ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ МОДЕЛИРОВАНИЯ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Большаков А.С., Раковский Д.И.*

Ключевые слова: *информационная система (инфосистема), программное обеспечение, информационная безопасность, угрозы, уязвимости, банк данных, модель угроз, базовая модель угроз.*

Аннотация.

Цель работы: *совершенствование научно-методической базы оценки защищенности информационных систем (инфосистем).*

Метод исследования: *моделирование угроз безопасности аппаратно-программных технологий на основе нормативной федеральной методики для определения угроз безопасности информации в инфосистемах. При анализе вероятности и возможности появления угроз применялись соответствующие нормативной федеральной методике статистические и экспертные оценки характеристик угроз. Оценка адекватности построенных моделей угроз производилась с использованием меры сходства выборок различного объема.*

Результаты: *разработано программное обеспечение (ПО) для моделирования угроз безопасности информации в инфосистемах различного назначения с учетом аппаратно-программных технологий федерального банка данных. Функционал разработанного ПО позволяет группировать и ранжировать угрозы федерального банка данных по объектам их воздействия на информационные ресурсы инфосистем, что имеет практическую ценность с точки зрения выработки мер по обеспечению информационной безопасности. Анализ адекватности моделирования угроз с применением разработанного ПО показал хорошее значение меры сходства моделируемых и экспертных видов угроз. Моделирование угроз с помощью ПО выявило, что набор актуальных угроз в основном зависит от степени защищенности инфосистем и параметров модели нарушителя. ПО используется для изучения мер нейтрализации угроз в лабораторном практикуме учебного процесса.*

DOI: 10.21681/1994-1404-2020-1-26-39

Введение

В условиях построения электронных структур информационного общества («электронного» и «цифрового» государства, «электронного» правительства, «электронного» правосудия и др.) актуальность противодействия угрозам безопасности информации в государственных информационных системах (инфосистемах) значительно возросла, в том числе в инфосистемах правовой сферы [4]. Нормативное правовое регулирование отношений в области обеспечения информационной безопасности осуществляет Федеральная служба по техническому и экспортному контролю (ФСТЭК) России, издающая методические материалы для унификации соответствующих мер и мероприятий.

В частности, создание базовой модели угроз при разработке политики безопасности инфосистем персональных данных является обязательным условием с момента утверждения в 2019 г. перечня[1] нормативных правовых актов ФСТЭК. Обязательным является также использование *банка данных* ФСТЭК при построении модели угроз государственных инфосистем. Для построения модели специалисту информационной безопасности необходимо ознакомится с перечнем актуальных нормативных актов и документов ФСТЭК, банками данных угроз и уязвимостей последней версии.

Любая инфосистема включает в себя средства обработки, передачи и хранения информации, а также поддерживающую инфраструктуру, выполненную в виде аппаратно-программного комплекса [5, 6]. Инфосистема может

[1] *См.:* Приказ ФСТЭК России от 16 июля 2019 г. № 135 «Перечень нормативных правовых актов или их отдельных частей, оценка соблюдения которых является предметом государственного контроля (надзора) в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

* ***Большаков Александр Сергеевич,*** *кандидат технических наук, доцент Московского технического университета связи и информатики, Российская Федерация, г. Москва.*

E-mail: alexbol57@mail.ru

Раковский Дмитрий Игоревич, *студент Московского технического университета связи и информатики, Российская Федерация, г. Москва.*

E-mail: dimitor1998@mail.ru

Таблица 1

Сравнение действующего программного обеспечения[5]

Наименование ПО	Поддержка разработчиком ПО	Соответствие стандартам ФСТЭК	Моделирование с учетом:		Универсальность ПО
			угроз	уязвимостей	
AdTool	Да	Нет	Нет	Нет	Да
Trike	Да	Нет	Да	Нет	Да
MS Threat Modeling Tool 2016	Да	Нет	Да	Да	Да
Cisco ThreatBuilder	Да	Нет	Да	Да	Нет
Threat-model.com	Нет	Да	Да	Нет	Да
R-Vision Risk Manager	Да	Да	Да	Да	Нет

иметь сложную физическую и логическую топологию, функционировать на нескольких уровнях известной сетевой модели *OSI/ISO*. Для построения модели угроз специалисту необходимо изучить и проанализировать (помимо технических особенностей инфосистем) штат сотрудников, обслуживающих работу инфосистем, на предмет выявления возможного внешнего и внутреннего нарушителя, а также наработки предыдущих специалистов информационной безопасности, работавших с анализируемой инфосистемой: существующую модель угроз, модель управления рисками и использованную при оценке рисков технологию [10, 11].

Авторами были изучены имеющиеся по данной тематике публикации [4, 7, 14] и проанализирован рынок программного обеспечения (ПО) на предмет способности решения следующих профильных задач:

- иметь постоянную поддержку разработчика, своевременно обновлять банки данных своего программного обеспечения (ПО), отслеживая изменения банка данных ФСТЭК;
- использовать методики моделирования угроз, закрепленные в нормативных документах ФСТЭК[2];
- учитывать при моделировании угрозы и уязвимости, способные приводить к нарушению информационной безопасности;
- быть универсальным, т. е. иметь возможность анализировать инфосистемы любого типа (локальные вычислительные сети, распределенные системы, АСУ ТП и пр.), любой топологии и на любом этапе оценки информационной безопасности (от проектирования до эксплуатации).

Обзор опций действующего ПО приведен в табл. 1. Как видно из таблицы, на период проведения исследования не зафиксировано ни одного продукта, полностью соответствующего всем требованиям, выдвинутым авторами. Максимально близко к заявленным требованиям подходит ПО «*Платформа R-Vision Incident Response Platform*»[3], *"Threat-model.com"*[4].

[2] *См., например:* Методика определения угроз безопасности информации в информационных системах: Методический документ. М.: ФСТЭК России, 2015. 43 с.

[3] *R-Vision Incident Response Platform. URL: https://rvision.pro* (дата обращения: 30.07.2019).

[4] *URL: http://www.threat-model.com* (дата обращения: 30.07.2019).

Постановка задачи

Если исследуемая инфосистема является сложной, как по своей топологии, так и по динамике изменения (находится в постоянном развитии), а предыдущая модель угроз либо не создана, либо перестала быть актуальной в связи с устареванием используемых банков данных или нормативных документов, то создание новой модели угроз или актуализация старой представляют собой трудоемкую задачу.

Встает вопрос автоматизации данного процесса. Исходя из табл. 1, все исследованные продукты, представленные на рынке, имеют один или несколько недостатков. Перед авторами стоит задача разработки ПО, способного соответствовать всем пунктам табл. 1.

Требуется создать ПО, автоматизирующее построение базовой модели угроз, а также модели угроз, учитывающей используемую аппаратно-техническую базу инфосистемы. Создаваемое ПО должно упрощать построение модели угроз, оказывать практическую помощь специалистам информационной безопасности при формировании модели угроз и принятии адекватных защитных мер.

Разрабатываемое ПО должно быть «дружелюбным» к пользователю, изучающему затронутые аспекты информационной безопасности (в частности, планируется внедрение данного ПО в лабораторный практикум). По замыслу авторов, разрабатываемое ПО должно сопровождать изучение угроз, приводящих к нарушению информационной безопасности инфосистем заданного типа с применением различных информационных технологий, содержащихся в банке данных ФСТЭК[5].

В результате моделирования должны выявляться актуальные угрозы и уязвимости, присущие конкретной инфосистемы. Актуальные угрозы должны выявляться не только в узлах инфосистемы, но и в каналах связи между этими узлами (с учетом среды передачи данных) в целях учета технических каналов утечки информации, присущих исследуемой инфосистеме [1].

Исходные данные, поступающие на вход ПО, представляют собой:

[5] Банк данных угроз ФСТЭК. URL: https://bdu.fstec.ru .

*Таблица **2***

Описание параметров угроз, представленных в банке данных угроз

Параметр	Пояснение параметра
Идентификатор УБИ	Порядковый номер в банке данных угроз от 1 до N, где N — количество угроз в банке данных
Наименование УБИ	
Описание	
Источник угрозы	В качестве источника угрозы приводятся нарушители и их потенциал
Объект воздействия	Объект или объекты, на которые может воздействовать угроза: средства передачи, хранения и обработки информации, а также поддерживающая инфраструктура
Нарушение конфиденциальности	Может принимать значение «1» (нарушается) или «0» (не нарушается).
Нарушение целостности	Может принимать значение «1» (нарушается) или «0» (не нарушается).
Нарушение доступности	Может принимать значение «1» (нарушается) или «0» (не нарушается).
Дата включения угрозы в БД	
Дата последнего изменения данных в БД	

- банк данных угроз в формате excel-таблицы — при разработке использовался банк данных угроз по состоянию на апрель 2019 г.;
- банк данных уязвимостей в формате excel-таблицы — при разработке использовался банк данных угроз по состоянию на апрель 2019 г.
- результаты пользовательского взаимодействия с интерфейсом программы на основе уже существующих базовых моделей угроз [3].

Каждая угроза безопасности информации (УБИ), содержащаяся в банке данных (БД) угроз, обладает определенными параметрами (табл. 2).

Каждая уязвимость, содержащаяся в банке данных уязвимостей, также обладает определенными параметрами (табл. 3).

*Таблица **3***

Описание параметров уязвимостей, представленных в банке данных уязвимостей

Параметр	Пояснение параметра
Идентификатор	Порядковый номер уязвимости в банке данных, в котором содержится информация о годе включения уязвимости и ее порядковом номере.
Наименование уязвимости	
Описание	
Вендор ПО	
Название ПО	
Версия ПО	
Тип ПО	В данной категории содержится категория ПО в первом приближении: СУБД, операционная система (ОС), прикладное ПО и др.
Наименование ОС и тип аппаратной платформы	Перечислены все ОС, которые поддерживают данное ПО
Класс уязвимости	В банке данных представлено 3 класса: • уязвимость кода; • уязвимость архитектуры; • уязвимость многофакторная
Дата выявления	
CVSS 2.0	Приведен базовый вектор уязвимости
CVSS 3.0	
Уровень опасности уязвимости	Приведена численная оценка CVSS.2.0, CVSS.3.0
Статус уязвимости	Статус уязвимости может быть либо подтвержденной производителем, либо носить потенциальный характер
Наличие эксплойта	Эксплойт либо имеется, либо еще не обнаружен

Параметр	Пояснение параметра
Информация об устранении	Уязвимость может быть либо устранена, либо нет
Ссылки на источники	Источники, подтверждающие наличие уязвимости
Идентификаторы других систем описания уязвимости	Идентификаторы в других системах идентификации уязвимостей
Прочая информация	Информация, которую невозможно отнести к той или иной категории данных. Чаще всего в данном поле приводится язык разработки ПО
Описание ошибки CWE	
Тип ошибки CWE	

Особенности разработанного программного обеспечения

Предлагаемое ПО разработано с использованием языка *C#* с использованием сторонней библиотеки *ClosedXML*[6] для работы с *excel*-таблицами банка данных ФСТЭК. При разработке моделирования инфосистемы применялись теоретические материалы дисциплины «сетевые технологии»[7], а также публикации, в которых были рассмотрены угрозы и уязвимости, присущие определенному каналу связи [17] или архитектуре сети [2, 4, 9, 12].

В связи с требованиями, изложенными в табл.1, большой зависимостью алгоритмов работы программы от нормативных документов и целесообразностью создания удобного пользовательского интерфейса, было принято разделить программу на две группы: группа пользовательских данных и группа данных ФСТЭК.

С целью удобного интегрирования динамически изменяющихся банков данных ФСТЭК был создан специальный редактор — «Информация, полученная от ФСТЭК». Хранение данных банка ФСТЭК реализуется с использованием собственных систем хранения данных: угрозы; уязвимости; нарушители; аппаратное/программное обеспечение; топологии инфосистемы.

Нормативная методика ФСТЭК «вшита» в исходный код программы, и за ее актуализацию ответственны авторы.

Ввод ролевого подхода управления программой позволяет разработчику и пользователю ПО в случае необходимости и целесообразности актуализировать входные данные, своевременно обновляя банки данных и используемую в программном обеспечении методику.

Ролевой подход приведен на диаграмме вариантов использования (рис. 1), созданной с применением правил унифицированного языка моделирования *UML* (для иллюстрации последующих процессов все диаграммы будут оформлены по правилам *UML*).

Процесс взаимодействия пользователя с ПО представлен на диаграмме последовательности создания модели угроз (рис. 2). На диаграмме отражены основные этапы работы пользователя с ПО на всех шагах моделирования, начиная с загрузки программного обеспечения и заканчивая моментом получения результатов.

Ввод данных осуществляется пользователем с помощью нескольких меню: «Задание топологии инфосистемы», «Выбор технических средств защиты (ТСЗ)», «Редактирование модели нарушителя», «Актуализация угроз». Данные процессы отражены на вышеприведенной диаграмме последовательности (см. рис. 2). Банк данных ФСТЭК на диаграмме разделен на два отдельных объекта: банк данных угроз и банк данных уязвимостей (на рис. 2 банк данных уязвимостей не изображен, в целях экономии места).

Процесс задания топологии рассмотрен на диаграмме последовательности задания топологии (рис. 3). На данном этапе пользователем формируется модель уязвимостей, а также задается ПО узлов топологии.

В процессе задания топологии инфосистемы пользователь выбирает с помощью графического интерфейса тип применяемого узлом инфосистемы программного/аппаратного обеспечения, который, в свою очередь, соотнесен с определенным набором уязвимостей банка уязвимостей ФСТЭК.

На любом этапе моделирования инфосистемы пользователю доступен справочный материал, синтезированный на основе информации из банков данных ФСТЭК.

Реализованы: поиск и сортировка угроз и уязвимостей; вывод уязвимостей, присущих определенному вендору или ПО. Вследствие чего пользователь имеет возможность по своему усмотрению исследовать угрозы, анализируя их происхождение, связности с соответствующими уязвимостями; на основе анализа принимать адекватные меры по их нейтрализации. Используется способ группирования угроз, отличный от примененного в банке данных и основанный на разделении угроз по ресурсам инфосистемы: грид-система, физические компоненты системы, аппаратное обеспечение, реестр и др.

Практическая ценность предложенной классификации заключается в том, что при наличии нескольких критических узлов инфосистемы (двух и более контролируемых зон, наличие периметров инфосистемы, нескольких серверов разной архитектуры) пользователь сможет визуально наблюдать перечень угроз, нацеленных на каждый кон-

[6] *ClosedXML. URL: https://github.com/ClosedXML/ClosedXML .*

[7] Руденков Н. А., Долинер Л. И. Основы сетевых технологий : учебник для вузов. Екатеринбург : Изд-во Уральского Федерального ун-та, 2011. 300 с.

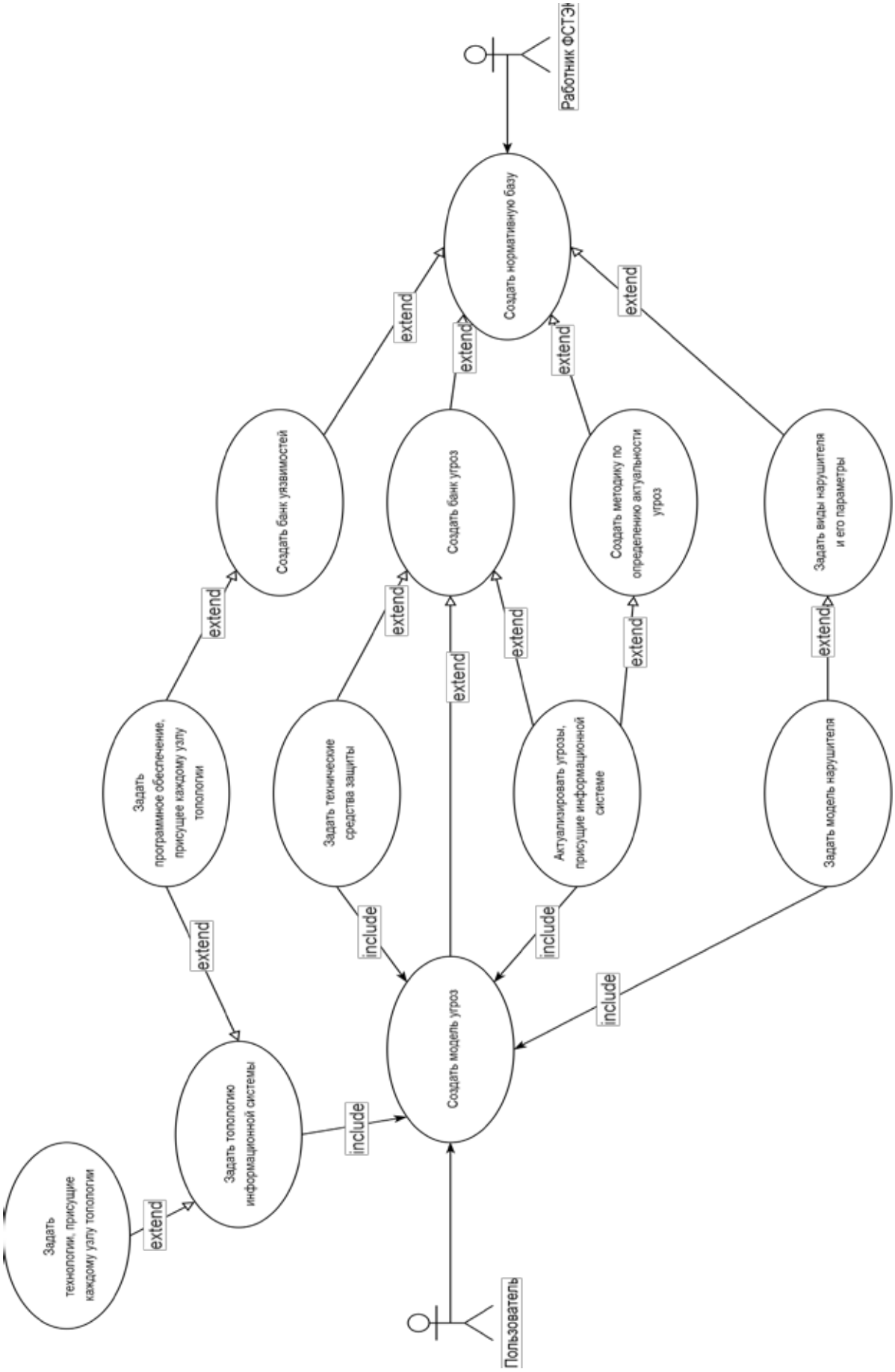

Рис. 1. Диаграмма вариантов использования программного обеспечения

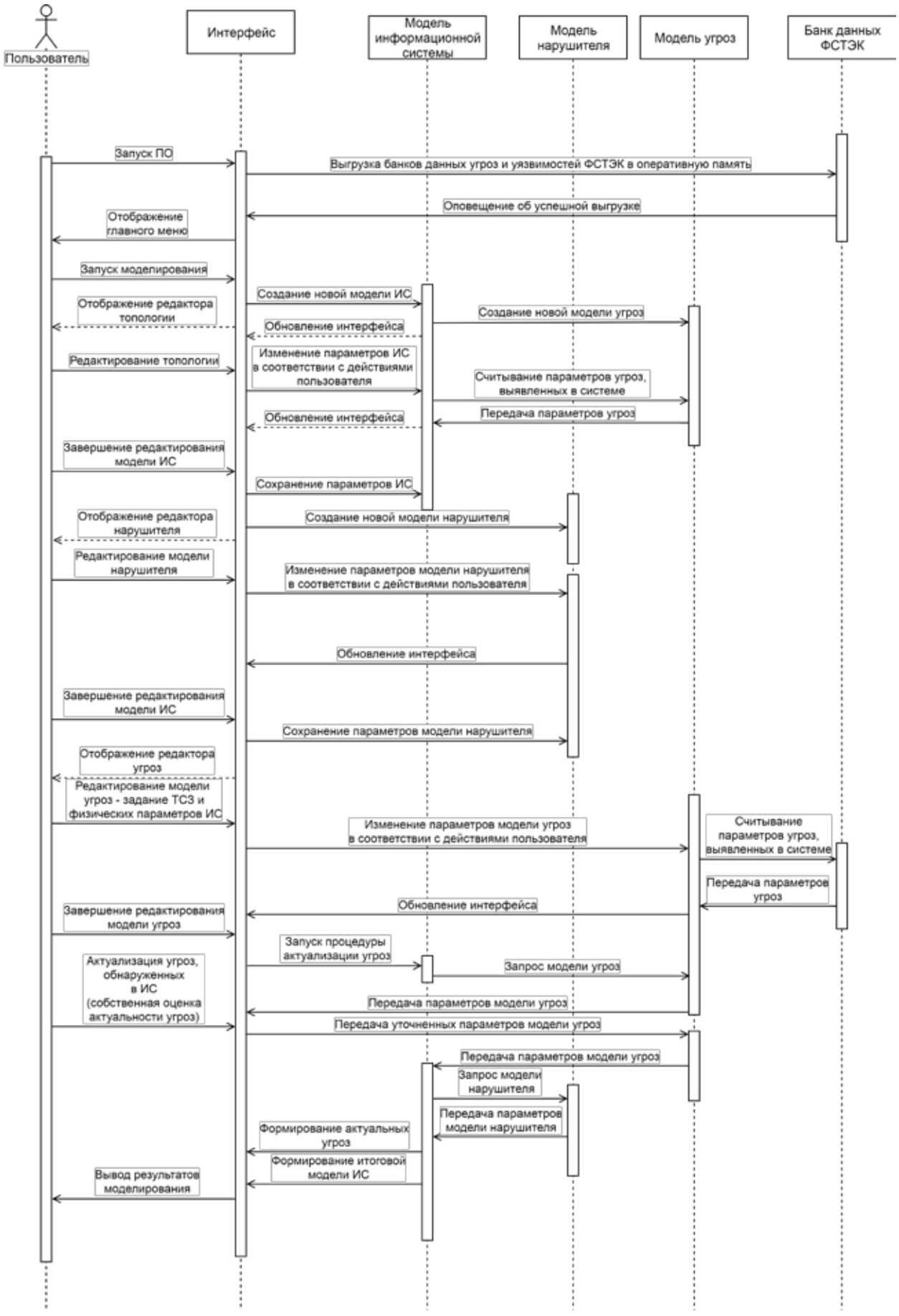

Рис. 2. Диаграмма последовательности создания модели угроз

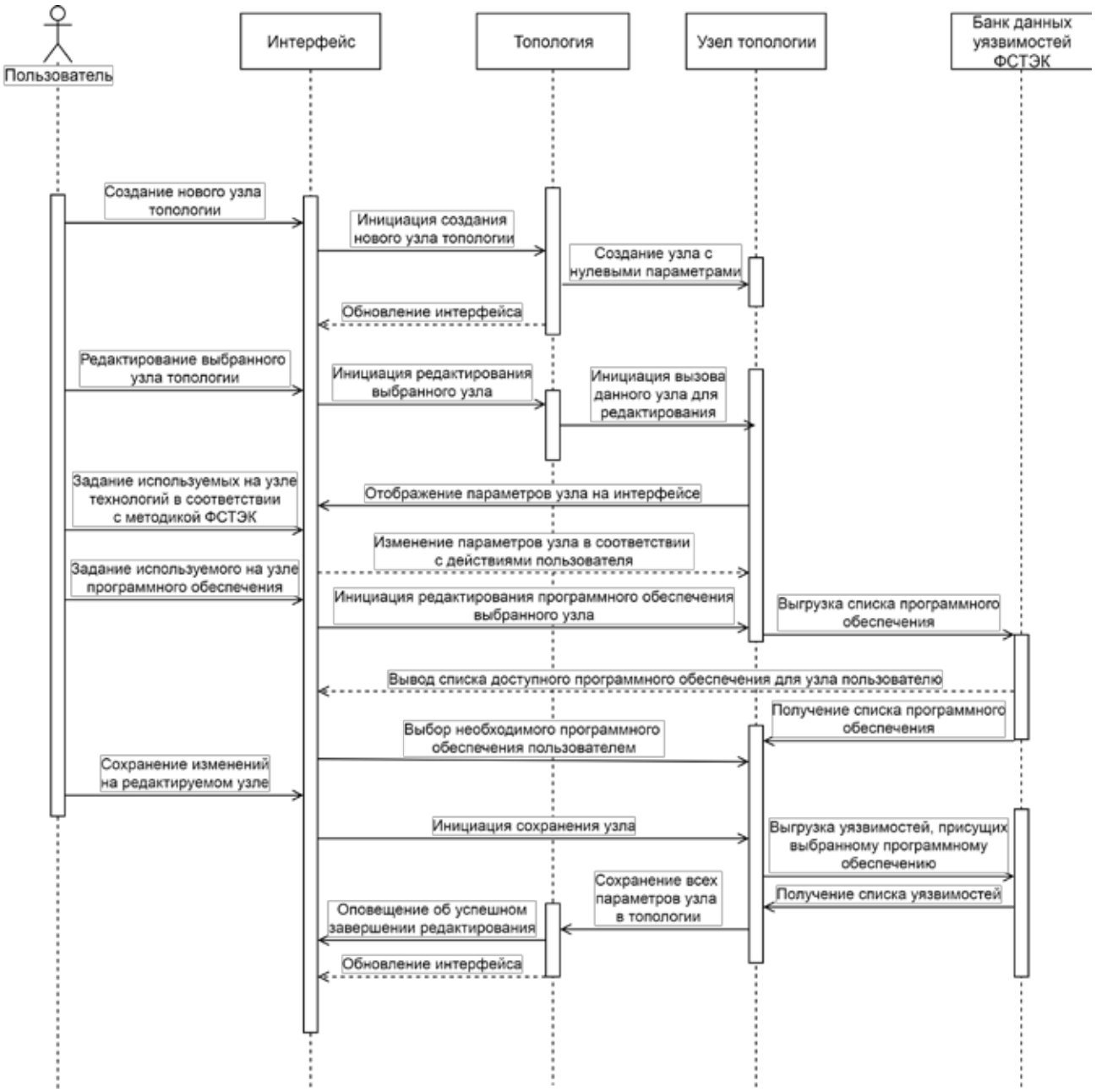

Рис. 3. Диаграмма последовательности задания топологии инфосистемы

кретный узел инфосистемы. Перечень ранжированных угроз «привязан» к ресурсам узла, на которые могут быть направлены смоделированные угрозы, что может помочь в выборе адекватных мер по их нейтрализации.

Реализация каждой угрозы зависит от конфигурации модели нарушителя, его потенциала, мотивации — параметры нарушителя в предложенном программном обеспечении обусловлены методикой ФСТЭК.

Таким образом, пользователь поэтапно формирует исходные данные для моделирования угроз. Заканчивая настройку модели, пользователь получает неактуализированную модель угроз, в которой:

- учитывается тип возможного нарушителя, его навыки, мотивации и потенциал;
- выявляются угрозы, направленные на каждый конкретный элемент системы, с учетом характеристик нарушителя;
- ранжируются уязвимости в каждом элементе рассматриваемой инфосистемы в зависимости от версии программного обеспечения и типа аппаратной реализации.

Анализ введенных параметров и характеристик исследуемой инфосистемы выполняется на последнем этапе моделирования системы: на этапе актуализации обнаруженных угроз.

Актуальность угроз безопасности ($УБИ_j^A$) для действующей и проектируемой инфосистемы определяет-

ся в разработанном программном обеспечении согласно следующему алгоритму ФСТЭК:

1. В качестве показателя актуальности угрозы безопасности информации принят следующий двухкомпонентный вектор:

$УБИ_j^A$ = [вероятность реализации угрозы (P_j); степень ущерба (X_j)],

где значение P_j, вводимое пользователем при актуализации угрозы, должно быть получено от экспертов после анализа статистических данных о частоте реализации угроз безопасности информации в действующей инфосистемы и степени соответствующего ущерба X_j.

2. При отсутствии вышеуказанной статистики актуальность угрозы безопасности информации на основе оценки возможности реализации угрозы безопасности информации (Y_j) в проектируемой инфосистемы определяется по формуле:

$УБИ_j^A$ = [возможность реализации угрозы (Y_j); степень ущерба (X_j)],

где значение Y_j, вводимое пользователем при актуализации угрозы, находится на основании учета потенциала возможного нарушителя, уровня защищенности инфосистемы и степени ущерба (X_j) в соответствии с критериями и табл. 4, 5 ФСТЭК, внесенными в библиотеку разработанного ПО.

Таблица 4

Определение возможности реализации j-й угрозы инфосистеме

Потенциал нарушителя	**Уровень защищенности инфосистемы**		
	Высокий	**Средний**	**Низкий**
Низкий	Низкая	Средняя	Высокая
Средний	Средняя	Высокая	Высокая
Высокий	Высокая	Высокая	Высокая

Таблица 5

Определение актуальности j-й угрозы инфосистеме

Возможность реализации угрозы, Y_j	**Степень возможного ущерба, X_j**		
	Низкая	**Средняя**	**Высокая**
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная

При завершении моделирования с использованием разработанного ПО специалист по информационной безопасности получает:

- полную информацию об угрозах и уязвимостях каждого элемента инфосистемы в соответствии с банком данных ФСТЭК;
- рекомендации к устранению уязвимостей в соответствии с банком данных ФСТЭК;
- оценку о проектной защищенности инфосистемы в соответствии с методикой ФСТЭК, которая может принимать значения: «высокая», «средняя» или «низкая», в зависимости от структурно-функциональных характеристик инфосистемы и условий ее эксплуатации.

Результаты моделирования собраны в виде нескольких меню. При этом пользователь имеет возможность просматривать информацию как по отдельному узлу, так и по всей модели в целом. Разработанное ПО оперирует такими показателями информационной безопасности, как *частость угроз* банка данных ФСТЭК, направленная на конкретный информационных ресурс; потенциал нарушителя (качественные параметры нарушителя ФСТЭК, представленные в числовом виде).

Такая информация собрана в виде гистограмм, графиков и таблиц и удобна для визуального восприятия. Пример такой гистограммы для анализа уязвимостей элементов приведен на рис. 4.

Как видно из рис. 4, согласно моделированию, проведенному для представленной на рис. 5 инфосистемы, на узле «файловый сервер» сосредоточено 633 уязвимости, отсортированных по оценке *CVSS.v2*. Подобное представление результатов моделирования угроз и уязвимостей особенно важно при анализе крупномасштабных распределенных инфосистем, когда выявляются тысячи уязвимостей — в этом случае упорядоченный набор гистограмм по уровню *CVSS.v2*/*v3* легче воспринимается визуально, в отличие от текстового представления.

Для удобства пользователя, разработанное ПО позволяет анализировать угрозы и уязвимости по методике ФСТЭК в интерактивном режиме путем наведения курсора и активации любой области такой гистограммы, способной отображать характеристику уязвимости и угрозы, а также соответствующие меры их нейтрализации.

Описания уязвимостей снабжены ссылками на источники. При желании пользователь может воспользоваться ими для перехода на сайт производителя или авторитетного издания для получения более подробной информации (рис. 6).

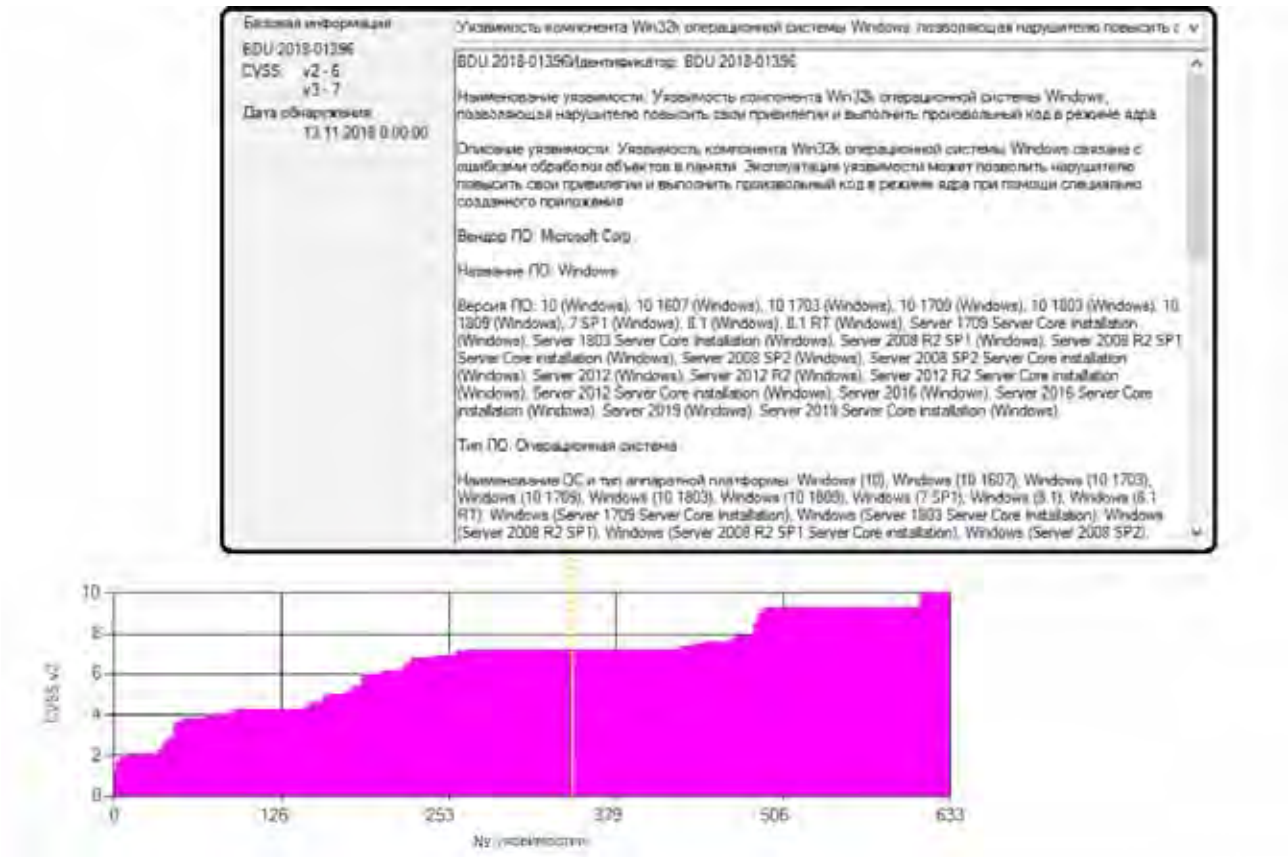

Рис. 4. Распределение уязвимостей по оценкам их опасности для узла «файловый сервер» инфосистемы (иллюстрация анализа выбранной пользователем уязвимости)

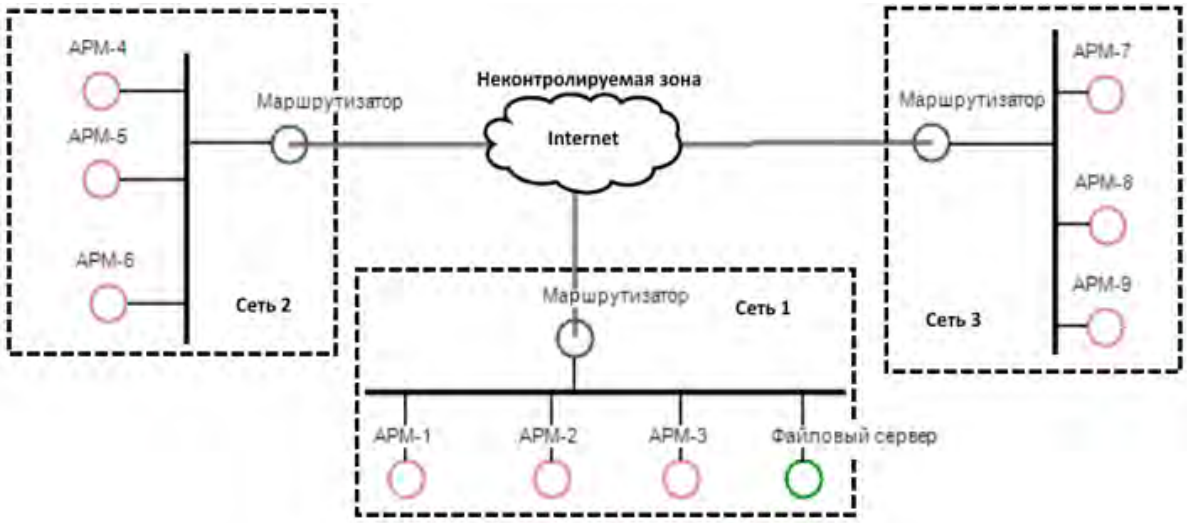

Рис. 5. Моделируемая топология распределенной сети

Адекватность полученных результатов моделирования

Для проверки адекватности моделирования угроз реальным условиям, в качестве «экспертной» оценки были использованы результаты публикации [10], в которой приведены сформированные экспертами характерные угрозы ФСТЭК для инфосистемы телекоммуникационного предприятия без уточнения использованного программного и аппаратного обеспечения.

Результаты моделирования представлены в табл. 6 (22 смоделированные угрозы против 24, сформиро-

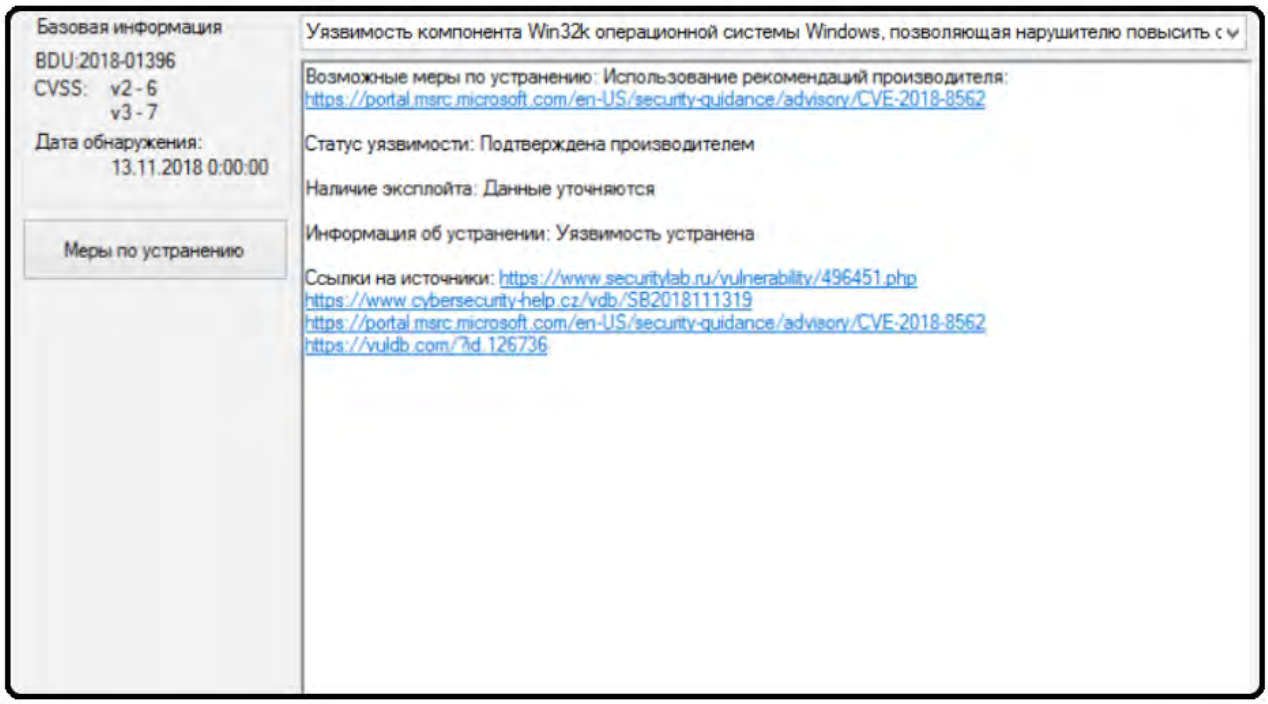

Рис. 6. Демонстрация взаимодействия пользователя с программным обеспечением

Рис. 7. Пояснение к определению адекватности моделирования угроз

ванных экспертами путем эвристического анализа безопасности примененных информационных технологий телекоммуникационной системы предприятия).

Следует заметить, что по результатам прохождения опроса уровень проектной защищенности исследуемой инфосистемы был определен как «низкий». В соответствии с табл. 4, всем обнаруженным угрозам присваивался параметр «возможность реализации» = «высокая». В связи с этим, в соответствии с табл. 5, все обнаруженные угрозы в инфосистеме являются актуальными.

Путем применения разработанного программного обеспечения получена модель угроз для типового фрагмента телекоммуникационной инфосистемы, топология которой представлена на рис. 5.

Таблица 6

Сравнение результатов работы программного обеспечения и экспертной оценки

Получено с помощью ПО	Экспертная оценка
Всего угроз **22**. Приведены только угрозы с опасностью реализации «высокая» и «средняя». Зеленым цветом отмечены те угрозы, которые встречаются только в этом столбце. Желтым цветом отмечены угрозы, встречающиеся в обоих столбцах.	Всего угроз **24.** Оранжевым цветом отмечены те угрозы, которые встречаются только в этом столбце. Желтым цветом отмечены угрозы, встречающиеся в обоих столбцах
УБИ.14 [Опасность — высокая]: Угроза длительного удержания вычислительных ресурсов пользователями УБИ.18 [Опасность — высокая]: Угроза загрузки нештатной операционной системы» (018); УБИ.22 [Опасность — средняя]: Угроза избыточного выделения оперативной памяти УБИ.23 [Опасность — средняя]: Угроза изменения компонентов системы УБИ.34 [Опасность — средняя]: Угроза использования слабостей протоколов сетевого/локального обмена данными УБИ.113 [Опасность — средняя]: Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники УБИ.121 [Опасность — средняя]: Угроза повреждения системного реестра УБИ.122 [Опасность — средняя]: Угроза повышения привилегий УБИ.139 [Опасность — высокая]: Угроза преодоления физической защиты УБИ.140 [Опасность — высокая]: Угроза приведения системы в состояние «отказ в обслуживании» УБИ.155 [Опасность — средняя]: Угроза утраты вычислительных ресурсов УБИ.156 [Опасность — высокая]: Угроза утраты носителей информации УБИ.157 [Опасность — высокая]: Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации УБИ.158 [Опасность — высокая]: Угроза форматирования носителей информации УБИ.160 [Опасность — высокая]: Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации УБИ.170 [Опасность — средняя]: Угроза неправомерного шифрования информации УБИ.172 [Опасность — средняя]: Угроза распространения «почтовых червей» УБИ.173 [Опасность — средняя]: Угроза «спама» веб-сервера УБИ.182 [Опасность — высокая]: Угроза физического устаревания аппаратных компонентов УБИ.186 [Опасность — средняя]: Угроза внедрения вредоносного кода через рекламу, сервисы и контент УБИ.189 [Опасность — средняя]: Угроза маскирования действий вредоносного кода УБИ.192 [Опасность — средняя]: Угроза использования уязвимых версий программного обеспечения	— «угроза длительного удержания вычислительных ресурсов пользователями» (014); — «угроза загрузки нештатной операционной системы» (018); — «угроза избыточного выделения оперативной памяти» (022); — «угроза изменения компонентов системы» (023); — «угроза использования информации идентификации/аутентификации, заданной по умолчанию» (030); — «угроза использования слабостей протоколов сетевого/локального обмена данными» (034); — «угроза исследования механизмов работы программы» (036); — «угроза несанкционированного удаления защищаемой информации» (091); — «угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники» (113); — «угроза повреждения системного реестра» (121); — «угроза повышения привилегий» (122); — «угроза преодоления физической защиты» (139); — «угроза приведения системы в состояние «отказ в обслуживании» (140); — «угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации» (143); — «угроза утраты вычислительных ресурсов» (155); — «угроза утраты носителей информации» (156); — «угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации» (157); — «угроза форматирования носителей информации» (158); — «угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации» (160); — «угроза неправомерного шифрования информации» (170); — «угроза распространения «почтовых червей» (172); — «угроза физического устаревания аппаратных компонентов (182) — «угроза внедрения вредоносного кода через рекламу, сервисы и контент» (186); — «угроза маскирования действий вредоносного кода» (189)

Формирование модели проводилось на основании ответов на 20 вопросов разработанного ПО, без детализации и уточнения аппаратного и программного обеспечения каждого узла.

Для оценки адекватности результатов работы разработанного ПО с учетом ранжирования угроз по их опасности реализации (не включая «низкий» уровень опасности реализации) и актуальности, использовался метод сравнения множеств угроз по функции Джаккарда[8] [8, 13], полученных в результате моделирования с экспертной оценкой:

$$\mathrm{sim}\,(x,y)=\frac{|\{x_1,\dots,x_v\}\cap\{y_1,\dots,y_w\}|}{|\{x_1,\dots,x_v\}\cup\{y_1,\dots,y_w\}|}100\,\%,$$

где x, y — документы, схожесть которых устанавливается данной формулой: левый и правый столбцы табл. 6; v, w — количество лексем, т. е. абстрактных единиц языка, по которым идет сравнение (в данном случае — идентификаторы УБИ), в текстах документов x и y, соответственно;$\{x_1,\dots, x_v\}$, $\{y_1,\dots, y_w\}$ — множество лексем текстов x и y.

Рассчитана мера сходства sim(x,y) двух выборок согласно формуле и поясняющему рис. 7, численное значение которой составило порядка 76%.

Заключение

Проведенные исследования разработанного ПО показали, что результаты моделирования хорошо коррелируют с экспертными оценками, а само моделирование происходит с использованием методик, угроз и уязвимостей банка данных ФСТЭК. Иногда результаты моделирования угроз с помощью разработанного ПО показывали избыточные результаты, обусловленные нечетким выбором топологии сети и применяемых информационных технологий, а также низкой оценкой проектной защищенности системы. Однако большая часть угроз выявлена правильно, что дает основание сделать *вывод* о целесообразности использования на практике созданного программного продукта.

Полученные результаты показывают, что сформированную модель угроз можно использовать в качестве базовой, а в результате уточнения конфигурации каждого узла инфосистемы предложенное программное обеспечение позволяет актуализировать содержание модели угроз. Разработанное программное обеспечение позволит значительно сократить время, затрачиваемое специалистом на разработку базовой модели угроз для инфосистемы при построении модели управления рисками и анализе больших данных, передаваемых через исследуемую инфосистему [15,16].

Разработанное ПО используется в учебном процессе МТУСИ при изучении угроз, которые могут приводить к нарушению информационной безопасности инфосистем заданного типа с применением различных информационных технологий. Данное ПО было протестировано в ходе выполнения лабораторного практикума студентами специальности «11.04.02 — «Инфокоммуникационные технологии и системы связи» по дисциплине «Угрозы информационной безопасности информационных систем» в ходе осеннего семестра 2019—20 учебного года. Проведенный после выполнения лабораторных работ опрос среди студентов подтвердил хорошую наглядность предоставляемой пользователю информации, а также выявил слабые стороны дизайна и интерфейса ПО (предложенные студентами нововведения постепенно внедряются в ПО). Благодаря взаимодействию с банком данных ФСТЭК и разработанной на его базе библиотеке угроз и уязвимостей данное ПО можно использовать в учебном процессе как дополнительный глоссарий.

[8] Неелова Н. В., Сычугов А. А. Вычисление нечетких дублей по формуле Джаккарда с учетом синонимических замен и стоповых слов // Известия ТулГУ. Технические науки. 2009. № 4. С. 210—211;

[9] Елисеева И. И., Рукавишников В. О. Группировка, корреляция, распознавание образов (статистические методы классификации и измерения связей). М. : Статистика, 1977. 143 с.

Рецензент: ***Марков Алексей Сергеевич,*** *доктор технических наук, профессор кафедры ИУ8 «Информационная безопасность» МГТУ им. Н.Э. Баумана, Москва, Россия.*
E-mail: a.markov@bmstu.ru

Литература

1. Большаков А.С., Тюлькин Д.И. Оценка опасной зоны побочных электромагнитных излучений видеосистемы компьютера // Труды XIII Междунар. отраслевой науч.-техн. конф. «Технологии информационного общества» / МТУСИ. М. : «ИД Медиа Паблишер», 2019. С. 336—340.
2. Григорьев В. Р., Кузнецов В. С. Проблемы выявления уязвимостей в модели облачных вычислений // Спецтехника и связь. 2012. № 4. С. 42—46.
3. Ильченко Л. М., Брагина Е. К., Егоров И. Э., Зайцев С. И. Расчет рисков информационной безопасности телекоммуникационного предприятия // Открытое образование. 2018. № 2. С. 61—70. DOI: 10.21686/1818-4243-2018-2-61-70.
4. Ловцов Д. А. Проблема информационной безопасности ГАС РФ «Правосудие» // Российское правосудие. 2012. № 5. С. 103—109.
5. Ловцов Д. А. О современных концепциях информационной безопасности эргасистемы и безопасности информации // Информация и космос. 2003. № 1—2. С. 47—57.

6. Ловцов Д. А., Верхоглядов А. А. Информационная безопасность судебных автоматизированных информационных систем: правовое регулирование и юрисдикция // Российское правосудие. 2008. № 8. С. 55—64.
7. Ломаков Ю. А. Общие проблемы в моделировании угроз и оценивании рисков в информационных системах // Молодой ученый. 2014. № 3 (62). С. 324—327.
8. Неелова Н. В., Сычугов А. А. Сравнение результатов детектирования дублей методом шинглов и методом Джаккарда // Вестник Рязанского ГРТУ. 2010. № 4 (вып. 34). С. 72—78.
9. Нестерук С. В., Беззатеев С. В. Протокол парной аутентификации устройств в статических сетях без инфраструктуры // Технико-технологические проблемы сервиса ТТПС. 2017. № 3. С. 61—67.
10. Рогатнева Е. А., Большаков А. С. Применение нечеткой логики для управления информационным риском // Труды XIII Междунар. отраслевой науч.-техн. конф. «Технологии информационного общества» / МТУСИ. М. : «ИД Медиа Паблишер», 2019. С. 331—335.
11. Рогатнева Е. А., Большаков А. С. Оценка рисков информационной безопасности с использованием алгоритмов нечеткой логики // Телекоммуникации и информационные технологии. 2018. Т. 5. № 2. С. 142—147.
12. Сергеев Ю. К. Анализ угроз безопасности виртуальных информационных систем // История и архивы. 2011. № 13. С. 160—169.
13. Цыганов Н. Л., Циканин М. А. Исследование методов поиска дубликатов веб-документов с учетом запроса пользователя // Сб. работ участников конкурса «Интернет-математика 2007». Екатеринбург : Изд-во Уральского Федерального ун-та, 2007. С. 211—222.
14. Хлыстова Д. А., Попов К. Г. К вопросу о моделировании угроз персональным данным пользователей в системах дистанционного обучения образовательных организаций // Международный студенческий научный вестник. 2016. № 3-1. С. 96—97.
15. Шелухин О. И., Барков В. В., Полковников М. В. Классификация зашифрованного трафика мобильных приложений методом машинного обучения // Вопросы кибербезопасности. 2018. № 4 (28). С. 21—28. DOI: 10.21681/2311-3456-2018-4-21-28.
16. Шелухин О. И., Ванюшина А. В., Габисова М. Е. Фильтрация нежелательных приложений интернет-трафика с использованием алгоритма классификации random forest // Вопросы кибербезопасности. 2018. № 2 (26). С. 44—51. DOI: 10.21681/2311-3456-2018-2-44-51.
17. Шелухин О. И., Симонян А. Г., Иванов Ю. А. Особенности DDoS атак в беспроводных сетях // T-Comm. 2012. № 11. С. 67—71.

SOFTWARE FOR MODELLING INFORMATION SECURITY THREATS IN INFORMATION SYSTEMS

Aleksandr Bol'shakov, *Ph.D. (Technology), Associate Professor at the Moscow Technical University of Communication and Informatics, Moscow, Russian Federation.*
E-mail: alexbol57@mail.ru

Dmitrii Rakovskii, *student of the Moscow Technical University of Communication and Informatics, Moscow, Russian Federation.*
E-mail: dimitor1998@mail.ru

Keywords: *information system, software, information security, threats, vulnerabilities, data bank, threats model, basic threats model.*

Abstract.
Purpose of the work: *improving the scientific and methodological basis for assessing information systems security.*
Method of study: *modelling security threats for hardware and software technologies based on the normative federal methodology for identifying threats to information security in information systems. For analysing the possibility and probability of the occurrence of threats, statistical and expert estimates of the threats in compliance with the normative federal methodology were used. The assessment of the adequacy of the constructed threats models was carried out using a measure of similarity of samples of different sizes.*
Results obtained: *software for modelling information security threats in different information systems was developed taking into account hardware and software technologies of the federal data bank. The functionality of the developed software allows to group and rank the federal data bank threats by objects of their impact on information system information resources which is of practical value for developing information security measures. An analysis of the adequacy of threats modelling using the developed software showed a good value of the measure of similarity between simulated and expert*

types of threats. Modelling threats using the software indicated that a set of current/topical threats mainly depends on the degree of information system protection and the parameters of the intruder model. The software is used to study measures for neutralising threats in educational laboratory practice.

References

1. Bol'shakov A.S., Tiul'kin D.I. Otsenka opasnoi zony pobochnykh elektromagnitnykh izluchenii videosistemy komp'iutera. Trudy XIII Mezhdunar. otraslevoi nauch.-tekhn. konf. "Tekhnologii informatsionnogo obshchestva", MTUSI, M. : "ID Media Pablisher", 2019, pp. 336-340.
2. Grigor'ev V. R., Kuznetsov V. S. Problemy vyiavleniia uiazvimostei v modeli oblachnykh vychislenii. Spetstekhnika i sviaz', 2012, No. 4, pp. 42-46.
3. Il'chenko L. M., Bragina E. K., Egorov I. E., Zaitsev S. I. Raschet riskov informatsionnoi bezopasnosti telekommunikatsionnogo predpriiatiia. Otkrytoe obrazovanie, 2018, No. 2, pp. 61-70, DOI: 10.21686/1818-4243-2018-2-61-70.
4. Lovtsov D. A. Problema informatsionnoi bezopasnosti GAS RF "Pravosudie". Rossiiskoe pravosudie, 2012, No. 5, pp. 103-109.
5. Lovtsov D. A. O sovremennykh kontseptsiiakh informatsionnoi bezopasnosti ergasistemy i bezopasnosti informatsii. Informatsiia i kosmos, 2003, No. 1-2, pp. 47-57.
6. Lovtsov D. A., Verkhogliadov A. A. Informatsionnaia bezopasnost' sudebnykh avtomatizirovannykh informatsionnykh sistem: pravovoe regulirovanie i iurisdiktsiia. Rossiiskoe pravosudie, 2008, No. 8, pp. 55-64.
7. Lomakov Iu. A. Obshchie problemy v modelirovanii ugroz i otsenivanii riskov v informatsionnykh sistemakh. Molodoi uchenyi, 2014, No. 3 (62), pp. 324-327.
8. Neelova N. V., Sychugov A. A. Sravnenie rezul'tatov detektirovaniia dublei metodom shinglov i metodom Dzhakkarda. Vestnik Riazanskogo GRTU, 2010, No. 4 (vyp. 34), pp. 72-78.
9. Nesteruk S. V., Bezzateev S. V. Protokol parnoi autentifikatsii ustroistv v staticheskikh setiakh bez infrastruktury. Tekhniko-tekhnologicheskie problemy servisa TTPS, 2017, No. 3, pp. 61-67.
10. Rogatneva E. A., Bol'shakov A. S. Primenenie nechetkoi logiki dlia upravleniia informatsionnym riskom. Trudy XIII Mezhdunar. otraslevoi nauch.-tekhn. konf. "Tekhnologii informatsionnogo obshchestva", MTUSI, M. : "ID Media Pablisher", 2019, pp. 331-335.
11. Rogatneva E. A., Bol'shakov A. S. Otsenka riskov informatsionnoi bezopasnosti s ispol'zovaniem algoritmov nechetkoi logiki. Telekommunikatsii i informatsionnye tekhnologii, 2018, t. 5, No. 2, pp. 142-147.
12. Sergeev Iu. K. Analiz ugroz bezopasnosti virtual'nykh informatsionnykh sistem. Istoriia i arkhivy, 2011, No. 13, pp. 160-169.
13. Tsyganov N. L., Tsikanin M. A. Issledovanie metodov poiska dublikatov veb-dokumentov s uchetom zaprosa pol'zovatelia. Sb. rabot uchastnikov konkursa "Internet-matematika 2007", Ekaterinburg : Izd-vo Ural'skogo Federal'nogo un-ta, 2007, pp. 211-222.
14. Khlystova D. A., Popov K. G. K voprosu o modelirovanii ugroz personal'nym dannym pol'zovatelei v sistemakh distantsionnogo obucheniia obrazovatel'nykh organizatsii. Mezhdunarodnyi studencheskii nauchnyi vestnik, 2016, No. 3-1, pp. 96-97.
15. Shelukhin O. I., Barkov V. V., Polkovnikov M. V. Klassifikatsiia zashifrovannogo trafika mobil'nykh prilozhenii metodom mashinnogo obucheniia. Voprosy kiberbezopasnosti, 2018, No. 4 (28), pp. 21-28, DOI: 10.21681/2311-3456-2018-4-21-28.
16. Shelukhin O. I., Vaniushina A. V., Gabisova M. E. Fil'tratsiia nezhelatel'nykh prilozhenii internet-trafika s ispol'zovaniem algoritma klassifikatsii random forest. Voprosy kiberbezopasnosti, 2018, No. 2 (26), pp. 44-51, DOI: 10.21681/2311-3456-2018-2-44-51.
17. Shelukhin O. I., Simonian A. G., Ivanov Iu. A. Osobennosti DDoS atak v besprovodnykh setiakh. T-Comm, 2012, No. 11, pp. 67-71.