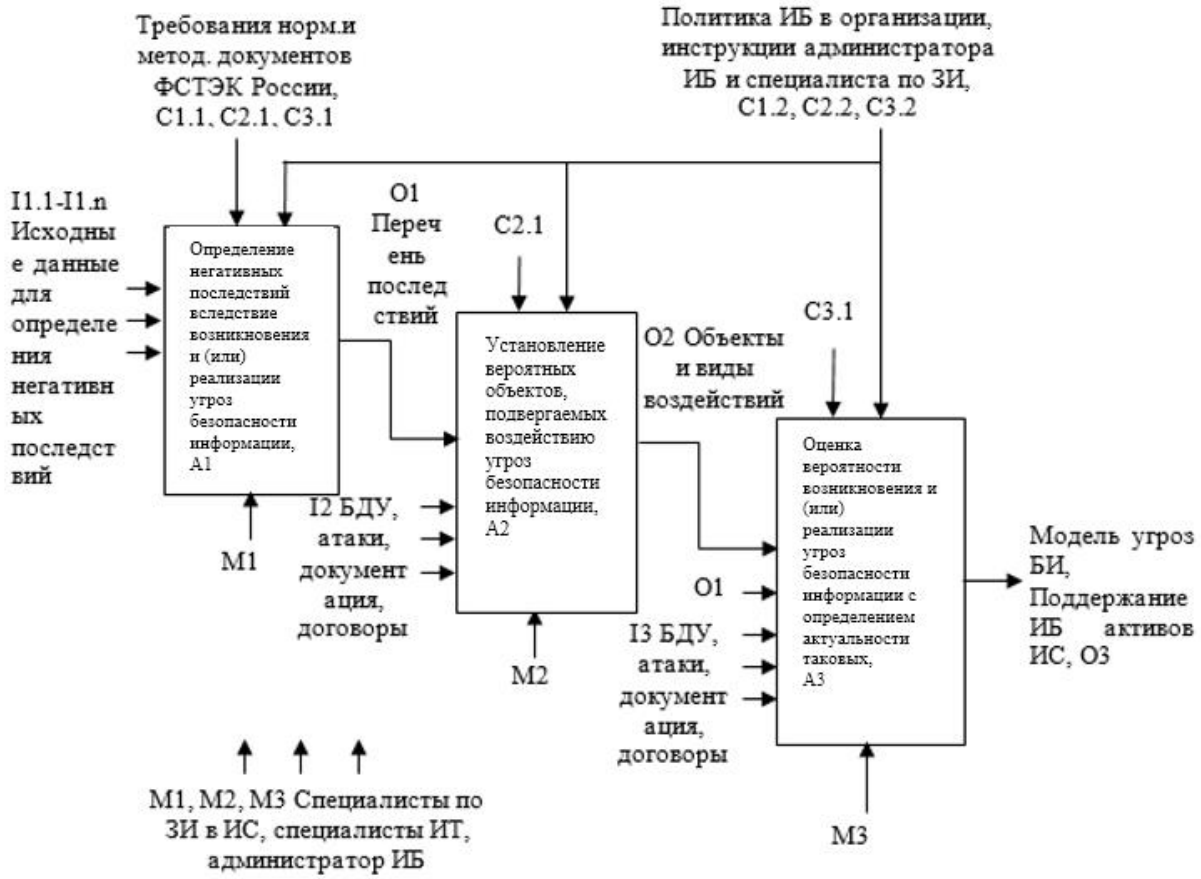

Рис. 2. Декомпозиция целевой функции «Оценка угроз безопасности информации», А0

Fig. 2. Decomposition of «Information security threat assessment» target function, A0

Для процесса, обозначенного выше как А1, исходными данными будут:

- БДУ безопасности информации ФСТЭК России (bdu.fstec.ru);
- документы (нормативные, распорядительные и иные), на основании которых вводятся в эксплуатацию ИС, с указанными в них сведениями о назначении, задачах и функциях систем и сетей, о правовом режиме обрабатываемой информации;

- эксплуатационные документы со сведениями о назначении и функциях, о составе и архитектуре систем и сетей;
- технологические, производственные документы (карты) на информационные системы, сети, в которых представлены основные критические процессы для владельца информации или оператора ИС;
- результаты оценки возможного ущерба от реализованных угроз, проведенной владельцем информации или оператором ИС.

Если в конкретной ситуации для данной ИС существуют другие исходные данные, не указанные выше, специалисты, проводящие оценку угроз БИ, могут их использовать в данной модели. Цель процесса А1 «Определение негативных последствий вследствие возникновения и (или) реализации угроз безопасности информации» – установление критически значимых для данной ИС событий безопасности информации, которые могут привести к значительному ущербу владельцу ИС или государству и оценка ущерба от их последствий. Возможный ущерб может быть определен на основе оценки независимых экспертов или на основе сведений, предоставленных специалистами обладателя информации или владельца ИС, при этом он должен учитываться применительно к данной ИС. Кроме установления возможного ущерба, в процессе оценки угроз БИ на ОИ решаются следующие задачи, которые при моделировании выделены в отдельные процессы, получаемые при декомпозиции процессов А2, А3 (рис. 3).

Рис. 3. Задачи, решаемые специалистом по защите информации в процесс оценки угроз БИ на ОИ

Fig. 3. Problems solved by an information security specialist in the process of information security threats assessment at an informatization facility

Первые две задачи по сути – декомпозиция процесса А2; остальные – декомпозиция процесса А3. Таким образом, декомпозиции процессов А2 и А3 можно представить в виде диаграмм (рис. 4 и 6). Все работы, соответствующие указанным процессам, должны выполняться специалистами или подразделением по защите информации при обязательном содействии ИТ-специалистов и привлечении профильных подразделений данной организации. Иначе оценка угроз безопасности информации может получиться недостоверной, что обязательно нанесет ущерб защищаемым активам организации. Таким образом, задачи по оценке угроз БИ охватывают более широкий спектр действий специалистов, а не только заключаются в определении угроз, которые возможны в информационных системах и сетях, эксплуатируемых в данной организации. При необходимости по решению оператора ИС или владельца информации для оценки угроз безопасности информации в соответствии с действующим законодательством могут быть привлечены иные специалисты, в том числе, сторонних организаций. При этом рекомендуется привлекать специалистов, обладающих знаниями и умениями по оценке рисков и технической защите информации.

В результате выполнения процессов А2.1 «Анализ исходных данных и инвентаризация ИС организации и А2.2 «Определение возможных объектов и видов воздействия угроз безопасности информации» специалист по ЗИ и ИТ-специалисты выявляют объекты (элементы) ИС, на которые могут воздействовать угрозы БИ, при этом как исходные данные могут быть использованы:

- БДУ безопасности информации ФСТЭК России (bdu.fstec.ru);
- сигнатуры известных компьютерных атак из соответствующих ресурсов сети Интернет (например, STIX, CAPEC, ATT&CK, OWASP и т.д.);
- сведения из конструкторской и эксплуатационной документации об имеющихся способах и системах защиты информации в эксплуатируемой ИС;
- правила доступа к центру обработки данных или облачного хранилища информации, если они предусмотрены в защищаемой ИС.

Кроме того, в качестве исходных данных следует обязательно использовать результаты процесса А1, а именно перечень негативных последствий, возникающих вследствие воздействия угроз безопасности информации на рассматриваемую ИС и несущих значительный ущерб для активов данной организации (рис. 4).

Объектами воздействия, как правило, могут быть: сама защищаемая информация, а также программное обеспечение и программно-технические средства обработки и хранения информации, внешние носители информации, сетевое (телекоммуникационное) оборудование, сами средства защиты информации, независимо от исполнения: программные или программно-технические, а также пользователи системы.

В процессе А2.2 также должны быть определены актуальные для анализируемой ИС виды воздействия на выявленные «критичные» объекты ИС. Типовые виды воздействий, приводящих к реализации угроз БИ [1] представлены на рис. 5.

Исходными данными для процесса А3.1 «Установление источников угроз БИ и оценка возможности нарушителей реализовать данные угрозы» являются:

- БДУ безопасности информации ФСТЭК России (bdu.fstec.ru);
- сигнатуры известных компьютерных атак из соответствующих ресурсов сети Интернет (например, STIX, CAPEC, ATT&CK, OWASP и т.д.);
- сведения из конструкторской и эксплуатационной документации об имеющихся способах и системах защиты информации в эксплуатируемой ИС;
- правила доступа к центру обработки данных или облачного хранилища информации, если они предусмотрены в защищаемой ИС.

Результаты выполнения процессов А1 и А2 следующие:

- результаты оценки ущерба, проведенной владельцем информации;

- установленный размер ущерба, возникшего в результате воздействия угроз безопасности информации;
- установленный процессом А2.2 перечень объектов, которые могут подвергаться угрозам БИ, а также воздействия, которые на них могут быть оказаны.

В результате процесса А3.1 должно быть определено:

- кто и как может реализовать угрозы БИ в ИС (т.е. актуальный перечень и возможности нарушителей БИ);
- возможные способы, которыми вероятные нарушители могут нанести ущерб ИС.

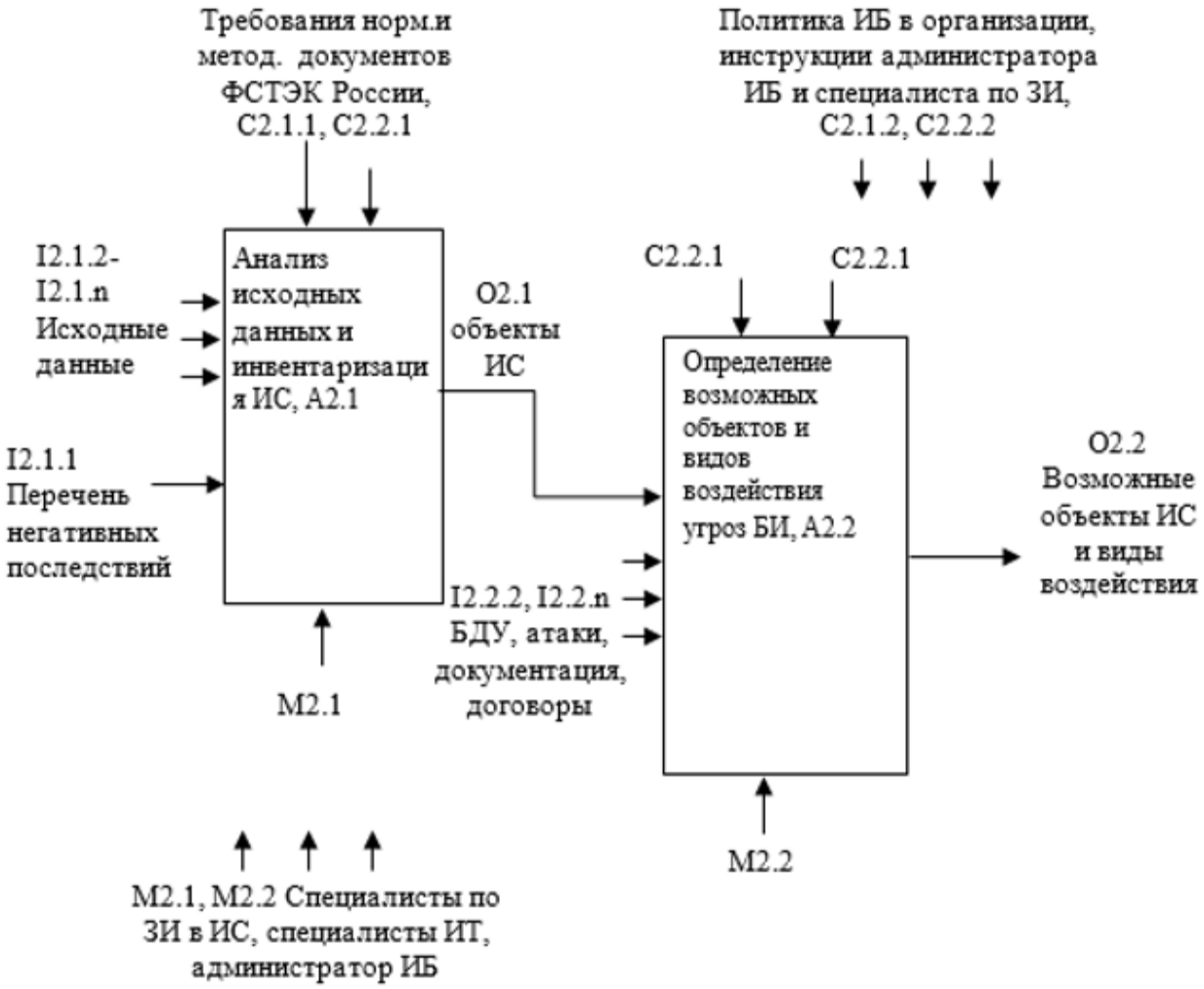

Рис. 4. Декомпозиция функции (процесса) А2 «Установление вероятных объектов, подвергаемых воздействию угроз безопасности информации»

Fig. 4. Decomposition of «Identification of probable facilities exposed to information security threats» A2 function (process)

Для процесса А3.2 «Определение порядка возникновения и (или) реализации угроз безопасности информации» исходными данными будут:

- БДУ безопасности информации ФСТЭК России (bdu.fstec.ru);
- сигнатуры известных компьютерных атак из соответствующих ресурсов сети Интернет (например, STIX, CAPEC, ATT&CK, OWASP и т.д.);
- сведения из конструкторской и эксплуатационной документации об имеющихся способах и системах защиты информации в эксплуатируемой ИС;

- правила доступа к центру обработки данных или облачного хранилища информации, если они предусмотрены в защищаемой ИС;
- перечень возможных нарушителей и способов, которыми они могут реализовать угрозы БИ.

Далее, как определяет методика оценки угроз БИ, необходимо выбрать только те способы реализации угроз, которые возможны в анализируемой ИС. В нашей модели это процесс А3.3.

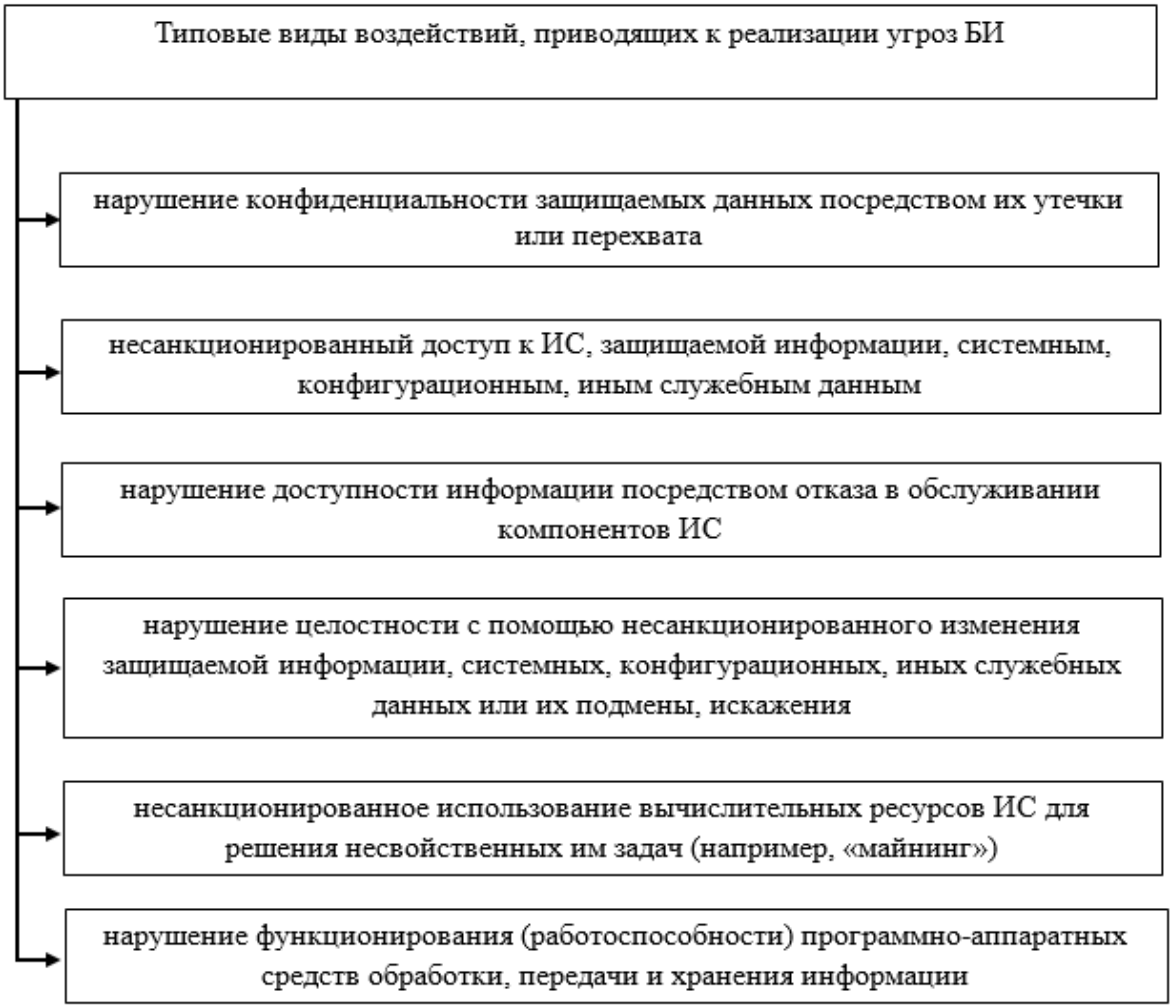

Рис. 5. Типовые виды воздействий, приводящих к реализации угроз БИ

Fig. 5. Typical types of impacts leading to the information security threats implementation

Исходные данные для процесса А3.3 «Оценка актуальности угроз БИ в ИС»:

- БДУ безопасности информации ФСТЭК России (bdu.fstec.ru);
- сигнатуры известных компьютерных атак из соответствующих ресурсов сети Интернет (например, STIX, CAPEC, ATT&CK, OWASP и т.д.);

а также, результаты выполнения процессов А1, А2, А3.1 и А3.2:

- результаты оценки ущерба, проведенной владельцем информации;
- установленный размер ущерба, возникшего в результате воздействия угроз безопасности информации;
- установленный процессом А2.2 перечень объектов, которые могут подвергаться угрозам БИ, а также воздействия, которые на них могут быть оказаны;

- кто и как может реализовать угрозы БИ в ИС (т.е. актуальный перечень и возможности нарушителей БИ);
- возможные способы, которыми вероятные нарушители могут нанести ущерб ИС.

В результате процесса А3.3 должна быть проведена оценка актуальности угроз БИ и подготовлены все необходимые данные для разработки организационно-распорядительного документа локального уровня «Модель угроз безопасности информации».

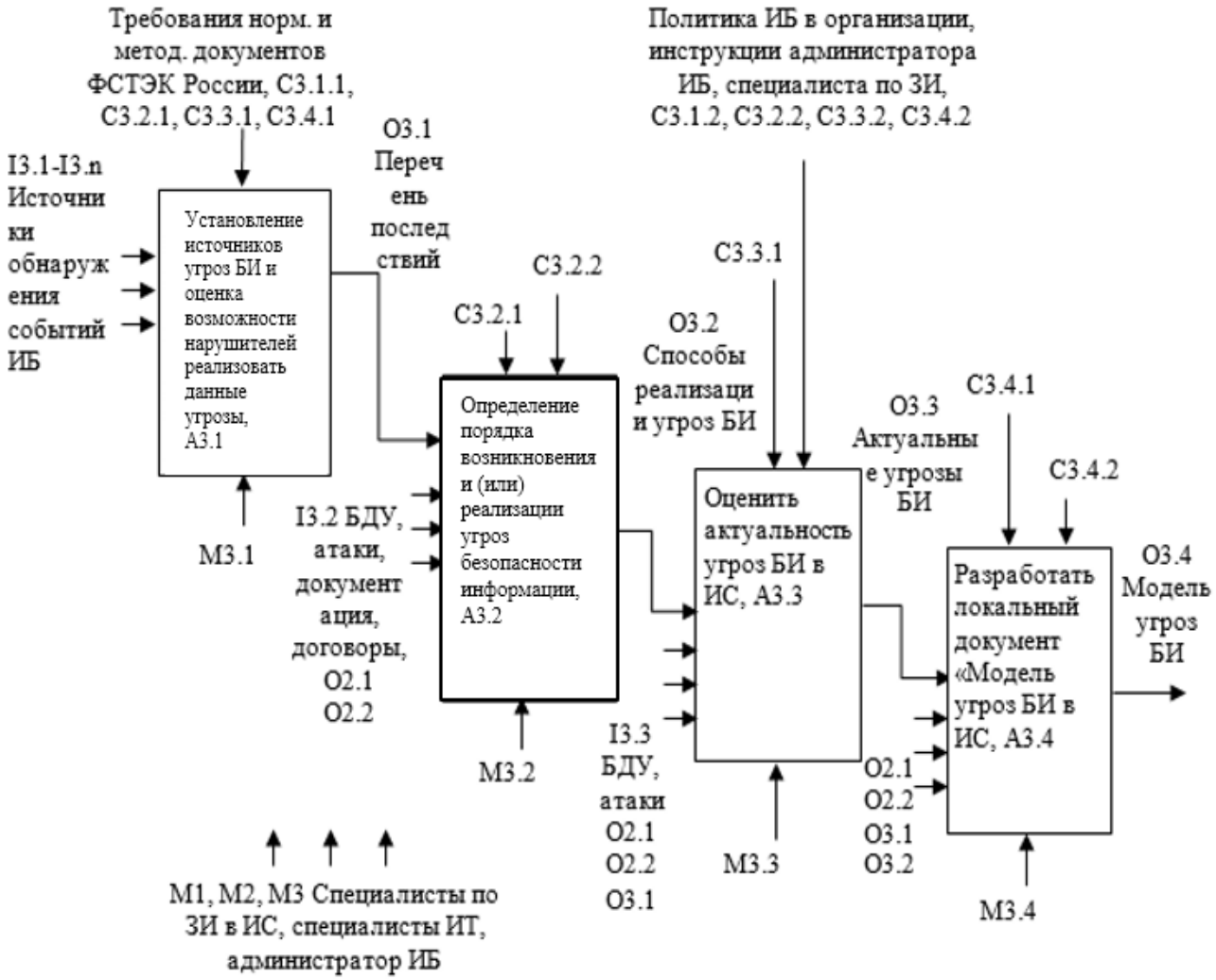

Рис. 6. Декомпозиция функции (процесса) А3 «Оценка вероятности возникновения и (или) реализации угроз безопасности информации с определением актуальности таковых»

Fig. 6. Decomposition of «Assessment of the probability of occurrence and (or) implementation of information security threats with determination of relevance thereof» A3 function (process)

Заключение

Содержание работ, выполняемых специалистом по защите информации при оценке угроз БИ, зависит от конкретных условий эксплуатации информационных систем, особенностей функционирования ИС и других индивидуальных факторов. Вместе с тем, последовательность действий и методика их выполнения всегда одна. В настоящей статье предпринята попытка смоделировать эти действия с целью помощи специалистам по защите информации в проведении оценки угроз БИ в соответствии с требованиями регулятора.

Библиографический список

1. «Методика оценки угроз безопасности информации», утв. ФСТЭК России 5 февраля 2021 г.: официальный сайт ФСТЭК России [Электронный ресурс] // Режим доступа: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/2170-metodicheskij-dokument-utverzhden-fstek-rossii-5-fevralya-2021) (Дата обращения 19.02.2022)
2. Integration DEFinition for function modeling (IDEF0). Draft Federal Information Processing Standards Publication 183, 1993 December 21 [Электронный ресурс] // Режим доступа: URL: http://idef.com/wp-content/uploads/2016/02/idef0.pdf. (Дата обращения 19.02.2022)
3. **Карпычев, В.Ю.** Функциональное моделирование (IDEF0) как метод исследования блокчейн-технологии // Труды НГТУ им. Р.Е. Алексеева. 2018. № 4 (123). С. 22-32.
4. **Лабутин, Н.Г.** Моделирование процессов выявления инцидентов информационной безопасности и реагирования на них / Н.Г. Лабутин, П.В. Костин, Н.Ю. Шадрунова // Труды НГТУ им. Р.Е. Алексеева. 2020. № 4 (131). С. 16-25.

Дата поступления
в редакцию: 22.10.2021