ISSN 1680-2772

АКАДЕМИЯ ВОЕННЫХ НАУК
ЦЕНТР ПРОБЛЕМ СТРАТЕГИЧЕСКИХ ЯДЕРНЫХ СИЛ

РОССИЙСКАЯ ИНЖЕНЕРНАЯ АКАДЕМИЯ
СЕКЦИЯ «ИНЖЕНЕРНЫЕ ПРОБЛЕМЫ СТАБИЛЬНОСТИ И КОНВЕРСИИ»

СТРАТЕГИЧЕСКАЯ СТАБИЛЬНОСТЬ

№ 2

СТРАТЕГИЧЕСКАЯ СТАБИЛЬНОСТЬ №2 (91) 2020

Научно-практический междисциплинарный журнал

Военная теория, военное строительство, стратегическое планирование и управление, вооружение и военная техника, системы контроля и испытаний

Отрасли наук: военные науки [военно – теоретические науки (20.01.00), военно – специальные науки (20. 02.00)].

АКАДЕМИЯ ВОЕННЫХ НАУК
ЦЕНТР ПРОБЛЕМ СТРАТЕГИЧЕСКИХ ЯДЕРНЫХ СИЛ

РОССИЙСКАЯ ИНЖЕНЕРНАЯ АКАДЕМИЯ
СЕКЦИЯ «ИНЖЕНЕРНЫЕ ПРОБЛЕМЫ СТАБИЛЬНОСТИ И КОНВЕРСИИ»

Издается с ноября 1997 г.
Свидетельство о регистрации ПИ №77-3705 от 09.06.2000 г.
ISSN 1680-2772.

Выходит 4 раза в год.

Журнал включен в «Перечень ведущих периодических изданий» ВАК и систему РИНЦ

СОДЕРЖАНИЕ

УДК 004.056

© Сидак А.А., Василенко В.В., Лыков В.В.

© Sidak A., Vasilenko V., Lykov V.

РЕЗУЛЬТАТЫ АПРОБАЦИИ МЕТОДИКИ МОДЕЛИРОВАНИЯ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ. РАСПРЕДЕЛЕНИЕ ЗОН ОТВЕТСТВЕННОСТИ

THE RESULTS OF THE INFORMATION SECURITY THREAT MODELLING METHODOLOGY APPROBATION IN INFORMATION SYSTEMS. DISTRIBUTION OF RESPONSIBILITY ZONES

Аннотация. *В статье проанализирован подход проекта нового методического документа Федеральной службы по техническому и экспортному контролю «Методика моделирования угроз безопасности информации» по распределению зон ответственности моделирования угроз безопасности информации между оператором информационной системы и поставщиком услуг центра обработки данных, на базе которого функционирует информационная система. Разработаны предложения по развитию данного подхода с учетом целевого характера угроз безопасности информации, модели обслуживания, осведомленности сторон о технологии обработки информации в информационной системе, используемым компонентам информационно-телекоммуникационной инфраструктуры, видов, категорий и потенциала нарушителей. Введено понятие сквозного сценария реализации угрозы.*

Abstract. *The article analyzes the approach of the draft new methodological document of the Federal Service for Technical and Export Control "Methodology for Modeling Information Security Threats" on the distribution of responsibility zones for modeling information security threats between the information system operator and the data center service provider, on the basis of which the information system operates. Suggestions have been developed for the development of this approach, taking into account the target nature of information security threats, the service model, the awareness of the parties about the information processing technology in the information system, the components of the information and telecommunication infrastructure, types, categories and potential of violators. The concept of an end-to-end threat implementation scenario is introduced.*

Ключевые слова*. Угроза безопасности информации, моделирование угроз, сценарий, сквозной сценарий, техника, цепочка событий, модель угроз, граница моделирования, зона ответственности, модель обслуживания, неопределенность, энтропия, центр обработки данных, облачная технология, поставщик услуг, оператор, нарушитель.*

Key words. *Information security threat, threat modeling, scenario, end-to-end scenario, technique, chain of events, threat model, modeling border, area of responsibility, service model, uncertainty, entropy, data center, cloud technology, service provider, operator, attacker.*

1. Введение

Современные информационные системы (ИС) подвержены большому числу угроз безопасности информации (БИ), реализация которых нарушителями путем воздействия на компоненты ИС может приводить к нарушению свойств безопасности обрабатываемых видов информации (ВИ), прерыванию предоставляемых информационных сервисов и в конечном счёте к негативным последствиям для поддерживаемых ИС бизнес-процессов в различных сферах деятельности, для экологии, жизни и здоровья граждан. Поэтому с целью разработки и принятия адекватных мер защиты информации (ЗИ) в ИС необходимо на систематической основе осуществлять моделирование угроз БИ.

Важная задача при моделировании угроз БИ – это выявление максимально возможного числа сценариев их реализации [1]. Указанная деятельность предполагает высокоинтеллектуальный труд, направленный на познание процессов в ИС, связанных с активностью внутренних и внешних нарушителей.

Усложняется эта деятельность тем, что в настоящее время, исходя из экономических и технологических факторов, многие ИС строятся на базе информационно-телекоммутационной инфраструктуры (ИТИ) центров обработки данных (ЦОД), реализующих облачные технологии (см. рис. 1).

При этом поставщик облачных услуг может предоставлять оператору ИС разные модели обслуживания, наиболее известными из которых являются следующие:

• программное обеспечение как услуга (software as a service, SaaS), в соответствии с которой операто-

Сидак Алексей Александрович *– кандидат технических наук, старший научный сотрудник, заместитель председателя, ООО «Центр безопасности информации», e-mail: sidak@cbi-info.ru;*
Василенко Владимир Васильевич *– доктор технических наук, профессор, заместитель председателя, ООО «Центр безопасности информации», e-mail: v.vasilenko@cbi-info.ru;*
Лыков Владимир Викторович *– директор департамента, ООО «Центр безопасности информации», e-mail: likov@cbi-info.ru.*

Sidak Aleksey *– candidate of technical science, senior researcher, deputy chairman, Information Security Center, e-mail: sidak@cbi-info.ru;*
Vasilenko Vladimir *– doctor of technical science, professor, deputy chairman, Information Security Center, e-mail: v.vasilenko@cbi-info.ru;*
Lykov Vladimir *– director of department, Information Security Center, e-mail: likov@cbi-info.ru.*

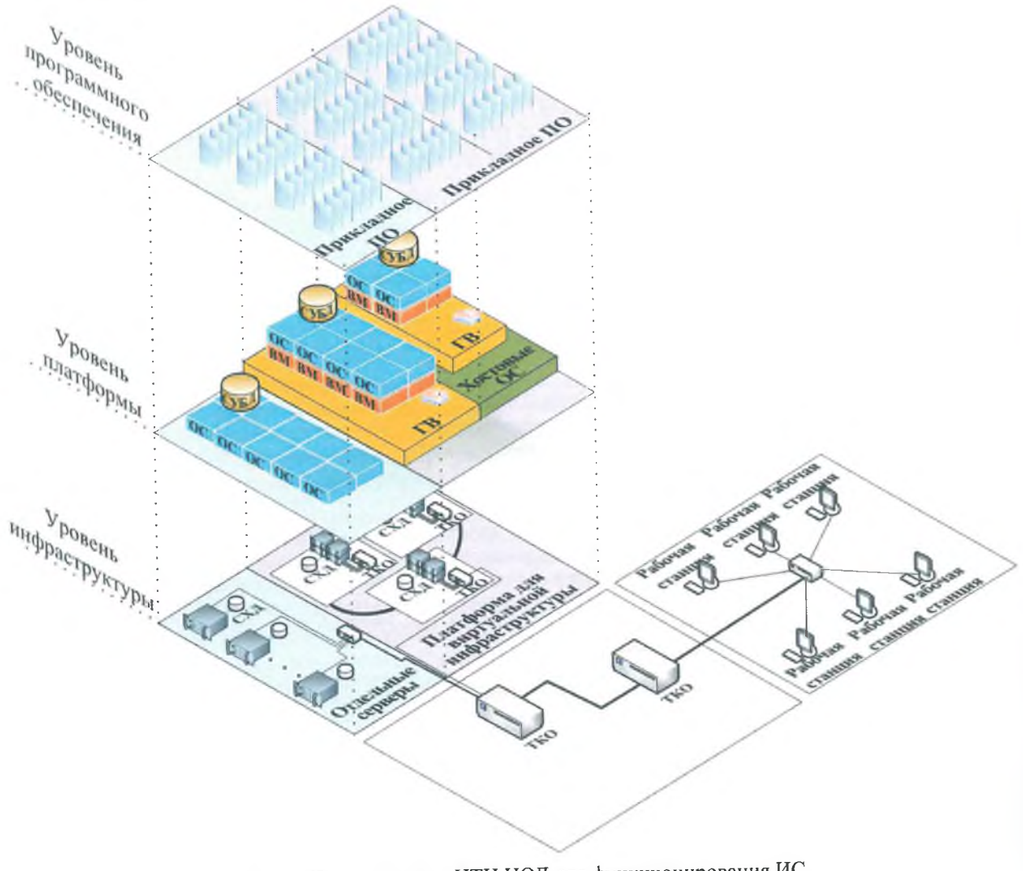

Рис. 1. Использование ИТИ ЦОД для функционирования ИС

ру ИС поставщиком услуг предоставляется возможность использования прикладного программного обеспечения (ПО) поставщика услуг (при этом контроль и управление компонентами ИТИ, включая предоставляемое оператору ИС прикладное ПО для использования его функциональных возможностей, осуществляет поставщик услуг);

• платформа как услуга (platform as a service, PaaS), в соответствии с которой оператору ИС поставщиком услуг предоставляется возможность использования ИТИ поставщика услуг для размещения прикладного ПО оператора ИС (при этом контроль и управление компонентами ИТИ, включая предоставляемые оператору гипервизоры (ГВ), операционные системы (ОС), системы управления базами данных (СУБД) для использования их функциональных возможностей, осуществляет поставщик услуг);

• инфраструктура как услуга (infrastructure as a service, IaaS), в соответствии с которой оператору ИС поставщиком услуг предоставляется возможность использования ИТИ поставщика услуг для размещения системного и прикладного ПО оператора (при этом контроль и управление физическими компонентами ИТИ, включая предоставляемые оператору сети, серверы и системы хранения данных (СХД) для использования их функциональных возможностей, осуществляет поставщик услуг).

Исходя из этого, при моделировании угроз БИ для ИС и, в частности, для выявления максимально возможного числа сценариев их реализации необходимо решить следующие задачи:

• определить общую границу моделирования;

• распределить зоны ответственности по моделированию угроз БИ между оператором ИС и поставщиком услуг.

Первая задача в соответствии с проектом документа ФСТЭК России «Методика моделирования угроз безопасности информации» [1] решается путем включения в границу моделирования как информационных ресурсов (ИР) и компонентов ИС оператора, так и используемых компонентов ИТИ ЦОД поставщика услуг (см. рис. 2).

Распределение зон ответственности по моделированию угроз БИ между оператором ИС и поставщиком услуг – это более сложная задача.

Её решение затруднено вследствие имеющегося противоречия между тем, что поставщик услуг изначально моделирует угрозы БИ для ЦОД без знания технологического процесса обработки информации в ИС оператора, значимости свойств безопасности обрабатываемых в ИС ВИ и данных, целей, видов, категорий и потенциала нарушителей по отношению к активам ИС оператора, возможных негативных последствий от реализации угроз БИ для автоматизируемых бизнес-процессов, с одной стороны, и недостаточностью результатов моделирования угроз БИ поставщиком услуг для их использования оператором ИС при построении сквозных сценариев реализации угроз БИ (в виде последовательности техник) по отношению к активам ИС, с другой стороны.

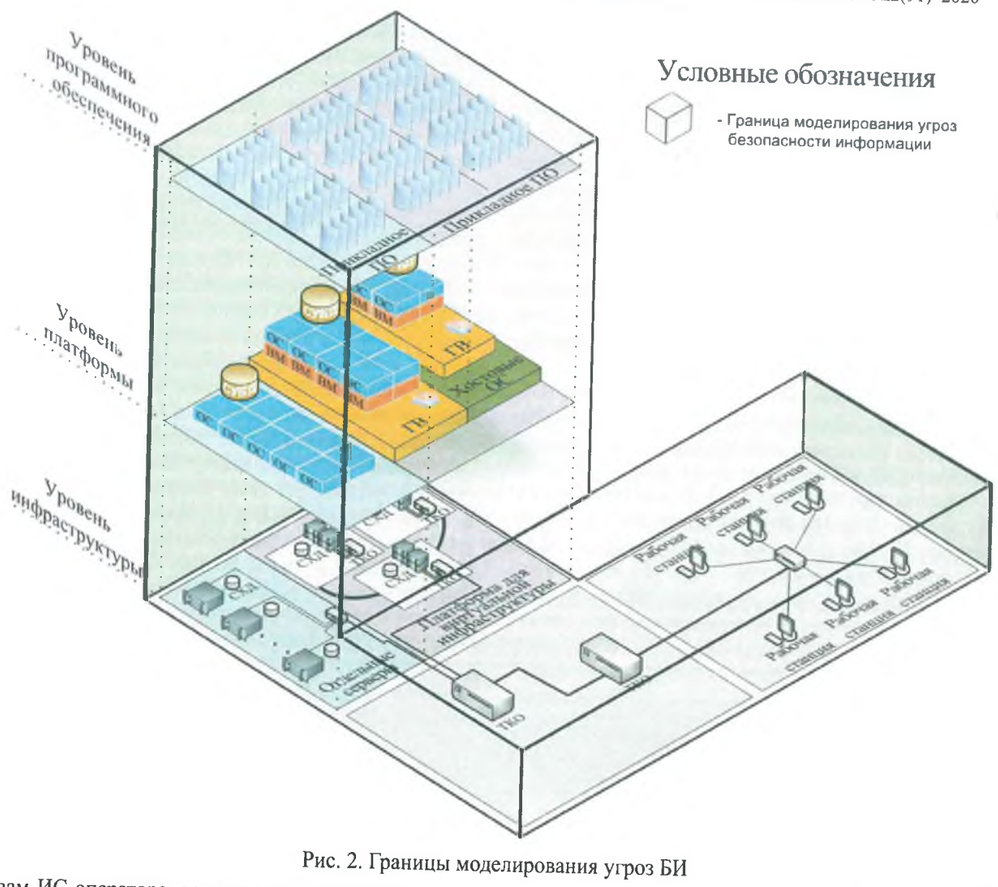

Рис. 2. Границы моделирования угроз БИ

Первое порождает неопределенность для поставщика услуг относительно того фрагмента сценария реализации угрозы ИБ, который относится к ИТИ, контролируемой поставщиком услуг. Таким образом, вследствие отсутствия понимания целевого характера угрозы БИ (поставщик услуг изначально на это не ориентирован), описание фрагмента сценария поставщиком услуг будет обладать большой энтропией, определяемой выражением

$$H_1=\log\Omega_1, \quad (1)$$

где Ω_1 – число сочетаний тактик в описании фрагмента сценария поставщиком услуг (связанных только с компонентами ИТИ ЦОД), приводящих к выводу поставщика услуг об адекватности описания фрагмента сценария.

Второе также порождает неопределенность относительно фрагмента сценария, относящегося к ИТИ, контролируемой поставщиком услуг, но уже для оператора ИС. Таким образом, выбор оператором ИС конкретного сценария из модели угроз ЦОД в качестве фрагмента сквозного сценария реализации угрозы БИ по отношению к активам ИС также будет обладать большой энтропией, определяемой выражением

$$H_2=\log\Omega_2, \quad (2)$$

где Ω_2 – число сочетаний вариантов решений, приводящих к выводу оператора ИС об адекватности выбора конкретного сценария из модели угроз ЦОД в качестве фрагмента сквозного сценария реализации угрозы БИ по отношению к активам ИС.

Снижение неопределенности в выражениях (1), (2) представляет собой актуальную научно-практическую задачу, решение которой необходимо для выявления сквозных сценариев реализации угроз БИ по отношению к активам ИС.

Решение этой задачи может быть основано на гипотезе, что разработать адекватные описания сквозных сценариев реализации угроз БИ можно за счет учета целевого характера угроз БИ, распределения зон ответственности моделирования угроз, исходя из контролируемых сторонами ИТИ, и двунаправленной обратной связи между оператором ИС и поставщиком услуг.

В качестве изучаемых и контролируемых переменных в процессе исследования целесообразно рассматривать:

• взаимосвязанные (в рамках сценариев) последо-

вательности техник реализации угроз БИ (конкретные техники могут браться из проекта методического документа ФСТЭК России [1] и из иных целевых ресурсов, например, https://bdu.fstec.ru, https://attack.mitre.org);

• цепочки событий безопасности [2] (с использованием ГОСТ Р «Защита информации. Регистрация событий безопасности. Требования к регистрируемой информации»), отражающих реализацию ключевых элементов (тактик) сценариев и регистрируемых компонентами ИТИ и средствами ЗИ ЦОД и ИС.

Ожидается, что предложенные в настоящей работе подходы, отражающие результаты проведенных исследований, минимизируют расхождение между значениями указанных переменных. Тем самым это будет свидетельствовать о снижении неопределенностей, определяемых выражениями (1), (2), и адекватности смоделированных сценариев действительным попыткам реализации угроз БИ по отношению к активам ИС.

2. Целевой характер угроз

Исходя из целевого характера можно выделить две группы угроз БИ (см. рис. 3):

• угрозы, направленные на активы ИС, которые могут приводить к негативным последствиям для поддерживаемых бизнес-процессов, экологии, жизни и здоровья людей (группа 1);

• угрозы, которые направлены на средства ЗИ, используемые для нейтрализации угроз первой группы (группа 2).

Проект документа ФСТЭК России «Методика моделирования угроз безопасности информации» [1] (подготовлен при участии экспертов Центра безопасности информации и других ведущих российских организаций в области информационной безопасности), в первую очередь, распространяется на угрозы первой группы. В целях противостояния угрозам БИ данной группы в ИС реализуются меры ЗИ [3], включающие организационные меры защиты информации и применение технических средств ЗИ (межсетевых экранов, средств антивирусной защиты, средств контроля съемных носителей информации и др.). Соответственно средства ЗИ сами становятся объектом реализации угроз БИ (группа 2), направленных на снижение эффективности применения средств ЗИ в ИС (обход, преодоление, отключение). Для противостояния данным угрозам реализуются механизмы ЗИ в составе самих средств ЗИ, а также в среде их функционирования. В настоящее время соответствующие функциональные требования безопасности регламентируются в специальных нормативных-правовых актах ФСТЭК России, профилях защиты на основе линейки стандартов ГОСТ Р ИСО/МЭК 15408 и иных документах.

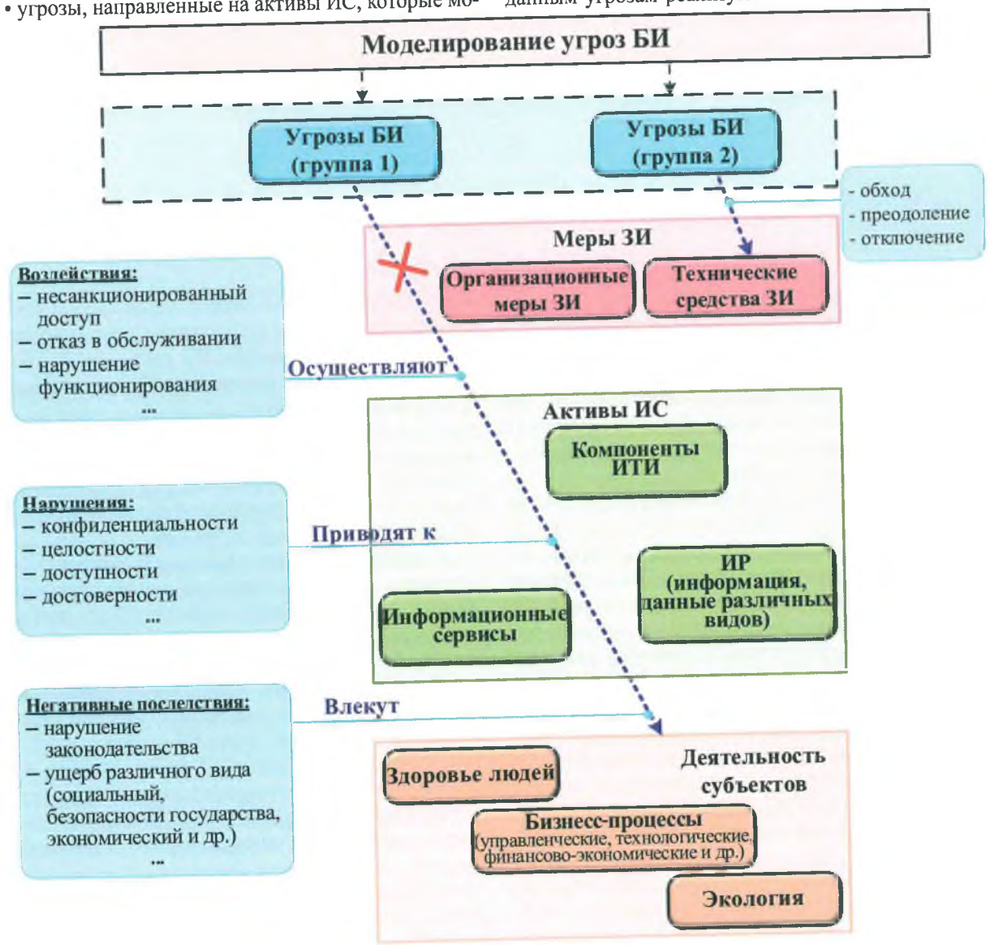

Рис. 3. Группы угроз БИ с учетом их целей

3. Распределение зон ответственности моделирования угроз БИ

В соответствии с гипотезой зоны ответственности моделирования угроз БИ предлагается определить в рамках контролируемых компонентов ИТИ оператора ИС и поставщика услуг соответственно.

При этом аренда части компонентов ИТИ ЦОД оператором ИС не исключает продолжение их контроля функционирования со стороны поставщика услуг. В то же время при предоставлении (в том числе, возможно, в форме договора аренды) оператору ИС программного обеспечения поставщиком услуг (например, в виде дистрибутива) для самостоятельной установки, настройки и технической поддержки, такое программное обеспечение может включаться в границу моделирования угроз БИ оператора ИС (зону ответственности оператора). Такая ситуация, например, может иметь место в случае модели обслуживания IaaS (см. рис. 4).

В случаях, когда предоставляемое для использования оператором ПО устанавливается и поддерживается поставщиком услуг, такое программное обеспечение целесообразно включать в границу моделирования угроз БИ поставщиком услуг (зону ответственности поставщика услуг). Такая ситуация, например, может иметь место в случае модели обслуживания SaaS (см. рис. 5).

При этом в зону ответственности оператора может быть включено ПО, которое генерируется, устанавливается и (или) настраивается оператором на базе ПО, предоставленного поставщиком услуг. Например, если поставщиком услуг предоставлены оператору функциональные возможности функционирующего ПО системы управления виртуализацией, то создаваемые оператором (в интересах своих систем и сетей) на его основе виртуальные машины (ВМ), виртуальные серверы и виртуальные каналы связи целесообразно включать в зону ответственности оператора ИС.

Другой пример (см. рис. 6) – если поставщиком услуг предоставлена оператору сгенерированная ВМ, то в этом случае ВМ (в отличие от предыдущего примера) включается в зону ответственности поставщика услуг, а ПО, устанавливаемое в неё и настраиваемое оператором – в зону ответственности оператора ИС.

Конкретное распределение зон ответственности может являться предметом соглашения между оператором ИС и поставщиком услуг; при этом должна быть обеспечена полнота охвата общих границ моделирования угроз БИ.

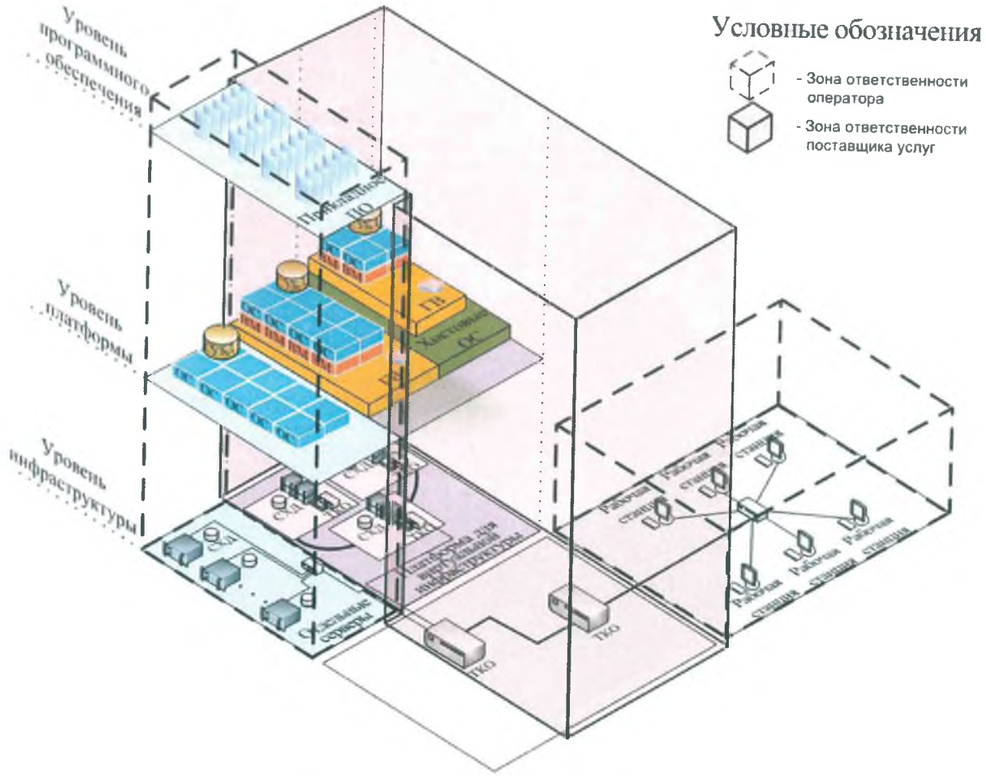

Рис. 4. Пример распределения зон ответственности (IaaS – предоставление серверов)

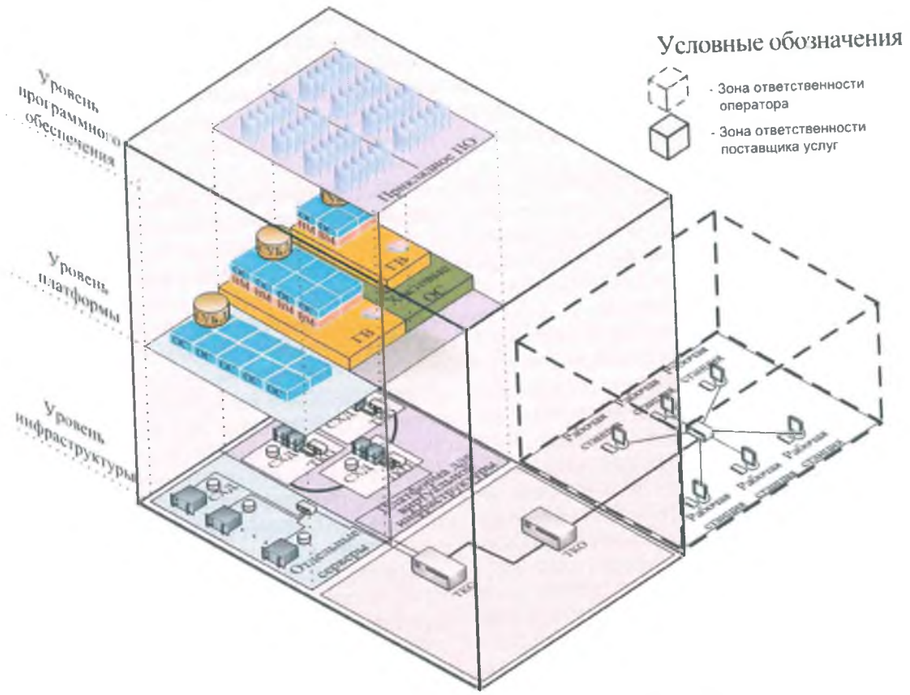

Рис. 5. Пример распределения зон ответственности (SaaS – предоставление ПО)

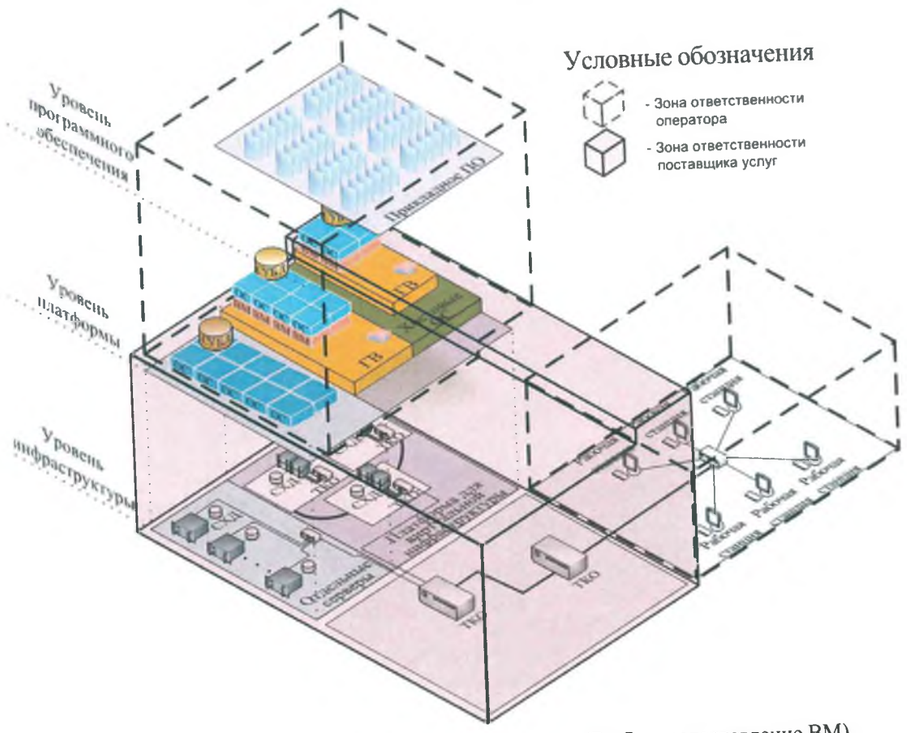

Рис. 6. Пример распределения зон ответственности (PaaS – предоставление ВМ)

4. Обратная связь при моделировании угроз БИ

В соответствии с проектом документа ФСТЭК России «Методика моделирования угроз безопасности информации» [1] предполагается, что поставщик услуг ЦОД передает оператору ИС результаты моделирования угроз БИ. Но без знания целей угроз БИ по отношению к активам ИС оператора, это в основном будет описание угроз БИ второй группы – для средств ЗИ и компонентов ИТИ ЦОД.

Результаты апробации показывают, что этого недостаточно, чтобы оператор ИС мог построить адекватные сквозные сценарии реализации угроз БИ. В дополнение к подходу проекта документа ФСТЭК России [1] необходима обратная связь от оператора ИС к поставщику услуг, чтобы поставщик услуг мог конкретизировать те фрагменты общего сквозного сценария, которые затрагивают контролируемые им компоненты ИТИ ЦОД, с учетом целей угроз БИ.

Кроме того, повышение эффективности моделирования угроз БИ можно достичь применением метода подобия, разработанного и изложенного в работах [4, 5], для учета ранее полученных результатов моделирования угроз БИ для иных ИС, в том числе функционирующих на базе ИТИ ЦОД поставщика услуг. Достоверность результатов моделирования к этому моменту уже может быть подтверждена путем верификации сценариев реализации угроз БИ (действительные / ложные) методом, разработанным и изложенным в работе [2] с использованием инструментальных средств мониторинга типа NeuroDAT.

5. Заключение

Проведенные научные исследования, результаты которых изложены в настоящей статье, были направлены на совершенствование методического обеспечения выявления максимально возможного числа сценариев реализации существующих угроз БИ как важнейшей задачи при моделировании угроз БИ для ИС.

Результаты проведенных исследований показали справедливость исходной гипотезы решения проблемы неопределенности при выявлении сценариев реализации угроз БИ.

По результатам апробации проекта «Методики моделирования угроз безопасности информации» разработаны следующие рекомендации по ее уточнению и развитию:

- распределение зон ответственности моделирования угроз, исходя из контролируемых сторонами компонентов ИТИ ЦОД и сегмента ИС оператора;
- реализация двунаправленной обратной связи между оператором ИС и поставщиком услуг для разработки адекватных сквозных сценариев реализации угроз БИ по отношению к активам ИС;
- применение метода подобия для использования результатов моделирования угроз БИ для иных (подобных) ИС;
- использование цепочек событий безопасности (на основе ГОСТ Р «Защита информации. Регистрация событий безопасности. Требования к регистрируемой информации») для верификации и контроля осуществления сценариев реализации угроз БИ средствами мониторинга типа NeuroDAT.

Указанные рекомендации могут найти отражение как в окончательной редакции самой методики, так и в отраслевых (ведомственных, корпоративных) методиках моделирования угроз БИ, а также непосредственно при моделировании угроз БИ для конкретных ИС.

В качестве перспективных направлений дальнейших экспериментальных исследований можно определить следующие:

- связывание контролируемых событий безопасности с тактиками реализации угроз БИ;
- развитие математического и методического обеспечения представления сценария реализации угрозы БИ в виде совокупности техник (в целях моделирования угроз БИ), а также в виде цепочки событий безопасности (с целью верификации средствами типа NeuroDAT при функционировании ИС и последующего уточнения модели угроз БИ).

Литература

1. Методический документ ФСТЭК России «Методика моделирования угроз безопасности информации» (проект)// ФСТЭК России: [сайт]. URL: https://fstec.ru/component/attachments/download/2727 (дата обращения: 15.04.2020).

2. Сидак А.А. Решение проблем эквифинальности автоматизированных систем при сценарном подходе моделирования угроз безопасности информации // Двойные технологии. – 2020. – № 1. – С. 89–94.

3. Методический документ. Меры защиты информации в государственных информационных системах, ФСТЭК России, 2014 (утв. ФСТЭК России 11.02.2014) // СПС КонсультантПлюс.

4. Сидак А.А. Обоснование требований по защите информации в автоматизированных системах // Стратегическая стабильность. – № 4. – 2009. – С. 7–9.

5. Сидак А.А. Применение метода подобия при моделировании угроз безопасности информации в автоматизированных системах // Стратегическая стабильность. – 2019. – № 4. – С. 17-20.

Материал поступил в редакцию 14.05.2020 г.