МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СИБИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ И ИНФОРМАТИКИ»

Вестник СибГУТИ Том 17, № 2, 2023

Выпускается ежеквартально, выходит с 2007 г.

Учредитель –
федеральное государственное бюджетное образовательное учреждение высшего образования
«Сибирский государственный университет телекоммуникаций и информатики»

Адрес редакции и издателя

630102, г. Новосибирск, ул. Кирова, д. 86 e-mail: vestnik@sibguti.ru

Информация о журнале доступна в сети Internet по адресу https://vestnik.sibsutis.ru.

Журнал включён в Перечень ВАК российских рецензируемых научных журналов, в которых должны быть опубликованы основные научные результаты диссертаций на соискание учёных степеней доктора и кандидата наук.

Журнал зарегистрирован Федеральной службой по надзору за соблюдением законодательства в сфере массовых коммуникаций и охране культурного наследия, свидетельство о регистрации ПИ № ФС77-25835 от 29.09.2006. ISSN 1998-6920. Подписной индекс в каталоге «Урал-Пресс» – 82519.

Дата выхода в свет 29.06.2023. Отпускная (редакционная) цена 750 руб.
Отпечатано в издательском центре СибГУТИ по адресу: 630102, г. Новосибирск, ул. Кирова, д. 86.
Бумага офсетная, формат А4. Тираж 300 экз.

СОДЕРЖАНИЕ

DOI: 10.55648/1998-6920-2023-17-2-3-11 УДК 681.84

О необходимости уточнения методик оценки качества звуковых трактов за счет применения психоакустических критериев

Н. О. Абросимова, А. А. Коротченко, М. С. Шушнов

Сибирский гос. унив. телекоммуникаций и информатики (СибГУТИ)

Аннотация: В статье рассмотрена связь электрических показателей качества звуковых трактов, используемых в современных методиках измерений, и психоакустических показателей качества субъективной оценки. Дается рекомендация о необходимости применения критериев психоакустической оценки, так как не все параметры, используемые при субъективной оценке качества звуковых трактов, могут быть измерены с помощью объективных методик.

Ключевые слова: звук, тракт, запись, усиление, методика, искажения, психоакустика.

Для цитирования: Абросимова Н. О., Коротченко А. А., Шушнов М. С. О необходимости уточнения методик оценки качества звуковых трактов за счет применения психоакустических критериев // Вестник СибГУТИ. 2023. Т. 17, № 2. С. 3–11. https://doi.org/10.55648/1998-6920-2023-17-2-3-11.

Статья поступила в редакцию 25.12.2022;
принята к публикации 10.01.2023.

1. Введение

В современном мире музыка, речь и иные звуки окружают нас со всех сторон. Звуковые тракты встречаются в телевизионных и радиовещательных студийно-аппаратных комплексах, студиях звукозаписи и мастеринга, при прослушивании фонограмм через бытовые устройства и т.п. Иными словами, любой звук, что мы слышим сегодня, опосредованно прошел через некий звуковой тракт – совокупность устройств снятия, усиления, обработки, передачи и воспроизведения звуковой информации. Сложно найти человека, который не оценит и не любит чистое и качественное звуковоспроизведение. Но в настоящее время нет однозначного понимания, от чего зависит качество звуковоспроизведения.

За приятный звуковой сигнал отвечает множество факторов, но ключевым и немаловажным является объективная оценка качества звуковых трактов с применением стандартных методик измерений. Однако все чаще возникают вопросы об адекватности и всесторонности объективных методов оценки качества, так как в среде профессиональных музыкантов, звукорежиссеров, меломанов и обычных слушателей все большее внимание отдается субъективной оценки, а данные о технических характеристиках большинство практически не интересуют.

Субъективная оценка включает в себя слепое или не слепое прослушивание звукового тракта с оценкой ряда психоакустических критериев качества звуковоспроизведения и дает

больше информации о качественных свойствах звукового тракта, чем проведение измерений только электрических характеристик. Принципы и критерии психоакустической субъективной оценки самостоятельно сформировались за последние 40–50 лет в среде любителей качественного звука, музыкантов, звукорежиссеров, аудиофилов и др.

2. Систематизация объективных и субъективных критериев оценки качества звука с установлением взаимосвязей

2.1. Система стандартов оценки качества

Любая существующая объективная методика оценки качественных характеристик аналоговых звуковых устройств [1–3] и цифровых трактов [4–7] – профессиональных и бытовых – реализуется с помощью одного или нескольких измерительных приборов, предназначенных для измерения электрических величин. Обобщая методики, можно выделить общие подходы к объективной оценке. Измерения электрических величин всегда затрагивают такие характеристики, как диапазон рабочих частот, неравномерность амплитудно-частотной характеристики (АЧХ), коэффициент нелинейных искажений (или коэффициент гармоник), коэффициент интермодуляционных искажений, характер переходного процесса при импульсном воздействии, отношение сигнал/шум на выходе и максимальный уровень сигнала или динамический диапазон, разделение каналов (в многоканальной системе). Однако ни одна из указанных электрических характеристик не имеет отношения к оценке восприятия слушателем результата.

Сегодня имеет место абсурдная ситуация: разработчики, производители и маркетологи в области аудиоустройств продолжают удивлять цифрами, говорящими о экстремально высоком качестве их устройств, а покупатели все чаще склоняются в сторону устройств с невысокими качественными показателями, устройствам «винтажным», ламповым конструкциям и устройствам без указания их качественных характеристик. Также ряд слушателей отказывается от цифровых носителей информации, стриминговых интернет-ресурсов и слушает записи с магнитной ленты, на виниловых дисках, хотя есть часть приверженцев, казалось, давно устаревшего формата CD-диска. В [8] указано, что иногда звукорежиссеры преднамеренно снижают качество звукового сигнала при обработке для придания приятного характера звучания создаваемой фонограмме, радиопрограмме и т.п.

Необходимо отметить, что хотя Приложение А ГОСТ IEC 61606-3-2014 [6] содержит указание на возможность применения альтернативной методики оценки электрических характеристик с целью получения б*о*льшей информации, однако оно не предусматривает возможности проведения субъективной оценки качества звука.

2.2. Объективная и субъективная методики оценки

В среде звукорежиссеров, меломанов, музыкантов и аудиофилов часто используются критерии оценки качества звучания, такие как различимость, полнота, громкость, теплота или нейтральность, тембр, тональный баланс, высокий регистр, темный фон, сцена, микродетальность, макродетальность, утомляемость или увлекательность. Существуют и иные субъективные критерии, но они либо встречаются редко, либо включают в себя указанные выше.

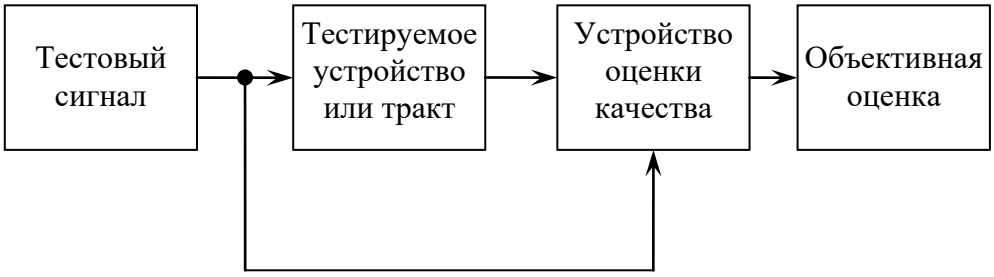

Рис. 1. Схема объективной оценки качества звукового тракта

На рис. 1 показана схема установления взаимосвязи электрических характеристик устройства психоакустическим критериям оценки. Сложность применения схемы заключается в нечетком понимании, какие именно электрические характеристики тестируемого устройства необходимо измерить электрически для совмещения результата с критериями психоакустической оценки, а также в формировании экспертной группы. По этой причине возможно введение новых качественных параметров оценки электрических характеристик аналоговых звуковых устройств и цифровых трактов, выходящих за рамки указанных в [1–7]. В качестве экспертов необходимо задействовать как профессионалов, имеющих опыт слуховой экспертизы или имеющих навык профессиональной оценки в ходе практической работы, так и группы непрофессионалов разных возрастных групп, так как свойства человеческого слуха меняются с возрастом. Хотя требование деления на возрастные группы не является обязательным. Схема тестирования при субъективной оценке показана на рис. 2.

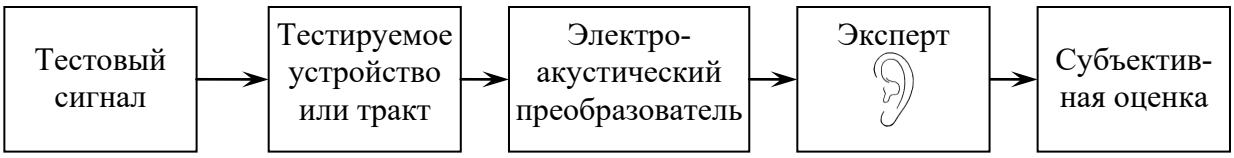

Рис. 2. Схема субъективной оценки качества звукового тракта

Как видно из рис. 2, при субъективной оценке имеет место человеческое восприятие, которое основывается на психоакустике. Эта схема не учитывает реакцию электрического измерителя – устройства оценки, как на рис. 1, но учитывает реакцию человека на результат прохождения звукового сигнала через оцениваемый тракт или устройство.

3. Психоакустические критерии оценки и их связь с электрическим трактом

В соответствии с делением объективных показателей качества и психоакустических критериев составлена диаграмма соответствия (рис. 3). Диаграмма составлена на основе систематизации и анализа имеющейся в сети Интернет информации с профильных ресурсов, а также на основе опроса покупателей аудиотехники и профессионалов-звукотехников и не учитывает возрастные группы. Сплошными линиями показаны установленные связи, а пунктирными – что взаимосвязь возможна, но не очевидна.

Рис. 3. Соответствие объективных показателей оценки качества звукового тракта субъективным характеристикам психоакустической оценки

Наличие неопределенностей в диаграмме на рис. 3 говорит о неполной оценке психоакустических свойств звуковых трактов существующими методиками измерения электрических характеристик.

Как видно из рис. 3, *полнота* (полновесность) звуковой картины, *сцена*, *микродетальность*, *макродетальность*, *утомляемость* или *увлекательность* не учитываются в объективной оценке, но при субъективной оценке считаются важными.

Так, показатель *полнота* может быть связан с эффектом компрессии динамического диапазона при усилении звукового сигнала и эффектом вариации характера переходного процесса при изменении уровня входного сигнала. В объективных электрических показателях эта оценка не учитывается, методика измерений не разработана.

Субъективный показатель *громкость* хоть и связан с уровнем сигнала (выходной мощностью или напряжением), но при прослушивании различных звуковых систем при одинаковых электрических параметрах дает различное восприятие.

Часто громкость связывается с утомляемостью или увлекательностью. Так, тракт, звучащий увлекательно, вызывает желание прослушать его на бо́льшей громкости, а звучащий утомительно – на низкой. Применение показателей *утомляемость и увлекательность* еще больше затрудняет установление четких связей с объективными характеристиками, так как для них не установлена взаимосвязь. Таким образом, эти критерии являются самыми сложными, так как сочетают в себе итоговую оценку качества звучания всего звукового тракта и должны формироваться на основе анализа ряда психоакустических характеристик.

Субъективный показатель *теплота/нейтральность* обычно связывается с наличием определенного спектра нелинейных искажений и их взаимным распределением. Так, преобладание второй гармоники и гармоник четных порядков обычно оценивается как некоторая

теплота. Преобладание третьей гармоники и гармоник нечетных порядков оценивается как агрессивность или резкость. Нейтральный характер обычно связывается с быстро убывающим спектром продуктов нелинейных искажений. Ряд электрических параметров измеряются в стандартных методиках [1–7], хотя отдельно уровни четных и нечетных гармоник не указываются.

Оценка *сцены* достаточно сложна. Часто можно встретить формулировку о близкой сцене или далекой сцене. Вероятно, это связано с укрупнением подачи звукового образа при наличии компрессии динамического диапазона, из-за чего тихие звуки становятся громче, а громкие – тише.

Микродетальность и макродетальность относят к характеристикам воспроизведения тихих звуков на фоне громких и маскирования громкими звуками тихих. При схожести формулировок ведется оценка мелких и крупных звуков отдельно, так как задействуются эффекты психоакустического маскирования человеческого слуха. В основе электрических явлений в звуковых трактах при изменении этих показателей лежат эффекты нелинейности, проявляющиеся при воздействии сигналов со сложным спектром. Стандартные методики [1–7] предусматривают оценку на основе воздействия пары стационарных сигналов с отличающимися частотами и определенным соотношением уровней, что не имеет отношения к реальному звуковому сигналу.

Таким образом, наличие множества перекрестных связей между параметрами или их отсутствие не дает точного ответа на вопрос, какой именно электрический параметр необходимо улучшать для повышения качества звучания при субъективной оценке.

4. Использование системы искусственного интеллекта для корректировки психоакустических критериев оценки

Так как в последнее время системы искусственного интеллекта (ИИ) начинают внедряться в научные и учебные области [9, 10], интересной представляется возможность получения бо́льшего объема сведений об изучаемых методиках оценки на основе анализа результатов опроса респондентов и синтеза имитационных моделей для создания (обработки) референсных фонограмм путем модификации структуры подпрограмм обработчиков звуковых данных (чейнов). Возможная структура системы ИИ опроса респондентов показана на рис. 4.

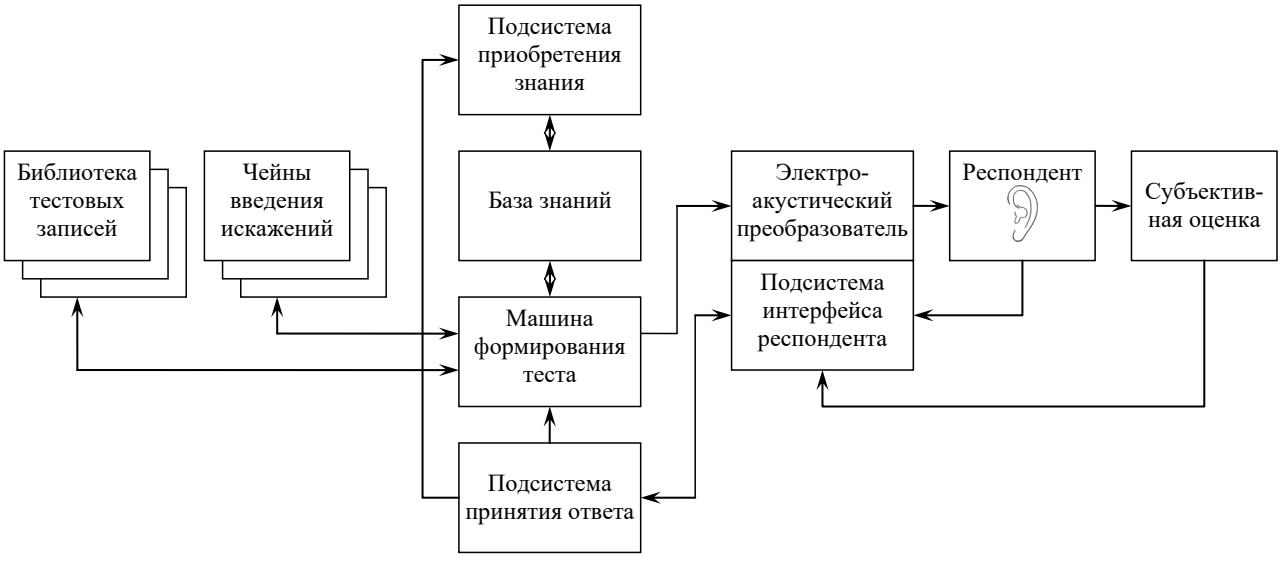

Рис. 4. Схема применения ИИ для опроса респондентов с целью уточнения психоакустических критериев оценки качества звуковых трактов

Система ИИ содержит библиотеку тестовых записей, которые могу обрабатываться чейнами введения искажений при формировании тестового задания для респондента машиной формирования теста. Машина формирования теста является рабочей областью, и на основании полученной от респондента через подсистему интерфейса респондента начальной информации генерирует тестовое задание и передает его через электроакустический преобразователь респонденту. Электроакустический преобразователь должен представлять собой референсный тракт из цифро-аналогового преобразователя, усилительного тракта и головных стереотелефонов или акустически подготовленного помещения и акустических систем.

Респондент во время исследований сообщает системе ИИ результаты субъективной оценки качества звучания через интерфейс респондента. Подсистема принятия ответа может принять ответ респондента, добавить или изменить тестовое задание для уточнения результата опроса.

База знаний хранит начальные сведения об исследовании, но в процессе приобретения знаний база знаний может изменяться и дополняться. Таким образом, можно выделить часто встречающиеся критерии психоакустической оценки и сопоставить им чейны введения искажений.

Чейны введения искажений могут меняться в процессе теста для уточнения степени влияния на психоакустическое восприятие электрических характеристик.

База тестовых записей подбирается под пожелания респондента на основе взаимодействия респондента с системой ИИ. На основе обратной связи с респондентом база данных тестовых записей может дополняться, так как записи различных стилей могут по-разному менять свои психоакустические свойства при обработке чейнами искажений.

Итогом работы системы ИИ является база знаний с критериями психоакустической оценки и сопоставляемыми им электрическими характеристиками.

5. Заключение

В настоящее время существует очевидная проблема несоответствия методик объективных измерений [1–7] требованиям слушателей и профессионального сообщества, что требует уточнения существующих методик оценки с применением психоакустических критериев.

Уточнение методик объективной оценки звуковых трактов путем учета показателей, связанных с психоакустическими свойствами, позволит улучшить их качественные характеристики, повысить заинтересованность слушателей информационными, музыкальными, образовательными программами за счет достижения комфортного характера подачи.

В звукотехнической индустрии построение устройств обработки звука, основанных на психоакустической оценке их качества звучания, позволит повысить конкурентоспособность устройств на рынке по сравнению с моделями, имеющими аналогичный функционал, но построенными без учета психоакустических свойств.

Не исключено, что психоакустические критерии могут быть использованы для преднамеренной коррекции характера звуковых материалов в рекламных компаниях и при публичных выступлениях, но такая возможность требует дополнительных исследований.

Литература

1. Наушники стереофонические. Методы измерений. Межгосударственный стандарт ГОСТ 28278-89. М.: Стандартинформ, 2006. 23 с.
2. Усилители сигналов звуковой частоты бытовые. Общие технические. Государственный стандарт СССР ГОСТ 24388-88. М.: Издательство стандартов, 1989. 11 с.

3. Аппаратура радиоэлектронная бытовая. Методы измерения электрических параметров усилителей сигналов звуковой частоты. Государственный стандарт СССР ГОСТ 23849-87. М.: Издательство стандартов, 1990. 66 с.
4. Аудио- и аудиовизуальное оборудование. Компоненты цифровой аудиоаппаратуры. Основные методы измерений звуковых характеристик. Часть 1. Общие положения. Межгосударственный стандарт ГОСТ IEC 61606-1-2014. М.: Стандартинформ, 2016. 36 с.
5. Аудио- и аудиовизуальное оборудование. Компоненты цифровой аудиоаппаратуры. Основные методы измерений звуковых характеристик. Часть 2. Бытовое применение. Межгосударственный стандарт ГОСТ IEC 61606-2-2014. М.: Стандартинформ, 2016. 36 с.
6. Аудио- и аудиовизуальное оборудование. Компоненты цифровой аудиоаппаратуры. Основные методы измерений звуковых характеристик. Часть 3. Профессиональное применение. Межгосударственный стандарт ГОСТ IEC 61606-3-2014. М.: Стандартинформ, 2020. 42 с.
7. Аудио- и аудиовизуальное оборудование. Компоненты цифровой аудиоаппаратуры. Основные методы измерений звуковых характеристик. Часть 4. Персональный компьютер. Межгосударственный стандарт ГОСТ IEC 61606-4-2014. М.: Стандартинформ, 2018. 28 с.
8. *Абросимова Н. О., Шушнов М. С.* Система стандартов измерения качества современной звуковой техники // Материалы МНТК «Современные проблемы телекоммуникаций», СибГУТИ, Новосибирск, 2021. С. 80–84.
9. *Люгер Ф.* Искусственный интеллект: стратегии и методы решения сложных проблем. 4-е изд.; пер. с англ. М.: Издательский дом «Вильямс, 2003. 863 с.
10. *Котлярова И. О.* Технологии искусственного интеллекта в образовании // Вестник ЮУрГУ. Серия «Образование. Педагогические науки». 2022. Т. 14, № 3. С. 69–82. DOI: 10.14529/ped220307.

Абросимова Надежда Олеговна
аспирант 2-го года обучения, Сибирский государственный университет телекоммуникаций и информатики (СибГУТИ, 630102, Новосибирск, ул. Кирова, 86), e-mail: skachok94@mail.ru, ORCID ID: 0009-0000-3057-8215.

Коротченко Анна Анатольевна
студент 2-го курса института телекоммуникаций, Сибирский государственный университет телекоммуникаций и информатики (СибГУТИ, 630102, Новосибирск, ул. Кирова, 86), e-mail: anitakorotchenko@mail.ru, ORCID ID: 0009-0004-5583-8369.

Шушнов Максим Сергеевич
к.т.н., доцент, заведующий кафедрой цифрового телерадиовещания и систем радиосвязи, Сибирский государственный университет телекоммуникаций и информатики (СибГУТИ, 630102, Новосибирск, ул. Кирова, 86), e-mail: efemerian@gmail.com, ORCID ID: 0000-0002-1713-5177.

Авторы прочитали и одобрили окончательный вариант рукописи.
Авторы заявляют об отсутствии конфликта интересов.
Вклад соавторов: *Каждый автор внес равную долю участия как во все этапы проводимого теоретического исследования, так и при написании разделов данной статьи.*

On the Need to Clarify the Methods of Evaluating the Tracts Sound Quality Through the Psychoacoustic Criteria Application

Nadezhda O. Abrosimova, Anna A. Korotchenko, Maxim S. Shushnov

Siberian State University of Telecommunications and Information Science (SibSUTIS)

Abstract: In this article, the electrical indicators connection of the sound tracts quality used in modern measurement methods and psychoacoustic indicators of the subjective assessment potential are considered. A recommendation on the need to apply psychoacoustic assessment criteria is given as not all of them used in subjective assessment of the sound tracts quality can be measured using objective techniques.

Keywords: sound, tract, record, amplification, methodology, distortion, psychoacoustics.

For citation: Abrosimova N. O., Korotchenko A. A., Shushnov M. S. On the need to clarify the methods of evaluating the tracts sound quality through the psychoacoustic criteria application (in Russisn). *The SibSUTIS Bulletin*, 2023, vol. 17, no. 2, pp. 3-11. https://doi.org/10.55648/1998-6920-2023-17-2-3-11.

The article was submitted: 25.12.2022;
accepted for publication 10.01.2023.

References

1. *Naushniki stereofonicheskiye. Metody izmereniy. Mezhgosudarstvennyy standart GOST 28278-89* [Stereophonic headphones. Measurement methods. Interstate Standard GOST 28278-89]. M.: Standartinform, 2006. 23 p.
2. *Usiliteli signalov zvukovoy chastoty bytovyye. Obshchiye tekhnicheskiye. Gosudarstvennyy standart SSSR GOST 24388-88* [Increased sound frequency signals. General technical. State Standard of the USSR GOST 24388-88]. M.: Izdatel'stvo standartov, 1989. 11 p.
3. *Apparatura radioelektronnaya bytovaya. Metody izmereniya elektricheskikh parametrov usiliteley signalov zvukovoy chastoty. Gosudarstvennyy standart SSSR GOST 23849-87* [The equipment is electronic household. Methods for measuring the electrical parameters of sound frequency signals. State Standard of the USSR GOST 23849-87]. M.: Izdatel'stvo standarto, 1990. 66 p.
4. *Audio- i audiovizual'noye oborudovaniye. Komponenty tsifrovoy audioapparatury. Osnovnyye metody izmereniy zvukovykh kharakteristik. Chast' 1. Obshchiye polozheniya. Mezhgo-sudarstvennyy standart GOST IEC 61606-1-2014* [Audio and audiovisual equipment. Components of digital audio equipment. Opestic methods for measuring sound characteristics. Part 1. General provisions. The inter-state standard GOST IEC 61606-1-2014]. M.: Standartinform, 2016. 36 p.
5. *Audio- i audiovizual'noye oborudovaniye. Komponenty tsifrovoy audioapparatury. Osnovnyye metody izmereniy zvukovykh kharakteristik. Chast' 2. Bytovoye primeneniye. Mezh-gosudarstvennyy standart GOST IEC 61606-2-2014* [Audio and audiovisual equipment. Components of digital audio equipment. Opestic methods for measuring sound characteristics. Part 2. Household application. The inter-state standard GOST IEC 61606-2-2014]. M.: Standartinform, 2016. 36 p.
6. *Audio- i audiovizual'noye oborudovaniye. Komponenty tsifrovoy audioapparatury. Osnovnyye metody izmereniy zvukovykh kharakteristik. Chast' 3. Professional'noye prime-neniye. Mezhgosudarstvennyy standart GOST IEC 61606-3-2014* [Audio and audiovisual equipment. Components of digital audio equipment. Opestic methods for measuring sound characteristics. Part 3. Professional example. Interstate Standard GOST IEC 61606-3-2014]. M.: Standartinform, 2020. 42 p.
7. *Audio- i audiovizual'noye oborudovaniye. Komponenty tsifrovoy audioapparatury. Osnovnyye metody izmereniy zvukovykh kharakteristik. Chast' 4. Personal'nyy komp'yuter. Mezhgosudarstvennyy standart GOST IEC 61606-4-2014* [Audio and audiovisual equipment. Components of digital audio equipment.

Opestic methods for measuring sound characteristics. Part 4. Personal computer. Interstate Standard GOST IEC 61606-4-2014]. M.: Standaftinform, 2018. 28 p.
8. Abrosimova N.O., Shushnov M.S. Sistema standartov izmereniya kachestva sovremennoy zvukovoy tekhniki [System of standards for measuring the quality of modern sound technology]. *Sovremennyye problemy telekommunikatsiy: Mezhdunar. nauch.-tekhn. konf: materialy konf.* Sib. state. University of telecommunications and informatics. Novosibirsk: SibGUTI, 2021. pp.80-84.
9. Luher F. *Iskusstvennyy intellekt: strategii i metody resheniya slozhnykh problem* [Artificial intelligence: strategies and methods for solving complex problems]. 4th ed. from English. M, Izdatel'skiy dom «Vil'yams», 2003. 863 p.
10. Kotlyarova I.O. Tekhnologii iskusstvennogo intellekta v obrazovanii [Technologies of artificial intelligence in education]. *Vestnik YUUrGU. Seriya «Obrazovaniye. Pedagogicheskiye nauki»*, 2022, vol. 14, no. 3, pp. 69-82. DOI: 10.14529/Ped220307.

Nadezhda O. Abrosimova
Postgraduate student, Siberian State University of Telecommunications and Information Science, e-mail: skachok94@mail.ru, ORCID ID: 0009-0000-3057-8215.

Anna A. Korotchenko
Student, Siberian State University of Telecommunications and Information Science, e-mail: anitakorotchenko@mail.ru, ORCID ID: 0009-0004-5583-8369.

Maxim S. Shushnov
Cand. of Sci. (Engineering), Associate Professor, Head of the Department of Digital Television, Radio Broadcasting and Radio Communication Systems, Siberian State University of Telecommunications and Information Science (SibSUTIS, Russia, 630102, Novosibirsk, Kirov St. 86), e-mail: efemerian@gmail.com, ORCID ID: 0000-0002-1713-5177.

DOI: 10.55648/1998-6920-2023-17-2-12-21 УДК 378.14+004.41

Экстремальное программирование как метод развития гибких и профессиональных навыков студентов IT-отрасли

К. И. Брагин, Д. В. Агапитов, Я. А. Колташев

Уральский технический институт связи и информатики (УрТИСИ СибГУТИ)

Аннотация: В статье описывается опыт применения экстремального программирования в качестве методики развития гибких и профессиональных навыков студентов технического вуза. Обсуждается практическая реализация профессионального образования в ходе участия студентов-программистов в соревнованиях, чемпионатах и хакатонах по направлению искусственного интеллекта, организованных как на всероссийском уровне, так и IT-компаниями.

Ключевые слова: экстремальное программирование, хакатон, цифровой прорыв, машинное обучение, искусственный интеллект, мотивация, гибкие навыки.

Для цитирования: Брагин К. И., Агапитов Д. В., Колташев Я. А. Экстремальное программирование как метод развития гибких и профессиональных навыков студентов IT-отрасли // Вестник СибГУТИ. 2023. Т. 17, № 2. С. 12–21. https://doi.org/10.55648/1998-6920-2023-17-2-12-21.

Статья поступила в редакцию 26.12.2022;
принята к публикации 10.01.2023.

1. Введение

Выступая на конференции, посвящённой системам искусственного интеллекта (ИИ), Президент Российской Федерации В. В. Путин отметил, что значение прорывов в сфере ИИ колоссально, от них зависит место страны в мире, возможности на качественно новом уровне решать задачи экономического, промышленного, социального развития. Это означает совершенно иной уровень подхода к развитию отечественных технологий в сфере компьютерного интеллекта и подчеркивает перспективы их внедрения в производство и экономику Российской Федерации. Открывающиеся возможности многогранны, поэтому уже сейчас государству необходимо занимать свою нишу в будущей технологической гонке [1].

Для обеспечения разработки и ускорения развития отечественных технологий необходимо проделать много организационной работы, начиная с подготовки специалистов и популяризации данной тематики в обществе. Ряд задач в этом направлении уже решается, о чем свидетельствуют регулярные всероссийские конференции по искусственному интеллекту, а также организация соревнований, чемпионатов и хакатонов, в которых проявить себя может любой желающий, независимо от уровня подготовки.

В данной статье исследуется мотивация студентов изучать и познавать совершенно новые для них инструменты из сферы программирования, учитывая их неявную применимость относительно основной образовательной программы, по которой осуществляется подготовка.

Стоит отметить, что обучение специалистов в сфере ИИ уже реализуется по программам бакалавриата и магистратуры в высших учебных заведениях, а также в рамках проекта «Цифровые профессии», являющегося частью национальной программы «Цифровая экономика Российской Федерации» [2]. При формировании современного IT-специалиста особое внимание уделяется развитию гибких навыков (англ. soft skills), что ставит перед преподавательским составом вузов нетривиальную задачу по разработке иных подходов к подаче материала и применению новых методик образования.

Современное поколение студентов в рамках теории поколений, разработанной Уильямом Штраусом и Нилом Хау [3], обладает своими специфическими чертами, которые важно учитывать в образовании. Проводимое исследование представляет интерес и в данном направлении, при учете, что указанная теория не является догмой.

2. Проблематика

2.1. Мотивация

Отличительной чертой студентов родного вуза авторов – Уральского технического института связи и информатики (филиал СибГУТИ в г. Екатеринбурге) – является личное непонимание, неясность дальнейшей профессиональной судьбы и рода деятельности после выпуска. Это связано с широтой, разнонаправленностью учебных программ, что на самом деле не является критическим недостатком. Напротив, при должной профориентационной работе и поддержании интереса у студентов это становится мощным и гибким инструментом при формировании качественных IT-специалистов. Данный тезис применим и к другим вузам.

Существуют определенные нюансы в освоении таких программ, один из которых – потеря интереса к изучаемому материалу со стороны студента, непонимание его практической значимости в жизни специалиста, что приводит к рутинизации процесса образования и падению качества знаний. Проблема мотивации, вовлеченности в учебный процесс отмечается авторами из собственного пережитого опыта, как с точки зрения студента, так и с точки зрения преподавателя-аспиранта. Кроме того, данный вопрос уже давно поднимается в широких научных кругах с позиции психологии и педагогики [4, 5].

Одним из предполагаемых решений данной проблемы может стать введение в учебную программу профориентационной дисциплины [6, 7]. Важную роль играют наставники студентов из числа преподавателей, научные руководители, кураторы. Студенты хотят чувствовать, что они являются полноценными участниками образовательного процесса, а их энергия направлена на достижение конкретных целей. При этом цель должна быть сформирована самим студентом (ведь это он выбирал направление при поступлении), задача наставников – помочь ему в этом, тогда обучение становится более контролируемым процессом. В большинстве случаев впоследствии возникает обратная связь, активность студентов выходит на новый уровень, что позволяет им самостоятельно выдвигаться на соревнования и влиять на репутацию как наставников, так и вуза в целом.

В крупнейших образовательных учреждениях приобретают популярность «индивидуальные образовательные траектории» [8, 9], где группе студентов позволяется выбирать профильные модули, состоящие из набора интересующих их дисциплин, в чем им помогает ответственный куратор, осуществляющий также профориентационную и адаптационную работу.

2.2. Взгляд с точки зрения теории поколений

Современные студенты очень быстро теряют интерес к образовательному процессу. Авторы попытались найти причины в популярной теории поколений [3]. Например, подавляющее большинство современных студентов можно отнести к «цифровому поколению». Они легко манипулируют информацией, широко используют различные гаджеты, общаются в социальных сетях. Представители поколения легко разбираются в технологиях, привыкли к многозадачности. Отсюда возникают и специфические отрицательные черты: неспособность долго концентрироваться на конкретной задаче, неприязнь к традиционным методам образования (написание конспектов, использование бумажных учебников). Выработанная способность фильтровать информацию по степени интересности и практической полезности приводит к возникновению барьеров в приобретении фундаментальных знаний.

Критическое отношение студента к информации и доступность интернет-ресурсов и других источников знаний поднимает проблему традиционного статуса преподавателя как непререкаемого авторитета, сомневаться в компетентности которого запрещается. Недостаточная интерактивность и монотонность занятий еще больше усугубляет проблему мотивации. Поэтому главными образовательными ресурсами для нового поколения чаще всего выступают видеоуроки, интернет-статьи, блоги, онлайн-курсы.

3. Развитие IT-специалиста

3.1. Профессиональные и гибкие навыки

При подготовке специалиста любого профиля важно уделять внимание формированию как профессиональных (в англоязычной литературе – «hard skills»), так и гибких навыков (англ. soft skills). В действительности это не новая парадигма в образовании, однако автоматизация труда в XX веке привела к идее о том, что образование должно быть построено на узкой специальности [10]. Человек обладает поразительной способностью приспосабливаться к новому виду деятельности, а её постоянная смена стала отличительной чертой нашего времени. Также следует учитывать, что современное поколение, развивающееся в цифровой среде, тяжело переносит монотонный труд и быстро теряет к нему интерес, что обуславливает частую смену работы или специализации.

Быстро адаптироваться и оставаться востребованным помогают гибкие навыки, которые упоминались в манифесте Международного экономического форума о навыках [11]. При массовой автоматизации всего, что только можно, ценным остается именно то, что нельзя заменить роботами. К этому можно отнести и качественное образование, педагогику.

Полный список гибких навыков вывести трудно, но различные IT-компании чаще всего обозначают свои культурные ценности. Так, например, внутри Яндекса выделяются универсальные навыки и навыки руководителей [11]. К наиболее приоритетным и востребованным можно отнести коммуникативность, умение работать в команде, критическое мышление, нацеленность на результат, адаптивность, стрессоустойчивость, готовность учиться и изучать новое.

Сложность эффективного приобретения гибких навыков заключается в необходимости воссоздания ситуаций, в которых они применимы, что не всегда просто во время классических лекционных и практических занятий. Поэтому возникает необходимость воссоздать среду, максимально возможно приближенную к той, в которой находятся специалисты-программисты. В школах, например, учат работать индивидуально, оценки являются персональным показателем академических успехов ученика, высшее образование предлагает работу в подгруппах, но этого может быть недостаточно. Именно в команде люди учатся брать на себя ответственность, распределять между собой роли, договариваться об общих целях и результатах.

Реализация проектного обучения и совместного выполнения заданий призвана помочь развитию гибких навыков. Важно учитывать проблематику, указанную ранее в тексте данной статьи, мотивация – двигатель перемен, а наиболее весомым её компонентом является интерес.

3.2. Экстремальное программирование

Экстремальное программирование (англ. Extreme programming, XP) – гибкая методология разработки программного обеспечения, применимая к небольшим и средним по размеру командам, впервые сформулированная и использованная американскими разработчиками Кентом Беком, Уордом Каннингемом (создателем концепции «вики»), Мартином Фаулером и другими в конце 90-х годов. Однако в некоторых крупных компаниях не относят экстремальное программирование к методикам и считают, что в чистом виде оно применимо крайне редко. Данную методологию называют гибкой в связи с тем, что она опирается на конкретные ценности и приёмы (рис. 1).

Рис. 1. Элементы экстремального программирования

К основным приёмам можно отнести:
– близость заказчика;
– парное программирование;
– непрерывная интеграция;
– простота проектирования;
– игра в планирование;
– частые и небольшие релизы [12].

Идея совместить приёмы экстремального программирования и образование в теории должна позволить создать необходимую для развития профессионального программиста среду. Однако важно провести анализ, выявить достоинства и недостатки, определить целесообразность использования приёмов экстремального программирования при формировании гибких и профессиональных навыков программиста в образовании.

4. Практический опыт

4.1. Первичные условия, установки и цели

Изначально исследование не планировалось заранее, не было какой-то конкретной методики и плана мероприятий, все детали формировались уже на последующих этапах – можно обозначить, что конкретной уверенности в совершенстве и работоспособности методики не было. Однако у авторов был неподдельный интерес к командообразованию, менеджменту и формированию гибких навыков как с точки зрения руководителя, так и будущего специалиста.

Ярослав Колташев и Денис Агапитов – студенты третьего курса по направлению 09.03.01 «Информатика и вычислительная техника» (ФГОС ВО 3++), профиль: программное обеспечение средств вычислительной техники и автоматизированных систем. В их группах (две разные группы курса) благодаря слаженной работе кураторов и преподавателей выпускающей кафедры велась профориентационная работа, проводились мероприятия для поднятия мотивации студентов, было организовано знакомство с учебным планом.

Для реализации личностного потенциала студентов организовывались кружки по интересам, в которых велась проектная работа. Одним из таких был кружок робототехники. Первым опытом его работы были массовые внеурочные занятия, однако это не показало большой эффективности, студенты быстро теряли интерес и уставали. Поэтому было принято решение создать небольшие команды разработки, которые работали над полезными проектами для института и участвовали в соревнованиях, таких как «IT-Планета» и «Huawei Cup».

4.2. Как искусственный интеллект помог в развитии навыков

Интерес к машинному обучению и науке о данных у Ярослава и Дениса проявился во время участия в направлении «Модели и методы искусственного интеллекта» соревнования «Huawei Cup 2021» [13]. Первоначальный уровень знаний участников был достаточно слабым, но большим плюсом участия в конкурсе являлась онлайн-школа второго этапа соревнования. Стоит отметить, что студенты участвовали в персональном зачете, но при этом изучали материал совместно, что подогревало интерес. Даже несмотря на то, что выйти в финал соревнования им не удалось, данный опыт следует рассматривать положительно с точки зрения развития интереса к ИИ, гибких и профессиональных навыков, знакомства с новыми инструментами и фреймворками в программировании.

Любой результат необходимо закреплять, иначе без практического применения интерес угасает, а навыки теряются. В 2022 году платформа «Россия – страна возможностей» продолжила развитие проекта «Цифровой прорыв», объявив сезон искусственного интеллекта. Главными целями проекта являются популяризация технологий ИИ в России среди молодых специалистов и студентов, формирование ИТ-сообщества с фокусом на ИИ, стимулирование создания решений на базе ИИ, а также создание решений на основе ИИ для бизнеса и государственного сектора [14].

Участие авторов статьи в «Цифровом прорыве» началось с окружного хакатона в г. Екатеринбурге, прошедшего в смешанном формате 24-26 июня. Окружной хакатон – это часть проекта, представляющая собой ограниченное во времени командное соревнование по созданию прототипов цифровых решений в рамках выбранного командой кейса, более половины участников которого являются жителями определенного федерального округа Российской Федерации.

Ограничение по времени, командная работа, постоянная связь с заказчиком кейса в виде прохождений контрольных точек, необходимость получения рабочего продукта в кратчайшие сроки являются элементами экстремального программирования.

Команда участвовала очно в составе из пяти человек: два разработчика в области ИИ (Я. Колташев, Д. Агапитов), разработчик пользовательских интерфейсов (англ. UI, user interface), разработчик backend-части, лидер команды (К. Брагин).

Примечательным элементом в данной команде была связка разработчиков ИИ (парное программирование). Каждый обладал своим собственным видением решения поставленной задачи, что вносило дополнительный вклад в командный и состязательный дух.

Предварительной подготовки к соревнованиям изначально не было, задачи и роли внутри команды распределялись сразу после старта. Материал, необходимый для разработки решения, приходилось изучать по мере возникновения труднорешаемых проблем. Как итог, полученный результат участия – предпоследнее место в общекомандном зачете.

Для закрепления опыта после поражения было принято решение продолжить участвовать в хакатонах и добиться не только выхода на призовое место, но и продвинуться в изучении систем искусственного интеллекта, чтобы в дальнейшем занять нишу разработчиков профессионально. Для этого было необходимо провести работу над ошибками.

Основной ошибкой являлся недостаточный опыт подготовки. В соревновании могли участвовать студенты, которые изучали ИИ по программе своего вуза (с такими соперниками действительно пришлось столкнуться), просто специалисты, уже работающие в этой сфере (заняли первое место в г. Екатеринбурге), поэтому команде необходимо было компенсировать преимущества соперников. Краткое описание задачи было доступно всем участникам за несколько недель до самого соревнования. В этот период можно было провести аналитику, предположить, каким должно быть решение и погрузиться в проблематику, изучая полезные инструменты и уже проведенные исследования.

Работа над ошибками принесла результат: уже в следующем окружном соревновании (Сибирский федеральный округ, г. Томск, дистанционное участие) команде удалось добиться 4-го места. Вновь был сделан разбор ошибок, отмечено недостаточное внимание к планированию работы и времени.

Последующие две попытки участия (Северо-Западный федеральный округ, Центральный федеральный округ) принесли попадание в пятерку лучших команд. Предположительно, такой застой связан со сложностью выбираемых задач – обе от Центрального банка Российской Федерации и требовали дополнительных знаний в области больших данных (англ. Big data) и экономики (инфляция, алгоритмы регрессии, индекс потребительских цен).

За рамками проекта «Цифровой прорыв» команда приняла участие в хакатоне от отечественной золотодобывающей компании «Полюс», где необходимо было разработать систему обнаружения негабаритов руды на движущейся конвейерной ленте. Итогом участия стало третье место, однако оно не являлось призовым по условиям соревнований.

На данном этапе было важно не допустить эмоционального выгорания участников команды, что могло перечеркнуть всю предыдущую работу. Для студентов начался новый учебный год. Было принято решение взять небольшой перерыв и вернуться к концу сезона «Цифрового прорыва».

Весь приобретенный опыт и выводы из работы над ошибками были задействованы в финальном окружном хакатоне «Цифрового прорыва» в Северо-Кавказском федеральном округе. Простая с первого взгляда задача идентификации с помощью искусственного интеллекта особей гренландских китов оказалась намного сложнее, чем изначально предполагалось. Однако это не помешало достичь значимых результатов и опередить соперников. Как итог, команда заняла первое место [15].

5. Заключение

Проблема мотивации студентов всегда будет играть одну из ключевых ролей в образовательном процессе. Технологии развиваются стремительными шагами, в актуальных и передовых областях, таких как искусственный интеллект и машинное обучение, специалисты нужны уже сейчас. Чтобы получить качественного и мотивированного профессионала, способного участвовать в развитии отрасли, необходимо учитывать черты современного «цифрового» поколения.

Проведение со студентами профориентационной работы, адаптация к будущей работе в IT-отрасли, контроль интереса и придание мотивации для движения к достижимым целям – все это должно реализовываться систематически. Конечно, во многих школах уже ведется такая работа, и она приносит свои плоды, но вероятность ситуации, в которой студенты старших курсов не до конца понимают, какой деятельностью они желают заниматься после выпуска, весьма высока.

Работа по развитию профессиональных и гибких навыков должна вестись в различных форматах, таких как познавательные часы куратора, курс «Введение в профессию», командные игры, участие в хакатонах и соревнованиях, развитие проектной деятельности. Работа в команде является дополнительным фактором мотивации, так как участники прикладывают больше усилий, чтобы не подводить своих коллег.

Использование приёмов экстремального программирования в образовании сопряжено с определенными рисками. Так же, как и в реальной профессиональной деятельности, важно уделять внимание эмоциональному выгоранию студентов, формировать умение выставлять приоритеты задачам, учить рационально использовать время.

Важно учитывать, что данная работа практически невозможна без грамотного наставника, способного организовать деятельность группы, направить студентов, подсказать ответы на интересующие их вопросы. Вопрос подготовки таких наставников заслуживает отдельного внимания.

Результатом данного исследования можно назвать не только достижение студентами призового места во всероссийском конкурсе, но и сформировавшееся стремление дальше развиваться в области искусственного интеллекта, желание попасть на стажировку, участвовать в мероприятиях большего масштаба, при этом, перспективы уже не настолько туманны.

Для закрепления результатов и формирования дополнительной доказательной базы необходимо воспроизвести исследование повторно, что позволит взглянуть на него с других, ранее неизученных, сторон.

Выражение благодарности

Авторы выражают благодарность коллегам из команды «ИИнтеграция» за совместную работу в соревнованиях и самоотверженный труд, без которых не было бы возможно достижения таких значительных результатов и успехов. Также, коллектив команды выражает слова признательности организаторам проекта «Цифровой прорыв», способствующих раскрытию молодых талантов и профессионалов.

Литература

1. Конференция по искусственному интеллекту // Президент России: [сайт]. URL: http://www.kremlin.ru/events/president/transcripts/69927 (дата обращения: 01.12.2022).
2. «Цифровая экономика РФ» // Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации: [сайт].URL: https://digital.gov.ru/ru/activity/directions/858/#section-docs (дата обращения: 28.111.2022).
3. Теория поколений: как она работает и работает ли вообще // РБК Тренды: [сайт]. URL: https://trends.rbc.ru/trends/education/6156efb59a79477bf9ca5893 (дата обращения: 28.11.2022).
4. *Дуэк К.* Гибкое сознание. Новый взгляд на психологию развития взрослых и детей М.: Манн, Иванов и Фербер, 2022. 304 с. ISBN 978-5-00057-927-5.
5. *Стародубцева В. К.* Мотивация студентов к обучению // Современные проблемы науки и образования. 2014. № 6. С. 432.
6. *Беганцова И. С., Болотин Е. Ю., Завражнов В. В., Щелина Т. Т.* Профориентационная работа с молодежью как социально- и психолого-педагогическая проблема // Russian Journal of Education and Psychology. 2011. Т. 2, № 6. С. 154–157.
7. *Михайлов А. Н., Наумова А. Г., Стародуб К. А.* Проблемы профориентационной работы в вузе и пути их решения // Образование и право. 2019. № 4. С. 255–259.
8. Индивидуальные образовательные траектории в российских вузах // Министерство науки и высшего образования Российской Федерации: [сайт]. URL: https://www.minobrnauki.gov.ru/press-center/news/novosti-ministerstva/21499/ (дата обращения: 30.11.2022).
9. Индивидуальные образовательные траектории в университете: ключевые точки внедрения. Опыт ТюмГУ // Forbes Education: [сайт]. URL: https://education.forbes.ru/special-projects/iot-main/iot-unmn (дата обращения: 30.11.2022).
10. *Раицкая Л. К., Тихонова Е. В.* Soft skills в представлении преподавателей и студентов российских университетов в контексте мирового опыта // Вестник российского Университета дружбы народов. Серия: Психология и педагогика. 2018. Т. 15, № 3. С. 350–363.
11. Что такое soft skills и зачем им нужно учиться на самом деле? // Академия Яндекса: [сайт]. URL: https://academy.yandex.ru/journal/chto-takoe-soft-skills-i-zachem-im-nuzhno-uchitsya-na-samom-dele (дата обращения: 02.12.2022).
12. *Ауэр К., Миллер Р.* Экстремальное программирование: Постановка процесса с первых шагов до победного конца. СПб.: Питер, 2003. 368 с.
13. Huawei Cup: [сайт]. URL: https://huaweicup.ru/ (дата обращения: 04.12.2022).
14. Цифровой прорыв 2022: хакатоны и чемпионаты по искусственному интеллекту: [сайт]. URL: https://hacks-ai.ru/ (дата обращения: 04.12.2022).
15. Уральские айтишники разработали для Минприроды РФ систему идентификации гренландских китов на основе данных, полученных с дронов // Официальный сайт Правительства Свердловской области: [сайт]. URL: https://midural.ru/news/list/document207545/ (дата обращения: 04.12.2022)

Брагин Кирилл Игоревич
старший преподаватель, аспирант кафедры инфокоммуникационных технологий и мобильной связи, Уральский технический институт связи и информатики (УрТИСИ СибГУТИ, 620109, Екатеринбург, ул. Репина, д. 15), e-mail: braga.k.urtisi@gmail.com, ORCID ID: 0000-0003-4334-0307.

Агапитов Денис Вадимович
студент, Уральский технический институт связи и информатики (УрТИСИ СибГУТИ), e-mail: koshkidadanet@gmail.com, ORCID ID: 0000-0002-3008-5469.

Колташев Ярослав Андреевич
студент, Уральский технический институт связи и информатики (УрТИСИ СибГУТИ), e-mail: y.koltashev@mail.ru, ORCID ID: 0000-0003-3007-4863.

Авторы прочитали и одобрили окончательный вариант рукописи.
Авторы заявляют об отсутствии конфликта интересов.
Вклад соавторов: *Каждый автор внес равную долю участия как во все этапы проводимого теоретического исследования, так и при написании разделов данной статьи.*

Extreme Programming as a Method for Developing Student's Soft and Hard Skills in IT Industry

Kirill I. Bragin, Denis V. Agapitov, Yaroslav A. Koltashev

Ural Technical Institute of Communications and Informatics (UTICI SibSUTIS, Yekaterinburg)

Abstract: In this paper, the experience of using extreme programming as a method for developing student's soft and hard skills is presented. The practical implementation of professional education during the participation of IT students in competitions, championships and hackathons in the field of artificial intelligence organized at the country level and by IT companies is considered.

Keywords: extreme programming, hackathon, digital breakthrough, machine learning, artificial intelligence, motivation, soft skills.

For citation: Bragin K. I., Agapitov D. V., Koltashev Y. A. Extreme programming as a method for developing student's soft and hard skills in IT industry (in Russian). *The SibSUTIS Bulletin*, 2023, vol. 17, no. 2, pp. 12-21. https://doi.org/10.55648/1998-6920-2023-17-2-12-21.

The article was submitted: 26.12.2022;
accepted for publication 10.01.2023.

References

1. *Konferentsiya po iskusstvennomu intellektu* [Artificial Intelligence conference. President of Russia], available at: http://www.kremlin.ru/events/president/transcripts/69927 (accessed: 01.12.2022).

2. *Tsifrovaya ekonomika RF* [Digital economy in Russian Federation], available at: https://digital.gov.ru/ru/activity/directions/858/#section-docs (accessed: 28.11.2022).
3. *Teorija pokolenij: kak ona rabotaet i rabotaet li voobshhe* [The theory of generations: how it works and whether it works at all], available at: https://trends.rbc.ru/trends/education/6156efb59a79477bf9ca5893 (accessed: 28.11.2022).
4. Carol S. Dweck. *Gibkoe soznanie. Novyj vzgljad na psihologiju razvitija vzroslyh i detej* [Mindset. The New Psychology of Success]. Moscow, Mann, Ivanov i Ferber, 2022. 304 p.
5. Starodubceva V.K. Motivacija studentov k obucheniju [Motivating students to learn]. *Sovremennye problemy nauki i obrazovanija*, Moscow, 2014, no. 6, p. 432.
6. Begancova I.S., Bolotin E.Ju., Zavrazhnov V.V., Shhelina T.T. Proforientacionnaja rabota s molodezh'ju kak social'no- i psihologo-pedagogicheskaja problema [Career guidance with young people as a social and psychological and pedagogical problem]. *Russian Journal of Education and Psychology*, 2011, vol. 2, no. 06, pp. 154-157.
7. Mihajlov A. N, Naumova A. G., Starodub K. A. Problemy proforientacionnoj raboty v VUZe i puti ih reshenija [Problems of career guidance work in the university and ways to solve them]. *Obrazovanie i parvo*, 2019, no. 4, pp. 255-259.
8. *Individual'nye obrazovatel'nye traektorii v rossijskih vuzah* [Individual educational trajectories in Russian universities], available at: https://www.minobrnauki.gov.ru/press-center/news/novosti-ministerstva/21499/ (accessed: 30.11.2022).
9. *Individual'nye obrazovatel'nye traektorii v universitete: kljuchevye tochki vnedre-nija. Opyt TjumGU* [Individual educational trajectories at the university: key points of implementation. Experience of Tyumen State University], available at: https://education.forbes.ru/special-projects/iot-main/iot-unmn (accessed: 30.11.2022).
10. L. K. Raickaja, E. V. Tihonova. Soft skills v predstavlenii prepodavatelej i studentov rossijskih universitetov v kontekste mirovogo opyta [Soft skills in the representation of teachers and students of Russian universities in the context of world experience]. *Vestnik rossijskogo Universiteta druzhby narodov. Serija: psihologija i pedagogika*, 2018, vol. 15, no. 3, pp. 350-363.
11. *Chto takoe soft skills i zachem im nuzhno uchit'sja na samom dele?* [What are soft skills and why do they need to actually learn?], available at: https://academy.yandex.ru/journal/chto-takoe-soft-skills-i-zachem-im-nuzhno-uchitsya-na-samom-dele (accessed: 02.12.2022).
12. Auer Ken, Miller Roy. *Jekstremal'noe programmirovanie: Postanovka processa s pervyh shagov do pobednogo konca* [Extreme Programming Applied: Playing to Win]. Saint Petersburg, Piter, 2003. 368 p.
13. Huawei Cup, available at: https://huaweicup.ru/ (accessed: 04.12.2022).
14. *Cifrovoj proryv 2022: hakatony i chempionaty po iskusstvennomu intellektu* [Digital breakthrough 2022: Hackathons and AI championships], available at: https://hacks-ai.ru/ (accessed: 04.12.2022).
15. *Ural'skie ajtishniki razrabotali dlja Minprirody RF sistemu identifikacii gren-landskih kitov na osnove dannyh, poluchennyh s dronov* [Ural IT specialists have developed a system for identifying Green Land whales for the Ministry of Natural Resources of the Russian Federation based on data obtained from drones], available at: https://midural.ru/news/list/document207545 (accessed 04.12.2022).

Kirill I. Bragin
Senior lecturer, post-graduate student, Ural Technical Institute of Communications and Informatics (UTICI SibSUTIS, Yekaterinburg, Russia), braga.k.urtisi@gmail.com, ORCID ID: 0000-0003-4334-0307.

Denis V. Agapitov
Student, Ural Technical Institute of Communications and Informatics (UTICI SibSUTIS, Yekaterinburg, Russia), koshkidadanet@gmail.com, ORCID ID: 0000-0002-3008-5469.

Yaroslav A. Koltashev
Student, Ural Technical Institute of Communications and Informatics (UTICI SibSUTIS, Yekaterinburg, Russia), y.koltashev@mail.ru, ORCID ID: 0000-0003-3007-4863.

DOI: 10.55648/1998-6920-2023-17-2-22-36 УДК 512.876.5

Комплексное применение моделей системной динамики и агентного моделирования для принятия управленческих решений при внедрении инновационной технологии

Д. А. Клавсуц

Новосибирский государственный технический университет (НГТУ)

Аннотация: В работе предложен новый методический подход, направленный на развитие имитационных моделей системной динамики и агентного моделирования в условиях, когда предприятие внедряет инновационную запатентованную технологию на новых рынках, что требует разработки новых бизнес-моделей, стратегий, коммуникационных процессов. Действующие модели решения этих задач реализованы в системе имитационного моделирования AnyLogic.

Ключевые слова: инновационная технология управления качеством потребляемой электроэнергии, управленческие решения, долгосрочное прогнозирование, стратегическое планирование, имитационное моделирование рынка инновационных технологий, системная динамика, агентное моделирование.

Для цитирования: Клавсуц Д. А. Комплексное применение моделей системной динамики и агентного моделирования для принятия управленческих решений при внедрении инновационной технологии // Вестник СибГУТИ. 2023. Т. 17, № 2. С. 22–36. https://doi.org/10.55648/1998-6920-2023-17-2-22-36.

Статья поступила в редакцию 18.12.2022;
переработанный вариант – 04.02.2023;
принята к публикации 16.02.2023.

1. Введение

Одной из важнейших задач, возникающих при внедрении инновационных технологий, является разработка эффективных стратегических управленческих решений, позволяющих повысить точность и качество планирования инвестиций для управления производством на основе долгосрочного прогнозирования поведения рынка потенциальных пользователей этих технологий.

Объектом эмпирического исследования в работе является отечественное научно-производственное предприятие г. Новосибирска, занимающееся разработкой, производством и внедрением актуальной в мире высокотехнологичной электротехнической продукции. Производимые предприятием устройства – нормализаторы электроэнергии – являются инновационной запатентованной в 38 странах технологией управления качеством потребляемой электроэнергии. Устройства являются технологическим элементом и основным инструментом как традиционных, так и современных интеллектуальных электрических сетей. Применение устройств актуально для всех потребителей электрической энергии на уровне 0.4 кВ, приобретающих электрическую энергию (мощность) для собственных бытовых и производ-

ственных нужд: зданий, сооружений, промышленного оборудования, уличного освещения от одной единицы электрооборудования до комплекса зданий как на действующих, так и на строящихся объектах. При подключении устройств к электрическим сетям на стороне конечных потребителей улучшаются стандартизированные параметры качества и регулируется потребление электроэнергии, что позволяет существенно экономить все энергоресурсы в электроэнергетических системах любой страны мира [1–8].

Практические задачи научно-производственного предприятия по планированию инвестиций, как и многих других подобных, ставят управленческие проблемы и вопросы, требующие проведения научных исследований. В работе исследованы модели внедрения инновационной технологии управления качеством потребляемой электроэнергии в сегментах средних и малых предприятий города Новосибирска, РФ.

Автором разработаны имитационные модели прогнозирования поведения рынка инновационных технологий, основанные на концепции Ф. Басса [9] о разделении агентов рынка на инноваторов и имитаторов, которые функционируют под действием разных тенденций, имеющих существенное значение для продвижения инновационной технологии. Знание этих тенденций и регулируемых параметров позволяет их идентифицировать и эффективно управлять долгосрочным процессом внедрения инновационной технологии. Исследованы и реализованы две парадигмы имитационного моделирования: системная динамика [10] и агентный подход [11, 12]. Проведено их сравнение, показано, что они дают близкие результаты, что позволяет повысить обоснованность принимаемых решений. Простейшая действующая модель этой задачи реализована и доступна для исследований в системе имитационного моделирования AnyLogic [13–14].

Известно, что применение модели Ф. Басса для нескольких рынков мало изучено и исследовано на практике. В работе предложен новый методический подход к развитию этой модели в условиях, когда исследуемое инновационное предприятие выходит на несколько новых сегментов рынка. Выдвигаются и исследуются гипотезы о возникновении и значимом развитии коммуникаций между различными рыночными сегментами. Информация о динамике распространения инновационной технологии в одном из сегментов может влиять на поведение агентов в другом сегменте, и наоборот. Введение таких связей в разработанные автором имитационные модели происходит естественно и технически просто, однако их использование требует дополнительных исследований. Массовые имитационные прогоны разрабатываемых моделей с введением новых рыночных связей и параметров позволяют точнее понять механизмы поведения рынка инновационной запатентованной технологии, использовать эти механизмы для развития моделей, строить обоснованные долгосрочные прогнозы, разрабатывать реалистичные производственные планы, повысить эффективность управления внедрением инновационных технологий.

В разделах 2 – 3 рассматривается традиционный вариант по моделированию внедрения инновационной технологии. Предполагается, что рынки изолированы, не взаимодействуют между собой, хотя они могут внедрять схожие виды инновационной продукции. Для каждого рынка разрабатывается свой независимый проект. Причем проекты, как правило, выполняются последовательно. Исторически это оправдано. Действительно, молодые, бурно развивающиеся инновационные предприятия, как правило, начинают с небольших рынков или рыночных сегментов. И только после освоения нескольких сегментов, наработки опыта могут ставить задачу принципиального роста масштаба.

В разделе 2 исследуется простая системно-динамическая модель на примере внедрения инновационной технологии на изолированных сегментах рынка г. Новосибирска – средних и малых предприятиях. Модель подробно описывается, интерпретируются полученные результаты.

В разделе 3 исследуется агентная модель внедрения инновационной технологии на примере тех же изолированных сегментов рынка г. Новосибирска – средних и малых предприятиях. Описывается диаграмма состояний модели, показано, что полученные результаты сов-

падают с результатами системно-динамической модели, что повышает обоснованность решений.

В разделе 4 ставится новая важная для научно-производственного предприятия задача о выводе инновационной технологии сразу на несколько рынков (или рыночных сегментов) в рамках единого более масштабного проекта. Это позволяет перевести проекты на качественно новый уровень: получить эффект за счет масштаба производства, эффективного распределения ресурсов, сокращения затрат на продвижение и сопровождение внедрения технологии. Выдвигаются и исследуются гипотезы о существовании и развитии коммуникаций между рыночными сегментами и, в частности, о взаимном влиянии информации на различных сегментах рынка о распространении инновационной технологии.

Разработана имитационная системно-динамическая модель внедрения инновационной технологии совместно на нескольких сегментах рынка, в которую введены новые связи, соответствующие выдвинутым гипотезам. Представлен вариант совместной модели внедрения инновационной технологии для двух исследованных ранее сегментов рынка – средних и малых предприятий г. Новосибирска. Приведены результаты моделирования, на основе которых сформулированы управленческие решения по планированию производства инновационного предприятия. Даны рекомендации по разработке аналогичной агентной модели.

В заключении приводятся выводы о результатах работы, сформулированы управленческие решения по внедрению инновационной технологии на группы рыночных сегментов, особенности и ограничения модели Басса, ее реализации в AnyLogic, рекомендации по их использованию.

2. Модель системной динамики внедрения на изолированном рынке

Традиционные примеры реализации модели Ф. Басса распространения инноваций описывают поведение только одного рынка, причем розничного [9]. Распространение рассматриваемой в данной работе инновационной технологии управления качеством потребления электроэнергии происходит на нескольких различных рынках, на территориях, где технология защищена патентами (Россия, страны Евросоюза, Северной Америки, ЕАЭС), а также сегментов отдельных рынков (предприятия государственного и частного сектора, предприятия разных отраслей, предприятия средние, малые и т.п.). В данной работе рассматривается новосибирский рынок потенциальных потребителей инновационной технологии. На рынке могут присутствовать как розничные потребители, так и оптовые, причем разного уровня. Среди оптовых потребителей важное место занимают сегменты средних и малых предприятий. В качестве других сегментов могут также выступать потребители электрической энергии крупного бизнеса, разных отраслей и т.д.

В работе исследования проводятся в сегментах средних и малых предприятий. На настоящий момент в г. Новосибирске в качестве потенциальных клиентов инновационной технологии могут выступать до 5 тысяч малых и до 300 средних предприятий [оценка на основе источника: Малое и среднее предпринимательство Новосибирска `http://www.mispnsk.ru`].

Концепция системной динамики носит «централизованный» характер. При этом предполагаются известными общие закономерности поведения системы. Важной является структура различного типа связей и элементов модели – накопителей, потоков, факторов, параметров, переменных. Связи определяют динамику поведения всей системы, что позволяет прогнозировать её развитие. Причем даже для инновационных технологий, когда ещё нет или недостаточно ретроспективных данных.

Рассмотрим сначала применение для каждого отдельного сектора (средних и малых предприятий) простейшей модели системной динамики, ориентированной на типовые рынки, представленной разработчиками AnyLogic [13]. Традиционная модель системной динамики показана на рис. 1.

Обозначения модели на рис. 1:

PotentialAdopters – накопитель. Общее число потенциальных пользователей в текущий момент модельного времени. Начальное значение задаётся параметром TotalPopulation.

Adopters – накопитель. Число пользователей, установивших нормализаторы в текущий момент модельного времени. В начале эксперимента это число равно нулю: накопитель пуст.

TotalPopulation – параметр. Общее количество потенциальных пользователей инновационной технологии.

AdoptionRate – поток (скорость) внедрения инновационной технологии.

Market Saturation – отрицательная балансирующая (уравновешивающая, самокорректирующаяся) обратная связь. Результат прямого влияния продуктов маркетинга и рекламы на потенциальных пользователей инновационной технологии.

AdoptionFromAd – динамическая переменная. Фактор. Маркетинговые мероприятия.

AdEffectiveness – параметр. Эффективность маркетинговых мероприятий.

Word of Mouth – усиливающая обратная связь. Внедрение под влиянием «сарафанного радио».

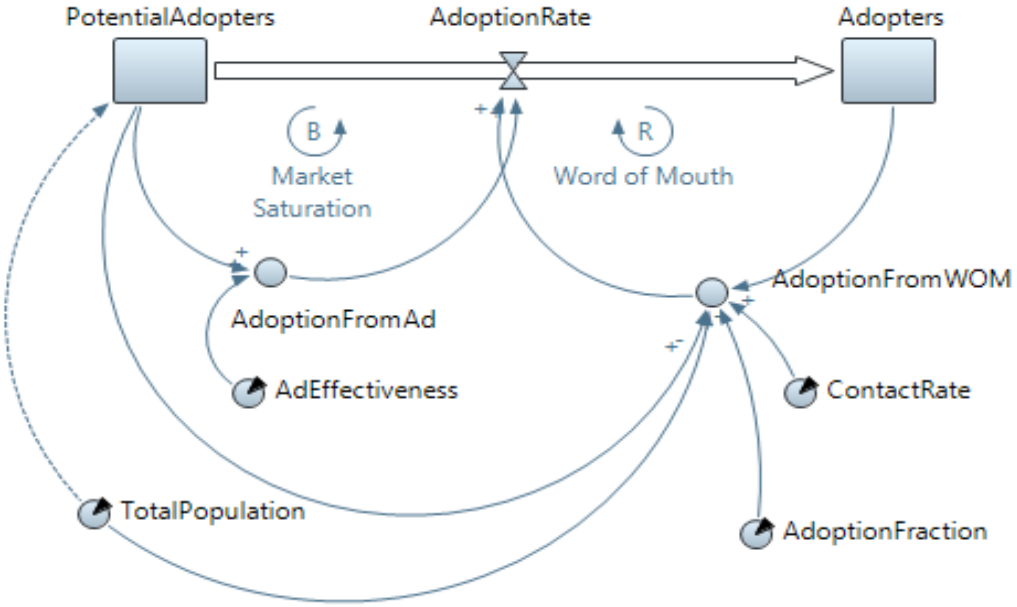

Рис. 1. Традиционная модель системной динамики

AdoptionFromWOM – динамическая переменная. Фактор. «Сарафанное радио».

ContactRate – параметр. Частота контактов в год потенциальных пользователей.

AdoptionFraction – параметр. Сила убеждения клиента, внедрившего инновационную технологию, влияние на фактор «сарафанное радио».

В представленной модели связь между накопителями – это поток внедрения инновационной технологии (устройств – нормализаторов) AdoptionRate, преобразующий потенциальных пользователей PotentialAdopters в пользователей инновационной технологии Adopters. Факторами, влияющими на накопители и поток, в представленной модели выбраны система направленного информационного влияния – AdoptionFromAd и внутрирыночные коммуникации – AdoptionFromWOM.

Регулируемым параметром для фактора AdoptionFromAd является её эффективность – AdEffectiveness (по рекомендации разработчиков принят типовой уровень 0.011), а для фактора внутрирыночных коммуникаций AdoptionFromWOM – численность популяции TotalPopulation (300 средних и 5 тысяч малых предприятий), частота контактов ContactRate, (в рассматриваемом примере 100 контактов в год среди участников Word of Mouth – «сарафанного радио», когда информация об инновационной технологии получена из уст как по-

тенциальных пользователей, так и пользователей инновационной технологии) и сила убеждения AdoptionFraction (0.015).

Первая обратная связь Market Saturation в модели – отрицательная, уравновешивающая, самокорректирующаяся. Усиление фактора AdoptionFromAd увеличивает число Adopters и уменьшает число потенциальных пользователей PotentialAdopters. Это ограничивает рост фактора и приводит к его снижению. Вторая обратная связь в модели так же уравновешивающая: увеличение Adopters под влиянием внутрикластерных коммуникаций AdoptionFromWOM увеличивает число Adopters и уменьшает число PotentialAdopters. Это также ограничивает рост фактора AdoptionFromWOM и приводит к его снижению. Третья обратная связь в модели – положительная, усиливающая. Увеличение внедрений нормализаторов под влиянием AdoptionFromWOM увеличивает число Adopters. Это приводит к еще большему росту AdoptionRate под влиянием AdoptionFromWOM и к падению со временем доли влияния системы направленного информационного влияния на поток AdoptionRate.

Поток внедрений устройств – нормализаторов AdoptionRate задается как производная по времени PotentialAdopters со знаком минус и Adopters со знаком плюс, как в выражении:

$$\begin{gathered}\frac{\mathrm{d}\left(\mathrm{PotentialAdopters}\right)}{\mathrm{dt}} = -\mathrm{AdoptionRate}, \\ \frac{\mathrm{d}\left(\mathrm{Adopters}\right)}{\mathrm{dt}} = \mathrm{AdoptionRate}.\end{gathered} \tag{1}$$

Модель предполагает следующие допущения:

1. Система направленного информационного влияния и внутрирыночные коммуникации влияют на поток AdoptionRate аддитивно и с одинаковым весом, как представлено в выражении:

$$\mathrm{AdoptionRate} = \mathrm{AdoptionFromAd} + \mathrm{AdoptionFromWOM}. \tag{2}$$

2. Поток внедрений устройств – нормализаторов под влиянием системы направленного информационного влияния – это произведение параметров эффективности системы направленного информационного влияния и количества потенциальных потребителей, как представлено в выражении:

$$\mathrm{AdoptionFromAd} = \mathrm{AdEffectiveness} \times \mathrm{PotentialAdopters}. \tag{3}$$

3. Поток внедрений устройств – нормализаторов под влиянием внутрикластерных коммуникаций AdoptionFromWOM – это произведение количества внедривших Adopters, количества контактов ContactRate, силы убеждения AdoptionFraction и доли PotentialAdopters в популяции TotalPopulation, как представлено в выражении:

$$\begin{gathered}\mathrm{AdoptionFromIC} = \mathrm{Adopters} \times \mathrm{ContactRate} \times \mathrm{AdoptionFraction} \times \frac{\mathrm{PotentialAdopters}}{\mathrm{TotalPopulation}} \mathrm{AdoptionFromWOM} = \mathrm{Adopters} \times \mathrm{ContactRate} \times \mathrm{AdoptionFraction} \times \\ \times \mathrm{PotentialAdopters} / \mathrm{TotalPopulation}.\end{gathered} \tag{4}$$

Все приведённые формулы (1) – (4) используются в AnyLogic при формировании модели системной динамики, представленной на рис. 1.

Исходные данные для моделирования сведены в табл. 1.

Таблица 1. Данные для моделирования внедрения инновационной технологии на рынке г. Новосибирска

Сектор рынка	TotalPopulation	AdEffectiveness	ContactRate	AdoptionFraction
Средние предприятия	300	0.011	100 в год	0.015
Малые предприятия	5000	0.011	100 в год	0.015

Текущие мгновенные результаты эксперимента непрерывно отображаются на всех элементах модели системной динамики, что неудобно представить в печатном виде на статическом рис. 1. Поэтому в модели есть возможность формировать динамически меняющиеся графики внедрения инновационной технологии.

На левом графике рис. 2. представлена динамика внедрения инновационной технологии в г. Новосибирске в рыночном сегменте средних предприятий на момент окончания эксперимента. На правом графике рис. 2 представлена динамика результатов моделирования внедрения инновационной технологии в сегменте малых предприятий.

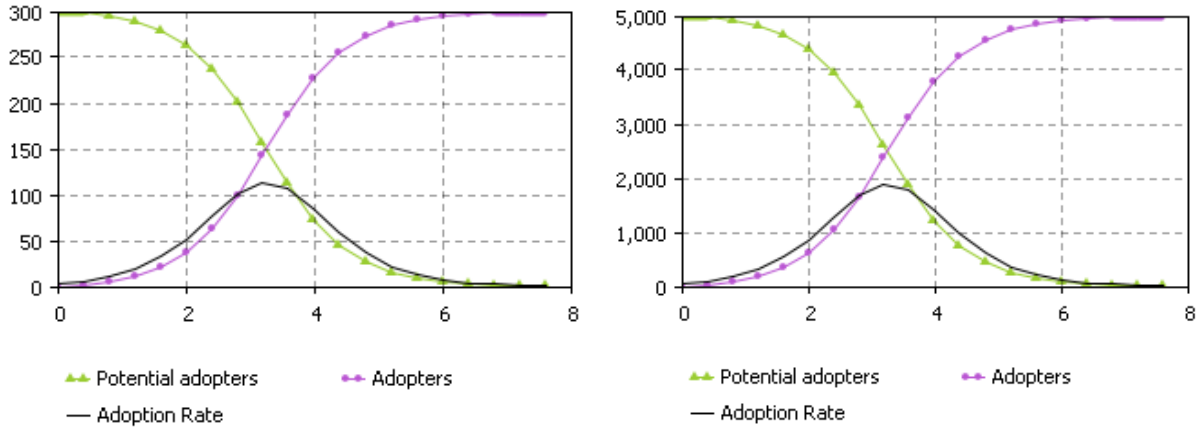

Рис. 2. Результаты системно-динамического моделирования внедрения инновационной технологии в сегментах рынка средних (левый график) и малых (правый график) предприятий

На рис. 2 видно, что число Adopters (внедривших инновационную технологию) в обоих сегментах растет от нуля в момент старта проекта до максимума (TotalPopulation) к концу восьмого года. Кривая роста имеет симметричный относительно точки перегиба S-образный вид. Число PotentialAdopters, наоборот, падает от максимума (TotalPopulation) до нуля к концу восьмого года. Поток внедрения AdoptionRate имеет колоколообразный вид и достигает максимума в момент времени, соответствующий точке перегиба S-образных кривых PotentialAdopters и Adopters. Для производителя это означает, что если, например, он планирует в основном обеспечить инновационным устройством сектор рынка примерно за 8 лет, как в показанном примере, то при выбранных параметрах модели его производственная программа должна соответствовать показанным на рис. 2 кривым. Причем пик внедрения инновационной технологии (устройств – нормализаторов) в обоих сегментах следует ожидать к началу четвертого года проекта (максимум кривой AdoptionRate), и производство должно быть к этому готово.

Главная задача при работе с подобными моделями – измерить и задать фактические рыночные параметры, представленные в табл. 1.

Эксперименты с моделью дают возможность разрабатывать более обоснованные производственные решения, повышая их эффективность. Предприятие – производитель инновационного продукта может увеличивать емкость рынка за счет, например, выпуска устройств, настроенных на конкретного клиента, постоянных внедрений модифицированных устройств,

соответствующих развитию как традиционных, так и современных интеллектуальных электрических сетей, позволяющих повысить эффективность управления качеством потребления электроэнергии. Кроме того, предприятие – производитель инновационного продукта может использовать коммуникации, возникающие между отдельными рынками и секторами рынков. Этот подход будет рассмотрен в данной работе.

3. Агентная модель внедрения на изолированном рынке

В этом разделе на примере рассмотренной задачи внедрения инновационной технологии обсудим методические основы агентного подхода, альтернативные системной динамике. Агент – это сущность, которая обладает активностью, автономным поведением, может принимать решения в соответствии с некоторым набором правил, может взаимодействовать с окружением и другими агентами, а также может изменяться (эволюционировать) [15]. Концепция агентного подхода, в отличие от системной динамики, носит «децентрализованный» характер, когда неизвестны общие закономерности системы, но известны правила поведения каждого отдельного элемента (агента), в нашем случае предприятия, внедряющего у себя инновационную технологию. Взаимодействия таких агентов и определяют закономерности поведения всей системы, что позволяет строить достоверные прогнозы и проводить обоснованное планирование [16]. Цель агентных моделей – получить представление о глобальных правилах, общем поведении системы, исходя из предположений об индивидуальном, частном поведении ее отдельных активных объектов и взаимодействии этих объектов в системе [17].

AnyLogic предоставляет для разработки агентных моделей набор средств визуальной графической разработки: стейтчарты, события, таймеры, синхронное и асинхронное планирование событий.

Если системно-динамические и агентные имитационные модели адекватно описывают систему, то можно ожидать, что они дадут близкие результаты прогнозов. И наоборот, близость результатов моделирования, полученных с помощью разных подходов, может выступать критерием адекватности моделей. Это утверждение и определяет концепцию данной работы.

На рис. 3 показана диаграмма состояний – основная часть агентной модели диффузии Ф. Басса. Модель представлена разработчиками AnyLogic PLE и называется Bass Diffusion Agent Based.

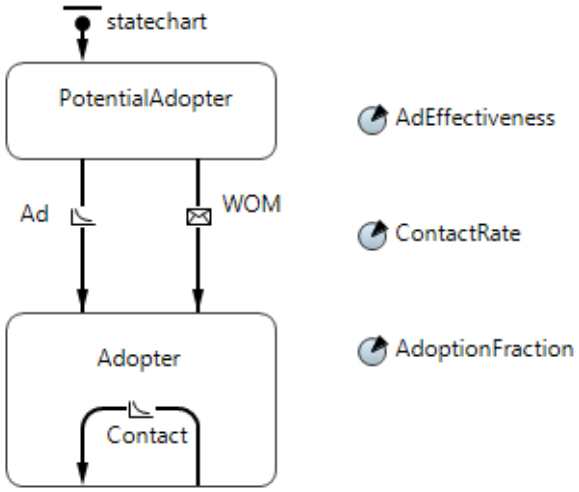

Рис. 3. Диаграмма состояний агентной модели внедрения инновационной технологии на изолированном рынке

Агент в описываемой автором системе – это потребитель инновационной технологии. Диаграмма состояний описывает поведение каждого отдельного потребителя рынка. Прямо-

угольники описывают состояния потребителя. Их в модели два: PotentialAdopter и Adopter. Это напоминает накопители в системной динамике. Но смысл они имеют другой. В системной динамике названия накопителей имели множественное число (PotentialAdopters и Adopters), другую размерность – количество предприятий. А здесь это состояния потребителя. Именем Statechart названо начало диаграммы состояний. Оно направлено в состояние PotentialAdopter. Поэтому состояние PotentialAdopter – начальное. Это состояние диаграммы означает, что потребитель еще не приобрел технологию. Состояние Adopter должно становиться активным в момент приобретения агентом технологии.

Время, необходимое для принятия решения о приобретении технологии, экспоненциально зависит от подверженности агента влиянию маркетинговых мероприятий. Поэтому переход, представленный стрелкой Ad (влияние маркетинговых мероприятий), в системе задается свойством «Происходит с заданной интенсивностью». Интенсивность этого перехода задается параметром AdEffectiveness (верхний параметр на рис. 3).

Переход WOM (влияние общения) задается свойством «Происходит при получении сообщения». Сообщение в этом примере задается строкой «Buy!» (на диаграмме состояний не показывается).

Еще один переход, представленный стрелкой Contact, задается свойством «Происходит с заданной интенсивностью». Интенсивность этого перехода задается произведением параметров ContactRate*AdoptionFraction (средний и нижний параметры на рис. 3). Действие перехода задается выражением (на диаграмме состояний не показывается) «send («Buy!», RANDOM_CONNECTED)». То есть случайно формируется сообщение «Buy!» для запуска перехода WOM. Так работает агентная модель Басса.

Представление (презентация) выполнения имитационной агентной модели может иметь различный дизайн. Один из вариантов приведен на рис. 4.

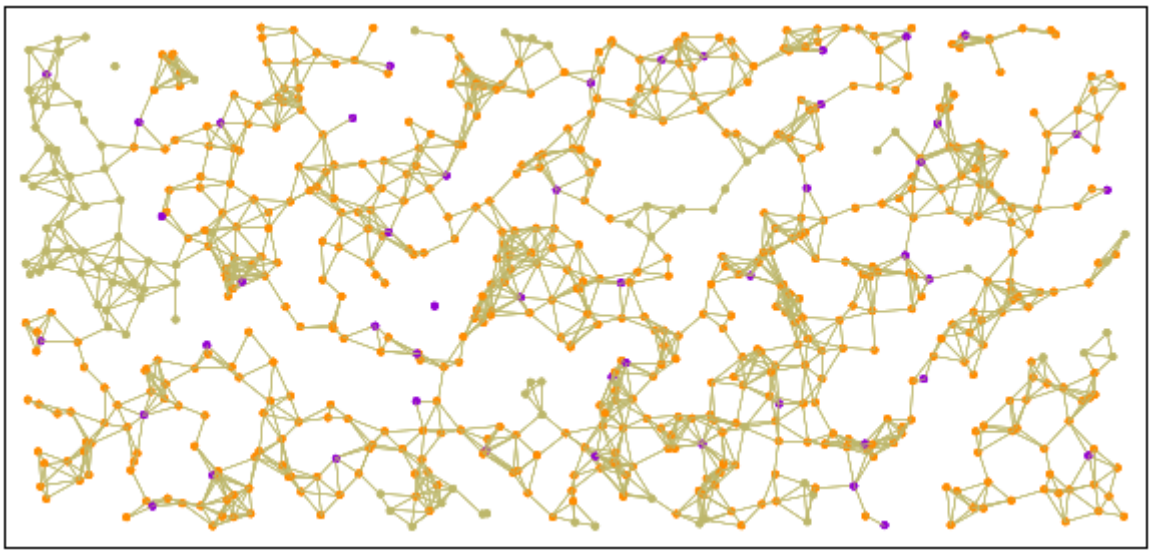

Рис. 4. Презентация мгновенного состояния агентной модели внедрения инновационной технологии на изолированном рынке

В данном случае состояния и связи агентов показаны точками и линиями в непрерывном двухмерном пространстве. Цвета точек показывают, под влиянием чего произошло приобретение технологии – маркетинговых мероприятий или «сарафанного радио». Линиями показаны агенты, между которыми происходил обмен информацией. Фиолетовыми точками обозначены предприятия-инноваторы, внедрившие (приобретшие) инновационный продукт на основе исключительно маркетинговых мероприятий, при этом, одна фиолетовая точка без линий связи (в центральной части рисунка) – предприятие-инноватор, внедрившее (приобретшее) инновационный продукт, но не имевшее контактов с другими предприятиями, т.е. не участвующее в процессе продвижения инновационной технологии на основе «сарафанного

радио». Желтыми точками обозначены предприятия, внедрившие инновационную технологию и передавшие информацию другим потенциальным покупателям под влиянием «сарафанного радио». Серыми точками обозначены предприятия, от которых исходила информация, и те, которые внедрили (приобрели) инновационную технологию и передали информацию другим предприятиям.

Основным результатом имитации агентной модели являются графики кривых распространения инновационной технологии, представленные на рис. 5.

Эти графики получены для тех же изолированных сегментов рынка – средних и малых предприятий, внедряющих инновационную технологию, с теми же параметрами, которые задавались в табл. 1 для системной динамики. Для нас важно, что агентный подход дает точно такие же результаты, что и системная динамика. График внедрения, полученный по агентной модели, совпадает с графиком на рис. 3.

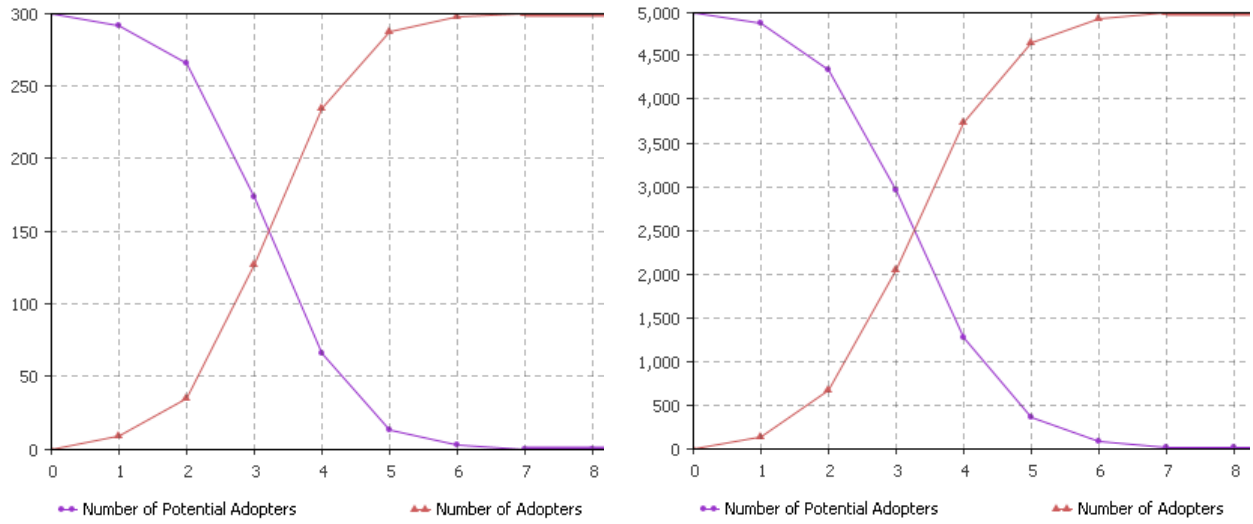

Рис. 5. Результаты агентного моделирования внедрения инновационной технологии в изолированных сегментах рынка средних (левый график) и малых (правый график) предприятий

Агентные модели наглядны. Можно на экране компьютера наблюдать в модельном времени переход потребителей из обычного состояния в состояние внедрения инновационной технологии. Трехмерная анимация, привязка к конкретным картам регионов на графических информационных системах (ГИС) дает дополнительные возможности для моделирования.

4. Модель внедрения на связанных рынках

В данном разделе модель Ф. Басса дополняется предположением о существовании и значимом развитии коммуникаций между рынками и рыночными сегментами. Это дополнение совершенно естественно для малых и средних предприятий, приобретающих инновационные устройства. Информация о динамике распространения инновационной технологии в одном из сегментов может быть использована и влиять на поведение агентов в другом сегменте, и наоборот. При этом открываются новые возможности управления внедрением инновационной технологии. Введение таких связей в разрабатываемые имитационные модели требует дополнительных исследований.

Итак, предположим, что сегменты предприятий г. Новосибирска имеют информационные связи. Например, через сайт завода-производителя, на котором разработчик инновационной технологии решил оперативно публиковать статистику её внедрения. Эта информация служит основанием для появления коммуникаций между сегментами рынка, что должно влиять на поведение рынка в целом. Назовем такой рынок связанным и построим модель связанного рынка.

Подробно остановимся на системно-динамической модели. Это оправданно, поскольку в разделе 3 было показано, что системно-динамические и агентные реализации модели Ф. Басса для изолированных рынков дают одинаковые результаты.

Для упрощения рассмотрим связанный рынок только двух сегментов, определенных в начале работы: средних и малых предприятий г. Новосибирска. Такая модель представлена на рис. 6.

Модель на рис. 6 состоит из двух элементов традиционной модели системной динамики, представленной на рис. 1, дополненных новыми связями между ними. Верхняя часть модели представляет сегмент средних предприятий, а нижняя часть – малых предприятий. Все обозначения сегментов соответствуют обозначениям на рис. 1, но с индексами 1 и 2 соответственно. В описываемом эксперименте все параметры модели соответствуют табл. 1. То есть в сегментах различаются только значения параметров TotalPopulation1 (300 средних предприятий) и TotalPopulation2 (5000 малых предприятий).

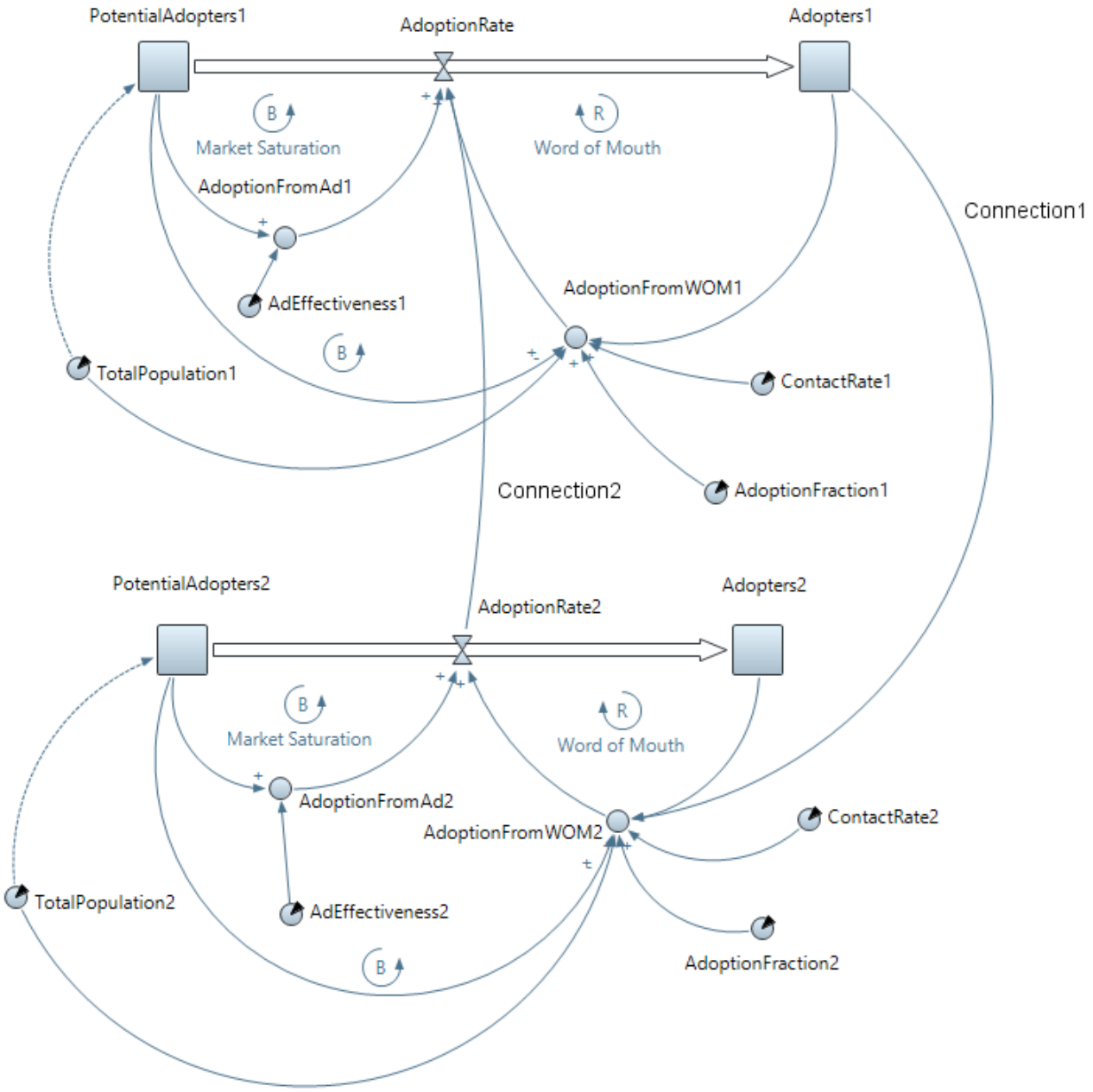

Рис. 6. Модель системной динамики внедрения инновационной технологии на связанный рынок двух сегментов средних (1) и малых (2) предприятий

Новая связь Connection1 реализует гипотезу о том, что число средних предприятий Adopters1, внедривших технологию, становится известным в сегменте малых предприятий и усиливает фактор продаж в этом сегменте под влиянием «сарафанного радио» Adoption-FromWOM. Связь Connection2 реализует гипотезу о том, что поток внедрения AdoptionRate2 в сегменте малых предприятий становится известным в сегменте средних предприятий и усиливает поток внедрения AdoptionRate1.

Результаты моделирования внедрения инновационной технологии управления качеством потребляемой электроэнергии одновременно в двух сегментах (средних и малых предприятий) показаны на рис. 7.

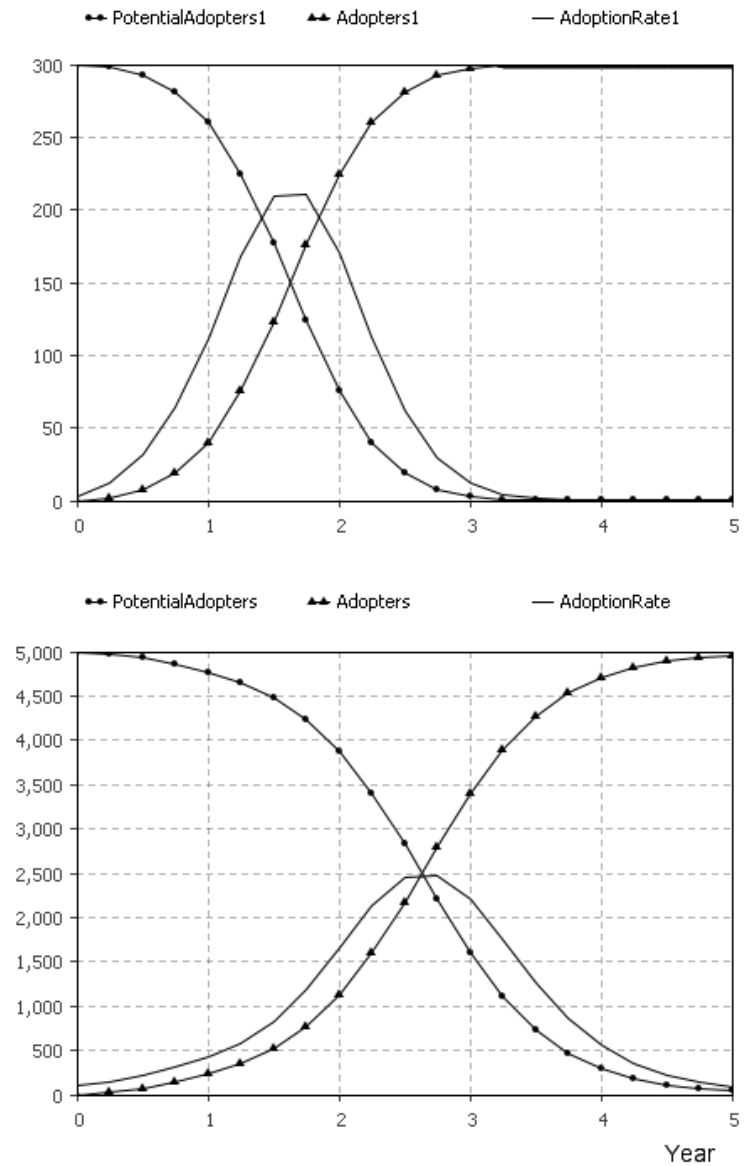

Рис. 7. Результаты моделирования внедрения инновационной технологии одновременно в двух сегментах рынка средних (верхний график) и малых (нижний график) предприятий

На верхнем графике рис. 7 представлен прогноз динамики внедрения инновационной технологии управления потреблением электроэнергии в сегменте средних предприятий, на нижнем – в сегменте малых предприятий г. Новосибирска. В результате внедрение инновационной технологии управления потреблением электроэнергии в сегменте малых предприятий стимулирует внедрение этой технологии в сегменте средних предприятий. Поэтому пик внедрения в сегменте 1 наступает раньше: не к середине третьего года, а к концу второго года проекта (верхний график на рис. 7). С другой стороны, при ограниченных ресурсах произ-

водства рост внедрений инновационной технологии в сегменте средних предприятий может отрицательно отразиться на потоке внедрений в сегменте малых предприятий. Поэтому пик внедрения инновационной технологии в сегменте 2 наступает позже: не к середине третьего года, а к началу четвертого года проекта (верхний график на рис. 7).

В этом разделе для упрощения визуального восприятия был представлен рынок внедрения инновационной технологии, состоящий из минимального количества сегментов. Кроме того, показано минимальное количество новых внутрирыночных и межрыночных связей. Очевидно, что приведенные модели могут быть расширены и адаптированы под другие конкретные рынки на основе изложенной методики.

5. Заключение

Проведено исследование комплексного применения моделей системной динамики и агентного моделирования, направленное на повышение точности и качества принятия управленческих решений при стратегическом планировании внедрения инновационной запатентованной технологии управления качеством потребляемой электроэнергии на основе долгосрочного прогнозирования поведения рынка потенциальных пользователей этой технологии.

Исследованы имитационные модели прогнозирования поведения рынка инновационной технологии, основанные на концепции Ф. Басса о разделении агентов рынка на инноваторов и имитаторов, которые функционируют под действием разных факторов. Знание этих факторов и регулируемых параметров позволяет их идентифицировать и эффективно управлять долгосрочным процессом внедрения.

Исследованы и реализованы две парадигмы имитационного моделирования: системная динамика и агентный подход. Проведено их сравнение, показано, что они дают близкие результаты, что позволяет повысить обоснованность принимаемых управленческих решений.

Показана важность и сложность задач измерения и регулирования рыночных параметров, используемых в имитационных моделях, решение которых реализовано в системе AnyLogic.

Особенностью работы и развитием известных моделей является предложенный автором новый методический подход о выводе инновационной технологии сразу одновременно на несколько рынков (или рыночных сегментов) в рамках единого более масштабного проекта, что позволяет перевести проекты на качественно новый уровень. В работе выдвигаются и исследуются гипотезы о возникновении и значимом развитии коммуникаций между рыночными сегментами. Информация о динамике распространения инновационной технологии в одном из сегментов может влиять на поведение агентов в другом сегменте, и наоборот. Введение таких связей в разрабатываемые имитационные модели происходит естественно и технически просто, однако их использование требует дополнительных исследований.

Представленные имитационные модели для принятия управленческих решений по внедрению инновационной технологии можно развивать далее.

Литература

1. *Klavsuts D. A., Klavsuts I. L., Rusin G. L.* Aspects of Evaluating the Efficiency of Introducing Innovative Method and Technology Demand Side Management in Smart Grid System // Proc. 48th IEEE International Universities' Power Engineering Conference (UPEC), Dublin Institute of Technology, Ireland, 2–5 Sept., 2013.
2. *Klavsuts I. L., Klavsuts D. A., Rusin G. L., Mezhov I. S* Perfecting business processes in electricity grids by the use of innovative technology of demand side management in the framework of the general conception of smart grids // Proc. 49th IEEE International Universities' Power Engineering Conference (UPEC), Romania, Cluj-Napoca, 2–5 Sept. 2014.

3. *Klavsuts D. A., Klavsuts I. L., Avdeenko T. V.* Providing the quality of electric power by means of regulating customers' voltage // Proc. 49th IEEE International Universities' Power Engineering Conference (UPEC), Romania, Cluj-Napoca, 2–5 Sept. 2014.
4. *Клавсуц И. Л., Русин Г. Л., Клавсуц Д. А.* Управление внедрением инновационной энергосберегающей технологии в старопромышленных регионах СНГ и в Северо-Восточных Азиатских регионах: опыт и перспективы // Сборник научных статей «Модернизация российской экономики: перспективы, парадигмы, решения». 2014. С. 40–47, http://elibrary.ru/item.asp?id=23814265.
5. *Klavsuts I. L., Klavsuts D. A., Rusina A. G., Rusin G. L.* Modes control of Smart Power Grids based on the usage of the innovative method and device of Demand Side Management // Proc. 50th IEEE International Universities' Power Engineering Conference (UPEC), UK, Stoke-on-Trent, 1–4 Sept. 2015. DOI: 10.1109/UPEC.2015.7339779.
6. *Клавсуц И. Л., Русин Г. Л., Хайруллина М. В.* Стратегические модели внедрения инновационной технологии управления потреблением электроэнергии на мировые рынки // Сборник трудов МНТК «Актуальные проблемы электронного приборостроения» (АПЭП), Новосибирск, 3–6 окт. 2016 г. Т. 11. С. 94–101. ISBN 978-5-7782-2991-4; 978-5-7782-3002-6.
7. *Klavsuts I. L., Rusina A. G., Klavsuts D. A.* The development of simulation model of innovative technology of AC voltage normalization for introduction into smart grid system // Proc. 51th IEEE International Universities' Power Engineering Conference (UPEC), Portugal, Coimbra, 6–9 Sept. 2016.
8. *Fishov A. G., Klavsuts I. L., Karjaubayev N. A., Klavsuts D. A.* Decentralized smart multi-agent voltage regulation in electric grids. Ideology and modeling // Proc. 53th IEEE International Universities' Power Engineering Conference (UPEC), UK, Glasgow, 4–7 Sept. 2018.
9. *Bass F. M.* A new product growth for model consumer durables // Management Science. 1969. V. 15, № 5. P. 215–227.
10. *Форрестер Дж.* Основы кибернетики предприятия (индустриальная динамика) / Под общ. ред. Д. М. Гвишиани. М.: Прогресс, 1969. 340 с.
11. *Brailsford S., Churilov L, and Dangerfield B.* Front Matter, in Discrete-Event Simulation and System Dynamics for Management Decision Making. John Wiley & Sons Ltd, Chichester, UK, 2014. DOI: 10.1002/9781118762745.
12. *Jones L.* Vensim and the development of system dynamics, in Discrete-Event Simulation and System Dynamics for Management Decision Making. John Wiley & Sons Ltd, Chichester, UK, 2014. DOI: 10.1002/9781118762745.ch11.
13. AnyLogic. Многоподходное имитационное моделирование [Электронный ресурс]. URL: http:/www.anylogic.com/ (дата обращения: 02.11.2022).
14. *Borshchev A.* Multi-method modelling: AnyLogic, in Discrete-Event Simulation and System Dynamics for Management Decision Making. John Wiley & Sons Ltd, Chichester, UK, 2014. DOI: 10.1002/9781118762745.ch12.
15. *Romanowska I., Wren C. D., Crabtree S. A.* Agent-Based Modeling for Archaeology: Simulating the Complexity of Societies. SFI PRSS, 2021. 442 p. ISBN 978-1947864252.
16. *Railsback S. F., Grimm V.* Agent-Based and Individual-Based Modeling: A Practical Introduction. Princeton University Press, 2019. 360 p. ISBN 978-0691190839.
17. *Crooks A., Malleson N., Manley E., Heppenstall A.* Agent-Based Modelling and Geographical Information Systems: A Practical Primer (Spatial Analytics and GIS). SAGE Publications Ltd, 2019. 408 p. ISBN 978-1473958654.

Клавсуц Дмитрий Александрович
магистр, аспирант кафедры теоретической и прикладной информатики, Новосибирский государственный технический университет (НГТУ, 630073, Новосибирск, пр. К. Маркса, 20, 1 корпус, ауд. 201), тел. +7 383 3460 600, e-mail: dklavsuts@gmail.com, ORCID ID: 0000-0002-9592-047X.

Автор прочитал и одобрил окончательный вариант рукописи.
Автор заявляет об отсутствии конфликта интересов.

Integrated Usage of System Dynamic Models and Agent-based Modeling for Taking Management Decisions when Introducing Innovative Technology

Dmitry Klavsuts

Novosibirsk State Technical University (NSTU)

Abstract: The paper proposes a new methodological approach aimed at developing simulation models of system dynamics and agent-based modeling in case an enterprise introduces an innovative patented technology in new markets. This task requires development of new business models, strategies, and communication processes. The operating models for solving these problems are implemented in the AnyLogic simulation system

Keywords: innovative technology for managing electricity consumption, management decisions, long-term forecasting, strategic planning, simulation of the market for innovative technologies, system dynamics, agent-based modeling.

For citation: Klavsuts D. A. Integrated usage of system dynamic models and Agent-based modeling for taking management decisions when introducing innovative technology (in Russian). *The SibSUTIS Bulletin*, 2023, vol. 17, no. 2, pp. 22-36. https://doi.org/10.55648/1998-6920-2023-17-2-22-36.

The article was submitted: 18.12.2022;
revised version: 04.02.2023;
accepted for publication 16.02.2023.

References

1. Klavsuts D. A., Klavsuts I. L., Rusin G. L. Aspects of Evaluating the Efficiency of Introducing Innovative Method and Technology Demand Side Management in Smart Grid System. *48 th International Universities' Power Engineering Conference – UPEC 2013*, hosted by Dublin Institute of Technology, Ireland, Section- Smart Grids, 2-5September,2013.
2. Klavsuts I. L., Klavsuts D. A., Rusin G. L., Mezhov I. S. Perfecting business processes in electricity grids by the use of innovative technology of demand side management in the framework of the general conception of smart grids. *49 International Universities power engineering conference (UPEC)*, Romania, Cluj-Napoca, 2-5 September, 2014, p. 4.
3. Klavsuts D. A., Klavsuts I. L., Avdeenko T. V. Providing the quality of electric power by means of regulating customers' voltage. *49 International Universities power engineering conference (UPEC)*, Romania, Cluj-Napoca, 2-5 September, 2014, p. 4.
4. Klavsuts I. L., Rusin G. L., Klavsuts D. A. Upravlenie vnedreniem innovatsionnoi energosberegayushchei tekhnologii v staropro-myshlennykh regionakh SNG i v Severo-Vostochnykh Aziatskikh re-

gionakh: opyt i perspek-tivy [Management of the introduction of innovative energy-saving technology in the old industrial regions of the CIS and in the North-East Asian regions: experience and prospects]. *Modernization of the Russian economy: prospects, paradigms, solutions" - Collection of scientific articles*, Novosibirsk, 2014, pp. 40-47.
5. Klavsuts I. L., Klavsuts D. A., Rusina A. G., Rusin G. L. Modes control of Smart Power Grids based on the usage of the innovative method and device of Demand Side Management. *50 International universities power engineering conference (UPEC 2015)*, United Kingdom, Stoke-on-Trent, 1-4 September, 2015, p. 6. DOI: 10.1109/UPEC.2015.7339779.
6. Klavsuts I. L., Rusin G. L., Khairullina M. V. Strategic models of introducing innovative technology for management of electric power consumption into world markets. *Actual problems of electronic instrument engineering (APEIE–2016)*, 13 intl. sci.-tech. Conf., Novosibirsk, 3-6 October, 2016, Novosibirsk, Publishing house of NSTU, vol 11, pp. 94–101.
7. Klavsuts I. L., Rusina A. G., Klavsuts D. A. The development of simulation model of innovative technology of AC voltage normalization for introduction into smart grid system. *51 International Universities power engineering conference (UPEC)*, Portugal, Coimbra, 6-9 September, 2016, p. 6.
8. Fishov A. G., Klavsuts I. L., Karjaubayev N. A., Klavsuts D. A. Decentralized smart multi-agent voltage regulation in electric grids. Ideology and modeling. *Proceeding 53 international universities power engineering conference (UPEC2018)*, United Kingdom, Glasgow, 4-7 September, 2018, p. 6. DOI: 10.1109/UPEC.2018.8542109.
9. Bass, Frank M. A new product growth for model consumer durables. *Management Science*, vol. 15, no. 5, January, 1969. pp. 215-227.
10. Forrester Dzh. Osnovy kibernetiki predpriyatiya (industrial'naya dinamika) [Fundamentals of enterprise cybernetics (industrial dynamics)]. Ed. Gvishiani D.M., Progress, 1969. 340 p.
11. Brailsford S., Churilov L. and Dangerfield B. (EDS) Front Matter. *Discrete-Event Simulation and System Dynamics for Management Decision Making*, John Wiley & Sons Ltd, Chichester, UK, 2014. DOI: 10.1002/9781118762745.
12. Jones L. Vensim and the development of system dynamics. *Discrete-Event Simulation and System Dynamics for Management Decision Making*. Eds. S. Brailsford, L. Churilov and B. Dangerfield. John Wiley & Sons Ltd, Chichester, UK, 2014. doi: 10.1002/9781118762745.
13. AnyLogic. Mnogopodkhodnoe imitatsionnoe modelirovanie [AnyLogic.Multi-approach simulation], available at: `http://www.anylogic.com`, (accessed 21.11.2022).
14. Borshchev, A. Multi-method modelling: AnyLogic.*Discrete-Event Simulation and System Dynamics for Management Decision Making*. Eds. S. Brailsford, L. Churilov and B. Danger-field. John Wiley & Sons Ltd, Chichester, UK, 2014. doi: 10.1002/9781118762745.
15. Iza Romanowska, Colin D. Wren, Stefani A. Crabtree *Agent-Based Modeling for Archaeology: Simulating the Complexity of Societies*. SFI PRSS, 2021. 442 p.
16. Steven F. Railsback, Volker Grimm *Agent-Based and Individual-Based Modeling: A Practical Introduction*. Princeton University Press, 2019. 360 p.
17. Andrew Crooks, Nick Malleson, Ed Manley, Alison Heppenstall *Agent-Based Modelling and Geographical Information Systems: A Practical Primer (Spatial Analytics and GIS)*, SAGE Publications Ltd, 2019. 408 p.

Dmitry A. Klavsuts

Graduate student, Department of Theoretical and Applied Computer Science, Novosibirsk State Technical University (NSTU, 20, Karla Marksa ave., Novosibrsk, Russia, 630073), phone: +7 383 3460 600, e-mail: `dklavsuts@gmail.com`, ORCID ID: 0000-0002-9592-047X.

DOI: 10.55648/1998-6920-2023-17-2-37-43 УДК 621.396

Исследование распределения статистических параметров системы определения местоположения в сети Wi-Fi

А. С. Брагин

Сибирский гос. унив. телекоммуникаций и информатики (СибГУТИ)

Аннотация: Для определения местоположения мобильного объекта в сети Wi-Fi применяются статистические и эвристические методы принятия решений на основе измерений физических параметров принятого сигнала. Для корректного их использования необходимо знание законов распределения выборочной совокупности измеренных значений. В работе предлагается проверка статистических критериев соответствия выборки нормальному закону. Были применены критерии Пирсона и Колмогорова, полученные результаты подтверждают предложенную гипотезу.

Ключевые слова: беспроводная связь, Wi-Fi, точка доступа, RSSI, зона покрытия, статистические критерии.

Для цитирования: Брагин А. С. Исследование распределения статистических параметров системы определения местоположения в сети Wi-Fi // Вестник СибГУТИ. 2023. Т. 17, № 2. С. 37–43. https://doi.org/10.55648/1998-6920-2023-17-2-37-43.

Статья поступила в редакцию 26.12.2022;
принята к публикации 10.01.2023.

1. Введение

В процессе исследования, связанного с построением системы локального позиционирования, экспериментальным путем было установлено, что наиболее точные результаты при определении координат объекта, находящегося внутри здания, обеспечивает метод три- или мультилатерации, который, однако, требует полного знания конфигурации помещений, материала и толщины стен, перегородок и перекрытий. Измерения параметра RSSI (уровень мощности принятого сигнала), применяемые для вычисления расстояния от точек доступа до мобильного объекта, не дают этого знания. Выходом из данной ситуации является применение статистических и эвристических методов принятия решений для грубой оценки местонахождения объекта [1, 2].

К статистическим методам оценки неизвестных параметров распределения относятся:

- метод подстановки;
- метод моментов;
- метод наименьших квадратов;
- метод максимального правдоподобия;
- наивный байесовский подход [3].

Эвристические методы анализа:

- метод взвешенной суммы критериев;
- таксиметрический метод;
- кластерный анализ [4].

Применение указанных выше механизмов требует проверки гипотезы о нормальном распределении выборки измерения параметров.

Существует множество статистических критериев для проверки гипотез, таких как:

- критерий Пирсона;
- критерий Пуассона;
- критерий Колмогорова;
- критерий Смирнова и т.д.

Автором в ходе экспериментального исследования были выбраны критерий Пирсона и критерий Колмогорова, применение которых будет подробно рассмотрено в следующих разделах.

2. Сравнительный анализ применения критериев Пирсона и Колмогорова для проверки гипотезы о нормальности выборочной совокупности измерения уровня сигнала в системе определения местоположения

2.1. Проверка распределения по критерию Пирсона

В ходе проведения экспериментов в опытной зоне системы позиционирования был проведен сбор данных (RSSI) с помощью ПО MultiScanner [5]. В процессе измерения были получены данные, значения которых находятся в диапазоне от -43 до -90 дБм, от 34 точек доступа. Из них были выбраны для дальнейшего анализа результаты, находящиеся в диапазоне от -43 до -66 дБм, и занесены в табл. 1.

Таблица 1. Исходные данные

Уровень мощности сигнала, дБм	(-43; -45)	(-46; -48)	(-49; -51)	(-52; -54)	(-55; -57)	(-58; -60)	(-61; -63)	(-64; -66)
Эмпирические частоты n_i, шт.	12	20	14	19	23	26	24	25

Задача заключается в том, чтобы на уровне значимости $\alpha = 0.025$ проверить гипотезу H_0 о нормальном распределении генеральной совокупности против конкурирующей гипотезы H_1 о том, что совокупность не соответствует нормальному распределению.

Для проверки гипотезы используется критерий согласия Пирсона [6]:

$$\chi^2 = \sum \frac{(n_i - n_i')^2}{n_i'}, \quad (1)$$

где n_i – эмпирические частоты;

n_i' – теоретические частоты.

Вводится формула для расчета теоретических частот:

$$n_i' = P_i \cdot N = N \cdot (\Phi(\frac{x_i - x_в}{\delta_в}) - \Phi(\frac{x_{i+1} - x_в}{\delta_в})),$$

где N – общая сумма эмпирических частот;

P_i – теоретическая вероятность попадания значения в заданный интервал;

Φ – функция Лапласа;

x_i и x_{i+1} – границы i-го интервала;

$x_в$ – выборочная средняя измеренных значений;

$\delta_в$ – выборочное стандартное отклонение измеренных значений.

Эмпирические частоты известны из предложенного интервального ряда, и необходимо найти теоретические. Для этого нужно вычислить выборочную среднюю $x_в$ и выборочное стандартное отклонение $\delta_в$. При помощи программы Excel эти значения рассчитаны: $x_в = -56.0368$, $\delta_в = 6.608907$.

Далее определяются теоретические вероятности P_i и теоретические частоты n_i', после чего можно найти количество чисел из выборки объема N, которое должно оказаться в каждом интервале при этом предположении (теоретические частоты). Для этого по таблице значений функции Лапласа найдем вероятность попадания значения в i-й интервал. Умножив полученные вероятности на объем выборки N, найдем теоретические частоты и занесем в табл. 2.

Таблица 2. Вычисление теоретических частот

x_i	x_{i+1}	n_i	P_i	n_i'
-43	-45	12	0.041918	6.832571
-46	-48	20	0.0832	13.56153
-49	-51	14	0.079497	12.95809
-52	-54	19	0.108307	17.654
-55	-57	23	0.120268	19.60364
-58	-60	26	0.108852	17.74281
-61	-63	24	0.154883	25.246
-64	-66	25	0.127205	20.7344
Сумма	$N = 163$			

Дальнейшая задача состоит в том, чтобы оценить, насколько значимо отличаются эмпирические частоты от соответствующих теоретических частот. Найдём критическое значение критерия согласия Пирсона:

$$\chi^2_{пр} = \chi^2_{пр}(\alpha, k) = \chi^2_{пр}(\alpha, m - r - 1),$$

где α – уровень значимости;

k – количество степеней свободы;

m – количество интервалов;

r – количество оцениваемых параметров рассматриваемого закона распределения.

У нормального закона оцениваются 2 параметра, поэтому:

$$\chi^2_{пр} = \chi^2_{пр}(0.025, 8 - 2 - 1) = \chi^2_{пр}(0.025, 5) = 12.8.$$

При $\chi^2_{жел} > \chi^2_{пр}$ нулевая гипотеза отвергается, а при $\chi^2_{жел} < \chi^2_{пр}$ таких оснований нет. Вычислим наблюдаемое значение критерия согласно формуле (1) и для этого заполним ещё одну расчётную таблицу.

Таблица 3. Расчет наблюдаемого значения критерия $\chi^2_{жел}$

n_i	n'_i	$\chi^2_{жел}$
12	6.832571	3.908093
20	13.56153	3.056726
14	12.95809	0.083776
19	17.654	0.102624
23	19.60364	0.588425
26	17.74281	3.842748
24	25.246	0.061496
25	20.7344	0.877542
Сумма		12.52143

В нижней строке таблицы представлено значение $\chi^2_{жел} \approx 12,5 < \chi^2_{пр}$, то есть на уровне значимости нет оснований отвергать гипотезу о том, что генеральная совокупность распределена по нормальному закону. Различие между эмпирическими и теоретическими частотами незначительно и обусловлено случайными факторами (случайностью самой выборки, способом группировки данных и т.д.).

2.2. Проверка распределения по критерию Колмогорова

Чтобы полностью удостовериться в правоте предложенной гипотезы о нормальности распределения, воспользуемся критерием Колмогорова с теми же исходными данными (табл. 1) [7].

Найдем точечные оценки параметров распределения. Для этого перейдем к простому вариационному ряду, выбрав в качестве варианта середины интервалов x_i, составим расчетную табл. 4.

Таблица 4. Вводные данные

x_i	n_i	$x_i n_i$	$(x_i - \overline{x})^2 n_i$
-44	12	-528	1696.342655
-47	20	-940	1580.489292
-50	14	-700	485.618578
-53	19	-1007	158.6427415
-56	23	-1288	0.280477248
-59	26	-1534	251.5440551
-62	24	-1488	896.0963529
-65	25	-1625	2074.998118
Сумма	163	-9110	7144.01227

Выборочное среднее:

$$\overline{x} = \frac{1}{N}\sum x_i n_i = -55.8896,$$

где N – общая сумма эмпирических частот;

x_i – середины интервалов уровня мощности сигнала;

n_i – эмпирические частоты.

Выборочная исправленная дисперсия:

$$S^2 = \frac{1}{N-1} * \sum (x_i - \bar{x})^2 n_i = 44.09884,$$

где N – общая сумма эмпирических частот;

x_i – середины интервалов уровня мощности сигнала;

n_i – эмпирические частоты;

$\bar{x}$ – выборочная средняя.

Выборочное исправленное среднее квадратическое отклонение:

$$S = \sqrt{44.09884} = 6.640696.$$

Предполагаем, что исследуемая величина имеет нормальный закон распределения с рассчитанными параметрами. С помощью критерия Колмогорова проверим, согласуется ли гипотеза с опытными данными на уровне значимости $\alpha = 0.025$. Табличное значение для данного уровня значимости составляет 1.48.

Вычислим теоретические значения функции распределения:

$$F*(x) = \int_{-\infty}^{x} \frac{1}{S\sqrt{2\pi}} \exp\left(-\frac{(t-\bar{x})^2}{2S^2}\right) = \frac{1}{2} + \Phi\left(\frac{x-\bar{x}}{S}\right),$$

где Φ – функция Лапласа;

$\bar{x}$ – выборочная средняя;

x – интервал уровней мощности сигнала.

Найдем наибольшее отклонение, затем вычисляем значение критерия. Результаты заносим в табл. 5.

$$\lambda = \max_{x_i} \left| F(x_i) - F*(x_i) \right| \sqrt{N},$$

где N – общая сумма эмпирических частот;

$F(x_i)$ – нижняя граница функции распределения;

$F*(x_i)$ – верхняя граница функции распределения.

Таблица 5. Расчет значения критерия

$F*(x_i)$	$F(x_i)$	$\max\left\|F(x_i) - F*(x_i)\right\|$	λ
1.473871	1.449479	0.024	0.306411
1.431788	1.413596	0.018	0.229809
0.785907	0.804218	0.018	0.229809
0.836058	0.853151	0.017	0.217041
0.895379	0.893404	0.002	0.025534
0.846793	0.829393	0.017	0.217041
0.72078	0.724883	0.004	0.051069
0.610982	0.625188	0.014	0.17874
Сумма			1.455455

Так как $\lambda \approx 1.4555 < \lambda_{0.025} = 1.48$, то распределение можно считать нормальным на уровне значимости 0.025.

3. Заключение

При проведении расчётов было показано, что в результате статистического анализа можно проверить математическое правило, в соответствии с которым принимается или отвергается та или иная статистическая гипотеза с заданным уровнем значимости. Построение критерия представляет собой выбор подходящей функции от результатов наблюдений (ряда эмпирически полученных значений), которая служит для выявления меры расхождения между эмпирическими значениями и гипотетическими.

Литература

1. *Лизнева Ю. С., Кокорева Е. В., Костюкович А. Е.* Прогнозирование местоположения мобильного абонента в сети Wi-Fi // Вестник СибГУТИ. 2022. № 3. С.101–111.
2. *Кокорева Е. В., Шурыгина К. И.* Повышение точности локального позиционирования оптимизацией размещения точек доступа // Материалы XI Международной научно-технической и научно-методической конференции «Актуальные проблемы инфотелекоммуникаций в науке и образовании» (АПИНО), Санкт-Петербург, 2022. С. 581–585.
3. *Roos T., Myllymäki P., Tirri H., Misikangas P.* A Probabilistic Approach to WLAN User Location Estimation // International Journal of Wireless Information Networks. 2002. № 9 (3). P. 155–164.
4. *Лапченко Д. А.* Теория принятия решений. Минск: БНТУ, 2021. 62 с.
5. Свидетельство о государственной регистрации программы для ЭВМ № 2022680963 Российская Федерация. Программа измерения и предварительной обработки параметров точек доступа локальной беспроводной сети в целях позиционирования / Шурыгина К. И., Кокорева Е. В.; правообладатель Российская Федерация, от имени которой выступает Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации; заявл. 11.10.2022; опубл. 08.11.2022.
6. Проверка гипотезы о нормальном распределении по критерию Пирсона [Электронный ресурс]. URL: `https://math.semestr.ru/group/example-normal-distribution.php` (дата обращения: 28.11.2022).
7. Критерий согласия Колмогорова [Электронный ресурс]. URL: `https://studref.com/552899/matematika_himiya_fizik/kriterii_soglasiya_kolmogorova` (дата обращения: 28.11.2022).

Брагин Антон Сергеевич
аспирант СибГУТИ (630102, Новосибирск, ул. Кирова, 86), e-mail: `bragin_ant@mail.ru`, ORCID ID: 0000-0001-9704-9676.

Автор прочитал и одобрил окончательный вариант рукописи.
Автор заявляет об отсутствии конфликта интересов.

Research on the Distribution of Statistical Parameters of the Wi-Fi Positioning System

A. S. Bragin

Siberian State University of Telecommunications and Information Science (SibSUTIS)

Abstract: Statistical and heuristic decision-making methods based on measurements of the received signal physical parameters are used to determine the location of a mobile object in the Wi-Fi network. It is necessary to know the distribution laws of the measured values' samples to use them correctly. In this paper, it is proposed to test the statistical criteria for the compliance of the sample with the normal law. Pearson and Kolmogorov criteria were applied. The obtained results confirm the proposed hypothesis.

Keywords: wireless communication, Wi-Fi, access point, RSSI, coverage area, statistical criteria.

For citation: Bragin A. S. Research on the distribution of statistical parameters the Wi-Fi positioning system (in Russian). *The SibSUTIS Bulletin*, 2023, vol. 17, no. 2, pp. 37-43. https://doi.org/10.55648/1998-6920-2023-17-2-37-43.

The article was submitted: 26.12.2022;
accepted for publication 10.01.2023.

References

1. Lizneva Yu. S., Kokoreva E. V., Kostyukovich A. E. Prognozirovanie mestopolozheniya mobil'nogo abonenta v seti Wi-Fi [Forecasting the location of a mobile subscriber on a Wi-Fi network]. *Vestnik SibGUTI*, 2022, no. 3, pp.101-111.
2. Kokoreva E.V., Shurygina K.I. Povyshenie tochnosti lokal'nogo pozitsionirovaniya optimizatsiei razmeshcheniya tochek dostupa [Improving the accuracy of local positioning by optimizing the placement of access points]. *Aktual'nye problemy infotelekommunikatsii v nauke i obrazovanii (APINO 2022). XI Mezhdunarodnaya nauchno-tekhnicheskaya i nauchno-metodicheskaya konferentsiya*, Saint-Petersburg, 2022, pp. 581-585.
3. Roos T., Myllymäki P., Tirri H., Misikangas P. A Probabilistic Approach to WLAN User Location Estimation. *International Journal of Wireless Information Networks, 2002, no. 9(3)*, pp. 155-164.
4. Lapchenko D. A. *Teoriya prinyatiya reshenii* [Theory of decision-making]. Minsk, BNTU, 2021. 62 p.
5. Shurygina K.I., Kokoreva E.V. *Svidetel'stvo o gosudarstvennoi registratsii programmy dlya EVM no. 2022680963. Programma izmereniya i predvaritel'noi obrabotki parametrov tochek dostupa lokal'noi besprovodnoi seti v tselyakh pozitsionirovaniya* [Certificate of state registration of the computer program no. 2022680963. A program for measuring and preprocessing the parameters of access points of a local wireless network for positioning purposes]. Copyright holder of the Russian Federation, on behalf of which the Ministry of Digital Development, Communications and Mass Communications of the Russian Federation acts; appl. 11.10.2022; publ. 08.11.2022.
6. *Proverka gipotezy o normal'nom raspredelenii po kriteriyu Pirsona* [Verification of the hypothesis of normal distribution according to the Pearson criterion], available at: https://math.semestr.ru/group/example-normal-distribution.php (accessed 28.11.2022).
7. *Kriterii soglasiya Kolmogorova* [Kolmogorov's criterion of consent], available at: https://studref.com/552899/matematika_himiya_fizik/kriterii_soglasiya_kolmogorova (accessed 28.11.2022).

Anton S. Bragin

Postgraduate student, Siberian State University of Telecommunications and Information Science (SibSUTIS, 630102, Novosibirsk, Kirova str., 86), e-mail: bragin_ant@mail.ru, ORCID ID: 0000-0001-9704-9676.

DOI: 10.55648/1998-6920-2023-17-2-44-50 УДК 004.056

Обзор методов прогнозирования сетевых аномалий

Д. С. Лизнев

Сибирский гос. унив. телекоммуникаций и информатики (СибГУТИ)

Аннотация: В работе проведен анализ методов прогнозирования сетевых аномалий. На примере реальных статистических данных показаны этапы настройки моделей прогнозирования. Показано влияние DDoS-атак на энтропию IP-адресов назначения.

Ключевые слова: модель экспоненциального сглаживания, авторегрессионная модель, энтропия, сетевые атаки.

Для цитирования: Лизнев Д. С. Обзор методов прогнозирования сетевых аномалий // Вестник СибГУТИ. 2023. Т. 17, № 2. С. 44–50. https://doi.org/10.55648/1998-6920-2023-17-2-44-50.

Статья поступила в редакцию 26.12.2022;
принята к публикации 10.01.2023.

1. Введение

Сетевая аномалия – действия с применением программных и (или) технических средств и с использованием сетевого протокола, направленные на реализацию угроз несанкционированного доступа к информации, воздействия на нее или на ресурсы автоматизированной системы [1].

Атаки можно классифицировать как Denial of Service/Distributed Denial of Service (DoS/DDoS), User to Root (U2R), Remote to Local (R2L) и Probe. В данной статье рассматривается возможность применения статистических методов для прогнозирования количества DDoS-атак, а также влияние указанного класса атаки на энтропию IP-адресов назначения.

DDoS-атаки приводят к тому, что целевая система становится полностью недоступной или нестабильной. Данный класс атаки делят на несколько типов, например, такие как Smurf (рассылка поддельных ICMP-запросов), Land (рассылка некорректных TCP-запросов), Neptune (одновременная множественная рассылка SYN-сегментов TCP) и т.д.

Согласно отчету [2] количество проводимых DDoS-атак неуклонно возрастает (рис. 1).

Анализ представленной на рис. 1 информации показывает рост количества DDoS-атак относительно предыдущего отчетного периода. В свою очередь, по рекомендациям, данным в отчетах компании Positive Technologies, важно не только выстроить регулярные процессы определения и устранения уязвимостей, но и знать о существовании новых атак, следовательно, уметь быстро на них реагировать [3].

Для противодействия атакам, направленным на отказ в обслуживании, в общем случае необходимо идентифицировать тип трафика, который загружает сеть, а затем разделить поток на вредоносный и обычный [4].

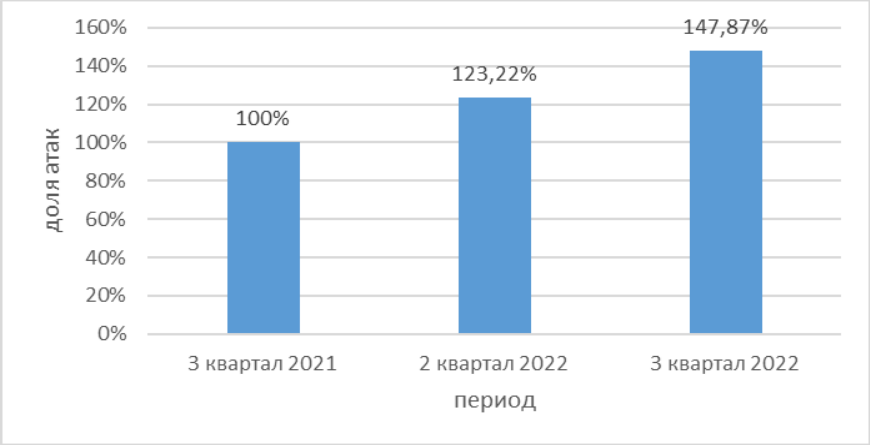

Рис. 1. Доля DDoS-атак в сравнении

В данной работе на примере статистических данных был проведен обзор методов прогнозирования аномалий.

2. Возможность использования энтропии для обнаружения DDoS-атак

Одним из признаков DDoS-атаки можно считать нетипично замедленную работу сетевого оборудования, что заметно без применения дополнительного анализа.

В [5] предложен алгоритм обнаружения аномалий, основанный на энтропии. Авторы показывают, что разработанный алгоритм обладает низкими вычислительными затратами, легкий в реализации, при этом обладает высокой скоростью обнаружения сетевых аномалий в режиме реального времени. Суть метода заключается в анализе влияния атаки на энтропию IP-адресов. DDoS-атака представляет собой большое количество запросов к конкретному сервису от одного узла-источника, то есть в общем трафике можно увидеть большое количество пакетов с одинаковыми IP-адресами – источника атаки и атакуемого сервера [6]. Атака за счет концентрации трафика на портах источника и портах назначения характеризуется уменьшением энтропии IP-адресов источника и IP-адресов назначения.

В качестве исходных данных для расчета энтропии воспользуемся базой KDD-2009 [7]. Из базы данных извлекаем записи, относящиеся к нормальному трафику и к DDoS-атакам. Далее из записи выделяем признак, относящийся к числу соединений с тем же самым IP-адресом порта назначения. На рис. 2 показано влияние DDoS-атаки на энтропию IP-адресов назначения.

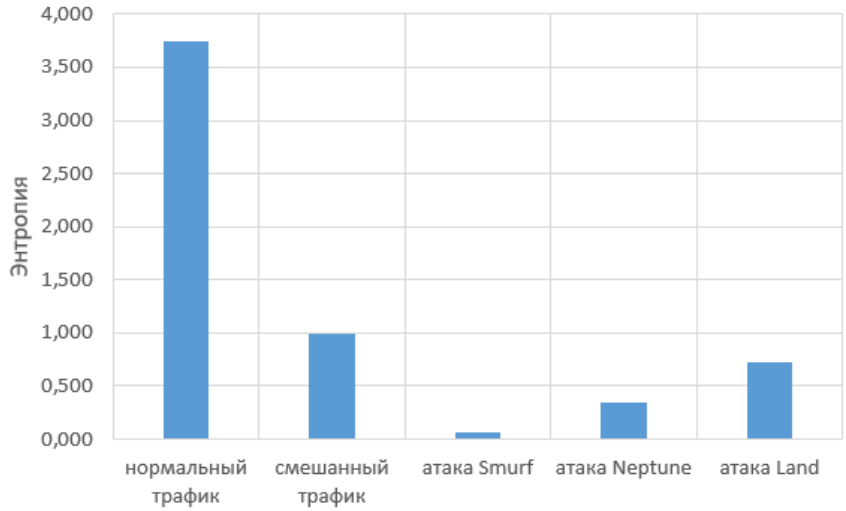

Рис. 2. Влияние DDoS-атаки на энтропию IP-адресов назначения

Анализ рис. 2 показал, что для нормального режима работы сети величина энтропии значительно превышает значения, рассчитанные для DDoS-атак. Таким образом, когда происходит DDoS-атака, число запросов на один IP-адрес резко увеличивается, что приводит к меньшему значению энтропии.

3. Прогнозирование DDoS-атак статистическими методами

Анализ исходных данных проводился на отрезке временного ряда данных с 1 ноября 2020 г. по 30 сентября 2022 г. [2].

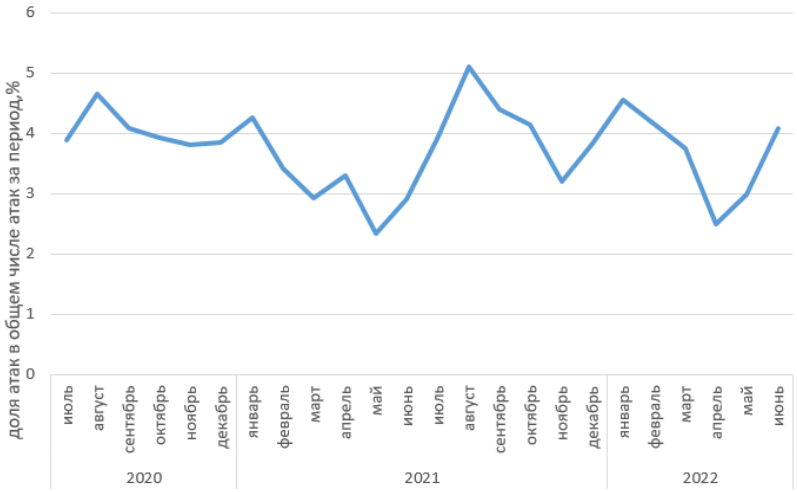

Рис. 3. Динамика DDoS-атак

Для прогнозирования динамики DDoS-атак используются различные методы и модели, которые различаются не только сложностью реализации, но и программной поддержкой. То есть выбор метода зависит от типа и цели прогноза, полноты исходных данных, доступности программного обеспечения и т.д.

В литературе описано большое количество методов статистического анализа и прогнозирования. К адаптивным моделям относят модель Брауна, модель Хольта и модель авторегрессии [8].

Метод экспоненциального сглаживания, на котором основаны модели Брауна и Хольта, позволяет анализировать временной ряд без предварительного задания уравнения тренда.

Основным моментом при использовании метода экспоненциального сглаживания является выбор параметра сглаживания α, начальных условий и степени полинома.

Если параметр сглаживания близок к нулю, значит, веса убывают медленно, и модель учитывает все значения рассматриваемого временного ряда. Напротив, если параметр близок к единице, это приведет к учету в прогнозе в основном влияния лишь последних наблюдений [8].

При разных значениях параметров сглаживания α результаты прогноза будут отличаться. Следовательно, параметр α выбирается таким образом, чтобы минимизировать ошибку прогноза.

Исследования показывают, что прогноз, учитывающий только один параметр α, нельзя считать абсолютно надежным. Для того, чтобы повысить точность прогноза, применяется модифицированная модель:

$$F_t(y) = \alpha \cdot y_t + (1-\alpha)(F_{t-1}(y) + T_{t-1}), \quad (1)$$

где выражение для тренда

$$T_t(y) = \beta \cdot (F_t - F_{t-1}) + (1-\beta) \cdot T_{t-1}, \quad (2)$$

где β – сглаживающая постоянная для тренда.

Меру отклонения прогноза от фактических значений можно оценить с помощью стандартной ошибки прогнозирования. В процессе настройки модели подбираются такие α и β, при которых стандартная ошибка отклонения будет минимальна. При этом необходимо учитывать условие применимости модели: если вышеописанные параметры принимают значения больше 0.7, прогноз нельзя считать достоверным.

Для расчета ошибки на основании исходных данных (рис. 3) подставляем в расчетную модель каждый параметр, изменяя его значение с 0 до 0.6 с шагом 0.1. Результаты расчета представлены на рис. 4.

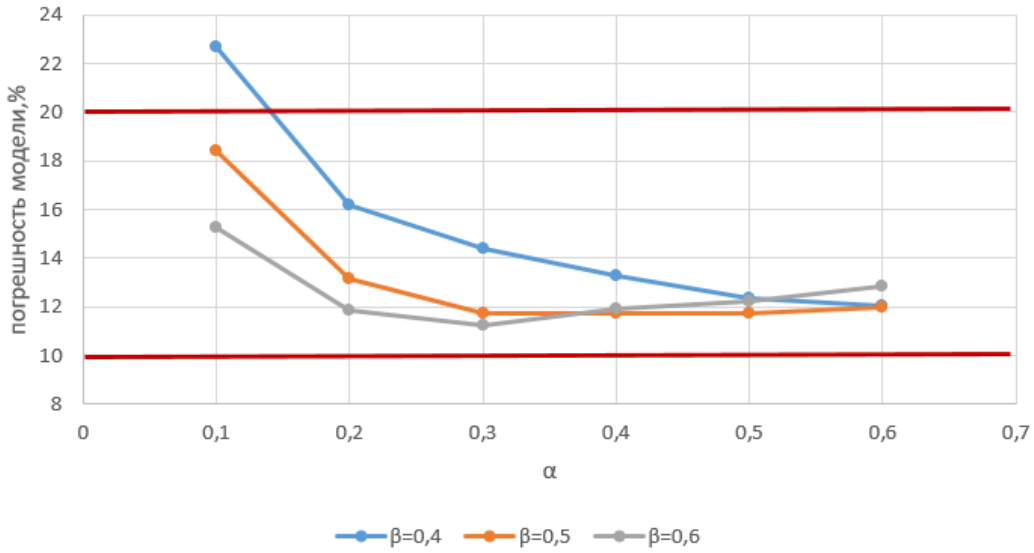

Рис. 4. Зависимость абсолютной ошибки модели от параметра сглаживания α для различных значений β

На рис. 4 видно, что минимальная ошибка достигается при α = 0.3, β = 0.6. Результаты расчета ошибки прогноза на тестовых данных приведены на рис. 5. Анализ рис. 5 показал, что минимальная ошибка тестирования достигается при α = 0.2, β = 0.4.

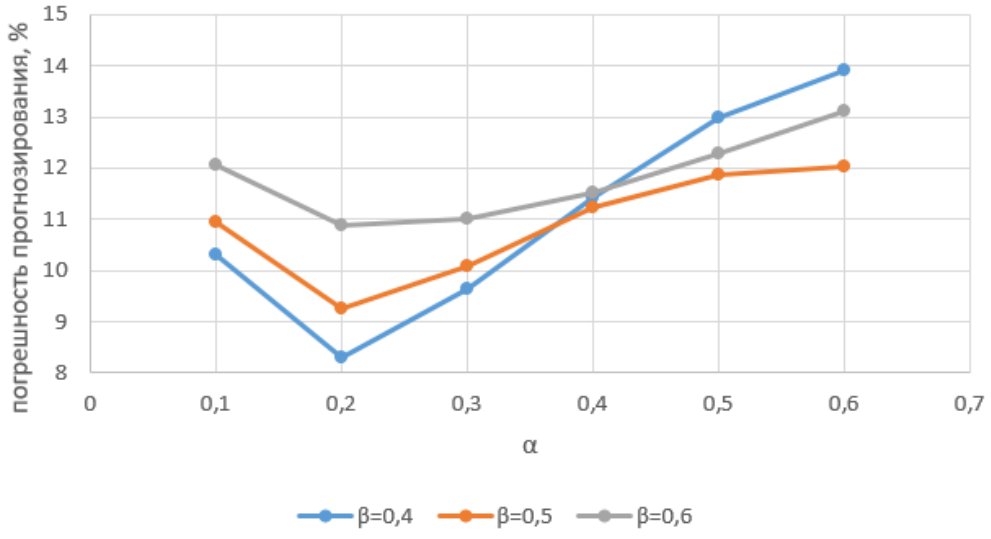

Рис. 5. Зависимость абсолютной ошибки тестирования модели от параметра сглаживания α для различных значений β

Так как значения α и β на обучающем и тестовом множествах не совпадают, учитывая, что для хорошей точности абсолютная ошибка находится в пределах от 0 % до 10 %, выбираем средние значения параметров, то есть $\alpha = 0.3$, $\beta = 0.5$.

В предложенных Дж. Боксом и Г. Дженкинсом моделях, в отличие от моделей, рассмотренных выше, применяется индивидуальный подход к каждому ряду. Существуют следующие модели Бокса–Дженкинса: авторегрессионная модель, модель скользящего среднего, смешанная модель с авторегрессией и скользящим средним, интегрированная модель авторегрессии (ARIMA) [5].

При построении ARIMA требуется анализ и выбор параметров модели. Кроме того, данные временных рядов должны быть стационарными, чтобы исключить корреляцию и мультиколлинеарность. Если исходный ряд не является стационарным, то его следует привести к стационарной форме.

Используя данные рис. 3, определим сезонный лаг при помощи спектрального анализа Фурье. Для этой цели был получен график периодограммы (рис. 6).

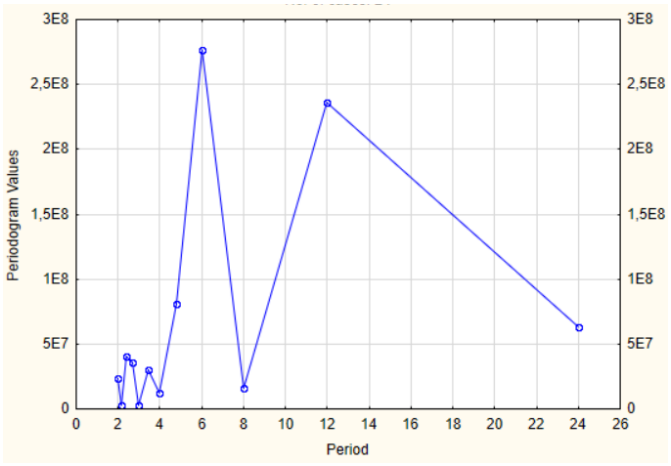

Рис. 6. График периодограммы

На графике видно максимальное значение в точке 6, то есть это значение является определяющим период сезонной составляющей рассматриваемого ряда.

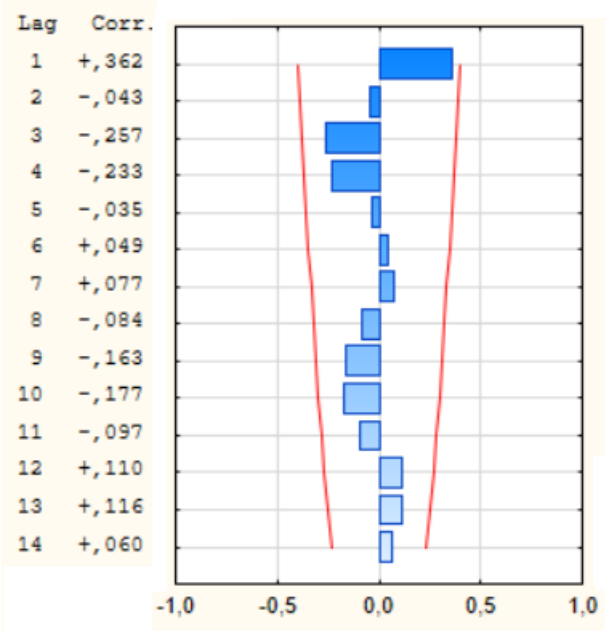

Рис. 7. Вычисленная коррелограмма преобразованного ряда

Так как коррелограмма ряда затухает с ростом лага и не превышает значения |0.3|, можно сделать вывод, что ряд обладает свойством стационарности, и для прогнозирования можно использовать модель ARIMA.

Расчеты показали, что ошибка моделирования составляет 9.1 %, что не превышает 10 %, позволяя выбрать эту модель для дальнейшей работы.

Таким образом, рассмотренные методы включают в себя следующие этапы построения: настройку моделей; отображение прогнозируемых данных в табличном или графическом виде; тестирование модели и расчет ошибки прогнозирования.

Литература

1. ГОСТ Р 53114-2008. Обеспечение информационной безопасности в организации [Электронный ресурс]. URL: https://docs.cntd.ru/document/1200075565 (дата обращения: 22.11.2022).
2. Лаборатория Касперского. Отчеты [Электронный ресурс] URL: https://www.kaspersky.ru/enterprise-security/resources (дата обращения: 22.11.2022).
3. Positive Technologies. Аналитика [Электронный ресурс] URL: https://www.ptsecurity.com/ruru/research/analytics/ (дата обращения 22.11.2022).
4. Методы защиты от DDOS нападений [Электронный ресурс]. URL: http://www.securitylab.ru/analytics/216251.php (дата обращения: 22.11.2022).
5. *Shanshan Yu, Jicheng Zhang, Ju Liu, Xiaoqing Zhang, Yafeng Li, Tianfeng Xu*. A cooperative DDoS attack detection scheme based on entropy and ensemble learning in SDN [Электронный ресурс]. URL: https://www.researchgate.net/publication/348891807 (дата обращения: 22.11.2022).
6. *Jung Woo Seo, Sangjin Lee*. A study on efficient detection of_network-based IP spoofing DDoS and malware-infected Systems [Электронный ресурс]. URL: https://www.researchgate.net/publication/309467794 (дата обращения: 22.11.2022)
7. The NSL-KDD Data Set. [Электронный ресурс]. URL: https://www.unb.ca/cic/datasets/nsl.html (дата обращения 22.11.2022).
8. *Афанасьев В. Н*. Анализ временных рядов и прогнозирование: учебник. Саратов: Ай Пи Ар Медиа, Оренбург: Оренбургский гос. ун-т, 2020. 286 с.

Лизнев Денис Сергеевич

аспирант СибГУТИ (630102, Новосибирск, ул. Кирова, 86), e-mail: liznev.denis@gmail.com, ORCID ID**:** 0009-0003-2599-8989.

Автор прочитал и одобрил окончательный вариант рукописи.
Автор заявляет об отсутствии конфликта интересов.

Overview of the Methods for Predicting Network Anomalies

Denis S. Liznev

Siberian State University of Telecommunications and Information Science (SibSUTIS)

Abstract: In this paper, the methods of predicting network anomalies are analyzed. Using the example of real statistical data, the stages of setting up forecasting models are shown. The effect of a DDoS attack on the destination IP-addresses' entropy is shown.

Keywords: exponential smoothing model, autoregressive model, entropy, network attacks.

For citation: Liznev D. S. Overview of the methods for predicting network anomalies (in Russian). *The SibSUTIS Bulletin*, 2023, vol. 17, no. 2, pp. 44-50. https://doi.org/10.55648/1998-6920-2023-17-2-44-50.

The article was submitted: 26.12.2022;
accepted for publication 10.01.2023.

References

1. GOST R 53114-2008. *Obespechenie informacionnoj bezopasnosti v organizacii* [Information security provision in organization], available at: https://docs.cntd.ru/document/1200075565 (accessed 22.11.2022).
2. *Laboratoriya Kasperskogo. Otchety* [DDoS reports], available at: https://www.kaspersky.ru/enterprise-security/resources (accessed 22.11.2022).
3. *Positive Technologies. Analitika* [Analytics], available at: https://www.ptsecurity.com/ruru/research/analytics/ (accessed 22.11.2022)
4. *Metody zashchity ot DDOS napadenij* [Methods of protection against DDOS attacks], available at: http://www.securitylab.ru/analytics/216251.php (accessed 22.11.2022)
5. Shanshan Yu, Jicheng Zhang, Ju Liu, Xiaoqing Zhang, Yafeng Li, Tianfeng Xu. *A cooperative DDoS attack detection scheme based on entropy and ensemble learning in SDN*, available at: https://www.researchgate.net/publication/348891807 (accessed 22.11.2022)
6. Jung Woo Seo, Sangjin Lee. *A study on efficient detection of_network-based IP spoofing DDoS and malware-infected Systems*, available at: https://www.researchgate.net/publication/309467794 (accessed 22.11.2022)
7. *The NSL-KDD Data Set*, available at: https://www.unb.ca/cic/datasets/nsl.html (accessed 22.11.2022)
8. Afanas'ev V. N. *Analiz vremennyh ryadov i prognozirovanie* [Time series analysis and forecasting]: Saratov, Aj Pi Ar Media, Orenburg, Orenburgskij gos. un-t, 2020. 286 p.

Denis S. Liznev
Postgraduate student, Siberian State University of Telecommunications and Information Science (SibSUTIS, Novosibirsk, Russia), e-mail: liznev.denis@gmail.com, ORCID ID: 0009-0003-2599-8989.

DOI: 10.55648/1998-6920-2023-17-2-51-58 УДК 378.14:004.891.2

Концепция оценки сформированности индикаторов достижений компетенций дисциплины на основе балльно-рейтинговой системы

А. О. Вознюк, Е. Ю. Кунц, И. А. Щербакова

Сибирский гос. унив. телекоммуникаций и информатики (СибГУТИ)

Аннотация: В статье описана концепция применения метода балльно-рейтинговой системы для оценки сформированности индикаторов достижения компетенций. Предложена математическая модель их формирования, а также представлены результаты эксперимента ручного использования описанной методики. В результате выявлена необходимость автоматизации этого процесса, подготовлены решения, необходимые для реализации автоматизированной оценки в рамках подсистемы цифрового профиля обучающегося, в том числе часть логической модели базы данных. Также предложены варианты масштабирования представленных решений.

Ключевые слова: компетенция, индикаторы достижения компетенций, цифровой профиль обучающегося, балльно-рейтинговая система, весовой коэффициент, логическая модель данных.

Для цитирования: Вознюк А. О., Кунц Е. Ю., Щербакова И. А. Концепция оценки сформированности индикаторов достижений компетенций дисциплины методом балльно-рейтинговой системы // Вестник СибГУТИ. 2023. Т. 17, № 2. С. 51–58. https://doi.org/10.55648/1998-6920-2023-17-2-51-58.

Статья поступила в редакцию 25.12.2022;
принята к публикации 10.01.2023.

1. Введение

В настоящее время вузы все чаще акцентируют свое внимание на необходимости оценки уровня сформированности различных компетенций у студентов в период их обучения [1]. При этом преподаватели оценивают уровень сформированности компетенций, полагаясь на субъективное мнение, или используют методики расчета. Стоит отметить, что чаще всего методики могут быть формализованы в пределах дисциплины или учебного заведения. Однако оценка сформированности компетенций еще не получила широкого распространения в нашей стране, но исследуются возможности принятия управленческих решений в образовательных организациях с использованием компетентностных моделей образовательных программ [2]. Одной из проблем является дополнительная нагрузка на преподавателя, а именно затрачиваемое на оценку компетенций время.

Компетенции, формируемые в рамках дисциплины, принято декомпозировать на индикаторы достижения компетенций (ИДК), которые уточняют и раскрывают формулировку компетенций в виде конкретных действий, выполняемых студентом [3]. Оценка компетенций через отдельные индикаторы позволяет формировать более полную картину об уровне сформированности компетенций и точнее определять сильные и слабые стороны студента даже в рамках одной компетенции.

2. Использование балльно-рейтинговой системы для расчета уровня сформированности ИДК

Балльно-рейтинговая система (БРС) – система, которая позволяет оценивать уровень успешности изучения дисциплины обучающимся на основе накопительного принципа. Применение БРС позволяет оценивать результаты изучения дисциплины с учетом текущей работы обучающегося в течение периода изучения дисциплины, а не только на основе итоговых аттестаций. Это говорит о возможности объективно контролировать всю учебную деятельность студентов [4].

Для применения метода БРС при оценке сформированности ИДК и дальнейшей автоматизации процесса необходимо предварительно сопоставить каждой работе ИДК, которые она формирует, и весовой коэффициент конкретного ИДК в конкретной работе для дальнейшего формирования ИДК по дисциплине.

Таким образом, можно определить математическую модель оценки уровня сформированности ИДК:

$$R = \frac{\sum_{t=1}^{n}\left(x_t \cdot k_t\right)}{\sum_{t=1}^{n} x_{tmax}} \cdot 100$$

при следующем условии:

$$\sum_{t=1}^{n} k_t = 1 ,$$

где R – балльное значение уровня сформированности ИДК;

n – количество работ, участвующих в формировании конкретного ИДК;

x_t – оценка, полученная за конкретно взятую работу;

x_{tmax} – максимальная оценка за конкретную работу;

k_t – весовой коэффициент конкретной работы.

Таким образом, в результате расчета оценки уровня сформированности ИДК получается числовое значение, которое можно сопоставить с уровнем сформированности ИДК. Для этого необходимо заранее определить методику перевода диапазона оценок в определенный уровень сформированности по принципу, представленному в табл. 1.

Таблица 1. Концепция перевода баллов в уровень сформированности ИДК

Диапазон оценок	Уровень сформированности ИДК
$< a$	Не сформирован
$[a; b]$	Низкий
$(b; c]$	Средний
$> c$	Высокий

Стоит отметить, что описанная математическая модель предложена для конкретного случая и в дальнейшем может быть изменена с учетом особенностей отдельных дисциплин для получения наилучшего эффекта от ее использования.

3. Необходимость автоматизации процесса оценки уровня сформированности ИДК

Для определения возможности применения метода для оценки ИДК был проведен эксперимент. Участниками эксперимента были студенты магистратуры, аспирантуры и преподаватели в количестве 15 человек. В ходе эксперимента участникам была представлена математическая модель для расчета оценки сформированности ИДК, а также список соответствия лабораторных работ (8 штук) и ИДК (6 штук) с указанием весовых коэффициентов и информация об оценках работ 10 студентов.

На рис. 1 представлены результаты оценивания сформированности ИДК одного студента.

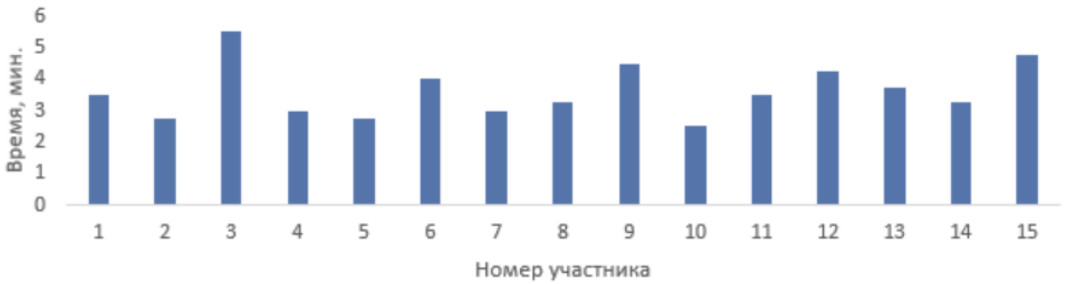

Рис. 1. Время оценки сформированности ИДК одного студента

Среднее время расчета ИДК одного студента составило 3 минуты 10 секунд. На оценку ИДК 10 студентов в среднем понадобилось 24 минуты 25 секунд. При этом двое испытуемых допустили по одной ошибке в расчетах в работах 4 и 6, трое испытуемых допустили по две ошибки в работах 4, 7 и 6, 8. В результате эксперимента было выявлено, что ручной расчет уровня сформированности ИДК является трудоемким процессом, а также не исключает возможности возникновения ошибок при расчете.

Сократить время, затрачиваемое на оценку сформированности ИДК, а также минимизировать вероятность появления ошибочных результатов (исключив влияние человеческого фактора) можно за счет автоматизации процесса оценки уровня сформированности ИДК. В простом варианте можно использовать частичную автоматизацию процесса, исключив необходимость непосредственно производить расчеты. Для этого, используя программы для работы с таблицами, необходимо настроить шаблон, в который заранее внести формулы. В таком случае преподавателю останется только внести данные по оценкам студентов за каждую работу. Тогда программа сама произведет необходимые (заранее настроенные) расчеты и выведет результаты оценки сформированности каждого ИДК по каждому студенту. При использовании данного метода также необходимо будет для каждой отдельной дисциплины настраивать шаблоны и затрачивать время на перенос данных оценок за выполненные работы студентов.

Другим вариантом является автоматизация процесса с помощью создания информационной системы (ИС), которая будет получать результаты работ и автоматически рассчитывать оценку уровня сформированности ИДК. На реализацию ИС потребуется больше времени, чем для ранее предложенных вариантов, но в долгосрочной перспективе данное решение может повысить эффективность применения БРС для расчета уровня сформированности ИДК за счет наличия типового решения, которое в удобном формате позволяет произвести «разметку» дисциплины, сопоставив каждой работе формируемые ей ИДК и соответствующие им весовые коэффициенты формирования ИДК по дисциплине.

4. Применение предложенной концепции при реализации подсистемы «Цифровой профиль студента»

Представленная методика определения уровня сформированности ИДК будет использована для реализации подсистемы «Цифровой профиль студента», рассмотренной в статье [5], которая является частью системы цифрового двойника преподавателя (ЦДП). Общая концепция ЦДП представлена на рис. 2.

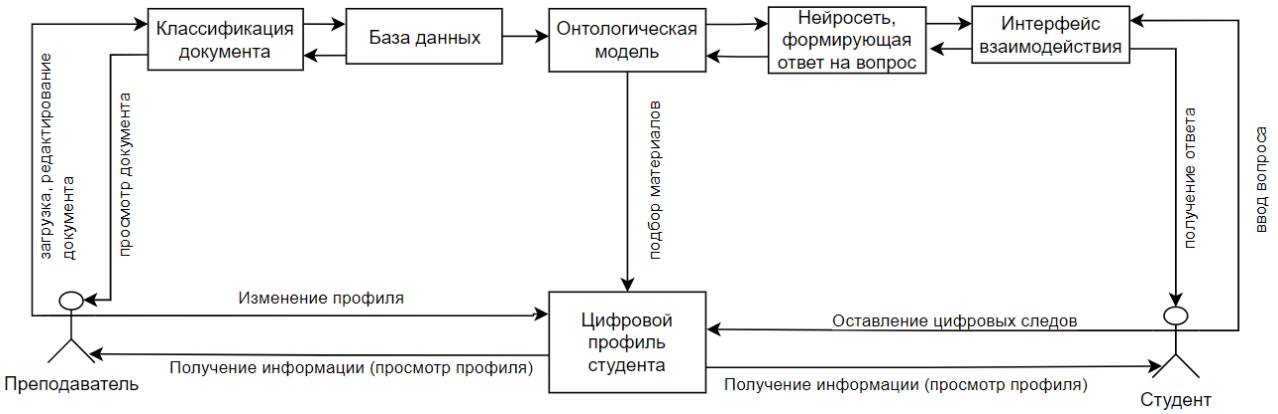

Рис. 2. Концепция ЦДП

Для использования предложенной методики в существующей подсистеме необходимо автоматизировать следующие подпроцессы:

– расчет каждого ИДК, формирующегося в рамках каждой работы;

– расчет каждого ИДК по результатам всех работ;

– перевод числового значения ИДК в соответствующий ему уровень.

Для этого предварительно были сопоставлены работы, выполняемые студентами в течение семестра, и компетенции, формирующиеся в результате их выполнения. Дополнительно тестовыми данными (для оценки возможности применения методики) были заполнены весовые коэффициенты каждой работы для конкретных компетенций. Результат представлен на рис. 3.

Индикатор достижения компетенции	Номер лабораторной работы	Весовой коэффициент
УК-1.1. Знает принципы сбора, отбора и обобщения информации, методики системного подхода для решения профессиональных задач	1	0.4
	2	0.6
УК-1.2. Умеет анализировать и систематизировать разнородные данные, оценивать эффективность процедур анализа проблем и принятия решений профессиональной деятельности	2	0.4
	3	0.6
УК-1.3. Владеет навыками научного поиска и практической работы с информационными источниками; методами принятия решений	3	0.4
ОПК-6.1. Знает основы теории систем и системного анализа, дискретной математики, теории вероятностей и математической статистики	4	0.7
	5	1
ОПК-6.2. Умеет применять методы теории систем и системного анализа, математического, статического и имитационного моделирования для автоматизации задач принятия решений, анализа информационных потоков, расчета экономической эффективности и надежности информационных систем и технологий	4	0.3
	6	0.8
	7	0.25
ОПК-6.3. Владеет навыками проведения инженерных расчетов основных показателей результативности создания и применения информационных систем и технологий	6	0.2
	7	0.75
	8	1

Рис. 3. Соотнесение ИДК и лабораторных работ

Также была определена методика, по которой будет производиться перевод баллов в уровень сформированности ИДК (табл. 2).

Таблица 2. Методика перевода баллов в уровень сформированности ИДК

Диапазон баллов	Уровень сформированности ИДК
< 60	Не сформирован
[60; 74]	Низкий
(74; 89]	Средний
> 89	Высокий

Для автоматизации процесса расчета уровня сформированности ИДК и его дальнейшего использования необходимо модернизировать существующую структуру базы данных, используемую для реализации подсистемы «Цифровой профиль студента». Спроектированный фрагмент логической модели БД для предложенной методики представлен на рис. 4.

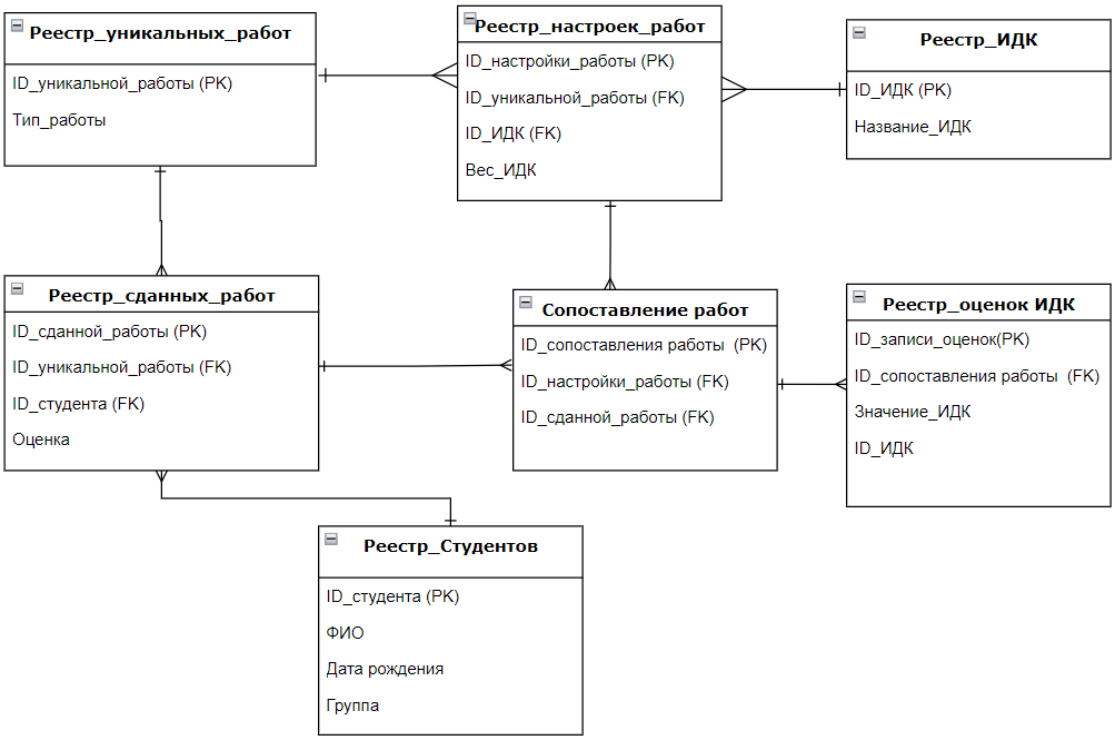

Рис. 4. Фрагмент логической модели данных

На основе представленных выше материалов будет реализовано программное решение для автоматизации процесса оценки сформированности ИДК по дисциплине для каждого студента.

5. Заключение

Применение предложенного метода балльно-рейтиноговой системы для оценки сформированности индикаторов достижений компетенций дисциплины в подсистеме «Цифровой профиль студента» позволит автоматизировать процесс расчета уровня достижения ИДК, что, в свою очередь, позволит непосредственно на основании полученных результатов фор-

мировать сводные отчеты по ИДК в профиле каждого студента и визуализировать их с помощью колес компетенций.

Автоматизация данного процесса позволит преподавателю затрачивать минимальное время для оценки уровня сформированности ИДК каждого студента. На основании полученных результатов можно будет производить анализ успешности освоения компетенций по группам, а на основе этого анализа – принимать решения о необходимости усовершенствования курса и распределения нагрузок на каждый вид работ.

Дальнейшим развитием можно считать усовершенствование методики расчета, например, за счет предоставления возможности преподавателю оценивать каждую выполненную работу непосредственно по каждой формируемой ИДК по отдельности, а не одной общей оценкой за выполненную работу.

Литература

1. *Бершадская М. Д., Серова А. В., Чепуренко А. Ю., Зима Е. А.* Компетентностный подход к оценке образовательных результатов: опыт Российского социологического образования // Высшее образование в России. 2019. Т. 28, № 2. С. 38–50.
2. *Кунц Е. Ю., Ложников П. С.* Использование компетентностной модели образовательной программы для принятия управленческих решений в образовательной организации // Прикаспийский журнал: управление и высокие технологии. 2022. № 2 (58). С. 27–34.
3. *Бершадская М. Д., Серова А. В.* Универсальные компетенции: индикаторы, опыт разработки и оценивания [Электронный ресурс] // Научно-методическая конференция ассоциации классических университетов, 23 мая 2018. URL: https://knastu.ru/media/files/page_files/teachers/Bershadskaya_UK_-_indikatory_opyt_razrabot..tsenivaniya_Seminar_AKUR_05.2018.pdf (дата обращения: 26.10.2022).
4. *Данилова С. А.* Применение балльно-рейтинговой системы как условие повышения качества обучения // Научно-методический электронный журнал «Концепт». 2017. Т. 11. С. 68–70. URL: https://e-koncept.ru/2017/770155.htm (дата обращения: 26.10.2022).
5. *Вознюк А. О., Кунц Е. Ю., Смирнов А. В.* Принцип формирования цифрового компетентностного профиля обучающегося // Материалы РНТК «Общество, политика, финансы», Новосибирск, 2022. С. 210–218.

Вознюк Алина Олеговна
студентка магистратуры кафедры математического моделирования и цифрового развития бизнес-систем, Сибирский государственный университет телекоммуникаций и информатики, e-mail: a.voznyuk@stud.sibguti.ru, ORCID ID: 0000-0002-5929-3990.

Кунц Екатерина Юрьевна
старший преподаватель кафедры математического моделирования и цифрового развития бизнес-систем, Сибирский государственный университет телекоммуникаций и информатики (СибГУТИ, 630102, Новосибирск, ул. Кирова, 86), тел. +7 383 2698 299, e-mail: kuntsey@sibguti.ru, ORCID ID: 0000-0003-3903-4737.

Щербакова Ирина Александровна
студентка кафедры математического моделирования и цифрового развития бизнес-систем, Сибирский государственный университет телекоммуникаций и информатики, e-mail: irina-shbk@mail.ru, ORCID ID: 0000-0001-5148-1383.

Авторы прочитали и одобрили окончательный вариант рукописи.
Авторы заявляют об отсутствии конфликта интересов.
Вклад соавторов: *Каждый автор внес равную долю участия как во все этапы проводимого теоретического исследования, так и при написании разделов данной статьи.*

The Concept of Assessing the Achievements' Indicators Formation of the Discipline's Competencies by the Score-rating System

Alina O. Voznyuk, Ekaterina Yu. Kunts, Irina A. Sherbakova

Siberian State University of Telecommunications and Information Science (SibSUTIS)

Abstract: In this paper, the concept of using the method of the score-rating system to assess the achievements' indicators formation of competencies is considered. A mathematical model of their formation is proposed and the results of the manual use experiment of the described technique are presented. As a result, the need for automation of this process has been identified and solutions necessary for the implementation of automated assessment within the subsystem of the digital profile of the student, including part of the logical database model, have been prepared. Options for scaling the presented solutions are also proposed.

Keywords: competence, indicators of competence competencies, digital profile of the student, point-rating system, weight factor, logical data model.

For citation: Voznyuk A. O., Kunts E. Yu., Sherbakova I. A. The concept of assessing the achievements' formation of the discipline's competencies by the score-rating system (in Russia). *The SibSUTIS Bulletin*, 2023, vol. 17, no. 2, pp. 51-58. https://doi.org/10.55648/1998-6920-2023-17-2-51-58.

The article was submitted: 25.12.2022;
accepted for publication 10.01.2023.

References

1. Bershadskaya M. D., Serova A. V., Chepurenko A. Yu., Zima E. A. Kompetentnostnyj podhod k ocenke obrazovatel'nyh rezul'tatov: opyt Rossijskogo sociologicheskogo obrazovaniya [Competence-based Approach to the Evaluation of Learning Outcomes: Russian Experience in Sociological Education]. *Vysshee obrazovanie v Rossii = Higher Education in Russia*, vol. 28, no. 2, pp. 38-50.
2. Kunts E. Yu., Lozhnicov P. S. Ispol'zovanie kompetentnostnoj modeli obrazovatel'noj programmy dlya prinyatiya upravlencheskih reshenij v obrazovatel'noj organizacii [Using the competence model of an educational program for making managerial decisions in an educational organization]. *Prikaspijskij zhurnal: upravlenie i vysokie tekhnologii*, 2022, no. 2 (58), pp. 27-34.
3. Bershadskaya M. D., Serova A. V. Universal'nye kompetencii: indikatory, opyt razrabotki i ocenivaniya [Universal competencies: indicators, development and evaluation experience]. *Nauchno-metodicheskaya konferenciya associacii klassicheskih universitetov*, 23 May, 2018, available at: https://knastu.ru/media/files/page_files/teachers/Bershadskaya_UK_-_indikatory_opyt_razrabot..tsenivaniya_Seminar_AKUR_05.2018.pdf (accessed 26.10.2022).
4. Danilova S. A. Primenenie ball'no-rejtingovoj sistemy kak uslovie povysheniya kachestva obucheniya [The use of a point-rating system as a condition for improving the quality of education]. *Nauchno-*

metodicheskij elektronnyj zhurnal «Koncept», 2017, vol. 11, pp. 68–70, available at: https://e-koncept.ru/2017/770155.htm (accessed 26.10.2022).

5. Voznyuk A. O., Kunts E. Yu., Smirnov A. V. Princip formirovaniya cifrovogo kompetentnostnogo profilya obuchayushchegosya [The principle of forming a digital profile of a student in the concept of a digital double of a teacher]. *Obshchestvo, politika, finansy. Materialy Rossijskoj nauchno-tekhnicheskoj konferencii*, Novosibirsk, 2022, pp. 210-218.

Alina O. Voznyuk

Master's student, the Department of Mathematical Modeling and Digital Development of Business Systems, Siberian State University of Telecommunications and Information Science, e-mail: a.voznyuk@stud.sibguti.ru, ORCID ID: 0000-0002-5929-3990.

Ekaterina Yu. Kunts

Senior Lecturer, the Department of Mathematical Modeling and Digital Development of Business Systems, Siberian State University of Telecommunications and Information Science (SibSUTIS, Russia, 630102, Novosibirsk, Kirov St. 86), phone: +7 383 2698 299, e-mail: kuntsey@sibguti.ru, ORCID ID: 0000-0003-3903-4737.

Irina A. Sherbakova

Student, the Department of Mathematical Modeling and Digital Development of Business Systems, Siberian State University of Telecommunications and Information, e-mail: irina-shbk@mail.ru, ORCID ID: 0000-0001-5148-1383.

DOI: 10.55648/1998-6920-2023-17-2-59-68 УДК 004.04:576.08

Система показателей цифровой зрелости научно-педагогического работника[1]

Т. Л. Самков[1], А. Н. Полетайкин[1, 2]

[1] Сибирский гос. унив. телекоммуникаций и информатики (СибГУТИ)
[2] Кубанский государственный университет (КубГУ)

Аннотация: Рассматривается задача оценивания цифровой зрелости работников образовательной организации высшего образования (ООВО). Целью исследования является повышение адекватности оценивания цифровых компетенций в задаче оценивания цифровой зрелости ООВО. На основе анализа существующих технологий оценивания цифровых компетенций выполнен синтез авторской модели оценивания цифровой зрелости научно-педагогического работника ООВО. Новизна исследования состоит в разработке взвешенной системы показателей цифровой зрелости работника посредством построения и исследования знакового графа когнитивной карты с применением групповой экспертизы и метода анализа иерархий.

Ключевые слова: цифровая зрелость работника, показатели цифровой зрелости, система показателей, когнитивная карта, знаковый граф, метод анализа иерархий.

Для цитирования: Самков Т. Л., Полетайкин А. Н. Система показателей цифровой зрелости научно-педагогического работника // Вестник СибГУТИ. 2023. Т. 17, № 2. С. 59–68. https://doi.org/10.55648/1998-6920-2023-17-2-59-68.

Статья поступила в редакцию 25.12.2022;
принята к публикации 10.01.2023.

1. Введение

В рамках выполнения в 2022 году кафедральной научно-исследовательской работы (НИР) «Модели, алгоритмы гибридного моделирования и информационные технологии конструктивной цифровой трансформации деятельности образовательной организации»[1] разработана новая технология оценивания цифровой зрелости (ЦЗ) образовательной организации высшего образования (ООВО) [1]. При этом полученные результаты по слою 2 Компетенции, главным образом по показателю 2.1 «Уровень развития цифровых компетенций сотрудников», оказались существенно выше относительно других блоков, прежде всего оценок ряда показателей, так или иначе связанных с цифровой компетентностью субъекта деятельности, что вызывает обоснованные сомнения в достоверности этих оценок. Дополнительные исследования [2] показали адекватность этих методик и обнаружили проблему повышения достоверности оценок цифровой зрелости.

[1] Работа выполнена при финансовой поддержке Фонда прикладных научных исследований СибГУТИ.

2. Оценивание цифровых компетенций работников ООВО

В настоящее время определить уровень своей цифровой грамотности предлагают многие новаторы от цифровизации. Рассмотрим 3 наиболее характерных примера таких решений.

I. Наиболее популярный ресурс ЦифровойДиктант.рф – платформа для измерения и повышения цифровой грамотности пользователей Рунета, а также проведения партнерских и корпоративных тестирований в области digital. Ежегодные всероссийские акции «Цифровой Диктант», проводимые на этой платформе с 2019 года, признаны самыми масштабными в России проверками знаний в области цифровой грамотности [3]. На платформе реализован ряд дополнительных возможностей, таких как проведение корпоративных диктантов и пр.

II. Еще одно популярное решение – «Сервис готовности к цифровой экономике» [4] – предлагает Университет 20.35 – первый в России инновационный сетевой университет, сочетающий в себе исследовательскую и образовательную организации и IT-компанию.

Предусмотрено 5 направлений для оценки компетенций: цифровые устройства и сети, цифровая безопасность, коммуникации и сотрудничество, работа с информацией и цифровым контентом, цифровая личность. Результаты тестирования и сертификат сохраняются в цифровом профиле. Результаты вычисляются в баллах согласно шкале от 0 до 100 баллов с дифференциацией уровней: недостаточный, начальный, средний, продвинутый.

III. Наконец, третий платформенный сервис регионального уровня привлёк наше внимание в частности направленностью процедуры оценивания на научно-педагогических работников (НПР). Портал «Цифровой гражданин Югры» позволяет проверить уровень своих цифровых компетенций для а) рядовых сотрудников организаций, б) руководителей исполнительных органов власти, в) преподавателей вузов, г) школьных учителей [5].

Испытуемому предлагается проанализировать свои сильные и слабые стороны в использовании цифровых технологий в обучении и оценить себя по каждой из 22-х компетенций, выбрав 1 из 5 вариантов ответа, потенциально отражающих разные уровни ЦЗ НПР. Все компетенции оцениваются в баллах и соотносятся с шестью уровнями опыта согласно шкале от 0 до 100 с дифференциацией уровней: новичок, исследователь, интегратор, эксперт, лидер, новатор.

Сравнительный анализ рассмотренных решений показан в табл. 1. Все они позволяют не только оценить уровень цифрового развития работника, но и проанализировать его текущее состояние цифровой зрелости (для решений I и II провести работу над ошибками) и сформировать индивидуальную траекторию развития недостающих цифровых знаний и навыков. По итогам успешной оценки выдается электронный сертификат в форме официального документа, который в некотором приближении можно понимать как паспорт ЦЗ работника.

Таким образом, любая из рассмотренных методик может быть принята для оценивания цифровых компетенций. Однако, учитывая специфику предметной области, наиболее логично выбрать решение III в модификации в) для преподавателей вузов.

3. Разработка авторской системы показателей цифровой зрелости НПР

Для идентификации осознаваемых связей конкретных навыков применения информационных технологий в профессиональной деятельности НПР организован опрос работников кафедры ММиЦРБС. Выдвигая в качестве инструмента исследования данный опросник, ставится цель определить, какие навыки работников ООВО и приемы в применении IT-технологий в рамках учебного процесса влияют на другие, такие же навыки, используемые сотрудниками (кафедры, вуза).

Респондентам предлагалось дать оценку 42 сравнительным ситуациям по 7 основным компетенциям этого опросника. И далее сделать то же самое для подчиненных компетенций, входящих в указанные компетенции, что в среднем составляет 12 сравнительных ситуаций для каждой основной компетенции.

Таблица 1. Сравнительный анализ существующих решений для оценивания цифровых компетенций работника

Показатель	Решение I	Решение II	Решение III
Специализированная направленность	Нет	Да	Да
Уровень интеграции платформы	Федеральный		Региональный
Число категорий респондентов	4	Нет	4
Стратификация респондентов	Возрастная	Нет	Профессиональная
Число блоков компетенций	4	5	6
Число контрольных заданий	48	65	22
Тип контрольных заданий	Выбор из множества ответов		
Форма ответа на задания	Выбор правильных ответов		Самооценка
Число уровней развития на шкале	10	4	6
Возможность работы над ошибками	Да	Да	Нет
Наличие рекомендаций по итогам	Нет	Да, кратко	Да, развёрнуто

В результате каждая основная и каждая подчиненная компетенции (факторы) получат свои обоснованные веса, которые помогут понять как отдельным работникам ООВО, так и структурным подразделениям, на каких именно компетенциях им стоит особенно сосредоточить свои ресурсы, в том числе финансовые.

Предлагаемый опрос даст возможность пересмотреть собственные подходы НПР к переводу своих образовательных технологий в цифру и их взаимодействию. В рамках данного опроса необходимо вынести свое суждение, основываясь на своем опыте, по взаимодействию 28 аспектов научно-преподавательской работы НПР, состоящих из 6 личностных характеристик и 22 компетенций, отобранных по результатам более ранних исследований. Оценочная ситуация, для которой нужно вынести свое суждение, имеет вид сравнения предлагаемых двух факторов, куда и входят указанные выше 28 аспектов, называемых далее подфакторами, объединенных в основные факторы. При этом сначала сравниваются основные 7 факторов между собой, а далее – от 3 до 5 подфакторов, входящих в каждый основной фактор. Свое мнение НПР, выступающий в роли эксперта, по каждой оценочной ситуации формулировал по трехбалльной шкале:

– 1: один фактор ослабляет другой, рост одного приводит к снижению другого и наоборот (отрицательная связь);

0: один фактор никак не влияет на другой, и то же самое верно относительно обратного влияния (отсутствие связи);

+ 1: один фактор усиливает другой, рост одного приводит к росту другого и наоборот (положительная связь).

Основные факторы, выражая и обобщая цифровые компетенции НПР, состоят из набора характеристик, представленных в табл. 2.

Для указанных факторов, зная их содержание в рамках учебного процесса, заполняется таблица попарного сравнения их влияния друг на друга для дельнейшего их взвешивания по важности когнитивных связей согласно трехбалльной шкале, приведенной выше. Необходимо проставить значения -1, 0, +1, причем если от одного фактора до другого идет один тип связи, то обратно тип может меняться, или связь вообще отсутствует, если об этом говорит профессиональный опыт НПР.

Подчиненные или составляющие факторы (подфакторы). После оценки взаимосвязей основных факторов, проведенной на первом этапе, возникает необходимость также оценить преимущества подфакторов этих основных факторов над другими. При оценке принимают: один подфактор значимее другого – 1, иначе – 0, при их равнозначности – 0.5. Принцип по-

строения таблиц попарного сравнения аналогичен рассмотренному выше примеру. По каждому фактору формируется матрица, размерность которой определяется содержанием опросного листа.

Таблица 2. Список основных факторов с их именами и категориями

Фактор	Мощность*	Категория	Описание
1. Статус преподавателя	5	1 тип: навыки IT-грамотности	имеющиеся у опрашиваемого должность, возраст, стаж, опыт в IT (в годах), доля преподавания IT (в %)
2. Профессиональные обязанности	4	2 тип: итоги обучения и НИР	регулярное использование IT в общении, совместной работе со студентами и НПР в группах и вне их, а также в развитии цифровых навыков и самообучения
3. Цифровые ресурсы	3	2 тип: итоги обучения и НИР	стабильное применение IT для поиска информационных ресурсов, создания своих материалов, защиты личной информации
4. Преподавание и обучение	4	1 тип: навыки IT грамотности	уверенное задействование IT для целеполагания внедрения IT в учебе, интерактивного контроля учебы, организации учебы в группах, создания среды самообучения студентов
5. Оценка студентов	3	2 тип: итоги обучения и НИР	постоянное задействование IT в отслеживании прогресса студентов, для контроля тех из них, кого нужно поддерживать, предоставления студентам обратной связи
6. Рост прав/потенциала студентов	3	2 тип: итоги обучения и НИР	постоянное наращивание через IT создания для студентов цифровых заданий, оценки сложностей их выполнения, персонализации обучения студентов, способствование учебной активности
7. Рост IT-грамотности студентов	5	2 тип: итоги обучения и НИР	четкое стимулирование студентов в областях IT: оценка достоверности информации, ввод IT в коворкинг студентов, креативизация цифрового контента, обучение безопасному применению IT, побуждение к IT-подходу в решении задач

* – Число вопросов в опроснике

Подобный анализ работы (навыков) преподавателя более информативен и подробен, чем просто оценка профессиональных качеств НПР сторонним наблюдателем. Для организации такого когнитивного анализа этого оценочного процесса предлагается использовать следующую схему.

1. Определяют значимые факторы 1-го типа – навыки IT-технологий преподавателя.

2. Определяют значимые факторы 2-го типа – итоги учебной и научной работы преподавателя.

3. Выписывают в отдельных строках таблицы все возможные сочетания указанных факторов, не различая типы, т.к. между факторами одинаковых типов могут быть неочевидные связи (или нет).

4. По каждому сочетанию для конкретного преподавателя группа экспертов (численность группы неограниченна) оценивает попарно на отношения причинности факторов (обозначаемых x и y):

"+" – положительное (с увеличением или уменьшением значения x увеличивается или уменьшается значение y);

"–" – отрицательное (с увеличением или уменьшением значения x уменьшается или увеличивается значение y);

"0" – нулевое (отсутствие отношения причинности).

5. Делается вывод об общей причинности связи конкретного сочетания факторов того или иного преподавателя на базе преобладающего мнения экспертов (чего больше всего – "+", "–" или "0").

6. Усредняют результаты отношений причинности всех преподавателей по каждому набору факторов на основе преобладающего числа преподавателей с одинаковым характером причинности.

7. На основании связей с ненулевым отношением причинности строят знаковый граф – он, собственно, и является когнитивной картой ситуации.

8. Из графа выделяют одну или несколько т.н. «роз» – замкнутых подграфов с замкнутыми вокруг одной вершины (фактора) циклов разной длины, состоящих из набора вершин и ребер (связей).

9. Для каждой «розы» проводят анализ ее связей, на локальную и глобальную устойчивость, стабильность и нестабильность факторов, на базе чего определяются веса факторов – это далее служит обоснованием приложения усилий по наращиванию IT-навыков к факторам с наибольшими весами.

Расчет балльных и весовых оценок факторов, чьи возможные попарные сочетания были рассмотрены группой экспертов, достаточно прост. Сначала для каждого из факторов берут сочетания, исходящие из него, и поочередно для экспертов считают накопленные суммы их балльных оценок относительно наличия связи в данном сочетании:

$$v_{ki} = \sum_{j=1}^{m-1} v_{kij}, i = \overline{1,m},\ k = \overline{1,n}, \quad (1)$$

где $v_{k\,i}$ – балльная оценка i-го фактора k-ым экспертом, а $v_{k\,i\,j}$ – трехбалльная (-1, 0, 1) степень связи между факторами i и j, данная экспертом k. Тогда общая балльная оценка i-го фактора v_i рассчитывается как среднее по всем n экспертам:

$$v_i = \sum_{k=1}^{n} v_{ki}, i = \overline{1,m}, \quad (2)$$

а веса факторов w_i на его основе находим с помощью стандартной процедуры:

$$w_i = v_i / \sum_{i=1}^{m} v_i, i = \overline{1,m}. \quad (3)$$

Так, получены следующие веса основных факторов: w_1 = 0.145; w_2 = 0.203; w_3 = 0.110; w_4 = 0.128; w_5 = 0.110; w_6 = 0.140; w_7 = 0.163.

Далее необходимо вычислить веса подфакторов для каждого из семи основных факторов. Обозначим число подфакторов для каждого фактора w_i как r_i, а счетчик подфакторов будет l. Тогда веса подфакторов фактически являются долями от веса основного фактора, и для них можно записать:

$$w_{il} = w_i \cdot p_{il}, i = \overline{1,m}, l = \overline{1,r_i}, \quad (4)$$

где w_{il} и p_{il} – соответственно вес и доля l-го подфактора относительно i-го основного фактора. При этом должно выполняться требование «укладывания» суммы весов подфактора в границы их основного родительского фактора:

$$w_i = \sum_{l=1}^{r_i} w_l, i = \overline{1,m}. \quad (5)$$

Сам же поиск долей p_l подфакторов также осуществляется на основе группового опроса тех же экспертов из числа НПР кафедры, только по верхней половине матрицы сравнения, где мнения экспертов усредняются следующим образом (l и h – индексы подфакторов в матрице сравнения):

$$q_{kil} = \sum_{h=1}^{r_i-1} q_{kilh}, i = \overline{1,m},\ l = \overline{1,r_i},\ k = \overline{1,m}, \quad (6)$$

где q_{kil} – балльная оценка сравнения l-го фактора с другими подфакторами i-го фактора k-ым экспертом, а q_{kilh} – трехбалльная (0, 0.5, 1) степень превосходства фактора l над фактором h, данная экспертом k для фактора i.

Агрегированная балльная оценка l-го подфактора i-го фактора q_{il} рассчитывается как среднее по всем n экспертам:

$$q_{il} = \sum_{k=1}^{n} q_{kil},, i = \overline{1,m},\ l = \overline{1,r_i}. \quad (7)$$

Тогда средние балльные оценки рассчитываются путем их накопления в сумме:

$$q_{il} = \sum_{h=l+1}^{r_i} q_{ilh}, i = \overline{1,m},\ l = \overline{1,r_i}. \quad (8)$$

Доли (веса) подфакторов p_{il} находим с помощью стандартной процедуры:

$$p_{il} = q_{il} / \sum_{l=1}^{r_i} q_{il}, i = \overline{1,m},\ l = \overline{1,r_i}. \quad (9)$$

Далее на основе приведенных в данном разделе формул и экспертных опросов НПР найдем веса подфакторов основных факторов. В итоге получим ряд таблиц, одна из которых показана в табл. 3. Из табл. 3 и формулы (1) ищем доли подфакторов в весе фактора 3 (w_3 = 0.110) и их веса: p_{31} = 0.26; p_{32} = 0.30; p_{33} = 0.30, откуда следует, что w_{31} = 0.049; w_{32} = 0.043; w_{33} = 0.018.

Таблица 3. Балльные и весовые оценки подфакторов для фактора 3 в рамках групповой экспертизы

эксперты / факторы		Оценки экспертов									Σ баллов	Веса факторов
		№ 1	№ 2	№ 3	№ 4	№ 5	№ 6	№ 7	№ 8	№ 9		
x	y	q_{13lh}	q_{23lh}	q_{33lh}	q_{43lh}	q_{53lh}	q_{63lh}	q_{73lh}	q_{83lh}	q_{93lh}	q_{il}	p_{il}
3.1	3.2	0.5	1	1	0.5	0	0.5	0.5	1	0.5		
3.1	3.3	0.5	0.5	1	1	1	1	0.5	0	1		
q_{k31}		1.00	1.50	2.00	1.50	1.00	1.50	1.00	1.00	1.50	1.33	0.44
3.2	3.1	0.5	0	0	0.5	1	0.5	0.5	0	0.5		
3.2	3.3	0.5	0	1	0.5	1	1	1	1	1		
q_{k32}		1.00	0.00	1.00	1.00	2.00	1.50	1.50	1.00	1.50	1.17	0.39
3.3	3.1	0.5	0.5	0	0	0	0	0.5	1	0		
3.3	3.2	0.5	1	0	0.5	0	0	0	0	0		
q_{k33}		1.00	1.50	0.00	0.50	0.00	0.00	0.50	1.00	0.00	0.50	0.17

Связи основных факторов могут быть неустойчивы либо, наоборот, отличаться повышенной стабильностью, влияя при этом в большей, чем видится экспертам, степени на другие факторы. Поэтому на основе результатов опросов экспертов, учитывая условия обработки этих результатов, необходимо:

– выбрать дуги, их знаки и на основе этого построить знаковый граф;

– выработать рекомендации для всевозможных изменений знаков дуг, образующих замкнутые циклы.

1. Рассчитаем итоговые результаты по таблице оценки экспертов отношений причинности, а также наличие когнитивной связи между факторами, изображаемой как дуга между точками, представляющими эти факторы. Это берется за начальную базу построения графа, и на основе этих результатов строится первый вариант знакового графа с предварительным описанием дуг и их знаков. При этом направлением дуги считается стрелка, идущая от пере-

менной *x* к *y*, и если большинство экспертов указали суждение типа "0", то считается, что связи нет, и дуга не проводится.

2. Построим граф по результативным оценкам экспертами и правил выше для знаков "0", "+", "–". Результаты анализа наличия дуг по результатам опроса показывает, что большинство экспертов скептически относятся к наличию обратных связей между факторами, т.е. не признают саморегулирующихся процессов, поэтому в графе, который будет представлять когнитивную карту, появится только одна отрицательная дуга, вокруг неё и планируется делать розу. Кроме того, многие эксперты скептически относятся к связям фактора 1 – качающихся личных качеств НПР – с остальными факторами, в силу чего дуги от него часто отсутствуют.

Знаковый граф (когнитивная карта ситуаций), построенный по опросам экспертов, обычно получается достаточно сложным. В данном исследовании он получил вид, представленный на рис. 1а. Знаковый граф может быть использован для качественной оценки влияния отдельных вершин знакового графа на устойчивость системы.

В силу сложности графа ограничимся лепестками длины 2 при построении розы. На рис. 1б циклами в розе будут пути с дугами (1–2–1), (3–2–3), (4–2–4), (5–2–5), (6–2–6), (7–2–7), имеющими значения отношений причинности (–, +), (+, +), (+, +), (+, +), (+, +), (+, +). Соответственно, обратные связи могут привести к неустойчивости системы.

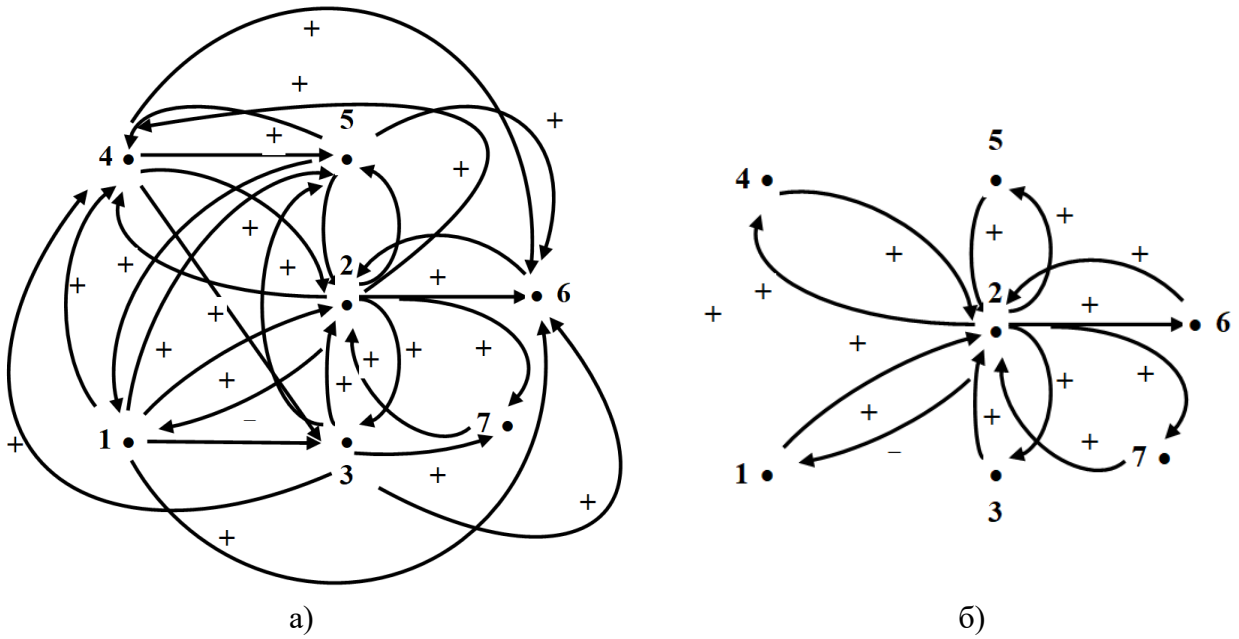

Рис. 1. Структура когнитивной карты в виде:
а) знакового графа, б) основной розы когнитивной карты на базе знакового графа

Соответственно, те факторы, которые чаще других присутствуют в тех дугах, которые при изменении их знака придают розе устойчивость (локальную и глобальную), – это значимые факторы, поэтому они должны быть скорректированы, получив определенную «прибавку» к своим весам. Это же касается и тех факторов, которые стоят в тех дугах, изменение знаков которых не оказывает существенного влияния на устойчивость розы, – это незначимые факторы, поэтому только их веса должны быть уменьшены, увеличивая тем самым значимые факторы.

В результате проведенного анализа, расчеты по которому опущены в силу их громоздкости, выяснилось, что значимыми являются факторы 2, 3, 4, 5, а незначимыми – факторы 1, 6, 7. Таким образом, получаем таблицу итоговых весов основных факторов и их подфакторов, которая показана на рис. 2.

Номер и наименование фактора	Вес
1. Статус преподавателя	**0,083**
1.1. Должность	0,020
1.2. Возраст	0,020
1.3. Стаж	0,015
1.4. Опыт в IT (в годах)	0,016
1.5. Доля преподавания IT (в %)	0,012
2. Профессиональные обязанности	**0,251**
2.1. Контакты с НПР и студентами	0,066
2.2. Коворкинг со студентами и НПР	0,075
2.3. Развитие цифровых навыков	0,075
2.4. Цифровое самообучение	0,035
3. Цифровые ресурсы	**0,158**
3.1. Поиск информационных ресурсов	0,070
3.2. Создание своих материалов	0,062
3.3. Защита личной информации	0,026
4. Преподавание и обучение	**0,176**
4.1. Целеполагания внедрения IT в учебе	0,055
4.2. Интерактивный мониторинг учебы	0,050

Номер и наименование фактора	Вес
4.3. Организация учебы в группах	0,046
4.4. Создание среды самообучения студентов	0,024
5. Оценка студентов	**0,158**
5.1. Отслеживание прогресса студентов	0,079
5.2. Контроль студентов для поддержки	0,050
5.3. Защита личной информации	0,029
6. Рост прав/потенциала студентов	**0,080**
6.1. Создание цифровых заданий	0,038
6.2. Персонализация обучения студентов	0,018
6.3. Способствование учебной активности	0,024
7. Рост IT-грамотности студентов	**0,093**
7.1. Оценка достоверности информации	0,016
7.2. Ввод IT в коворкинг студентов	0,019
7.3. Креативизация цифрового контента	0,022
7.4. Обучение безопасному применению IT	0,017
7.5. Ориентация на IT-подход в решении задач	0,019

Рис. 2. Список основных факторов и их подфакторов с соответствующими весами

По итогам данного выполненного этапа по комплексу работ были получены следующие результаты:

– даны краткие названия и нумерация всем 7 основным факторам и 27 подфакторам, введенным при выполнении предшествующих этапов НИР;

– разработана и описана многошаговая процедура экспертного опроса по оценке значимости указанным 7 основным факторам и 27 подфакторам, введенным при выполнении предшествующих этапов НИР;

– произведен поиск первичных весов основных факторов и подфакторов на основе данных попарного сравнения, полученных на основе опроса;

– осуществлено построение знакового графа на основе мнений экспертов по наличию когнитивных связей между основными семью факторами на основе несимметричного парного сравнения;

– выделена роза из построенного знакового графа в виде усеченного графа с замкнутыми циклами вокруг ее центра и исследована на устойчивость процессов, протекающих внутри ее замкнутых циклов – лепестков;

– определены на основе анализа устойчивости процессов выделенной розы значимые и незначимые факторы, представленные в ней в качестве ее вершин;

– скорректированы веса факторов обоих видов путем перераспределения части совокупных весов незначимых факторов в качестве своего рода «прибавок» к значимым факторам при сохранении общей суммы весов факторов равной единице;

– сформирована таблица итоговых весов факторов после проведенных расчетов.

4. Заключение

Полученные веса могут в дальнейших исследованиях корректироваться, равно как и состав факторов. Однако, вне зависимости от вариации указанных характеристик проводимого анализа такого рода, полученные веса можно использовать в качестве долевого соотношения предлагаемых курсов повышения квалификации НПР, так или иначе привязанных к компетенциям, которые выражены исследуемыми факторами, а также соотношениями объемов финансирования проведения таких курсов (оплата преподавателей, серверы для дистанционного преподавания, подготовка и содержание учебных аудиторий для очных занятий).

Литература

1. Модели, алгоритмы гибридного моделирования и информационные технологии конструктивной цифровой трансформации деятельности образовательной организации / В.С. Канев, Л.Ф. Данилова, Ю.В. Шевцова, А.Н. Полетайкин, Т.И. Монастырская, Т.Л. Самков, С.М. Лукина // Отчет о НИР, 2022. 146 с.
2. *Полетайкин А.Н., Шевцова Ю.В., Монастырская Т.И., Данилова Л.Ф.* Перспективы и вызовы цифровой трансформации образовательной деятельности в СибГУТИ // Актуальные проблемы высшего профессионального образования в России: перспективы и вызовы. Материалы LXIV межвузовской научно-методической конференции, 9 февраля – 10 февраля 2023 г. / Сибирский государственный университет телекоммуникаций и информатики. – Новосибирск: СибГУТИ, 2023. С. 123-130.
3. Цифровой Диктант [электронный ресурс]. URL: `https://digitaldictation.ru/about` (дата обращения: 30.12.2021).
4. Сервис готовности к цифровой экономике [электронный ресурс]. URL: `https://готовкцифре.рф` (дата обращения: 30.12.2021).
5. Цифровые компетенции / Портал «Цифровой гражданин Югры» [официальный сайт]. URL: `https://цифровойгражданинюгры.рф/gosuslugi/` (дата обращения: 30.12.2021).

Самков Тимур Леонидович

к.т.н., доцент кафедры математического моделирования и цифрового развития бизнес-систем, СибГУТИ (630102, Новосибирск, ул. Кирова, 86), тел. +7 383 2698 278, e-mail: `ermin@ngs.ru`, ORCID ID: 0000-0001-6400-7672.

Полетайкин Алексей Николаевич

к.т.н., доцент, доцент кафедры информационных технологий, Кубанский государственный университет (350040, Краснодар, ул. Ставропольская, 149), e-mail: `alex.poletaykin@gmail.com`, ORCID ID: 0000-0002-5128-1952.

Авторы прочитали и одобрили окончательный вариант рукописи.

Авторы заявляют об отсутствии конфликта интересов.

Вклад соавторов: *Каждый автор внес равную долю участия, как во все этапы проводимого теоретического исследования, так и при написании разделов данной статьи.*

The System of Digital Maturity Indicators of a Scientific and Pedagogical Staff

Timur L. Samkov[1], Aleksey N. Poletaikin[1, 2]

[1] Siberian State University of Telecommunications and Information Science (SibSUTIS)
[2] Kuban State University (KubSU, Krasnodar, Russia).

Abstract: The problem of assessing digital maturity of employees of an educational organization of higher education (EOHE) is considered. The aim of the study is to increase the assessment of digital competencies adequacy in the task of assessing the digital maturity of the EOHE. Based on the analysis of existing technologies for assessing digital competencies, the synthesis of the author's model for assessing the digital maturity of a scientific and pedagogical employee of the EOHE was carried out. The novelty of the research lies in the development of indicators

weighted system of an employee digital maturity via the construction and study of the iconic graph of the cognitive map using group expertise and the method of hierarchy analysis.

Keywords: digital maturity of an employee, indicators of digital maturity, a system of indicators, a cognitive map, a sign graph, a method for analyzing hierarchies.

For citation: Samkov T. L., Poletaikin A. N. The system of digital maturity of a scientific and pedagogical staff (in Russian). *The SibSUTIS Bulletin*, 2023, vol. 17, no. 2, pp. 59-68. https://doi.org/10.55648/1998-6920-2023-17-2-59-68.

The article was submitted: 25.12.2022;
accepted for publication 10.01.2023.

References

1. Kanev V. S., Danilova L. Ph., Shevtsova Yu. V., Poletaikin A. N., Monastyrskaya T. I., Samkov T. L., Lukina S. M. Modeli, algoritmy gibridnogo modelirovaniya i informatsionnyye tekhnologii konstruktivnoy tsifrovoy transformatsii deyatel'nosti obrazovatel'noy organizatsii [Models, algorithms for hybrid modeling and information technologies for constructive digital transformation of the activities of an educational organization]. *Research report*, 2022, 146 p.
2. Poletaikin A. N., Shevtsova Yu. V., Monastyrskaya T. I., Danilova L. Ph. Perspektivy i vyzovy tsifrovoy transformatsii obrazovatel'noy deyatel'nosti v SibGUTI [Prospects and challenges of digital transformation of educational activities at SibSUTIS]. *Actual problems of higher professional education in Russia: prospects and challenges. Materials of the LXIV interuniversity scientific and methodological conference*, Novosibirsk, Siberian State University of Telecommunications and Information Science, 9-10 February, 2023, pp. 123-130.
3. *Tsifrovoi Diktant* [Digital Dictation], available at: https://digitaldictation.ru/about (accessed 30.12.2021).
4. *Servis gotovnosti k tsifrovoi ekonomike* [Digital economy readiness service [electronic resource], available at: https://готовкцифре.рф (accessed 30.12.2021).
5. Tsifrovye kompetentsii [Digital competencies]. *Portal "Digital Citizen of Yugra"*, available at: https://цифровойгражданинюгры.рф/gosuslugi/ (accessed 30.12.2021).

Timur L. Samkov
Cand. of Sci. (Engineering), Assistant professor, Siberian State University of Telecommunications and Information Science (SibSUTIS, Novosibirsk, Russia). e-mail: ermin@ngs.ru, ORCID ID: 0000-0001-6400-7672, ResearcherID: AAA-2145-2020.

Aleksey N. Poletaikin
Cand. of Sci. (Engineering), Assistant professor, Kuban State University (KubSU, Krasnodar, Russia), Siberian State University of Telecommunications and Information Science (SibSUTIS, Novosibirsk, Russia). e-mail: alex.poletaykin@gmail.com, ORCID ID: 0000-0002-5128-1952, Scopus AuthorID: 57213829361, ResearcherID: ABF-6799-2020.

DOI: 10.55648/1998-6920-2023-17-2-69-83 УДК 621.315.61.004.6:621.3.049.77

Отказы интегральных схем, вызванные пробоем диэлектрика

В. В. Шубин

Сибирский гос. унив. телекоммуникаций и информатики (СибГУТИ)

Аннотация: В статье описаны некоторые проблемы отказов в работе интегральных схем (ИС) и их предотвращение конструктивно-технологическими и схемо-топологическими способами. Рассмотрены, обобщены и систематизированы вопросы, связанные с проблемами отказов ИС, вызванных пробоем диэлектрика. Представлены примеры, которые могут быть использованы в практической деятельности при разработке ИС для повышения их надёжности на ранних этапах проектирования с учётом современных тенденций развития в области микроэлектроники.

Ключевые слова: пробой диэлектрика, электростатический разряд.

Для цитирования: Шубин В. В. Отказы интегральных схем, вызванные пробоем диэлектрика // Вестник СибГУТИ. 2023. Т. 17, № 2. С. 69–83. https://doi.org/10.55648/1998-6920-2023-17-2-69-83.

Статья поступила в редакцию 08.02.2023;
переработанный вариант – 20.02.2023;
принята к публикации 20.03.2023.

1. Введение

Отказы интегральных схем (ИС), вызванные ***электрическими перенапряжениями*** (***Electrical OverStress, EOS***), связаны с воздействием повышенных напряжений и токов, приложенных к рабочим компонентам ИС. Помимо общепринятых технологических методов противодействия отказам, вызванных электрическими перенапряжениями, в практике проектирования ИС применяются конструктивные схемо-топологические меры предосторожности, которые позволяют минимизировать вероятность двух типов EOS-отказов. ***Пробой диэлектрика*** (***Dielectric Breakdown***, ***DB***) происходит вследствие явления деградации оксида под воздействием повышенных напряжений или других форм перенапряжений и приводит к возможным отказам ИС. Определённые ограничения правил проектирования топологии помогут уменьшить вероятность отказов. ***Электростатический разряд*** (***ElectroStatic Discharge***, ***ESD***) представляет собой форму электрического перенапряжения, вызванного статическим электричеством. Добавление специальных защитных структур к уязвимым контактным площадкам может минимизировать отказы, вызванные ESD.

2. Пробой диэлектрика

В современном производстве изделий микроэлектроники доминирующую долю в общем объёме технологических процессов в размере около 90 % составляют CMOS- и BiCMOS-процессы, в которых одними из наиболее уязвимых с точки зрения отказов являются нарушения диоксида кремния. Основу CMOS-технологии составляют процессы изготовления MOS-транзисторов с изолированным затвором, в которых используется необычайно тонкий подзатворный слой диэлектрика. Толщина подзатворного оксида MOS-транзисторов типового 5 В CMOS-процесса составляет примерно 200 Å, а подзатворного оксида современного 1.8 В CMOS-процесса – 90 Å. Так как средняя длинна связи атомов оксида кремния (silicon-oxygen bond) равняется приблизительно 1.5 Å, то толщина 90 Å представляет собой всего 60 атомных слоёв оксида. Такие тонкие диэлектрики чрезвычайно уязвимы к электрическому перенапряжению. Поэтому пробой подзатворного диэлектрика является одним из важнейших факторов, определяющих рабочее напряжение и надёжность приборов на основе MOS-структур.

2.1. Механизм действия

Пробой диэлектрика (***Dielectric Breakdown***, ***DB***) вовлекает физические процессы, объединяемые термином ***туннелирование***, которые позволяют носителям проникать через пространство внешне непреодолимых препятствий – подзатворный слой диэлектрика. Скорость туннелирования электронов уменьшается по экспоненциальной зависимости по мере роста преодолеваемого пространства и ограничивается на уровне 45 Å. Дырки также способны туннелировать, но из-за их бóльшей эффективной массы на меньшую величину дистанции.

Различают несколько механизмов пробоя подзатворного диоксида кремния. Принято считать, что при высоких напряжённостях электрического поля (E > 8÷10 МВ/см) пробой происходит вследствие ударной ионизации в объёме диэлектрика – так называемый собственный пробой [1, 2, 3]. Также этот процесс часто называют ***сквозным*** или ***непосредственным туннелированием электронов*** (***direct electron tunneling***). В этом механизме пробоя электроны могут проникать в диэлектрики на расстояние не более 45 Å (рис. 1A). Обычно механизм сквозного туннелирования электронов в подзатворных или конденсаторных диэлектриках не встречается, так как их толщина слишком велика.

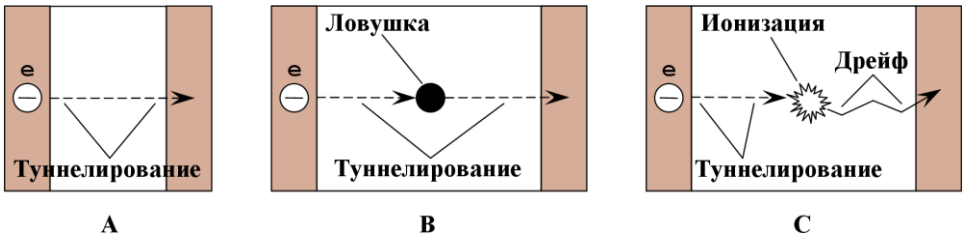

Рис. 1. Визуализация схемы механизмов туннелирования в подзатворных оксидах:
A – сквозное (непосредственное) туннелирование электронов;
B – туннелирование электронов посредством ловушек;
C – механизм туннелирования по Фаулеру–Нордхейму

Электроны могут туннелировать через бóльший интервал с помощью ***туннелирования посредством ловушек*** (***trap-assisted tunneling***). При данном способе туннелирования носителя заряда через диэлектрический слой ловушка служит промежуточным этапом в двухшаговом или многошаговом процессе переноса. Количество шагов, т.е. количество ловушек, через которые могут проходить носители через диэлектрический слой в процессе туннелирования, зависит от толщины диэлектрика, концентрации ловушек, типа источника инжекции (полупроводниковый или металлический электрод) и его положения в диэлектрике относи-

тельно первой ловушки. После прохождения последней ловушки электрон попадает в зону проводимости полупроводника или в металлический слой в зависимости от того, из какого слоя осуществляется инжекция [4]. Для электронов ловушки действуют по методу ступенчатого туннелирования (stepping-stone method). До тех пор, пока электроны могут перемещаться последовательными скачками до 45 Å каждый, они «просачиваются» через заполненные ловушками диэлектрики. Высококачественные диэлектрики имеют некоторое количество ловушек, расположенных на расстоянии, превышающем 45 Å. Туннелирование всё ещё происходит от одной стороны диэлектрика до ловушек вблизи центра и затем на другую сторону (рис. 1B). В высококачественных диэлектриках носители не могут преодолевать расстояние более ~90 Å. В низкокачественных диэлектриках из-за множества ловушек носители могут легко преодолевать много бóльшие расстояния. Этот процесс в низкокачественных диэлектриках позволяет просачиваться через них, независимо от их толщины [5].

Даже более толстые (более 90 Å) и более высококачественные диэлектрики могут быть подвержены туннелированию. Механизм такого туннелирования впервые описан Р.Х. Фаулером и Л. Нордхеймом в 1928 г. Поэтому этот механизм был назван именами его основателей – ***туннелирование по Фаулеру–Нордхейму*** (***Fowler–Nordheim tunneling***) [6]. Данный механизм возникает, когда к диэлектрику приложено интенсивное электрическое поле. Если в такое поле инжектирован электрон, то его энергия увеличивается пропорционально величине поля, и если энергии электрона за счёт ионизации достаточно для последующего дрейфа, то он может проходить весь интервал толщины диэлектрика, как показано на рис. 1C.

Туннелирование по Фаулеру–Нордхейму инжектирует электроны в диэлектрик, где электрическое поле усиливает их энергию и трансформирует их в горячие электроны. Горячие электроны сталкиваются с внутренними атомами диэлектрика, соударяясь со свободными валентными электронами. Этот процесс генерирует дырки и способствует прохождению этих дырок через присутствующие в оксиде ловушки. Поэтому диэлектрики, подверженные туннелированию по Фаулеру–Нордхейму, постепенно деградируют и в конце концов начинают течь. Возникающий ток называется ***током утечки, вызванным перенапряжением*** (***stress-induced leakage current, SILC***) [7, 8].

Ток утечки, вызванный перенапряжением, может привести к катастрофическим отказам, если диэлектрик остаётся под напряжением. Некоторые электроны, инжектированные в диэлектрик за счет туннелирования посредством ловушек, утекают из своих ловушек под воздействием энергии электрического поля. Последующие столкновения с атомами диэлектрика генерируют дополнительные ловушки, которые, в свою очередь, увеличивают ток утечки. Наиболее слабые места диэлектриков непропорционально подвержены воздействию процесса SILC, так как площадь, через которую он протекает, уменьшается, и ток утечки увеличивается. В конце концов в этом месте диэлектрика начинают протекать такие большие токи, что диэлектрик расплавляется. Проводящий материал, смежный с диэлектриком, проникает через это место пробоя, приводя к необратимому отказу в виде короткого замыкания схемы.

Диэлектрики, подверженные большому перенапряжению, могут пробиваться в течение нескольких наносекунд. С другой стороны, диэлектрики, подверженные граничным напряжениям, могут функционировать месяцы или даже годы вплоть до тех пор, пока не произойдёт отказ. Такие отложенные отказы называются ***пробоем диэлектрика, зависящим от времени*** (***time-dependent dielectric breakdown, TDDB***). Уязвимость диэлектриков TDDB существенно зависит от состава диэлектрика, его толщины и однородности структуры.

2.2. Методы противодействия отказам ИС, вызванным пробоем диэлектрика

Все различные формы пробоев диэлектриков существуют вследствие чрезмерных электрических перенапряжений, приложенных к затворным оксидам или другим тонким изолирующим слоям. Существует одно очевидное средство противодействия отказам ИС, вызванным пробоем диэлектрика: предотвращение воздействий чрезмерных электрических перенапряжений на тонкие диэлектрики. К сожалению, это условие довольно трудно выполнить,

так как не существует способа точного определения величины напряжения, являющейся чрезмерной. Главная проблема заключается не в том, что электрическое поле приложено к диэлектрику, а в том, что оно неоднородно. Диэлектрик непременно имеет более тонкие и ещё более тонкие области, а электрическое поле может концентрироваться в некоторых точках (например, таких как острые углы в проводниках). Ловушки, ответственные за возникновение утечек, в диэлектрике также распределены непредсказуемо и неоднородно. Поэтому операции надёжного технологического процесса всегда требуют большого запаса прочности. По этой причине более толстые диэлектрики могут оказаться даже более уязвимыми к пробою диэлектрика, чем более тонкие, так как они могут содержать большее количество непредсказуемых неоднородностей. Обычное максимально допустимое напряжение для сухого оксида толщиной 300÷500 Å равно около 3.5÷4.0 МВ/см, в то время как максимальное напряжение, допустимое для более тонких оксидов, равно около 4.0÷4.5 МВ/см [5].

Известно множество различных проблем сохранения ***целостности затворного оксида*** (***gate oxide integrity, GOI***) в процессе его создания. Проблемы GOI находятся среди наиболее трудных задач, стоящих перед современными фабриками, производящими пластины в CMOS- или BiCMOS-процессах. На самом деле отказы, вызванные GOI, весьма трудно идентифицировать, и поэтому дефектные кристаллы нередко доходят до заказчика. Таким образом, проблемы нарушений GOI определённо являются причинами многих внезапных и неожиданных отказов электронных приборов, которые традиционно приписывают переходным процессам в шинах источников питания [5].

В результате многочисленных исследований был разработан метод, который позволяет выявлять дефекты кристалла GOI до поставки заказчику. Этот метод, названный ***тестирование нагрузки перенапряжением*** (***overvoltage stress testing***, ***OVST***), использует управляемое воздействие перенапряжением на затворный оксид. Обычно величина такого напряжения определяется удвоенным значением установленного предельно допустимого рабочего напряжения. Допускается только однократное воздействие OVST и только на очень короткий промежуток времени (не более 100 мс). Если во время процедуры OVST происходит отказ одного из приборов на кристалле, то этот кристалл забраковывается. Если во время OVST выявляются отказы нескольких кристаллов пластины, то бракуется вся пластина. Если выявляется несколько пластин партии, подверженных отказам OVST, то бракуется вся партия. Обычно фабрики-изготовители ИС предупреждают заказчика о возможности отказов OVST, которые не выявляются стандартными методами обнаружения GOI-проблем. В случае возникновения OVST-отказов технологический цикл изготовления ИС должен быть приостановлен вплоть до выявления всех причин этих отказов и их полного устранения.

Существует много других причин, которые могут ослаблять диэлектрик. Например, атомы тяжёлых металлов могут препятствовать росту однородного оксида, способствуя возникновению слабых мест, которые впоследствии уменьшают целостность оксида. Большинство технологических процессов изготовления ИС используют подложки, выращенные ***методом Чохральского*** (***Czochralski-grown substrate***). В процессе роста кремния по методу Чохральского кислород, присутствующий в кварцевом тигле, попадает в кремний. Если кремний нагреть до 1000 ºС на несколько часов, то кислород собирается в локализованных областях, формируя зоны оксида, которые называются ***кислородными преципитатами*** (***oxygen precipitates***), или оксида, содержащего кислородные остатки. Эти преципитаты ***связывают***, или ***поглощают***, атомы тяжёлых металлов, нейтрализуя их от вмешательства в поверхностное окисление. Этот процесс очень существенно улучшает целостность затворного оксида.

Диффузия высоколегированной примеси N+-типа, которая встречается на ранних этапах технологического процесса изготовления ИС, также может поглощать атомы тяжёлых металлов. Например, заглублённый переход N+-типа или NBL (скрытый слой). Они также могут улучшать целостность затворного оксида прибора (GOI) в пределах определённого расстояния от затворного оксида, называемого ***расстоянием поглощения*** (***absorption distance***), как показано на рис. 2. Обычно расстояние поглощения составляет около сотни микрон. Процессы, которые не требуют непосредственного использования кислородного осаждения

(oxygen precipitation), такие как, например, процессы DI (Dielectric Isolation), всё равно могут добавлять этап формирования заглублённых переходов N+-типа или NBL просто для улучшения целостности затворного оксида. В таких случаях правила проектирования топологии обязывают размещение блоков или полосок заглублённых переходов N+-типа по соседству с MOS-транзисторами.

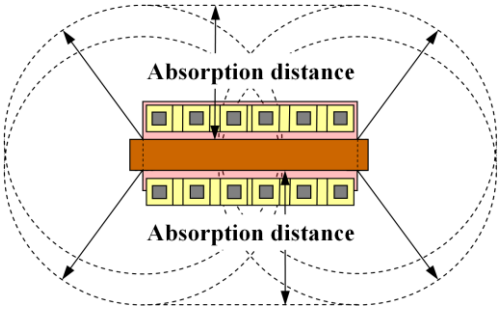

Рис. 2. Расстояние поглощения

Тот факт, что глубокая диффузия N+-типа поглощает примеси тяжёлых металлов, наводит на мысль, что оксиды, выращенные над областью такой глубокой диффузии, будут обладать меньшей прочностью. Этот эффект подтверждается фактическими наблюдениями. Хотя некоторые технологические процессы в силу разных причин могут позволять выращивание оксидов, образованных затворами MOS-транзисторов, над областью глубокой диффузии N+-типа, их действующие приборы будут иметь более слабую прочность оксидов, чем те, что выращены над слаболегированным кремнием. Поэтому следует избегать использования больших областей глубокой диффузии N+-типа под оксидами, образованными затворами MOS-транзисторов.

3. Электростатический разряд

Одним из наиболее известных законов физики, с которым мы сталкиваемся в повседневной жизни и который имеет реальное практическое применение, является ***закон Ома для электропроводности***. Этот закон устанавливает линейную связь между плотностью тока ***J*** и электрическим полем ***E*** и применяется к любым материалам, как к «хорошим» проводникам – металлам, так и к «плохим» – изоляторам. Коэффициент пропорциональности ***σ*** называется проводимостью (или электропроводностью) и является свойством материала:

$$J = \sigma E. \tag{1}$$

Разница материалов между проводниками и диэлектриками является чисто условной и определяется общепринятыми соглашениями. Принято, что проводимость ***σ*** «хороших» проводников (металлов) равна $\approx 10^{7}$ См, а «плохих» проводников (изоляторов) $\approx 10^{-10}$ См [9]. То есть любой физический объект можно считать тем или иным проводником, и, значит, он обладает некоторой ёмкостью, которая может аккумулировать определённый заряд (вплоть до ~10 000 В и выше) и хранить его определённое время. В современных ИС заряд даже менее 50 В может приводить к необратимому разрушению затворного оксида MOS-транзисторов. Так как ИС взаимодействуют с человеком в процессе изготовления и дальнейшей эксплуатации, то заряд, накопленный человеком, вносит высокий риск пробоя затворного оксида, вызванного явлением, названным ***электростатическим разрядом*** (***ElectroStatic Discharge***, ***ESD***).

3.1. Механизм действия

Все ИС проходят необходимые тестовые испытания, в том числе и на уязвимость ESD. При этих испытаниях используют три распространённые тестовые модели: модель человеческого тела (Human Body Model, HBM), машинная модель (Machine Model, MM) и модель заряженного прибора (Charged Device Model, CDM). Для испытаний по модели HMB используют схему на рис. 3A. Если переключатель замыкает цепь схемы испытания, то конденсатор ёмкостью 150 пФ, предварительно заряженный до некоторого напряжения (например, 2 кВ), разряжается через последовательно включённый резистор с сопротивлением 1.5 кОм на тестируемый прибор (Device Under Test, DUT). Идеально, если все пины (pins) ИС протестированы на уязвимость ESD, но на практике для уменьшения времени тестирования выборочно определяется ограниченное количество комбинаций пинов ИС. Каждый из тестируемых пинов подвергается воздействию последовательности положительных и отрицательных импульсов: например, три положительных и три отрицательных. От современных ИС ожидается, что они должны выдерживать 2 кВ при испытаниях по модели HBM. Однако для некоторых приборов могут быть установлены повышенные требования, например, способность держать 25 кВ.

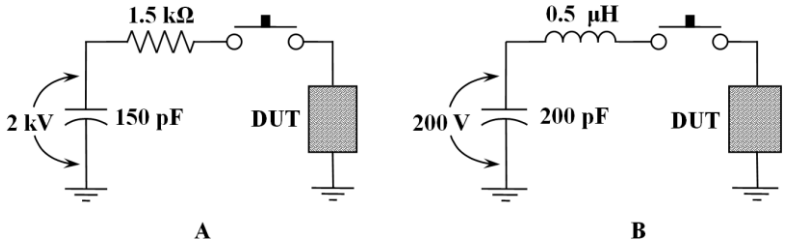

Рис. 3. Схемы моделей тестирования ИС:
A – модель тела человека (HBM) 2 кВ; B – машинная модель (MM) 200 В

На рис. 3B представлена схема тестирования по машинной модели (MM). Конденсатор ёмкостью 200 пФ, заряженный до установленного напряжения (например, 200 В), разряжается через катушку индуктивности 0.5 мкГн на тестируемый прибор DUT. При испытаниях по модели MM, так же, как и по модели HBM, каждый из пинов ИС подвергается воздействию определённой последовательности положительных и отрицательных импульсов. Теперь во время тестирования DUT по модели MM пиковый ток ограничен катушкой индуктивности незначительной величины – 0.5 мкГн, поэтому схема формирует более резкий импульс ESD, чем схема модели HBM. В зависимости от особенностей технологического процесса и используемых элементов защиты интерфейса ИС в тестовых испытаниях по модели MM некоторые приборы могут выдерживать воздействие до 500 В [5].

Третья модель испытаний ИС на отказ от пробоя ESD – модель заряженного прибора (CDM) – несмотря на более высокую трудоёмкость постепенно заменяет модель MM, т.к. более точно воспроизводит реальные условия воздействий ESD и более качественно контролируют слабые места ИС. Во время сборки кристаллов ИС в корпус в нём могут накапливаться статические заряды из-за индукции или трения. Как только какой-либо вывод ИС внезапно заземляется, через него разряжаются первоначально накопленные статические заряды. Это явление, которое может вызывать огромный ток (~10 А) за короткий промежуток времени (~1 нс), называется эффектом ESD по модели CDM (CDM ESD). На рис. 4 демонстрируется действие эффекта ESD по модели CDM.

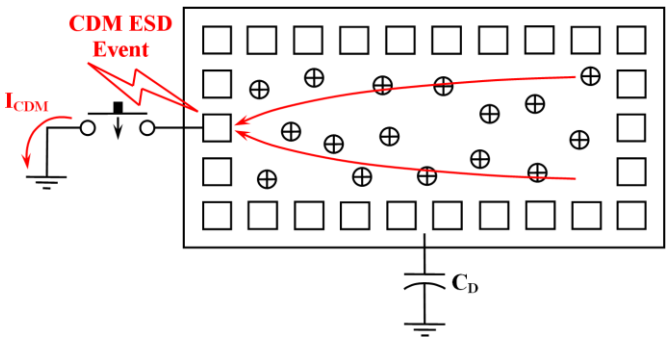

Рис. 4. Действие эффекта ESD по модели CDM:
накопленный в корпусе ИС положительный заряд быстро разряжается через заземлённый внешний терминал

Существует много ситуаций, когда пины ИС могут контактировать с заземлённой поверхностью. Оборудование, участвующее в производственном процессе, как правило, заземлено, поэтому возникает высокая вероятность случайного прикосновения пинов ИС с его заземлёнными поверхностями. На рис. 5 показано случайное падение заряженного корпуса ИС на заземлённую поверхность оборудования (рис. 5A) и принцип испытательного цикла по модели CDM (рис. 5B).

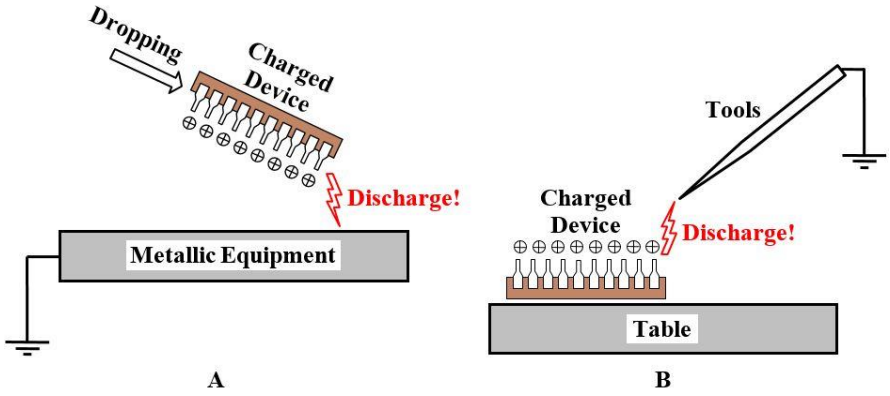

Рис. 5. Примеры CDM-модели в действии:
A – случайное падение заряженного корпуса ИС на заземлённую поверхность оборудования;
B – процесс испытательного цикла по модели CDM

ИС имеют различные размеры кристалла, так что их эквивалентные паразитные ёмкости (C_D) могут заметно отличаться друг от друга. Поэтому различные ИС имеют разные пиковые токи и различную прочность к воздействию ESD по модели CDM [10]. Если прибор тестируется по модели CDM с эквивалентной ёмкостью 4 пФ при заряде 1 кВ, ток через пин ИС может возрастать до значений 15 А за несколько нс [11]. На рис. 6 показан пробой подзатворного оксида NMOS-транзистора ИС после испытаний на пробой ESD по модели CDM [10].

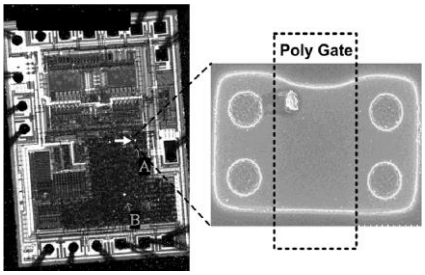

Рис. 6. Пробой подзатворного оксида NMOS-транзистора ИС после испытаний по модели CDM

Эквивалентная схема модели CDM представлена на рис. 7. Она позволяет понять механизм воздействия ESD на ИС по модели CDM и построить установку для соответствующих испытаний на пробой подзатворного оксида [12].

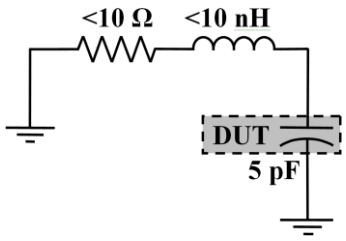

Рис. 7. Эквивалентная схема модели CDM

Воздействие по модели CDM является более быстрым, по сравнению с воздействием по моделям HBM и MM, и образует максимальный пиковый ток, как показано в табл. 1 [12].

Таблица 1. Электрические характеристики разряда ESD, показывающие пиковый ток ESD, длительность положительного фронта и полосу пропускания переходного процесса

Модель	I_{peak}, (A)	Длительность нарастания, (нс)	Полоса пропускания, (МГц)
HBM	1.33	10–30	2.1
MM	3.7–7	15–30	12
CDM	10	1	1100

3.2. Методы противодействия отказам ИС, вызванных ESD

Для минимизации рисков отказов компонентов ИС, чувствительных к ESD, требуется собдюдать меры предосторожности, предписанные соответствующими регламентами технологических процессов изготовления ИС и ТУ эксплуатации: заземлённые браслеты и паяльники, ионизаторы и антистатические маты, использование статико-экранированных упаковок и т.д. Эти меры предосторожности существенно снижают вероятность отказов ИС, вызванных ESD, но не исключают их полностью. Поэтому производители ИС, как правило, предусматривают разработку специальных встроенных защитных электронных устройств в элементы интерфейсов ИС – пинов, связанных с внешним миром. Такие защитные структуры позволяют поглощать и рассасывать умеренные уровни ESD и тем самым дополнительно защищать ИС от преждевременных отказов.

Все уязвимые пины ИС должны иметь структуры защиты от пробоя ESD, подсоединённые к соответствующим контактным площадкам. Сущность любой такой структуры схемы защиты заключается во введении в схему ИС элементов, обладающих способностью максимально быстро отводить чрезмерные токи, протекающие через рабочие элементы, связанные с внешним миром. Наиболее распространённым таким элементом является сточный P-N-переход, смещённый в прямом направлении для стрессовых перенапряжений. Такой P-N-переход можно назвать защитным «сточным» диодом (ESD Clamp). Принцип действия такого диода в стандартном CMOS-процессе изготовления ИС поясняется схемой на рис. 8.

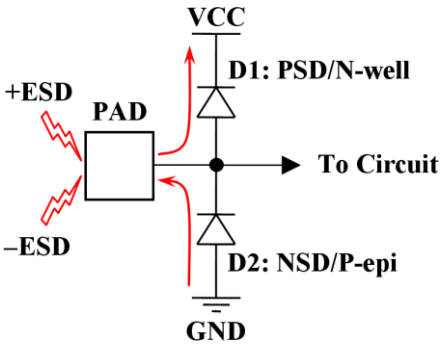

Рис. 8. Принцип действия «сточного» диода ESD

Как только потенциал заряда ESD превышает напряжение VCC на величину прямого напряжения «сточного» диода V_F (D1: PSD/N-well), P-N-переход диода D1 открывается в прямом направлении, и заряд +ESD стекает в узел источника питания VCC. Если потенциал заряда падает ниже напряжения земли GND на величину прямого напряжения «сточного» диода V_F (D2: NSD/P-epi), P-N-переход диода D2 открывается в прямом направлении, и заряд –ESD стекает в узел земли GND. Обычно прямое напряжение диодов PSD/N-well и NSD/P-epi в стандартном CMOS-процессе изготовления ИС составляет ~0.7 В. Таким образом, остаточные потенциалы ESD, проникающие на рабочие элементы внутрь схемы (To Circuit), не превышают VCC + V_F и GND – V_F.

Падение напряжения стекающих токов происходит на паразитных сопротивлениях источника ESD, траверсах, соединяющих выводы корпуса с контактной площадкой кристалла ИС (PAD) и сопротивлениях проводников внутри кристалла, соединяющих анод диода D1 и катод диода D2 с контактными площадками (PADs). Величина этих сопротивлений невелика, а мощность паразитных резисторов незначительна. Поэтому они могут приводить к выгоранию этих резисторов и потере работоспособности ИС. Таким образом, для того чтобы избежать данного эффекта, между контактной площадкой (PAD) и сточными защитными диодами в схеме защиты требуется введение более мощного рабочего токоограничительного резистора R_{ESD}. В зависимости от конструктивно-технологических особенностей конкретных ИС существует огромное количество разнообразных схемо-топологических решений встроенной схемы защиты элементов входа/выхода (I/O) от пробоя ESD [10, 12, 13, 14]. На рис. 9 представлена наиболее распространенная простейшая схема защиты от пробоя ESD.

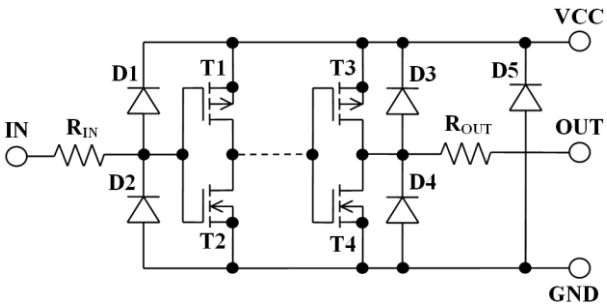

Рис. 9. Структурная схема CMOS ИС со стандартным цифровым входом и цифровым выходом и с традиционной схемой защиты от пробоя ESD

Некоторые пины ИС могут противодействовать ESD, не требуя дополнительной защиты. Примерами могут служить пины выходов мощных выходных инверторов (T3–T4) или элемента входа/выхода с мощным выходом, или входом (выходом) аналогового ключа, подсоединённого к пину ИС, или входом с защёлкой в обратной связи на входе, или определённые входные элементы, конструктивно имеющие соединения с закрытыми P-N-переходами. В этих случаях диоды D1–D2 или D3–D4 могут отсутствовать. Диод D5 предназначен для

защиты неконтролируемых скачков напряжения по шине питания VCC. В некоторых CMOS-процессах, где подложка пластины и терминалов подложки одного из типов транзисторов электрически составляют единое целое, а транзисторы другого типа расположены в соответствующем кармане, необходимость сточного диода D5 также отпадает. В этом случае функцию сточного диода D5 выполняет закрытый переход P-well/N-substrate (N-well/P-substrate). Если при этом паразитные сопротивления, соединяющие пины I/O с внутренними элементами схемы, удовлетворяют требуемому уровню защиты от ESD, то встроенная схема защиты не требуются. В этом случае P-N-переходы рабочих элементов схемы, подсоединённые к пинам ИС, могут иметь способность рассеивать и поглощать энергию ESD, выполняя функцию сточных диодов. Пины ИС или приборы, соединённые с ними, которые могут противостоять воздействию ESD без дополнительной схемы защиты, называют ***самозащищёнными***. Как правило, резисторы R_{IN} и R_{OUT} выполнены из затворного поликремния $R_S \sim 20$ Ом/□.

На рис. 10A показана схема входной защиты от пробоя ESD, которая обладает более высокими показателями защиты уязвимых элементов I/O ИС. Она дополнена сточными диодами, соединёнными непосредственно с контактными площадками ИС (PADs). Ещё более высокий уровень защиты предоставляют структуры, использующие распределённые совмещённые диодно-резистивные элементы, как показано на рис. 10 (B, C, D).

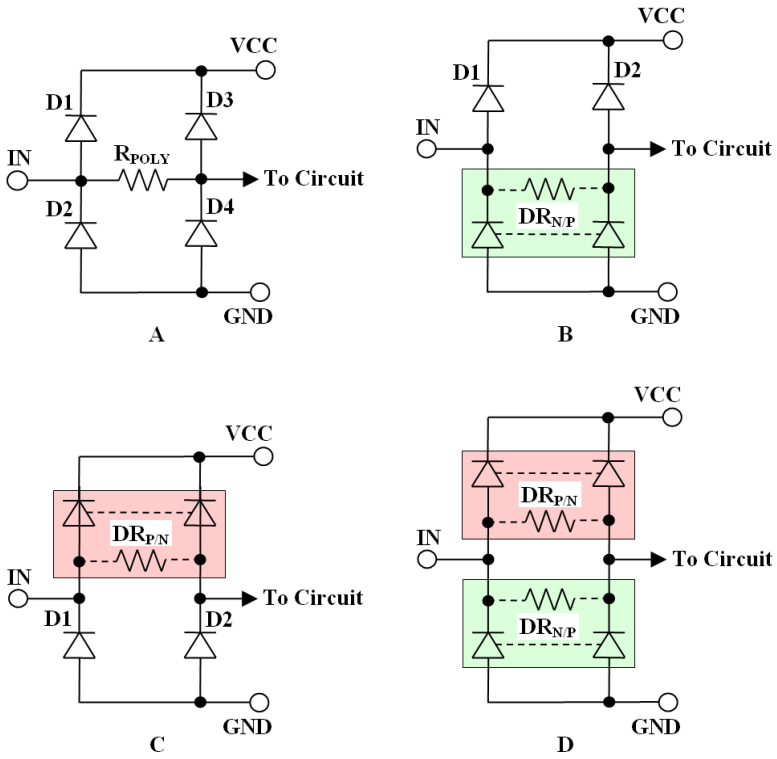

Рис. 10. Усовершенствованная схема входной защиты от пробоя заряда ESD.
A – схема с дополнительными сточными диодами D1–D2 и поликремниевым резистором;
B – схема с распределённым совмещённым диодно-резистивным элементом $DR_{N/P}$;
C – схема с распределённым совмещённым диодно-резистивным элементом $DR_{P/N}$;
D – схема, комбинирующая распределённые совмещённые диодно-резистивные элементы $DR_{P/N}$-$DR_{N/P}$

Если пины CMOS или BiCMOS ИС соединены с переходами относительно небольшой площади, то они являются уязвимыми к необратимому разрушению перехода, вызванному ESD. То есть переходы недостаточно большой площади не могут защитить самих себя. С другой стороны, повышение уровня защиты от ESD входных пинов ИС за счёт увеличения площадей P-N-переходов сточных диодов и сопротивлений токоограничительных входных резисторов R_{IN} приводит к росту входной RC-цепи и не может гарантировать сохранение параметров ТУ по быстродействию и величине входной ёмкости. Неконтролируемое увеличе-

ние выходного защитного резистора R_{OUT}, помимо потери быстродействия, также приводит к снижению уровня выходного тока, росту выходного сопротивления ИС и длительности фронтов выходного сигнала. Поэтому разработчик топологии должен использовать любую возможность уменьшения величины паразитных характеристик элементов входа/выхода без ущерба сохранения требуемых параметров ТУ ИС [5, 12]. Например, если удельная ёмкость металла контактной площадки (PAD) невелика, то сама контактная площадка имеет большую площадь и, значит, ёмкость, вносящую заметный вклад в паразитную ёмкость пина.

В связи с ограниченными возможностями более ранних установок для изготовления рабочих шаблонов в производстве ИС исторически была принята и сохраняется до сих пор тенденция использования квадратной формы топологии рабочих контактных площадок (КП) (рис. 11A). Иногда требуется расположить на кристалле дополнительные тестовые КП, которые могут участвовать в групповом зондовом тестировании на пластине, но не участвуют в монтажной сборке кристалла в корпус. В этом случае тестовая КП должна визуально отличаться от рабочих. Простейшей визуализацией отличий тестовых КП от рабочих без ущерба размера рабочей поверхности КП при зондировании ИС является преобразование топологии КП в октагональную форму за счёт обрезки углов (рис. 11B) [15, 16].

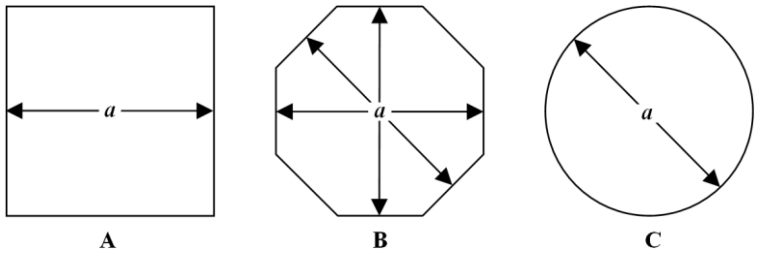

Рис. 11. Формы контактных площадок:
A – квадратная рабочая контактная площадка; B – октагональная тестовая контактная площадка;
C – круглая контактная площадка будущего

Эволюцию масштабирования современных ИС отличает важная особенность: не все правила проектирования топологии масштабируются пропорционально базовому характеристическому размеру. В частности, при масштабировании характеристического размера с 3 мкм до 180–90 нм (уменьшение в ~25 раз) размер рабочей КП изменился со 140–120 мкм до 90–60 мкм (уменьшение в ~1.7 раза). Ёмкость КП носит паразитный характер и в общем виде равна:

$$C_{КП} = \sum C_{уд} \cdot S_{об}. \qquad (2)$$

Здесь $\boldsymbol{C_{уд}}$ – обобщённая удельная ёмкость паразитного конденсатора, образованного КП, $\boldsymbol{S_{об}}$ – обобщённая площадь верхней обкладки конденсатора, образованного КП (PAD). В данном случае нижней обкладкой конденсатора является подложка кристалла, которая полностью перекрывает площадь КП.

При расчётах следует учитывать, что обобщённая площадь $\boldsymbol{S_{об}}$ состоит из двух составляющих – $\boldsymbol{S_{гор}}$ (площади горизонтальной поверхности КП) и $\boldsymbol{S_{бок}}$ (площади боковой поверхности КП). Для каждой площади определена своя удельная ёмкость – $\boldsymbol{C_{гор}}$ (удельная ёмкость горизонтальной поверхности КП) и $\boldsymbol{C_{бок}}$ – (удельная ёмкость боковой поверхности КП), различие которых поясняется на рис. 12.

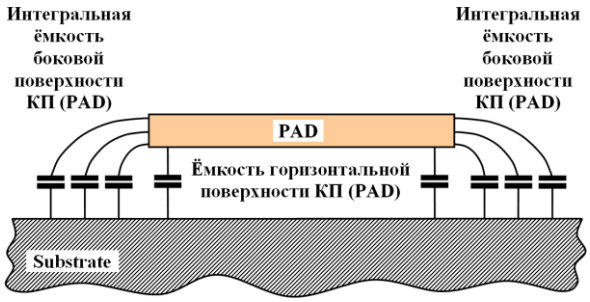

Рис. 12. Паразитная ёмкость контактной площадки (PAD)

Учитывая, что $S_{бок} = P \cdot h$ (где P – периметр фигуры и h – толщина слоя металла КП), можно провести качественное сравнение площадей горизонтальной $S_{гор}$ и боковой $S_{бок}$ наложением всех трёх КП друг на друга, как показано на рис. 13.

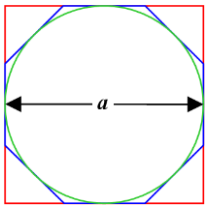

Рис. 13. Наложение топологического рисунка КП (рис. 12A, 12B, 12C) друг на друга

Рис. 13 позволяет убедиться, что $S_{гор.Квадрата} > S_{гор.Восьмиугольника} > S_{гор.Круга}$; $P_{Квадрата} > P_{Восьмиугольника} > P_{Круга}$ и, следовательно, $S_{бок.Квадрата} > S_{бок.Восьмиугольника} > S_{бок.Круга}$. В табл. 2 сведены количественные отличия площадей трёх форм КП.

Таблица 2. Количественные отличия площадей трёх форм КП

	$S_{гор}$		$S_{бок}$	
Квадрат	a^2	a^2	$4a \cdot h$	$4a \cdot h$
Восьмиугольник	$2a^2(\sqrt{2}-1)$	$\sim 0.828a^2$	$8a(\sqrt{2}-1) \cdot h$	$\sim 3.312a \cdot h$
Круг	$\pi a^2/4$	$\sim 0.785a^2$	πa	$\sim 3.142a \cdot h$

Так как приближение к физическим пределам масштабирования наступает с неумолимой неизбежностью, разработчик топологии ИС обязан использовать любые возможности достижения предельно допустимых характеристик. Предположительно, одной из таких возможностей может стать в том числе и переход на круглые КП.

Биполярные схемы также обладают своими уязвимостями к отказам, вызванными ESD, среди которых наиболее известен переход база-эмиттер NPN-транзисторов. Образование лавинного пробоя переходов база-эмиттер NPN-транзистора ведёт к постоянной деградации его бета (β). Обсуждение принципов защиты от пробоя ESD аналоговых биполярных схем является отдельной и весьма обширной темой. Так как формат публикации ограничен, а прогнозирование уязвимости ESD затруднено, общая рекомендация – добавлять защиту приборов ко всем пинам везде, где это возможно без экономических потерь или характеристик ИС.

4. Заключение

Данная работа является первой частью цикла публикаций, посвящённого теме отказов ИС и методов противодействия этим отказам. Автор предполагает продолжить обсуждение темы методов противодействия отказам ИС и повышения их надёжности в последующих публикациях, где будут представлены описания других типов отказов ИС, вызванных порою весьма неординарными причинами.

Литература

1. *DiStefano T. H., Shatzkes M.* Impact ionization model for dielectric instability and breakdown // Appl. Phys. Lett. 1974. V. 25. P. 685–687.
2. *Solomon P.* Breakdown in silicon oxide – a review // J. Vac. Sci. Technol. 1977. V. 14. P. 1122–1130.
3. *Klein N.* Electrical breakdown mechanisms in thin insulators // Thin Solid Films. 1978. V. 50. P. 223–232.
4. *Yeo Y. C., King T. J., Hu C.* MOSFET Gate Leakage Modeling and Selection Guide for Alternative Gate Dielectrics Based on Leakage Considerations // IEEE Transactions on Electron Devices. 2003. V. 50, № 4. P. 1027–1035.
5. *Hastings A.* The Art of Analog Layout. New Jersey: Pearson Prentice Hall, 2006. 648 p.
6. *Fowler R. H., Nordheim L.* Electron emission in intense electric fields // Proc. R. Soc. London, Ser. A. 1928. V. 119. P. 173–181.
7. *Larcher L., Passagnella A., Ghidman G.* A Model of the Stress Induced Leakage Current in Gate Oxides // IEEE Trans. Electron Devices. 2001. V. 48, № 2. P. 285–288.
8. *Lenahan P. M., Mele J. J., Campbell J. P., Kang A. Y., Lowry R. K., Woodbury D., et al.* Direct Experimental Evidence Linking Silicon Dangling Bond Defects to oxide Leakage Currents // Proc. International Reliability Physics Symp. 2001. P. 150–155.
9. *Яворский Б. М., Детлаф А. А., Лебедев А. К.* Справочник по физике для инженеров и студентов вузов / изд. 8-е, перераб. и испр. М.: Оникс; Мир и Образование, 2006. 1056 с.
10. *Ker Ming-Dou, Yuan-Wen Hsiao.* CDM ESD Protection in CMOS Integrated Circuits // Proc. The Argentine School of Micro-Nanoelectronics, Technology and Applications, 2008. P. 61–65.
11. *Henry L., Barth J., Hyatt H., at al.* Charged device model metrology: limitations and problems // Microelectron. Reliab. Jun. 2002. V. 42, № 6. P. 919–927.
12. *Dabral S., Maloney T. J.* Basic ESD and I/O Design. Toronto: John Wiley & Sons Inc. 1998. V. XIII. 328 p.
13. *Chen J. Z., Amerasekera A., Duvvury Ch.* Design Methodology for Optimizing Gate Driven ESD Protection Circuits in Submicron CMOS Processes // Proc. EOS/ESD Symp., 1997. P. 1–10.
14. *Richier C., Salome P., Mabboux G., at al.* Investigation on different ESD protection strategies devoted to 3.3 V RF applications (2 GHz) in a 0.18 m CMOS process // Proc. EOS/ESD Symp., Sep. 2000. P. 251–259.
15. *Clein D.* CMOS IC LAYOUT. Concepts, methodologies and tools. Boston: Newnes. 2000. № XV. 261 p.
16. *Razavi B.* Design of Analog CMOS Integrated Circuits. McGraw-Hill Education. NY, 2017. 782 p.

Шубин Владимир Владимирович
к.т.н., доцент кафедры технической электроники СибГУТИ;
начальник отдела по разработке аналоговых ИМС АО «НЗПП Восток» (630082, Новосибирск, ул. Дачная, 60), e-mail: shubin@nzpp.ru, ORCID ID: 0000-0002-2974-0497.

Автор прочитал и одобрил окончательный вариант рукописи.
Автор заявляет об отсутствии конфликта интересов.

Failures of ICs Caused by Dielectric Breakdown

Vladimir V. Shubin

Siberian State University of Telecommunications and Information Science (SibSUTIS)

Abstract: The paper describes some problems of operation failures of integrated circuits (ICs) and corresponding preventative measures by constructive-technological, schematic-topological methods at the early stages of design process. The issues related to the problems of IC failures caused by dielectric breakdown are considered, generalized and systematized. Some examples that can be used in practice when developing ICs to improve their reliability, taking into account current trends in the microelectronics field.

Keywords: dielectric breakdown, electrostatic discharge.

For citation: Shubin V. V. Failures of ICs caused by dielectric breakdown (in Russisn). *The SibSUTIS Bulletin*, 2023, vol. 17, no. 2, pp. 69-83. https://doi.org/10.55648/1998-6920-2023-17-2-69-83.

The article was submitted: 08.02.2023;
revised version: 20.02.2023;
accepted for publication 20.03.2023.

References

1. DiStefano, T. H. Impact ionization model for dielectric instability and breakdown. *Appl. Phys. Lett*, 1974, vol. 25, pp. 685-687.
2. Solomon, P. Breakdown in silicon oxide. J. *Vac. Sci. Technol*, 1977, vol. 14, pp. 1122-1130.
3. Klein, N. Electrical breakdown mechanisms in thin insulators. *Thin Solid Films*, 1978, vol. 50, pp. 223-232.
4. Yeo, Y. C. MOSFET Gate Leakage Modeling and Selection Guide for Alternative Gate Dielectrics Based on Leakage Considerations. Y. *IEEE Transactions on Electron Devices*, 2003, vol. 50, no. 4, pp. 1027-1035.
5. Hastings, Alan. *The art of Analog layout*, New Jersey: Pearson Prentice Hall, 2006. p. 648.
6. Fowler, R. H. Electron emission in intense electric fields. *Proc. R. Soc. London*, Ser. A, 1928, vol. 119, pp. 173-181.
7. Larcher, L. A Model of the Stress Induced Leakage Current in Gate Oxides. *IEEE Trans. Electron Devices*, 2001, vol. 48, no. 2, pp. 285-288.
8. Lenahan, P. M. Direct Experimental Evidence Linking Silicon Dangling Bond Defects to oxide Leakage Currents. *Proc. International Reliability Physics Symp*, 2001, pp. 150-155.
9. Yavorskii, B. M. Spravochnik po fizike dlya inzhenerov i studentov VUZov [Handbook of Physics for engineers and university students]. 8th ed., Moscow: Onyx; World and Education, 2006. p.1056.

10. Ker, Ming-Dou. CDM ESD Protection in CMOS Integrated Circuits. *Proceedings of the Argentine School of Micro-Nanoelectronics*, Technology and Applications, 2008, pp. 61-65.
11. Henry, L. Charged device model metrology: limitations and problems. *Microelectron. Reliab*, Jun. 2002, vol. 42, no. 6, pp. 919-927.
12. Dabral, Sanjay. *Basic ESD and I/O Design*, Toronto: John Wiley & Sons Inc., 1998, vol. XIII, p. 328.
13. Chen, J. Z. Design Methodology for Optimizing Gate Driven ESD Protection Circuits in Submicron CMOS Processes. *Proc. EOS/ESD Symp.*,1997, pp. 1-10.
14. Richier, C. Investigation on different ESD protection strategies devoted to 3.3 V RF applications (2 GHz) in a 0.18 m CMOS process. *Proc. EOS/ESD Symp.*, sep. 2000, pp. 251-259.
15. Clein, D. Cmos ic layout. *Concepts, methodologies and tools*, 2000, no. XV, p.261.
16. Razavi, B. Design of Analog CMOS Integrated Circuits. *2nd Ed. McGraw-Hill Education*, 2017, pp. 782.

Vladimir V. Shubin

Cand. of Sci. (Engineering), assistant professor of the Department of Technical Electronics of Sib-SUTIS, Head of the Development of analog ICs of JSC "NZPP Vostok department" (630082, Novosibirsk, Dachnaya str., 60), e-mail: shubin@nzpp.ru, ORCID ID: 0000-0002-2974-0497.

DOI: 10.55648/1998-6920-2023-17-2-84-92 УДК 004.054.53

Метод оценивания рисков в системах принятия решений с учетом защиты информации

В. В. Селифанов, А. Ю. Солдатов, Е. Ю. Солдатов, А. П. Подлегаев, В. С. Скориков

Сибирский государственный университет геосистем и технологий

Аннотация: В статье предложен подход, с помощью которого возможно осуществлять анализ влияния защищенности информации на процесс управления решениями. Использование подхода в жизненном цикле системы приведет к снижению рисков и будет способствовать выявлению «узких мест», в том числе в области информационной безопасности. Работоспособность показана на примерах.

Ключевые слова: информационная безопасность, анализ рисков, защита информации, управление решениями.

Для цитирования: Селифанов В. В., Солдатов А. Ю., Солдатов Е. Ю., Подлегаев А. П., Скориков В. С. Метод оценивания рисков в системах принятия решений с учетом защиты информации // Вестник СибГУТИ. 2023. Т. 17, № 2. С. 84–92. https://doi.org/10.55648/1998-6920-2023-17-2-84-92.

Статья поступила в редакцию 25.12.2022;
принята к публикации 10.01.2023.

1. Оценивание рисков и подходы к моделированию

Ключевой целью процесса управления решениями служит обеспечение аналитической основы для определения, характеристики и оценки большинства предпочтительных и наилучших решений, а также вектор действий на каждом этапе жизненного цикла системы.

В процессе управления решением могут возникать угрозы нарушения требуемых условий, необходимых для защиты информации (требований к защите информации системы). Эти риски обычно связаны с объективными и субъективными факторами, ориентированными на защищаемые активы и информацию, в том числе с неопределенностью ответственности за обеспечение защиты информации во время принятия решений [1].

Под риском информационной безопасности понимается возможность того, что угроза сможет воспользоваться уязвимостью актива или группы активов и тем самым нанесет ущерб организации.

Итогом процесса управления решениями служат следующие результаты:

– варианты решений, требующие альтернативного системного анализа;

– альтернативные варианты действий;

– предпочтительные решения и вектор действий;

– документально зафиксированные обоснования решений и принятые в обосновании предложения и допущения [2].

Применительно к проектируемой системе, которая в нашем случае представляет собой модель «черного ящика», расчетные показатели следующие [3]:

– риск нарушения надежности реализации процесса управления решениями в течение периода прогноза $R_{\text{надежн}}\left(T_{\text{зад}}\right)$ рассчитывают по моделям и рекомендациям В.2 ГОСТ 59338-2021;

– риск нарушения требований информационной безопасности в процессе управления решениями $R_{наруш}\left(T_{зад}\right)$ рассчитывают по моделям и рекомендациям В.3 ГОСТ 59338-2021 ($T_{\text{зад}}$ – заданный период прогноза);

– интегральный риск нарушения реализации процесса управления решениями с учетом требований по защите информации.

Исследуемые системы могут рассматриваться в виде простой или сложной структуры. В данном исследовании представлена система, построенная по принципу «черного ящика». В данной системе внешнему наблюдателю предоставлены исключительно входные и выходные данные, а структура и внутренние составляющие неизвестны. В случае с моделью системы сложной структуры учитывается совокупность взаимосвязанных элементов, каждый из которых представлен в виде «черного ящика».

2. Интегральный риск

Прогнозирование интегрального риска оценивается в сопоставлении с возможными потерями по следующей формуле [4]:

$$R_{\text{интегр.уч}}\left(T_{\text{зад}}\right)=1-\left[1-R_{\text{надеж}}\left(T_{\text{зад}}\right)\right]\cdot[\,1-R_{\text{наруш}}\left(T_{\text{зад}}\right)],$$

где $R_{\text{надежн}}\left(T_{\text{зад}}\right)$ – риск нарушения надежности реализации процесса управления решениями при периоде прогноза $T_{\text{зад}}$ без учета требований защиты информации и $R_{\text{наруш}}\left(T_{\text{зад}}\right)$ – риск нарушения требований защиты информации в процессе управления решениями в течение периода прогноза $T_{\text{зад}}$.

Сами значения рисков $R_{\text{надежн}}\left(T_{\text{зад}}\right)$ и $R_{\text{наруш}}\left(T_{\text{зад}}\right)$ предлагается рассчитывать по методам, подробно описанным в литературе.

Риск нарушения надежности реализации процесса управления решениями в течение периода прогноза $T_{\text{зад}}$ вычисляется по формуле:

$$R_{\text{надежн}}\left(T_{\text{зад}}\right)=1-P_{\text{возд}}(\sigma,\,\beta,\,T_{\text{меж}},\,T_{\text{диаг}},\,T_{\text{зад}}), \qquad (1)$$

где σ – частота возникновения источников угроз в моделируемой системе с точки зрения нарушения надежности реализации процесса управления решениями,

β – среднее время развития угроз (активизации источников угроз) с момента их возникновения до нарушения целостности моделируемой системы (выполняемых действий процесса, выходных результатов и/или защищаемых активов) с точки зрения нарушения надежности реализации процесса;

$T_{\text{меж}}$ – среднее время между окончанием предыдущей и началом очередной диагностики целостности моделируемой системы;

$T_{\text{диаг}}$ – среднее время системной диагностики целостности моделируемой системы;

$T_{\text{зад}}$ – задаваемая длительность периода прогноза.

При соблюдении условий независимости исходных данных риск отсутствия нарушений надежности реализации процесса управления решениями в течение заданного периода прогноза рассчитывают по формуле (вариант 1) [3]:

$$R_{\text{возд}(1)} = \begin{cases} \left(\sigma - \beta^{-1}\right)^{-1} \left\{\sigma \cdot \exp(-T_{\text{зад}} / \beta) - \beta^{-1} \exp(-\sigma \cdot T_{\text{зад}})\right\}, \text{ если } \sigma \neq \beta^{-1} \\ \exp(-\sigma \cdot T_{\text{зад}})\left[1 + \sigma \cdot T_{\text{зад}}\right], \text{ если } \sigma = \beta \end{cases} \quad (2)$$

В случае следующего варианта при соблюдении условия независимости исходных данных вероятность отсутствия нарушений надежности проведения процесса управления решениями в течение периода прогноза рассчитывают по формуле:

$$P_{\text{возд}(2)} = P_{\text{серед}} \times P_{\text{кон}}, \quad (3)$$

где $P_{\text{серед}}$ – вероятность отсутствия нарушений надежности проведения процесса управления решениями в течение всех заданных периодов между системными контролями, полностью вошедшими в рамки заданного периода времени $T_{\text{зад}}$, вычисляемая по формуле:

$$P_{\text{серед}} = P^{N}_{\text{возд}(1)}(\sigma, \beta, T_{\text{меж}}, T_{\text{диаг}}, T_{\text{зад}} + T_{\text{диаг}}), \quad (4)$$

где N – число периодов между диагностиками, которые полностью вошли в рамки заданного периода времени $T_{\text{зад}}$, с округлением до целого числа.

Вероятность отсутствия нарушений надежности реализации процесса управления решениями после последнего системного контроля вычисляется по формуле:

$$P_{\text{кон}} = P_{\text{возд}(1)}(\sigma, \beta, T_{\text{меж}}, T_{\text{диаг}}, T_{\text{ост}}), \quad (5)$$

где $T_{\text{ост}}$ – остаток времени в общем заданном периоде $T_{\text{зад}}$ по завершении N полных периодов, вычисляемый по формуле:

$$T_{\text{ост}} = P_{\text{зад}} - N\left(T_{\text{меж}} + T_{\text{диаг}}\right). \quad (6)$$

3. Пример расчета интегрального риска

В рамках примера при оценке риска были выбраны такие модели, как (рис. 1):

– модели ГОСТ Р 59338-2021 для анализа действий, связанных с планированием управления решениями (действие 1), принятием решений и управлением решениями (действие 3);

– модели, связанные со сбором, обработкой и анализом информации для принятия решений (действие 2), – по ГОСТ Р 59341.

Данное итоговое описание позволяет спроектировать моделируемую систему как структуру следующих последовательных элементов, связанных с действиями процесса управления решениями (рис. 2) [5]:

▪ для планирования процесса управления решениями:

– 1-й элемент – действие 1 для производственного процесса;

– 2-й элемент – действие 1 для процесса технического обслуживания;

– 3-й элемент – действие 1 для процесса контроля качества;

– 4-й элемент – действие 1 для процесса инвентаризации;

▪ для принятия решений и управления решениями:
– 5-й элемент – действие 2 для производственного процесса;
– 6-й элемент – действие 2 для процесса технического обслуживания;
– 7-й элемент – действие 2 для процесса контроля качества;
– 8-й элемент – действие 2 для процесса инвентаризации.

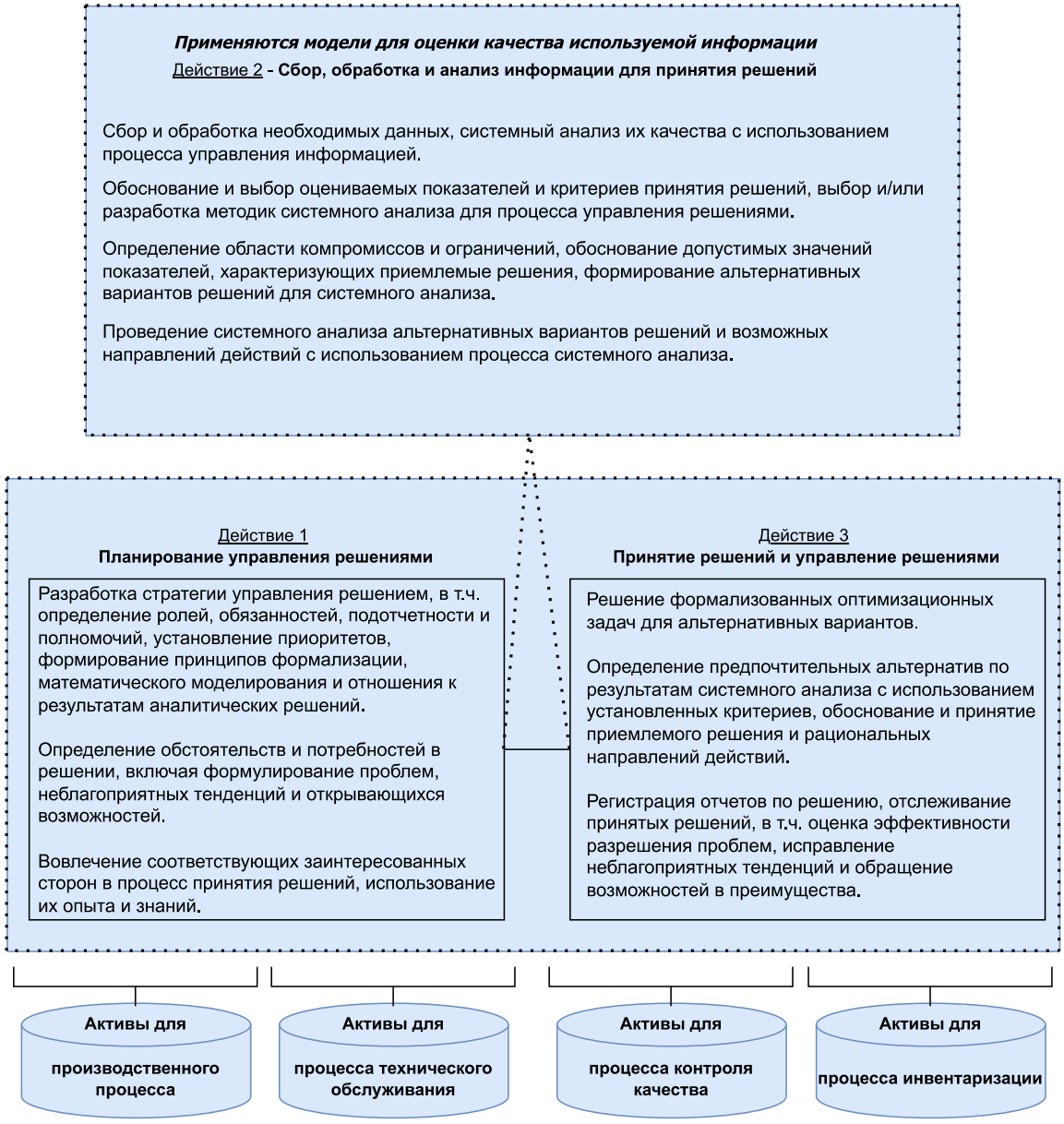

Рис. 1. Представление комплекса действий для оценки риска нарушения надежности

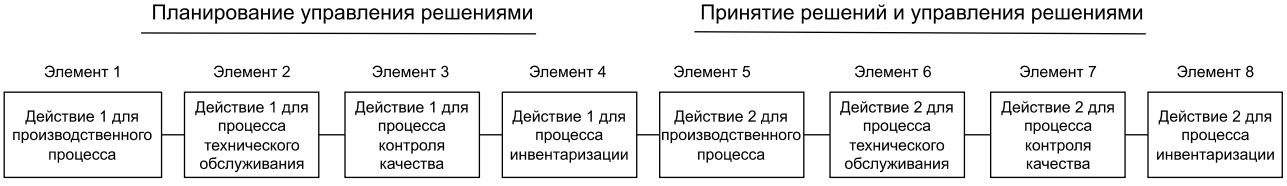

Рис. 2. Структура моделируемой системы без учета требований
по защите информации

В табл. 1 представлены исходные данные для каждого составного элемента.

Таблица 1. Исходные данные для прогнозирования риска нарушения надежности реализации процесса управления решениями

Значения и комментарии		
Исходные данные	для 1-го / 2-го / 3-го / 4-го элементов	для 5-го / 6-го / 7-го / 8-го элементов
σ – частота появления источников угроз нарушения надежности процесса	5 раз в год / 1 раз в год / 1 раз в год / 1 раз в год – это угрозы антропогенных и технических ошибок	2 раза в год / 1 раз в год / 1 раз в год / 1 раз в год – это частота угроз потерь от неразумных действий
β – время от начала возникновения источника угрозы до нарушения с возможными потерями	2 недели / 1 год	6 месяцев / 6 месяцев
$T_{\text{меж}}$ – среднее время между диагностиками возможностей конкретного элемента	8 часов / 8 часов / 8 часов / 8 часов	1 час / 1 неделя / 1 неделя / 1 неделя
$T_{\text{диаг}}$ – среднее время диагностики состояния элемента	10 минут / 10 минут / 10 минут / 10 минут – время обследования перед работой	полминуты – контроль целостности оборудования / 1 час – диагностика / полминуты – длительность контроля / полминуты – длительность инвентаризации
$T_{\text{восст}}$ – среднее время восстановления элемента после выявления нарушений	полчаса / полчаса / полчаса / полчаса – это время, потраченное на замену сотрудника, который был отстранен от работы	4 часа – время, затраченное на восстановление конкретного оборудования / 8 часов – время, затраченное на восстановление тех. процесса / полчаса — время, затраченное на переустановку ПО / 8 часов – время, затраченное на восстановление инвентаризации
$T_{\text{зад}}$ – задаваемая длительность периода прогноза	от 1 месяца до 1 года период, в течение которого сохраняется уверенность в отсутствии превышения риска нарушения надежности	

Единцы измерения всех исходных данных табл. 1 приводятся к тем единицам измерения, которые указаны при задаваемой длительности периода прогноза $T_{\text{зад}}$.

Используя формулы (1–6) и исходные данные табл. 1, мы можем определить вероятность нарушения надежности реализации процесса управления решениями для элемента 1. Подставив значения и проведя математические вычисления, получаем $R_{\text{надежн}}\left(T_{\text{зад}}\right) = 0.067$. Повторяем действия для каждого элемента системы.

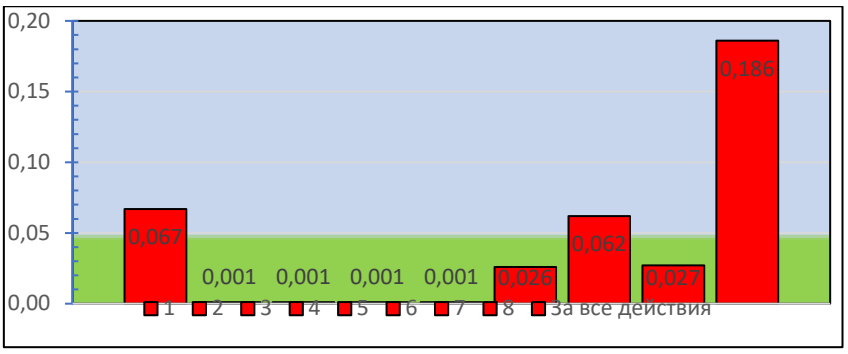

Рис. 3. Риск без учета качества используемой информации

Сложив значения всех элементов, получим значение риска нарушения надежности реализации процесса управления решениями, равное 0.186 (рис. 3). Получаем для 1-го элемента значение 0.067, а для последнего элемента 0.062, что совместно составляет более 69 % от общего риска по всем элементам.

Исходные данные по каждому из 8 элементов, которые учитывают в себе вероятные уязвимости, представлены в табл. Г.2 ГОСТ Р 59338-2021.

Используя данный ГОСТ для вычисления $R_{\text{наруш}}\left(T_{\text{зад}}\right)$, и исходные данные табл. Г.2, получаем значение 0.0025 для элемента 1. Рассчитывая для остальных элементов системы, в 1 – 5, 7 – 8 – около 0.002. Для 6-го элемента – 0.0005. Анализируя, можно сделать вывод, что все активы защищены равнопрочно.

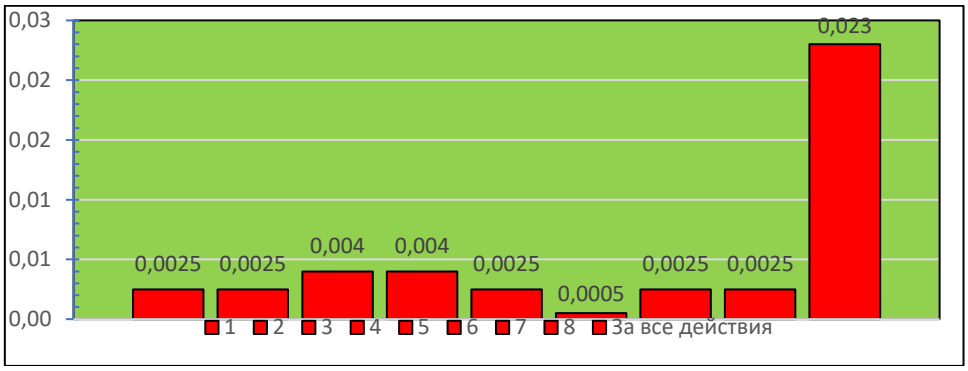

Рис. 4. Риск нарушения требований в течение одного месяца

Основной причиной высокого интегрального риска, значительно превышающего риски повреждения надежного производственного оборудования, является относительно низкий уровень качества используемой информации. Если этот уровень качества будет признан приемлемым или не улучшаемым и клиент (или аналитиком) решит не брать в расчеты качество используемой информации, то может быть использована другая полученная оценка, т.е. в нашем случае 0.012. И тогда, учитывая все вышесказанное, выбираем значение $R_{\text{надежн}}\left(T_{\text{зад}}\right) = 0.012$, а $R_{\text{наруш}}\left(T_{\text{зад}}\right)$ = 0.023. В таком случае:

$$R_{\text{интегр.уч}}\left(T_{\text{зад}}\right) = 1 - \left[1 - 0.012\right] \cdot \left[\ 1 - 0.023\right] = 0.034 .$$

Таким образом, интегральный риск нарушения реализации процесса управления решениями с учетом требований по защите информации меньше установленного допустимого уровня 0.05, что подтверждает сбалансированность применяемых технических решений с точки зрения достижения целей системной инженерии.

4. Вывод

Данный подход позволяет проводить анализ того, как защищенность информации влияет на реализацию процесса управления решениями. Актуальность и достоверность подтверждена на уровне реализации методов, предложенных в ГОСТ Р 59338-2021 «Системная инженерия. Защита информации в процессе управления решениями».

Литература

1. *Костогрызов А. И., Степанов П. В*. Инновационное управление качеством и рисками в жизненном цикле систем. М.: Изд. «Вооружение, политика, конверсия», 2008. 404 с.
2. *Kostogryzov A.* Probabilistic Modeling in System Engineering // IntechOpen. 2018. 278 p. DOI: 10.5772/intechopen.71396.
3. ГОСТ Р 59338-2021. Системная инженерия. Защита информации в процессе управления решениями. М.: Национальный стандарт РФ, 2021. 45 с.
4. ГОСТ Р 59341-2021. Системная инженерия. Защита информации в процессе управления информационной системы. М.: Национальный стандарт РФ, 2021. 56 с.
5. *Grigoriev L., Kostogryzov A., Krylov V., Nistratov A., Nistratov G*. Prediction and optimization of system quality and risks on the base of modelling processes // American Journal of Operation Researches. Special Issue. 2013. V. 1. P. 217–244. http://www.scirp.org/journal/ajor/

Селифанов Валентин Валерьевич
доцент кафедры информационной безопасности, Сибирский государственный университет геосистем и технологий (СГУГиТ, 630108, Новосибирск, ул. Плахотного, д. 10), e-mail: sfo1@mail.ru, ORCID ID: 0000-0002-6691-5647.

Солдатов Александр Юрьевич
студент, Сибирский государственный университет геосистем и технологий, e-mail: dglasmann@mail.ru, ORCID ID: 0000-0002-5218-1013.

Солдатов Егор Юрьевич
студент, Сибирский государственный университет геосистем и технологий, e-mail: wilgieforz@mail.ru, ORCID ID: 0000-0002-7937-8502.

Подлегаев Александр Игоревич
студент, Сибирский государственный университет геосистем и технологий, e-mail: sanyi_p@mail.ru, ORCID ID: 0000-0001-8617-9731.

Скориков Виталий Сергеевич
студент, Сибирский государственный университет геосистем и технологий, e-mail: isaac.newton01@mail.ru, ORCID ID: 0000-0001-8218-9529.

Авторы прочитали и одобрили окончательный вариант рукописи.
Авторы заявляют об отсутствии конфликта интересов.
Вклад соавторов: *Каждый автор внес равную долю участия как во все этапы проводимого теоретического исследования, так и при написании разделов данной статьи.*

Risk Assessment Method in Decision-making Systems Taking into Account Information Protection

Valentin.V. Selifanov, Aleksandr.Yu. Soldatov, Egor.Yu. Soldatov, Aleksandr.P. Podlegaev, Vitaly.S. Skorikov

Siberian State University of Geosystems and Technologies

Abstract: The article suggests an approach by which it is possible to analyze the impact of information security on the decision management process. The use of the approach in the life cycle of the system will reduce risks and contribute to the identification of "bottlenecks" including information security. The efficiency of the approach is demonstrated by examples.

Keywords: information security, risk analysis, information security, decision management.

For citation: Selifanov V. V., Soldatov A. Yu., Soldatov E. Yu., Podlegaev A. P., Skorikov V. S. Risk assessment method in decision-making systems taking into account information protection (in Russisn). *The SibSUTIS Bulletin*, 2023, vol. 17, no. 2, pp. 84-92. https://doi.org/10.55648/1998-6920-2023-17-2-84-92.

The article was submitted: 25.12.2022;
accepted for publication 10.01.2023.

References

1. Kostogryzov A. I., Stepanov P. V. *Innovacionnoe upravlenie kachestvom i riskami v zhiznennom cikle sistem* [Innovative quality and risk management in the systems life cycle]. Moscow, Publishing house “Armament, politics, conversion”, 2008. 404 p.
2. A.Kostogryzov. *Probabilistic Modeling in System Engineering*. IntechOpen, London, 2018, 278 p. DOI: 10.5772/intechopen.71396.
3. *GOST R 59338-2021. Sistemnaya inzheneriya. Zashchita informatsii v protsesse upravleniya resheniyami* [Russian Standard No. 59338-2021 System engineering. System engineering. Protecting Information in Decision Management], available at: https://internet-law.ru/gosts/gost/75539/ (accessed 06.11.2022).
4. *GOST R 59341-2021. Sistemnaya inzheneriya. Zashchita informatsii v protsesse upravleniya informatsionnoi sistemy* [Russian Standard No. 59341-2021 System engineering. Protection of information in the process of managing an information system], available at: https://docs.cntd.ru/document/1200179349 (accessed 18.11.2022).
5. Grigoriev L., Kostogryzov A., Krylov V., Nistratov A., Nistratov *G*. Prediction and optimization of system quality and risks on the base of modelling processes. *American Journal of Operation Researches. Special Issue*, 2013, v. 1, pp. 217-244, available at: http://www.scirp.org/journal/ajor/ (accessed 19.11.2022).

Selifanov Valentin Valerievich
Associate Professor, Department of Information Security, Siberian State University of Geosystems and Technologies (SSUGiT, 630108, Novosibirsk, Plakhotnogo St., 10), e-mail: sfo1@mail.ru, ORCID ID: 0000-0002-6691-5647.

Soldatov Alexander Yurievich
Student, Siberian State University of Geosystems and Technologies, e-mail: dglasmann@mail.ru, ORCID ID: 0000-0002-5218-1013.

Soldatov Egor Yurievich
Student, Siberian State University of Geosystems and Technologies, e-mail: wilgieforz@mail.ru, ORCID ID: 0000-0002-7937-8502.

Podlegaev Alexander Igorevich
Student, Siberian State University of Geosystems and Technologies, e-mail: sanyi_p@mail.ru, ORCID ID: 0000-0001-8617-9731.

Skorikov Vitaly Sergeevich
Student, Siberian State University of Geosystems and Technologies, e-mail: isaac.newton01@mail.ru, ORCID ID: 0000-0001-8218-9529.

DOI: 10.55648/1998-6920-2023-17-2-93-103 УДК 004

Технология формирования интегрированной антифишинговой системы в цифровом обществе

А. Б. Архипова, Д. А. Нечаев

Новосибирский государственный технический университет (НГТУ)

Аннотация: В данной работе рассматривается проблема фишинга в интернет-пространстве. Также проанализированы причины актуальности проблемы фишинга, рассмотренные через призму злоумышленника. Далее определено понятие канала связи и его корреляция с явлением фишинга на примере почтовых атак. В работе разработана технология формирования антифишинговой системы на примере модели взаимодействия злоумышленника и пользователя. Проанализированы меры защиты от почтового фишинга. Разработано программное обеспечение PufferPhish, предполагающее интеграцию системы защиты в процесс доставки почтовых сообщений.

Ключевые слова: фишинг, реактивная мера защиты, цифровая безопасность, угроза безопасности, стратегия злоумышленника, социальная инженерия, сценарий атаки, антифишинговая система, интегрированная система защиты.

Для цитирования: Архипова А. Б., Нечаев Д. А. Технология формирования интегрированной антифишинговой системы в цифровом обществе // Вестник СибГУТИ. 2023. Т. 17, № 2. С. 93–103. https://doi.org/10.55648/1998-6920-2023-17-2-93-103.

Статья поступила в редакцию 25.12.2022;
принята к публикации 10.01.2023.

1. Введение

С развитием технологий стремительно увеличивается число товаров и услуг, приобретаемых дистанционно. Процесс цифровизации неизбежно ведет не только к увеличению объема информации в интернет-пространстве, но и увеличению шанса ее компрометации. На этой почве общество все чаще сталкивается с проблемами мошенничества и киберпреступлений [18].

Обращаясь к истории цифровых технологий, можно проследить экспоненциальную динамику роста масштабов киберпреступлений. Начиная с 1960-х годов, когда совершались первые противоправные действия, оказывающие воздействие на информационные системы [14, 18], вариативность подходов к реализации компьютерных атак значительно увеличилась. На данный момент фишинг является одним из самых популярных способов совершения преступных действий в Интернете. И несмотря на то, что вопрос разработки и внедрения различных средств и организационных мер по защите информации стоит наиболее остро, темпов снижения роста киберпреступлений не наблюдается.

2. Тенденции развития киберпреступлений и системы защиты в цифровом обществе

Управление информационной безопасностью является очень важным вопросом для всех, кто работает в области технологий, или для всех, кто подвергается риску нарушения безопасности и понимает последствия этих уязвимостей. Многие организации постоянно находятся под угрозой нарушения безопасности. Организации могут легко столкнуться с компрометацией информации, возникающей в результате утечки данных. В условиях постоянно возникающих угроз безопасности данных организации всегда работают над обеспечением защиты своих данных [2, 8–10].

Сегодня проведение аудита систем управления информационной безопасностью – необходимое и обязательное мероприятие. Ряд организаций, бизнес которых тесно связан с использованием информационных технологий, таких как банки, нефтяные, газовые, энергетические и телекоммуникационные компании, в последнее время активизировались в проведении аудитов систем управления информационной безопасностью.

В нормативной базе РФ нет прямого определения термина «фишинг», однако в банке данных угроз ФСТЭК можно ознакомиться с одним из примеров частного описания реализации фишинга по описанию угрозы безопасности информации УБИ.175: «Угроза «фишинга»». Так, фишинг понимают как процесс убеждения нарушителем, имеющим цель неправомерного ознакомления с защищаемой информацией, пользователя с помощью методов социальной инженерии осуществить переход на поддельный сайт с целью ввода защищаемой информации или открыть вредоносное вложение в письме [13]. Для более точного понимания концепции фишинга стоит внести корректировки. Понятие «фишинг» можно трактовать как процесс получения злоумышленником личной идентификационной информации пользователя с помощью применения методов социальной инженерии и информационных технологий в личных целях. Под личной информацией пользователя в данном контексте понимается вся та информация, которая влечет выгоду для злоумышленника, а именно данные банковских карт, счетов; персональные данные (биометрия); данные учетных записей – логины и пароли.

Для построения модели взаимодействия между пользователем и злоумышленником стоит определить личность интернет-мошенника, его мотивы, потребности и поведение в интернете. Анализ литературы позволил сформировать образ злоумышленника. К ключевым методам, способствующим реализации атаки, стоит отнести оказание психологического воздействия на потенциальную жертву. Так, например, используя различные манипуляции над чувствами человека, злоумышленник внушает необходимое поведение со стороны жертвы, ведущее к успешности атаки. Среди используемых методов оказания психологического воздействия можно выделить наиболее популярные, такие как:

- претекстинг – использование злоумышленником предлога для того, чтобы привлечь внимание жертвы и заставить ее сообщить необходимую информацию;
- квид про кво – получение злоумышленником информации в обмен на несуществующее получение выгоды жертвой (наследство, приз);
- использование чувств человека (страх, любопытство) для ослабления бдительности жертвы;
- использование полученной информации о пользователе (зачастую из открытых источников) для повышения доверия к себе;
- обратная социальная инженерия – случай, когда жертва сама обращается к злоумышленнику [20].

Что касается мотивации мошенника к исполнению киберпреступления, можно выделить три основных причины: корыстный мотив (получение выгоды), исследовательский интерес и хулиганство. Также стоит отметить ключевые причины, из-за которых злоумышленники становятся киберпреступниками, а именно разницу в опыте в сфере технологий между мошенником и жертвой, а также высокую вероятность безнаказанности за совершенные в сети пре-

ступления [15]. Отметим, что на основе используемой той или иной методики социальной инженерии строится сценарий атаки.

Для реализации фишинга необходима цифровая среда, в которой злоумышленник может осуществлять атаки. В контексте исследования среду реализации фишинга будем детерминировать понятием «канал связи» и определим данный термин как совокупность программно-аппаратных средств, с помощью которых пользователи могут обмениваться информацией между собой. Для наибольшего охвата атакуемой аудитории злоумышленники используют такие каналы связи, как:

- электронная почта;
- социальные сети;
- мессенджеры;
- сотовая связь;
- Wi-Fi-сеть.

Каждый из каналов связи обладает собственными технологиями для организации и реализации передачи информации между субъектами сетевого взаимодействия. В связи с этим возникает потребность в формировании набора защитных мер для обнаружения и предотвращения фишинга. В рамках данного исследования будет рассмотрен фишинг, реализуемый по электронной почте.

Согласно статистике электронная почта является самым распространенным каналом связи [3]. Злоумышленники прибегают к различным техникам для реализации фишинга, а также комбинируют их для наибольшей вероятности успешной атаки. Разберем возможные техники реализации фишинга.

1. Использование вредоносных вложений. Злоумышленники (фишеры) в почтовых сообщениях прикрепляют файлы различных расширений – от стандартных docx, xls, pdf до нетипичных для электронных сообщений – bat, exe. Фишеры используют различные предлоги для того, чтобы пользователь открыл вложение. Если говорить об обмане рядовых пользователей Интернета, то обычно темой писем являются различного рода скидки, приглашение на работу, информация об обновлении системы и т.д. Что касается сотрудников компаний, предлогом для успеха реализации фишинга являются почтовые сообщения об отпуске, проблемах с начислением заработной платы или неправильно заполненных документах. Сам злоумышленник, чтобы войти в доверие, представляется заинтересованным лицом либо создает адрес электронной почты, схожий с корпоративным [16, 19].

2. Ссылка на поддельный веб-сайт. В тексте письма может содержаться ссылка на веб-ресурс, на котором может находиться опасный контент. Злоумышленники могут использовать различные предлоги для использования ссылки на свой поддельный сайт. Одним из вариантов является создание схожего по названию адреса сайта компании путем внесения корректировок в доменное имя в виде дополнительных символов или замены существующих на варианты, схожие по написанию. Также злоумышленник может использовать уникальный по названию сайт, имитирующий работу сервиса, предоставляющего спектр услуг.

3. Поддельный домен отправителя. Использование поддельного домена позволяет злоумышленнику применять методы социальной инженерии, аналогичные технике формирования ссылок на поддельные веб-сайты. Так, например, злоумышленник может использовать домен, схожий с легитимным, используя в адресе символы из других языков, имитирующих базовую латиницу. Также для скорой массовой рассылки злоумышленники могут использовать автоматически сгенерированные последовательности символов в адресе домена [17].

4. Социальная инженерия в тексте сообщения. Злоумышленник применяет техники психологического давления с целью получения идентификационных данных пользователя ответом на свою почту.

5. Email spoofing (спуфинг). Используя программные средства, злоумышленник может выдать себя за другого пользователя, например, указывая при отправке сообщений поддельный почтовый домен.

Определив техники для реализации фишинговой атаки злоумышленником, построим модель взаимодействия между злоумышленником и жертвой (рис. 1).

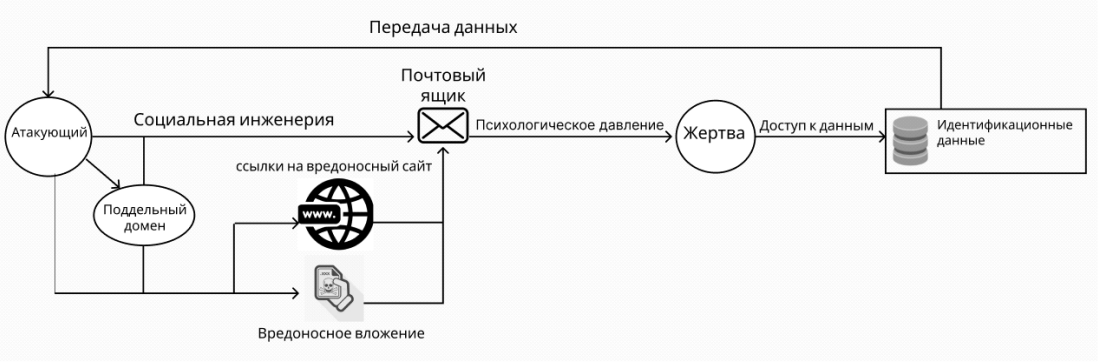

Рис. 1. Модель взаимодействия участников фишинговой атаки без защиты жертвы

В данной модели рассматривается случай фишинговой атаки со стороны злоумышленника, при которой отсутствуют защитные меры со стороны жертвы.

Объекты – атакующий и жертва – трактуются как учетные записи участников взаимодействия, с которых осуществляется формирование, отправка и соответственно прием и чтение электронных почтовых сообщений. Поддельный домен принимает роль спуфингового адреса. Также в модели учитываются три основных тактики для проведения атаки – использование психологического текста, вредоносных ссылок и вложений, причем возможны комбинации тактик, а также совмещение с отправкой со спуфингового адреса для увеличения шанса успешной атаки. Получив письмо, атакуемый пользователь при ознакомлении подсознательно подвергается психологическому давлению, что влияет на последующее срабатывание тактик, которое и приводит к конечной цели фишера – получению идентификационных данных.

Таким образом, модель взаимодействия участников фишинговой атаки без защиты жертвы показывает актуальность проблемы изучения фишинга в существующем цифровом обществе, одной из причин которых является отсутствие средств защиты со стороны жертвы, влияние человеческого фактора и в результате низкий порог входа для мошенников [2, 12].

Отметим, чтобы противостоять проблеме фишинга, пользователи применяют различные меры защиты. В данном исследовании определим три типа применяемых мер – превентивные, реактивные и проактивные меры.

Превентивные меры. В контексте фишинга под превентивными мерами будем понимать применение организационных и технических мер, благодаря которым для атакуемого пользователя отсутствует необходимость в принятии решения относительно того, фишинговое ли сообщение или нет. Так, например, организационной мерой является вовлеченность государства для противодействия фишингу, то есть все сайты подвергаются проверке на фишинг со стороны государственного сервиса [6]. С технической точки зрения предотвратить доставку фишингового сообщения до конечного пользователя можно с помощью системы защиты от спама почтовых агентов, а также таргетированных антифишинговых продуктов, устанавливаемых между доменами отправителей и корпоративной почтой сотрудников компании.

Реактивные меры. Реализация реактивных мер подразумевает, в отличие от превентивных, проверку уже доставленных сообщений. В качестве защиты используют такие средства, как браузерный механизм проверки сайтов, предупреждающий пользователей о потенциально опасном контенте, плагины для браузеров с аналогичным принципом работы, а также программные антифишинговые решения, устанавливаемые на рабочем месте пользователя [1]. Среди организационных мер можно отметить повышение пользователями осведомленности в области информационной безопасности.

Проактивные меры. В случае успешности реализации фишинговой атаки злоумышленник получает идентификационные данные пользователя. Однако и на этом этапе имеется возможность избежать потерь. Проактивными мерами в данном случае можно считать использование двухфакторной аутентификации в сервисах, в которых применяют скомпроме-

тированные идентификационные данные; блокировка карты, а также смена скомпрометированного пароля [7].

Разница между антифишинговыми средствами, относящимися к реактивному и превентивному типу мер, заключается в том, что первое средство устанавливается на рабочее место пользователя, а другая система в основном устанавливается в крупных организациях в одной точке сети для фильтрации входящих писем большого числа пользователей, что экономит время и ресурсы относительно установки приложения на все рабочие места в организации.

3. Технология формирования антифишинговой системы

Целью формирования технологии создания антифишинговой системы является интеграция приложения в процесс получения почтовых сообщений. Данная система относится к реактивному типу применяемых мер защиты, так как, в отличие от антифишинговых средств, благодаря которым до пользователя не доходят фишинговые письма, пользователи имеют возможность ознакомиться с мошенническим письмом. Целевой аудиторией системы являются обычные пользователи Интернета либо организации с малым или средним штатом, имеющие рабочие места в количестве нескольких единиц.

Преимуществом такой системы можно считать тот факт, что пользователь, получив фишинговое или потенциально опасное сообщение, сможет ознакомиться с указанной вредоносной или потенциально опасной сигнатурой и тем самым постепенно повышать уровень осведомленности в области информационной безопасности. Что касается недостатков такого подхода к построению системы, пользователь имеет возможность подвергнуться атаке, даже после проведенного системой анализа сообщения.

Достоинством предложенной системы защиты от фишинга является наличие таких функций, как использование нескольких почтовых адресов, проверка почтовых сообщений и их отображение по нажатию с результатами анализа опасного содержимого.

3.1. Модель приложения

На рис. 2 определена модель антифишинговой системы в виде программного приложения (PufferPhish). Можно заметить, что данное программное средство становится посредником в процессе доставки сообщения, поэтому пользователь может ознакомиться с содержимым письма без взаимодействия с оригиналом почтового агента, тем самым можно определить PufferPhish как имитатор почтового сервиса. В связи с этим можно выделить решение о создании защищенного почтового агента для исключения посреднической передачи данных, однако в рамках данной работы это решение рассматривается лишь как метод защиты.

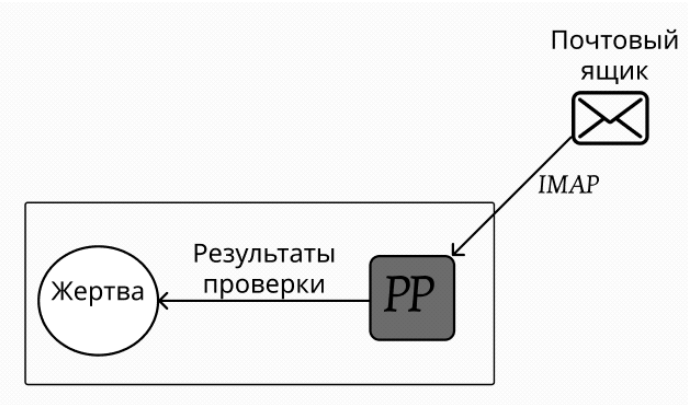

Рис. 2. Модель приложения программного продукта PufferPhish

Структура приложения. На рис. 3 представлена структура программного продукта с взаимодействием основных блоков и подблоков. Приложение с точки зрения классификации архитектуры является монолитным, так как оно написано как одна единица кода, чьи компоненты предназначены для совместной работы, используют одни и те же ресурсы и место на диске. Использование локального сервера исключает возможность компрометации информации приложения из внешних сервисов. Ядром системы является объект App веб-фреймворка следующего поколения Koa. FrontEnd- и BackEnd-части приложения написаны на языке JavaScript с использованием кроссплатформенной среды выполнения с открытым кодом Node.js. Пользователю при наличии возможности доступа и к серверной, и к веб-части достаточно взаимодействовать лишь с пользовательским интерфейсом приложения. Что касается серверной логики, при запуске приложения компонент index.ts запускает в работу компонент Router, посредством которого осуществляется связь с модулем проверки поступающих почтовых сообщений, базой данных, содержащей идентификационные данные проверяемых почтовых ящиков, данные о почтовых сообщениях – результаты проверки, а также id необходимых писем. Именно модуль Router осуществляет необходимую связь с веб-интерфейсом приложения через поступающие запросы.

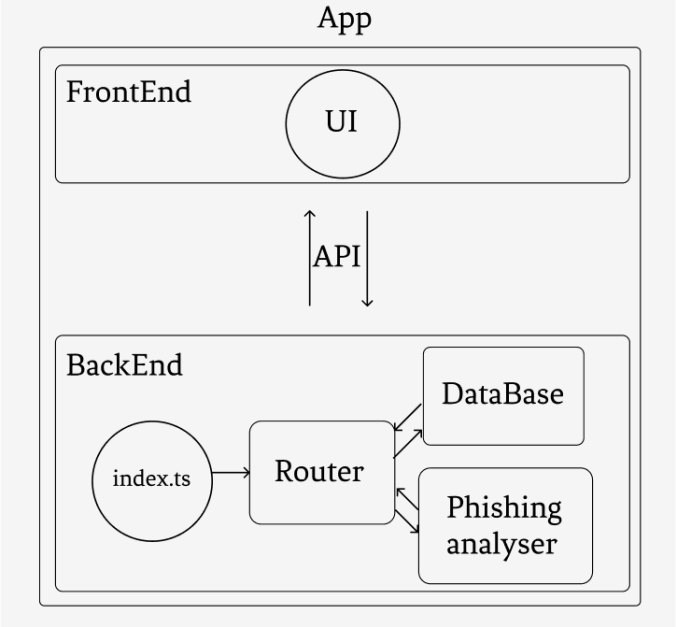

Рис. 3. Структура приложения

На рис. 4 представлена обновленная модель взаимодействия участников фишинговой атаки с интеграцией программного обеспечения. Стоит заметить, что доступ к идентификационным данным для злоумышленника доступен, так как в любом случае имеется возможность с помощью пользователя запустить вредоносное вложение или же перейти по ссылке.

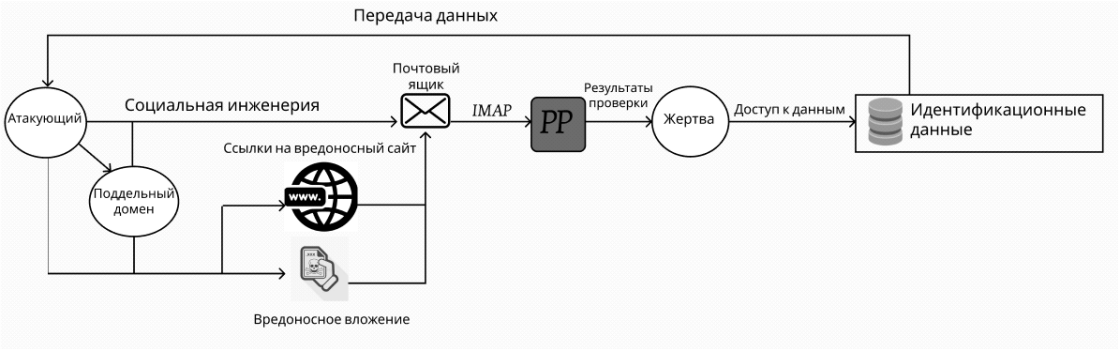

Рис. 4. Модель взаимодействия участников фишинговой атаки с интегрированной системой защиты

Разработанные модель взаимодействия (рис. 4) и технология формирования интегрированной антифишинговой системы могут также иметь применение на практике в учебном процессе для специалистов по информационной безопасности в формате игропрактик (ролевые игры, квесты по информационной безопасности, киберучения) [4, 11, 12, 20]. Использование ролевых игр для задач информационной безопасности имеет множество преимуществ. Помимо чёткой задачи моделирования реальной ситуации, можно отметить снятие психологических барьеров во взаимодействии игроков, а также получение доступа к практическим случаям, которые сложно интегрировать в другие виды игр.

4. Заключение

Фишинг является серьезной проблемой, так как затрагивает всех пользователей Интернета, тем самым становясь актуальной угрозой на международном уровне. В силу стремительного развития технологий и непоспевающего развития техник защиты киберпреступники надежно закрепились в цифровом пространстве и обладают много большей свободой действий и площадью для атаки, чем обычные преступники, в связи с чем у мирового сообщества возникает необходимость в принятии оперативных действий по противодействию киберпреступлениям и фишингу в частности. Важно понимать, что одним лишь набором технических средств защиты от фишинга обойтись невозможно, так как, например, такой вид атаки, как фишинг использует для реализации киберпреступления социальную инженерию, эксплуатируя человеческий фактор, являющийся более предпочтительным в качестве вектора атаки. Поэтому неотъемлемой частью рекомендованных для использования мер защиты является собственное понимание концепции фишинга пользователями и постоянное повышение осведомленности в области информационных технологий и информационной безопасности в частности. Получив набор различных принимаемых мер для защиты от фишинга, пользователь имеет возможность качественно защититься от фишинга. Однако стоит учитывать, что полная защита невозможна в силу постоянного развития технологий и возникновения новых сценариев атаки, а также по причине невозможности полного исключения человеческого фактора. Поэтому конечной целью противодействия фишингу является использование сочетания различных мер для минимизации вероятности реализации фишинга. Одним из возможных методов снижения риска фишинга является разработанная система защиты PufferPhish, реализующая функцию проверки почтовых сообщений на фишинг. При проведении приложением анализа осуществляется проверка возможных используемых в сообщении тактик реализации фишинга. Также для получения наиболее эффективных результатов интеграции системы защиты в приложении используется функция отображения следов фишинга для повышения осведомленности пользователя в области информационной безопасности.

Научная работа поддержана Благотворительным фондом Владимира Потанина № ГК23-000864.

Литература

1. *Mohammed A., Bakar A., Azaliah N., and Fiza R.* Anti-Phishing Tools: State of the Art and Detection Efficiencies // Applied Mathematics & Information Sciences. 2022. № 16. P. 929–934. DOI: 10.18576/amis/160609.
2. *Arkhipova A. B.* Multisociometrical readiness characteristics in information security management // CEUR Workshop Proceedings. 2022. V. 3094: Advanced in Information Security Management and Applications (AISMA 2021), Stavropol–Krasnoyarsk, 1 Oct. 2021. P. 25–34. URL: http://ceur-ws.org/Vol-3094/paper_2.pdf (access date: 28.03.2022).

3. *Blagojević I.* Phishing Statistics // 99 firms. [Электронный ресурс]. URL: https://99firms.com/blog/phishing-statistics/.
4. *Karagiannis S., Maragkos E., Magkos E.* An Analysis and Evaluation of Open Source Capture the Flag Platforms as Cybersecurity e-Learning Tools // Proc. IFIP World Conference on Information Security Education, 2020. DOI: 10.1007/978-3-030-59291-25.
5. *Krokhaleva A. B., Belov V. M.* The human factor in the system of socially significant activity // Mathematical structures and modeling. 2017. № 4 (44). P. 85–99.
6. *Kucek, S., Leitner, M.* An Empirical survey of functions and configurations of open source capture the Flag (CTF) environments // Journal of Network and Computer Applications. 2019. 102470. https://doi.org/10.1016/j.jnca.2019.102470.
7. *Sinha R., and Hemant K.* A Study on Preventive Measures of Cyber Crime. 2018. DOI: 10.13140/RG.2.2.14212.04480.
8. *Snyman D. P., Kruger H. A.* Information Security Behavioural Threshold Analysis in Practice: An Implementation Framework / In: Clarke, N., Furnell, S. (eds) Human Aspects of Information Security and Assurance. HAISA 2020. IFIP Advances in Information and Communication Technology. 2020. V. 593. Springer, Cham. https://doi.org/10.1007/978-3-030-57404-8_11.
9. *Somepalli S. H. et al.* Information Security Management // HOLISTICA – Journal of Business and Public Administration. 2020. V. 11, Is. 2. P. 1–16. DOI: 10.2478/hjbpa-2020-0015.
10. *Sri Harsha Somepalli, Sai Kishore Reddy Tangella, Santosh Yalamanchili*. Information Security Management // Journal of Business and Public Administration. 2020. № 11 (2). P. 1–16. DOI: 10.2478/hjbpa-2020-0015.
11. *Zolotarev V. V., Arkhipova A. B., Parotkin N. Y., Lvova A. P.* Strategies of social engineering attacks on information resources of gamified online education projects // CEUR Workshop Proceedings. 2021. V. 2861: International Scientific Conference on Innovative Approaches to the Application of Digital Technologies in Education (SLET), Stavropol, 12–13 Nov. 2020. P. 386–391. URL: http://ceur-ws.org/Vol-2861/.
12. *Архипова А. Б., Нечаев Д. А.* К вопросу построения модели фишинговой атаки на базе теории некооперативных игр // Материалы IX Всероссийской молодежной школы-семинара по проблемам информационной безопасности «Перспектива-2021», Красноярск, 30 сентября – 03 октября 2021 года. С. 6–12.
13. БДУ – Угрозы // Федеральная служба по техническому и экспортному контролю. [Электронный ресурс]. URL: https://bdu.fstec.ru/threat/ubi.175 (дата обращения: 01.10.2022).
14. *Грачев А. В.* История возникновения киберпреступлений // Материалы внутривузовской конференции «Информационная безопасность и вопросы профилактики киберэкстремизма среди молодежи», Магнитогорск, 09–12 октября 2015 г. С. 162–175.
15. *Комаров А. А.* Криминологические аспекты мошенничества в глобальной сети Интернет: специальность 12.00.08 «Уголовное право и криминология; уголовно-исполнительное право»: диссертация на соискание ученой степени кандидата юридических наук. Саратов, 2011. 262 с.
16. Маскировка вирусов // ilyarm. [Электронный ресурс]. URL: https://ilyarm.ru/txt-maskirovka-virusov-exe-to-txt-zamaskirovat-exe-pod-jpg.html (дата обращения: 03.10.2022).
17. *Меньшаков С.* Разминируем почту. Простое руководство по выявлению фишинга. / xakep. [Электронный ресурс]. URL: https://xakep.ru/2021/06/16/mail-phishing/ (дата обращения: 04.10.2022).
18. *Плотникова Т. В., Харин В. В.* Киберпреступность – угроза XXI века // Вестник общественной научно-исследовательской лаборатории «Взаимодействие уголовно-исполнительной системы с институтами гражданского общества: историко-правовые и теоретико-методологические аспекты». 2018. № 12. С. 153–161.

19. Самые опасные вложенные файлы // Warp Theme Framework. [Электронный ресурс]. URL: http://security.mosmetod.ru/moshennichestvo-v-seti/152-opasnye-vlozhennye-fajly (дата обращения: 07.10.2022).
20. *Фомина Н. А*. Использование методов социальной инженерии при мошенничестве в социальных сетях // Материалы внутривузовской конференции «Информационная безопасность и вопросы профилактики киберэкстремизма среди молодежи», Магнитогорск, 09–12 октября 2015 г. С. 443–453.

Архипова Анастасия Борисовна

к.т.н., доцент кафедры защиты информации, Новосибирский государственный технический университет (НГТУ, 630073, Новосибирск, пр. Карла Маркса, 20), e-mail: arhipova@corp.nstu.ru, ORCID: 0000-0003-0791-8087, Scopus Author ID: 57223676445, Author ID (РИНЦ): 593263, SPIN-код (РИНЦ): 3885-1932.

Основное направление научных исследований – математическое моделирование в информационной безопасности.

Нечаев Дмитрий Александрович

студент кафедры защиты информации, специальность 10.05.03 «Информационная безопасность автоматизированных систем», Новосибирский государственный технический университет, e-mail: dimanechaev9@gmail.com, ORCID: 0000-0001-8861-9147, Author ID (РИНЦ): 593263.

Авторы прочитали и одобрили окончательный вариант рукописи.

Авторы заявляют об отсутствии конфликта интересов.

Вклад соавторов: *Каждый автор внес равную долю участия как во все этапы проводимого теоретического исследования, так и при написании разделов данной статьи.*

Technology for the Formation of an Integrated Anti-phishing System in a Digital Society

Anastasiya B. Arkhipova, Dmitry A. Nechaev

Novosibirsk State Technical University (NSTU)

Abstract: The problem of phishing in the Internet space is considered in this paper. The reasons for the urgency of the phishing problem, considered through the prism of an attacker, are also analyzed. Furthermore, the concept of a communication channel and its correlation with the phenomenon of phishing is defined by the example of mail attacks. The technology of the formation of an anti-phishing system is developed on the example of a model of interaction between an attacker and a user. The measures of protection against mail phishing are analyzed. PufferPhish software has been developed, which offers the integration of a security system into the process of delivering mail messages.

Keywords: Phishing, reactive security measure, digital security, security threat, attacker strategy, social engineering, attack scenario, anti-phishing system, integrated protection system.

For citation: Arkhipova A. B., Nechaev D. A., Technology of formation of an integrated anti-phishing system in a digital Society (in Russisn). *The SibSUTIS Bulletin*, 2023, vol. 17, no. 2, pp. 93-103. https://doi.org/10.55648/1998-6920-2023-17-2-93-103.

The article was submitted: 25.12.2022;
accepted for publication 10.01.2023.

References

1. Alghenaim, M. F., Abu Bakar N.A., Abdul Rahim F. Anti-Phishing Tools: State of the Art and Detection Efficiencies. *Applied Mathematics & Information Sciences*, vol. 16, no. 6 (November. 2022), pp:929-934.
2. Arkhipova A. B. Multisociometrical readiness characteristics in information security management. *Advanced in Information Security Management and Applications*, proc. of the intern. workshop on advanced in information security management and applications (AISMA 2021), Stavropol–Krasnoyarsk, 1 October, 2021, pp. 25-34.
3. Ivan Blagojević. Phishing Statistics. available at: https://99firms.com/blog/phishing-statistics/.
4. Karagiannis S. An Analysis and Evaluation of Open Source Capture the Flag Platforms as Cybersecurity e-Learning Tools. *IFIP World Conference on Information Security Education*, 2020.
5. Krokhaleva A. B., Belov V. M. The human factor in the system of socially significant activity. *Mathematical structures and modeling*, 2017, no. 4(44), pp. 85-99.
6. Kucek, S., Leitner, M.: An Empirical survey of functions and configurations of open source capture the Flag (CTF) environments. *Journal of Network and Computer Applications*, 102470 (2019).
7. Sinha Raj, Hemant Kumar. A Study on Preventive Measures of Cyber Crime, Internationai Journal of Research in Social Sciences, vol. 8, iss. 11(1), November 2018, DOI: 10.13140/RG.2.2.14212.04480.
8. Snyman D.P., Kruger H.A. Information Security Behavioural Threshold Analysis in Practice: An Implementation Framework. *Human Aspects of Information Security and Assurance*. HAISA 2020. IFIP Advances in Information and Communication Technology, vol 593. Springer.
9. Somepalli S. H. Information Security Management. *Journal of Business and Public Administration*, vol. 11, iss. 2, 2020. pp. 1-16. DOI: 10.2478/hjbpa-2020-0015.
10. Sri Harsha Somepalli, Sai Kishore Reddy Tangella, Santosh Yalamanchili. Information Security Management. *Journal of Business and Public Administration*, vol. 11, iss. 2, pp.1-16, 2020. DOI: 10.2478/hjbpa-2020-0015.
11. Zolotarev V. V., Arkhipova A. B., Parotkin N. Y., Lvova A. P. Strategies of social engineering attacks on information resources of gamified online education projects. *International Scientific Conference on Innovative Approaches to the Application of Digital Technologies in Education (SLET–2020)*, Stavropol, 12-13 Novemder, 2020, pp. 386-391.
12. Arhipova A. B. K voprosu postroeniya modeli fishingovoj ataki na baze teorii nekooperativnyh igr [On the issue of constructing a phishing attack model based on the theory of non-cooperative games]. *Perspektiva-2021, Materialy IX Vserossijskoj molodezhnoj shkoly-seminara po problemam informacionnoj bezopas-nosti*, Krasnoyarsk, 30 September – 03 October, 2021, pp. 6-12.
13. BDU – Ugrozy [DBU – Threats]. *Federal'naya sluzhba po tekhnicheskomu i eksportnomu kontrolyu*, available at: https://bdu.fstec.ru/threat/ubi.175 (accessed 01.10.2022).
14. Grachev A. V. Istoriya vozniknoveniya kiberprestuplenij [The history of cybercrime]. *Informacionnaya bezopasnost' i voprosy profilaktiki kiberekstremizma sredi molodezhi*, Materialy vnutrivuzovskoj konferencii, Magnitogorsk, Magnitogorskij gosudarstvennyj tekhnicheskij universitet, 09-12 October, 2015, pp. 162-175.
15. Komarov A. A. *Kriminologicheskie aspekty moshennichestva v global'noj seti Internet: special'nost' 12.00.08 "Ugolovnoe pravo i kriminologiya; ugolovno-ispolnitel'noe pravo"* [Criminological aspects of fraud in the global Internet: specialty 12.00.08 "Criminal law and criminology; penal enforcement law"]. Abstract of Ph. D. thesis. Saratov, 2011. 262 p.
16. Maskirovka virusov [Virus masking], available at: https://ilyarm.ru/txt-maskirovka-virusov-exe-to-txt-zamaskirovat-exe-pod-jpg.html (accessed 03.10.2022)

17. Men'shakov S. *Razminiruem pochtu. Prostoe rukovodstvo po vyyavleniyu fishinga*. [We clear the mail. A simple guide to detecting phishing], available at: https://xakep.ru/2021/06/16/mail-phishing/ (accessed 04.10.2022).
18. Plotnikova T. V., Harin V. V. Kiberprestupnost' - ugroza XXI veka [Cybercrime - the threat of the XXI century]. *Vestnik obshchestvennoj nauchno-issledovatel'skoj laboratorii «Vzaimodejstvie ugo-lovno-ispolnitel'noj sistemy s institutami grazhdanskogo obshchestva: istoriko-pravovye i teoretiko-metodologicheskie aspekty»*, 2018, no. 12, pp. 153-161.
19. Samye opasnye vlozhennye fajly [The most dangerous attachments], available at: http://security.mosmetod.ru/moshennichestvo-v-seti/152-opasnye-vlozhennye-fajly (accessed 07.10.2022).
21. Fomina, N. A. Ispol'zovanie metodov social'noj inzhenerii pri moshennichestve v so-cial'nyh setyah [The use of social engineering methods in fraud in social networks]. *Informacionnaya bezopasnost' i vo-prosy profilak-tiki kiberekstremizma sredi molodezhi*, Materialy vnutrivuzovskoj konferencii, Magnito-gorsk, Magnitogorskij gosudarstvennyj tekhnicheskij universitet, 09-12 October, 2015, pp. 443-453.

Anastasia B. Arkhipova

Cand. of Sci. (Engineering), Associate Professor of the Department of Information Security of Novosibirsk State Technical University (20 Karl Marx Ave., Novosibirsk, 630073), e-mail: arhipova@corp.nstu.ru, ORCHID: 0000-0003-0791-8087, Scopus Author ID: 57223676445, Author ID (RSCI): 593263, SPIN code (RSCI): 3885-1932.

The main direction of scientific research is mathematical modeling in information security.

Dmitry A. Nechaev

Student of the Department of Information Security specialty 10.05.03 "Information security of automated systems", Novosibirsk State Technical University, e-mail: dimanechaev9@gmail.com, ORCHID: 0000-0001-8861-9147, Author ID (RSCI): 593263.