Правовая информатика

НАУЧНО-ПРАКТИЧЕСКИЙ ЖУРНАЛ
№ 1, 2020 г.
Выходит 4 раза в год

Зарегистрировано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций
Свидетельство № 015372 от 01.11.1996 г.

Журнал входит в систему Российского индекса научного цитирования (РИНЦ) и международную систему идентификации научных публикаций CrossRef (DOI).

Учредитель и издатель:
Федеральное бюджетное учреждение
«Научный центр правовой информации
при Министерстве юстиции
Российской Федерации»

Отпечатано в РИО НЦПИ при Минюсте России.
Печать цветная цифровая.
Подписано в печать **.**.2020 г.
Общий тираж 100 экз. Цена свободная.

Адрес редакции:
125437, Москва, Михалковская ул.,
65, стр.1
Телефон: +7 (495) 539-25-29
E-mail: inform360@yandex.com
Требования, предъявляемые к рукописям,
размещены на сайте
http://uzulo.su/prav-inf

СОДЕРЖАНИЕ

Подписка на журнал осуществляется в почтовых отделениях по каталогу «Пресса России». Подписной индекс: 34077

LEGAL INFORMATICS

RESEARCH AND PRACTICE JOURNAL
2020, No.1
The journal is published quarterly.

Registered by the Federal Service for Supervision in the Sphere of Telecom, Information Technologies and Mass Communications
Registration Certificate No. 015372
of the 1st of November 1996.

The journal is registered in the Russian Science Citation Index (RINTs) and CrossRef, the official Registration Agency of the International Digital Object Identifier (DOI) Foundation

Founder and publisher:
Federal State-Funded Institution "Scientific Centre for Legal Information under the Ministry of Justice of the Russian Federation"

Printed by the Printing and Publication Division of the Scientific Centre for Legal Information under the Ministry of Justice of the Russian Federation.
Printed in digital colour. Approved for print on the **th of March 2020.
Number of items printed: 100. Free price.

Postal address:
Mikhalkovskaya str., bld. 65/1,
125 438, Moscow, Russia
Telephone: +7 (495) 539-23-14
E-mail: inform360@yandex.com
Guidelines for preparing manuscripts for publication can be found on the website
http://uzulo.su/prav-inf

CONTENTS

The journal can be subscribed to at post offices through the Press of Russia (Pressa Rossii) Catalogue. Publication index: 34077

ЭФФЕКТИВНОСТЬ ПРАВОВЫХ ЭРГАСИСТЕМ В ИНФОСФЕРЕ

Ловцов Д.А.*

Ключевые слова: *правовая эргасистема, правовое регулирование, целевая и технологическая эффективность, уровень, информационные показатели, проблема, правовые методы, принципы, информация, инфосфера, информационное и цифровое пространства, информационное право.*

Аннотация.

Цель работы: *совершенствование научно-методической базы теории правовой информатики.*

Метод: *системный анализ и формально-логическая разработка релевантных информационно-математических показателей эффективности систем правового регулирования.*

Результаты: *исследованы состояние проблемы обеспечения эффективности правовых эргасистем в инфосфере и пути ее решения на научно-методической базе современной теории информационного права; рассмотрены принципы-постулаты, учитывающие специфику отрасли информационного права; обосновано предложение о переходе к Информационному кодексу Российской Федерации; определены общие и специальные методы научно-правовых исследований в предметной области информационного права; формализованы прагматические информационные показатели целевой и технологической эффективности правовых эргасистем, применение которых позволит обеспечить рациональный уровень информационной эффективности реальных систем; обосновано создание единого информационного пространства правовых эргасистем на основе комплексного плана интеграции автоматизированных информационных систем правоохранительных органов с государственными системами и сервисами в сфере обеспечения правового регулирования для продуктивного мониторинга (включая количественную оценку) и обеспечения эффективности функционирования национальных правовых эргасистем в инфосфере, включая информационное и цифровое пространства.*

DOI: 10.21681/1994-1404-2020-1-04-14

Решение существующей *научной проблемы* обеспечения эффективности систем правового регулирования[1] (международных, национальных, федеральных, территориальных) информационных отношений в инфосфере (правовых эргасистем) в интересах развития и укрепления правовой безопасности России в условиях построения информационного общества представляется возможным на основе разработки соответствующих концептуально-теоретических и научно-методологических основ модельно-алгоритмического, лингвистического и организационно-правового обеспечения правового регулирования [3, 8].

Проблема обеспечения эффективности правовых эргасистем в инфосфере

Системологическая декомпозиция данной научной проблемы позволила выявить соответствующий комплекс основных взаимосвязанных *научных задач*, решение которых обеспечит разрешение существующего противоречия: отсутствие научно-методических средств оценки и обеспечения эффективности правовых эргасистем и директивного требования ее повышения, включая:

1. Системный анализ информационной сферы общественно-производственной деятельности и классификация информационных правоотношений.

2. Теоретико-правовой анализ ключевых проблем правового регулирования информационных отношений в инфосфере.

3. Разработка концептуально-теоретических и научно-методологических вопросов системологии правового регулирования информационных отношений в инфосфере.

[1] *Правовое регулирование* — процесс целенаправленной практической реализации правовых предписаний государства (норм права), предварительно подвергшихся осмыслению субъекта-правоприменителя, воздействующих на общественные отношения.

* ***Ловцов Дмитрий Анатольевич,*** *доктор технических наук, профессор, заслуженный деятель науки Российской Федерации, заместитель по научной работе директора Института точной механики и вычислительной техники им. С. А. Лебедева Российской академии наук, заведующий кафедрой информационного права, информатики и математики Российского государственного университета правосудия, Российская Федерация, г. Москва.*

E-mail: dal-1206@mail.ru

4. Разработка модельно-алгоритмического и организационно-правового обеспечения правового регулирования информационных отношений в инфосфере.

Совместное решение данного комплекса научных задач и соответствующей научной проблемы представляется возможным на научно-методической базе современной *теории информационного права*[2] [2, 5] с формализованным уточнением основных отраслевых *принципов* и *методов*, а также с учётом реальной *системы информационного законодательства* России и условий информатизации («цифровизации») правовых эргасистем.

Наиболее характерными для отрасли информационного права, т. е. учитывающими ее специфику, являются следующие ***принципы-постулаты*** (наряду с общеотраслевыми и межотраслевыми принципами права [5, 11]):

1. *Свободное обращение информации*. В основе этого принципа — положения Конституции РФ: «Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом» (ч. 4 ст. 29), право на «свободу мысли и слова» (ч. 1 ст. 29), право на свободу всех видов творчества и преподавания (ч. 1 ст. 44). Ограничения могут вводиться только федеральным законом.

2. *Гласность (открытость или публичность информации)*. В основе этого принципа — положения ч. 4 ст. 29 Конституции РФ, а также «право на благоприятную окружающую среду, достоверную информацию о её состоянии» (ст. 42), «право на доступ к культурным ценностям» (ч. 2 ст. 44), «право на образование» (ст. 43) и специальные федеральные законы, например, федеральные законы: от 22 декабря 2008 г. № 262-ФЗ «О доступе к информации о деятельности судов в Российской Федерации» и от 9 февраля 2009 г. № 8-ФЗ «О доступе к информации о деятельности органов государственной власти и органов местного самоуправления». Ограничения доступа к привилегированной информации могут вводиться только федеральным законом.

3. *Конфиденциальность информации о частной жизни.* В основе этого принципа — положения Конституции РФ: «Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну» (ч. 1 ст. 23), «право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений» (ч.2 ст. 23). Ограничения могут вводиться только по решению суда, «сбор, хранение, использование и распространение информации о частной жизни» — с согласия гражданина (ч. 1 ст. 24).

4. *Свобода массовой информации.* В основе этого принципа — положение Конституции РФ: «Гарантируется свобода массовой информации. Цензура запрещается» (ч. 5 ст. 29). Гарантированная реализация возможна при наличии «независимых» СМИ (например, глобальных телематических сетей типа Интернет, Релком, Ситек, *Sedab*, *Remart* и др.).

5. *Баланс информационных интересов личности, общества и государства при приоритетности интересов личности.* Этот принцип обусловлен наличием множества антитетических требований персональной, общественной и государственной безопасности, общественного порядка и нравственности, международных обязательств и др.; он базируется на перечисленных положениях и следующем положении Конституции РФ: «Признание, соблюдение и защита прав человека и гражданина — обязанность государства» (ст. 2).

Система информационного законодательства находится в стадии становления. Общую характеристику ее реального состояния можно представить фрагментом (см. табл. 1) действующего Классификатора правовых актов, утвержденного Указом Президента РФ от 15 марта 2000 г. № 511.

Знание структуры информационного законодательства [4] позволяет установить функциональные связи между компонентами (подотрасли, разделы, подразделы) системы информационного законодательства для выявления и оценки прагматических свойств целостности данной отрасли. Классификатор предназначен также для унификации компьютерных баз данных и упорядочения автоматизированного обмена *правовой информацией* (рис. 1).

Дальнейшее развитие системы информационного законодательства как формального источника информационного права предполагает постепенный переход к кодифицированному правовому акту в инфосфере — Информационному кодексу РФ [5].

Общую характеристику *предмета* соответствующей научной отрасли информационного права в настоящее время можно представить фрагментом (см. табл. 2) действующего Государственного рубрикатора научно-технической информации[3].

Знание структуры научной отрасли информационного права позволяет организовать целенаправленные научные исследования и рациональную «коллективную» разработку научно-методической базы соответствующей правовой отрасли и информационного законодательства.

В качестве ***правовых методов*** и ***средств*** в отрасли информационного права применяются все известные *методы* (*диспозитивный* — при регулировании информационной собственности: вещной и интеллектуальной и др.; *императивный* — при регулировании отношений в области информационной безопасности, СМИ и др.) и *средства* (запрет, дозволение, рекомендация, обязывание (повеление), управомочивание, стимулирование (поощрение, привилегия); санкция, включая наказание и др.) правового регулирования.

[2] *Информационное право* — относительно новая интегрированная (частично самостоятельная и частично комплексная) отрасль права, предметом которой являются способы и организационно-правовые механизмы (процедуры, протоколы, модели и алгоритмы) правового регулирования *информационных отношений в инфосфере* общественно-производственной деятельности или, иначе, *целевых* (предметных, не *обеспечивающих*) информационных отношений.

[3] Государственный Рубрикатор научно-технической информации (электронное издание). М.: НТЦ «Информрегистр», ВИНИТИ, 2007. URL: http://grnti.ru/metod.php .

Таблица 1

Структура информационного законодательства

Шифр	Наименование отрасли, подотраслей и разделов законодательства
120.000.000	**Информация и информатизация**
120.010.000	**Общие положения в сфере информации и информатизации**
120.020.000	**Управление в сфере информации и информатизации**
120.030.000	**Информационные ресурсы. Пользование информационными ресурсами**
120.030.010	Общие положения
120.030.020	Документирование информации. Делопроизводство
120.030.030	Обязательный экземпляр документов
120.030.040	Архивный фонд. Архивы
120.030.050	Информационные ресурсы по категориям доступа
120.030.060	Информация о гражданах (персональные данные)
120.030.070	Правовая информация
120.030.080	Предоставление информации. Информационные услуги
120.040.000	**Информатизация. Информационные системы, технологии и средства их обеспечения**
120.040.010	Информатизация
120.040.020	Информационные системы, технологии и средства их обеспечения
120.050.000	**Средства массовой информации**
120.060.000	**Реклама**
120.070.000	**Информационная безопасность. Защита информации и прав субъектов в области информационных процессов и информатизации**
130.040.000	**Средства массовой информации**
130.040.010	Общие вопросы
130.040.020	Информационные агентства
130.040.030	Телевидение. Радиовещание
130.040.040	Печатные издания
130.040.050	Другие средства массовой информации

Рис. 1. Классификация правовой информации

Таблица 2

Структура научной отрасли информационного права

Шифр	Наименование отрасли и подотраслей науки
10.19.00	**Информационное право**
10.19.01	Общие вопросы информационного права
10.19.25	Правовой режим информации, информационных систем и сетей
10.19.31	Право на информацию
10.19.35	Правовое регулирование средств массовой информации
10.19.43	Правовой режим информационных ресурсов
10.19.51	Правовое регулирование международного обмена информацией и использования глобальных информационных сетей
10.19.61	Правовое регулирование информационной безопасности
10.19.65	Правонарушения в области информатики. Ответственность в информационном праве

Методы научных исследований в предметной области информационного права включают как общие (традиционные) методы научно-правовых исследований, так и специальные, обусловленные спецификой предметной области.

В состав ***общих методов*** научно-правовых исследований входят, в частности, следующие:

• методология проблемно-ориентированного варианта системного подхода — комплексного «ИКС»-подхода («информационно-кибернетически-синергетического») [6], включая его базовые методы: системный анализ, структурный анализ, функциональный анализ;

• формально-догматический метод (основные процедуры: описание, толкование, классификация, систематизация);

• сравнительно-правовой метод (логическое сравнение элементов различных правовых систем, систем права и законодательства, систем правоотношений и правосознания);

• сравнительно-исторический метод (учёт исторических особенностей в развитии систем правового регулирования);

• социологический метод (наблюдение, анкетирование, верификация, статистическая обработка и др. способы выявления фактов);

• метод моделирования (вербального, концептуально-логического, логико-лингвистического, математического, имитационного или компьютерного);

• метод социально-правового эксперимента (натурного, имитационного) и др.

К ***специальным методам*** научно-правовых исследований в предметной области информационного права можно отнести следующие естественнонаучные методы:

• информационно-аксиологический (от греч. αξια — ценность) метод *правовой информологии*[4] — количественное оценивание качества правовой и иной содержательной информации, т. е. свойств информации, имеющих принципиальное значение для правового регулирования информационных отношений, а также информационной эффективности (целевой и технологической) и информационной безопасности жизнедеятельности (функционирования) личности, общества и государства;

• информационно-технологический метод *правовой информатики* — количественное оценивание качества и эффективности применения информационно-компьютерных технологий и электронно-вычислительной (компьютерной) техники в сфере юридически значимой электронной деятельности (автоматизированного судопроизводства, электронного голосования, электронной коммерции и др.).

С помощью известных мер количества информации *структурной* (например, алгоритмической меры А. Колмогорова, алгебраической меры А. Шилейко и В. Кочнева и др.) и *содержательной* (комбинаторной меры Ю. Шрейдера, вероятностной меры А. Харкевича и др. [7]5) можно оценить информационно-структурный (Q_v) и информационно-содержательный (Q_z) ресурсы эргасистемы соответственно, что, в частности, позволит обеспечить рациональное использование совокупного информационного ресурса в функционирующей эргасистеме для получения различных целевых (в управляемых объектах) и технологических (в информационных процессах) эффектов. Оценивание последних возможно на основе соответствующих *информационных показателей*, использующих данные классические информационные меры в качестве компонентов.

Например, для оценки целевой эффективности эргасистем применяются *показатели* их информационно-преобразующей способности, информационной добротности, коэффициента информационного усиления

[4] Исследует природу социально-правовой информации и её связанность с самоорганизующейся правовой системой общества.

[5] См. также: Ловцов Д. А. Модели измерения информационного ресурса АСУ // Автоматика и Телемеханика. 1996. № 9. С. 3—17.

и др., а для оценки технологической эффективности — коэффициент рациональности использования информационного ресурса, показатели информационной производительности и информационной надежности эргасистем и др. [7, 13].

Информационные показатели целевой эффективности правовых эргасистем в инфосфере[6]

В качестве информационных показателей[7] *целевой* эффективности и качества правовых эргасистем в инфосфере с произвольной топологической структурой информационной распределительной сети, имеющих практическое значение, можно использовать следующие [7, 13]:

1. *Информационно-преобразующая способность* (характеризует продуктивность переработки осведомляющей информации, поступающей в эргасистему или информационный узел от объектов регулирования):

$$J_{1ц} = Э_ц / t', \quad (1)$$

где $Э_ц$ — мера целевого эффекта; t' — средний интервал времени переработки осведомляющей информации Q_{zo} от одного управляемого (регулируемого) объекта.

2. *Информационная добротность* (характеризует информационную экономичность эргасистемы (узла) и определяется как отношение общего количества информации различного вида [7], хранящейся и циркулирующей в эргасистеме, и количества информации, характеризующего затраты основных («работающих») видов системных ресурсов):

$$J_{2ц} = I/[I_v(\Theta)+I_z(T)] = [Э_ц+I_o+I_v+I_z(T)]/[I_v+I_z(T)] = \\ = 1+[Э_ц+I_o]/[I_v+I_z(T)]; \quad (2)$$

где I — общее количество информации Q, которое хранится и циркулирует в эргасистеме (узле);

$I_v(\Theta)$ — количество используемой *структурной* [7, 13] информации, содержащейся в информационном узле, имеющем структуру Θ, определяющее затраты (информационные, вещественные, энергетические) на преобразование содержательной осведомляющей информации Q_{zo};

$I_z(T)$ — количество с*одержательной* информации Q_z эргасистемы, заключенной в ее общесистемном тезаурусе T;

I_o — количество информации, хранимой в информационной базе эргасистемы (узла).

3. *Коэффициент информационного усиления* (характеризует силу воздействия эргасистемы, узла):

$$J_{3ц} = I / Э_ц = [Э_ц+I_o+I_v+I_z(T)] / Э_ц = \\ = 1 + [I_o+I_v+I_z(T)] / Э_ц, \quad (3)$$

В выражениях (1)—(3) в качестве меры $Э_ц$ *целевого* эффекта, получаемого от данной эргасистемы (информационного узла) в результате выполнения технологического процесса переработки (преобразования) информационных массивов (ИМ), используется [13]:

$$Э_ц = \max\{I_{zo}(M, T)\} = \max \Sigma_m\{\ln [T(O_m)/T]\} = \\ = \max \Sigma_m\{\ln[(\Sigma_i n_{i(om)})/(\Sigma_i n_i)]\},$$

$m = 1,\ldots,M$, $i = 1,\ldots,I$,

где I_{zo} — количество содержательной [7] осведомляющей информации Q_{zo}, заключенной в множестве M получаемых эргасистемой ИМ, относительно общесистемного тезауруса T;

$T = \{<X, Y>, Z>\}$ — общее множество-тезаурус эргасистемы;

$X = \{x_i\}$, $i = 0,\ldots,n_x - 1$ — множество понятий <*имя-смысл-значение*>;

$Y = <\{y_j\}; \rightarrow, \leftarrow>$, $j = 1,\ldots,n_y$ — множество предикатов различного вида, а также двух отношений: включения ($\leftarrow$) и применимости ($\rightarrow$);

$Z = <\{z_k\}; \wedge, \vee, \neg;$ Я, Д, Ж, Ф>, $k = 1,\ldots,n_z$ — множество событий z_k, на котором заданы логические операции конъюнкции ($\wedge$), дизъюнкции ($\vee$), отрицания ($\neg$), а также специальные кванторы[8]: рождения «Я» (возникновения, введения в рассмотрение), дескрипции «Д» ($y_1[Дx]y_2x$ — «тот x, который обладает свойством y_2, обладает свойством y_1»), множественной дескрипции «Ж» для $x \in X$ ($y_1[Жx]y_2x$ — «те x, которые обладают свойством y_2, обладают свойством y_1»), общей дескрипции «Ф» для всех прогнозируемых объектов, которые в дальнейшем могут войти в X ($y_1[Фx]y_2x$ — «все те x, которые обладают свойством y_2, обладают свойством y_1», т. е. равносильно отношению $y_2 \leftarrow y_1$);

$O_m \in O$, $O_m = \{O_{mi}\}$, $i = 1,\ldots,I$ — оператор преобразования тезауруса T под воздействием соответствующего ИМ m;

n_i, $i = x, y, z$ — кардинальное число i-го множества.

Числовой пример. Пусть в эргасистеме получен текстовый ИМ-предписание:

m_j = <Действия злоумышленника считаются безопасными, если они выявлены и нейтрализованы>.

С использованием предикатов: y_1 — быть действиями, y_2 — злоумышленника (принадлежать злоумышленнику), y_3 — считаются (двуместный предикат), y_4 — выявлены, y_5 — нейтрализованы, y_6 — безопасные, можно представить соответствующую *смысловую* запись в виде:

$$S_j = < [Яx](y_1x); y_2[Дx](y_1x); (y_4[Дx]y_1x) = \\ = z_1; (y_5[Дx]y_1x) = z_2; z_1 \wedge z_2 = z_3; \\ y_3\{[Фx]z_3{*}x, [Фx]y_6x\} >,$$

где Я, Д, Ф — кванторы рождения (введения в рассмотрение), дескрипции и множественной дескрипции, соответственно; $\wedge$ — знак логического «И».

---

[6] Для информационно-аксиологического метода научно-правовых исследований в предметной области информационного права.

[7] *См.*: Ловцов Д. А. Информационные показатели эффективности функционирования АСУ сложными динамическими объектами // Автоматика и телемеханика. 1994. № 12. С. 143—150.

[8] *См.*: Шрейдер Ю. А. Об одной модели семантической теории информации // Проблемы кибернетики. 1965. Вып. 13. С. 233—240.

Согласно известной методике[9] реорганизации тезауруса определяется O_{mj}, по которому в T вводятся предикаты y_6 (если он там отсутствовал ранее) и z_3* (участвует в событии z_3); отношения включения $y_6 \leftarrow y_4$, $y_6 \leftarrow y_5$; отношение применимости $y_6 \rightarrow (y_1, y_2)$, а также события-высказывания z_1, z_2, z_3.

Тогда $I_{zo}(m_j, T) = \ln[(n_{yj} + n_{zj})/n_y] = \ln[(10+3)/5] = 0{,}96$ *нат*.

В выражениях (2), (3) в качестве меры количества структурной информации можно использовать [7]:

$$I_v(\Theta) = m_s\ln(n_s)+m_r\ln(n_r)+\{(\Sigma_i\ln\{\Lambda_i/\varepsilon_{ci}\})\vee$$
$$\vee[m_c\ln(2)]+[m_a\ln(n_a)+m_b\ln(2)]\}\vee$$
$$\vee[\Sigma_k m_{ck}\ln(2)]+m_\delta\ln(n_\delta),\ i = 1,\ldots,n_c;\ k = 1,\ldots,J,$$

где m_s, m_r, m_c, m_δ, m_a, m_b — число подстрингов (символов), отражающих элементы $s \in S$, $r \in R$, $c \in C$, $\delta \in \Delta$, $a \in A$, $b \in B$, соответственно, в минимальном (m_s+m_r, $m_c+m_\delta+m_a+m_b$=min) стринге (упорядоченная последовательность символов), представляющем собой математическое описание (модель) Θ эргасистемы (узла);

S, R, C, Δ, A, B — множества средств, ресурсов (дополнительных средств), информационных связей, ситуационных структур, задач переработки информации (с учетом целей, стоящих перед эргасистемой), связей-дуг (отображающих частичный порядок в технологическом процессе переработки информации) эргасистемы (узла), соответственно;

n_s, n_r, n_c, n_δ, n_a, n_b — количество элементов множеств S, R, C, Δ, A, B, соответственно;

Λ_i — максимально возможное значение интенсивности i-й информационной связи;

ε_{ci} — погрешность измерения интенсивности i-й связи;

2 — число возможностей при простом наличии-отсутствии информационной связи;

$\vee$ — знак логического «ИЛИ» (здесь означает, что при вычислении $Iv(\Theta)$ третье и пятое слагаемые могут иметь какое-либо одно из двух приведенных выражений, соответственно, в зависимости от характера информационных связей в системе).

Числовой пример. Для информационного узла эргасистемы, содержащего $n = |S| = 4$ однородных информационных преобразователей, использующих $k = |R| = 3$ видов общесистемных ресурсов и функционирующих совместно в сети с переменной структурой, имеющей $J = 2$ вариантов (радиальный и полносвязный):

$m_s = n$, $m_r = k$, $m_\delta = J$, $m_{c1} = 2(n—1)$, $m_{c2} = n(n—1)$;

$I_v(\Theta) = n\ln(n) + k\ln(k) + 2(n — 1)\ln(2) + n(n—1)\ln(2) + 2\ln(2) = 22{,}86$ *нат*.

Предложенный показатель (2) *информационной добротности* эргасистемы позволяет, в частности, оценить экономичность действий эргасистемы в ходе информационного соперничества с противостоящими (противоборствующими и враждебными) эргасистемами на основе дополнительного учета в (2) в составе общего количества I информации Q *количество*:

«содержательной» дезинформации ($Q_{zd1}(M,T)$; $Q_{zdj}(M,T)$, $j = 2,\ldots,J$) противостоящих эргасистем (рассматриваемой и J — 1враждебных);

структурно-статистической информации ($Q_{u1}(N)$; $Q_{uk}(N)$, $k = 2,\ldots,K$) о применении активных способов (методов) противодействия из определенного множества (N) возможных, заключенной в статистических структурах соответствующего множества сообщений о применении различных способов, при этом:

$I_u(N) = — \Sigma_i p_i \ln(p_i)$, $i = 1,\ldots,N$,

где p_i — вероятность i-го из возможных N ИМ (соответствующего сообщения-ИМ $m_i \in M$).

Информационные показатели технологической эффективности правовых эргасистем в инфосфере[10]

Для оценки *технологической* эффективности и качества правовых эргасистем в инфосфере как систем переработки правовой информации с произвольной топологической структурой информационной распределительной сети, а также для описания динамики преобразования информации в ходе алгоритмических преобразований можно использовать следующие информационно-энтропийные показатели, имеющие практическое значение [7, 13]:

1. *Коэффициент рациональности использования информационного ресурса* эргасистемы (информационного узла):

$$J_{1m} = Э_т / [\,Э_т + I_v(\Theta)\,],\ J_{1m} \in (0, 1); \quad (4)$$

где $Э_т$ — технологический эффект, получаемый от эргасистемы (узла) в результате выполнения технологического процесса переработки (преобразования) поступающей содержательной *осведомляющей* [7] информации Q_z.

2. *Информационная производительность* эргасистемы (узла):

$$J_{2m} = Э_т / \tau'; \quad (5)$$

где τ' — средний интервал времени между моментами формирования двух последовательных выходных (преобразованных) ИМ m_{1j}, $m_{1,j+1} \in M_1$, $j = 1,2,\ldots$;

3. *Информационная надежность* функционирования эргасистемы (узла):

$$J_{3m} = Э_т / H(M_1),\ J_{3m} \in (0, 1]; \quad (6)$$

где $H(M_1)$ — энтропия множества M_1 «выходных» (преобразованных) ИМ; надежность равна 1 в случае отсутствия дестабилизирующих факторов (ДФ), таких как возмущающие воздействия среды, искусственные воздействия внешних сил, ошибки и дефекты (конструктивные, технологические и эксплуатационные) распространения проявлений ДФ из-за причинно-следственных связей.

В выражениях (4)—(6) в качестве меры *технологического* эффекта $Э_т$, получаемого от данной эргасистемы (информационного узла) в результате выполнения

[9] Там же.

[10] Для информационно-технологического метода научно-правовых исследований в предметной области информационного права.

алгоритмического процесса переработки (преобразования) ИМ, используется[11]:

$$Э_т = \Sigma_i \Sigma_j p(m_{0i}, m_{1j}) \ln\{p(m_{0i}, m_{1j})/ p(m_{0i})\, p(m_{1j})\}. \quad (7)$$

где $m_{0i} \in M_0$, $i = 1,2,...$ — входные ИМ.

Выражение (7) преобразуется[12] к виду:

$$Э_т = H(M_1) - \Sigma_i p(m_{0i})\, H(M_1 | m_{0i}), \quad (8)$$

где $H(M_1) = \Sigma_j p(m_{1j}) \ln\{p(m_{1j})\}$; $H(M_1 | m_{0i}) = \Sigma_j p(m_{1j} | m_{0i}) \ln\{p(m_{1j} | m_{0i})\}$.

Выражения (4)—(8) получены на основе общепринятых методов, основанных на том, что само понятие технологической эффективности имеет *статистический* характер.

Числовой пример. Рассмотрим информационный узел эргасистемы, содержащий $n = 4$ однородных элементов (информационных преобразователей), в котором реализуется алгоритм контроля состояния управляемого объекта путем проверки на допуск контролируемых параметров m_{0i}, $i = 1,\ldots,5$. Результатами работы алгоритма в условиях воздействия ДФ являются ИМ m_{1j}, $j = 1,\ldots,3$, имеющие значения «меньше нормы», «норма» и «больше нормы», соответственно. Узел описывается матрицей $f(M_0, M_1, \Omega)$ совместных вероятностей ИМ m_0 и m_{1j} (где Ω — множество факторов неопределённости):

$$f = \begin{Vmatrix} 0{,}05 & 0{,}08 & 0{,}12 & 0{,}10 & 0{,}03 \\ 0{,}12 & 0{,}02 & 0{,}04 & 0{,}04 & 0{,}02 \\ 0{,}10 & 0{,}05 & 0{,}03 & 0{,}12 & 0{,}08 \end{Vmatrix}.$$

Отсюда с учетом (7) получим:

$Э_т = 0{,}14$ *двед*; $P(M_1) = <0{,}38 \quad 0{,}24 \quad 0{,}38>$, что даёт $H(M_1) = 1{,}55$ *двед*.

Определим в (4) значения $I_v(\Theta)$ для радиальной (Θ_1) и полносвязной (Θ_2) структур информационного узла:

$I_v(\Theta_1) = n \log(n) + 2(n - 1)\log 2 = 14$ *двед*;

$I_v(\Theta_2) = n \log(n) + n(n - 1)\log 2 = 20$ *двед*

и положим в (5) $\tau' = 1$ единиц времени (*е.в.*). Тогда имеем:

$J_{1тр} = Э_т / [Э_т + I_v(\Theta_1)] = 0{,}01$;

$J_{1тп} = Э_т / [Э_т + I_v(\Theta_2)] = 0{,}007$;

$J_{2т} = Э_т / \tau' = 0{,}14$ *двед/е.в.*;

$J_{3т} = Э_т / H(M_1) = 0{,}1$.

В отношении показателей (4)—(6) справедливы следующие утверждения-теоремы[13].

Утверждение 1. Уровень информационно-технологической эффективности эргасистемы с произвольной топологической структурой (радиальной, кольцевой или комбинированной) информационной распределительной сети не превышает максимального уровня локальной информационно-технологической эффективности подсистем (информационных узлов) при любых условиях, т. е.

$$J_{1т} \le \max\{J_{1тl}\},\ l = 1,\ldots,L, \quad (9)$$

где L — номер выходного информационного узла эргасистемы.

Утверждение 2. Уровни информационно-технологических производительности и надежности эргасистемы с произвольной топологической структурой информационной распределительной сети определяются соответствующими локальными показателями выходной подсистемы (узла) при любых условиях, т. е.

$$J_{2т} \le J_{2тL},\ J_{3т} \le J_{3тL}. \quad (10)$$

Единое информационное и «цифровое» пространство правовых эргасистем

Для продуктивного мониторинга (включая количественную оценку) и обеспечения эффективности функционирования национальных систем правового регулирования (правовых эргасистем) представляется целесообразным формирование *единого информационного пространства* (ЕИП) как виртуальной области активного процессуального электронного взаимодействия работников (представителей, деятелей, персонала) и пользователей (участников, наблюдателей, граждан) сообщества правовых эргасистем, которая возникает в результате формирования соответствующей информационной среды, включающей национальную информационную инфраструктуру, информационно-технические средства, информационно-компьютерные («цифровые») технологии и организационно-юридические структуры правовых эргасистем, для целесообразной переработки *правовой информации*.

При этом под *информационной инфраструктурой* понимается совокупность правовых автоматизированных информационных систем (АИС), коммуникаций (информационно-телекоммуникационные и телематические сети), информационных ресурсов (информации библиотек, архивов, хранилищ и баз данных и знаний (БДЗ) и др.), находящихся в ведении государства.

Информационно-технические средства включают АИС правоохранительных органов, корпоративные и локальные информационно-вычислительные сети, информационно-правовое обеспечение (нормативно-правовые БДЗ, технологии их ведения и использования), информационно-лингвистическое обеспечение (классификаторы, словари, тезаурусы).

Информационная среда и соответствующее ЕИП судебной системы формируются на основе единых принципов и общих правил с осуществлением мероприятий по включению судебных информационных ресурсов в объединенные БДЗ, интернет-сайты (порталы) и установлением единых требований к их созданию, функционированию, обеспечению доступа к информации о деятельности судов, а также к их эксплуатационному обслуживанию и развитию [12].

Электронное взаимодействие в ЕИП осуществляется в интересах конституционного, гражданского (включая арбитражное), административного и уголовного судопроизводства — *целевое* (процессуальное) взаимодействие, а также для обеспечения деятельности

[11] *См.*: Шилейко А. В., Кочнев В. Ф., Химушин Ф. Ф. Введение в информационную теорию систем. М.: Радио и связь, 1985.

[12] *См.:* Шеннон К. Работы по теории информации и кибернетике. М.: ИЛ, 1963.

[13] Ловцов Д. А. Информационные оценки технологической эффективности переработки и нформации // НТИ. Сер. 2. Информ. процессы и системы. 1997. № 11. С. 22—26.

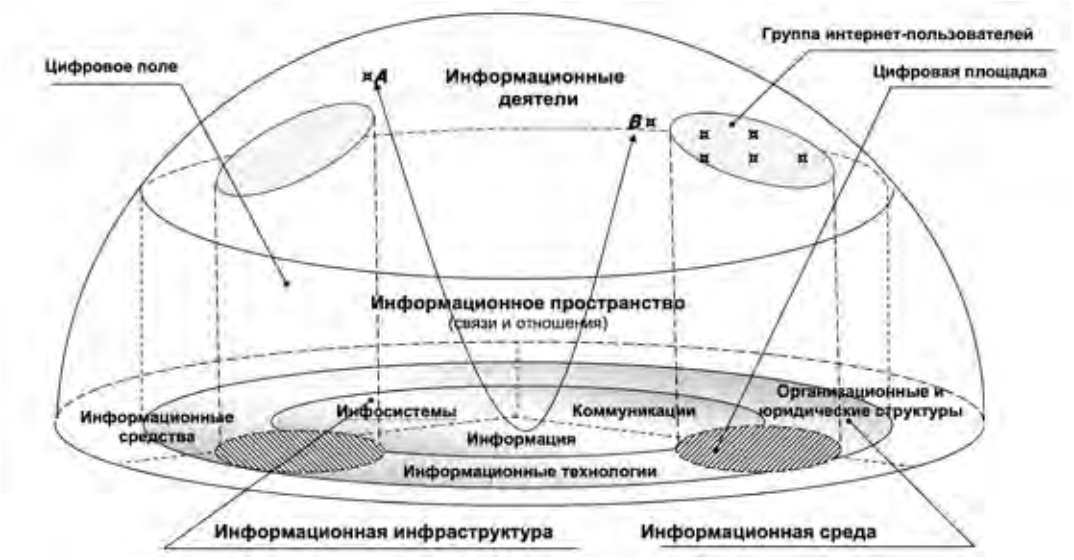

Рис. 2. Концептуально-логическая модель инфосферы

судов, органов судейского сообщества и Судебного департамента при Верховном Суде РФ — *технологическое* (обеспечивающее) взаимодействие.

«Цифровое» пространство — это составная часть информационного пространства, возникающая на основе функционирующей цифровой среды (части информационной среды), базирующейся на цифровой инфраструктуре (телематические системы и сети, хранилища и базы данных и знаний, электронные книги и др.), и объединяющая совокупность виртуальных цифровых полей, возникающих на основе функционирования соответствующих цифровых площадок (включающих цифровые средства и технологии определенных социальных групп, поддерживающих интернет-коммуникации) [1, 10] (рис. 2). Информационные деятели — источники и потребители информации (см. рис. 2) ***A*** и ***B*** (группы интернет-пользователей) взаимодействуют посредством определенной информационной среды (цифровых площадок) и соответствующего информационного пространства (цифровых полей).

На современном этапе создания и развития ЕИП правовых эргасистем представляется целесообразной разработка *комплексного плана* интеграции АИС правоохранительных органов (Генпрокуратуры, МВД, судебной системы и др.) со следующими государственными системами и сервисами в сфере обеспечения правового регулирования:

- единой системой нормативной справочной информации (для доступа к общегосударственным справочникам, классификаторам, реестрам, регистрам, словарям);
- информационным платежным шлюзам (для оплаты пошлин);
- единой системой идентификации и аутентификации (для авторизации субъектов и объектов взаимодействия);
- единым Порталом государственных услуг (для доступа граждан и судов к информации федеральных и региональных органов власти, в том числе к информации на «цифровых картах»[14]);
- информационно-справочными правовыми и учётными системами министерств и ведомств;
- государственной почтовой системой (для пересылки повесток судов, жалоб и предложений от граждан, в том числе с использованием СМС);
- системами дистанционного повышения квалификации работников правоохранительных органов в сфере правоприменения и др.

Для осуществления интеграции правовых АИС с элементами инфраструктуры «электронного правительства» представляется также целесообразным в рамках Государственной программы РФ «Информационное общество» (2011—2020 гг.) спланировать и организовать разработку нормативно-методической базы формирования и развития ЕИП правовых эргасистем, обеспечивающего информационное взаимодействие правоохранительных органов между собой и с федеральными органами исполнительной власти в электронном виде.

Создание и развитие ЕИП правовых эргасистем России представляет собой сложную комплексную научно-прикладную проблему. Ее решение сопряжено с выполнением широкого круга сложных задач организационно-правового обеспечения процессов информатизации правоохранительных органов и представляется возможным при объединении усилий и ресурсов заинтересованных государственных структур в рамках, например, перспективной целевой программы развития правоохранительной системы с учётом целей и задач формирования нового — информационного общества.

[14] Цифровые (электронные) карты, а также объемные модели местности (3D-модели) и спутниковые фотографии, снабженные подробными комментариями и разъяснениями, удобны для наглядной экспликации результатов различных аналитических, исследовательских и научных работ. Находятся под защитой авторских прав.

Заключение

Таким образом, рассмотрены состояние и пути решения проблемы обеспечения эффективности систем правового регулирования информационных отношений (правовых эргасистем) в инфосфере на научно-методической базе современной теории информационного права, в частности:

- определены методы научно-правовых исследований в предметной области информационного права;
- обосновано создание единого информационного пространства правовых эргасистем для продуктивного мониторинга и обеспечения эффективности функционирования национальных правовых эргасистем в инфосфере;
- формализованы прагматические показатели информационной эффективности эргасистем, позволяющие определить численные значения компонентов *научно-технического уровня* действующих эргасистем;
- установлены формальные соотношения между глобальными и локальными информационными показателями технологической эффективности переработки информации в эргасистемах, такими как рациональность использования (употребления) информационного ресурса систем и подсистем, информационные надежность и производительность, использующими классические и синтетические [7] информационные меры. Показано, что степень глобальной информационно-технологической эффективности эргасистемы с произвольной топологической структурой информационной распределительной сети не превышает максимальной степени локальной информационно-технологической эффективности подсистем при любых условиях.

Приведенные обоснованные информационно-математические соотношения (1)—(10) позволяют рассчитывать значения уровней целевой и технологической эффективности и качества реальных правовых эргасистем в инфосфере. Данные соотношения можно использовать при синтезе структур телематических систем и АИС для расчета требуемых характеристик информационно-преобразующей способности, добротности, производительности, надежности, ресурсоемкости и др. и обеспечения рационального уровня информационной эффективности реальных систем. При этом можно определить необходимые и достаточные информационные *условия наблюдаемости* и *управляемости* [17] информационных процессов для конкретной эргасистемы, включая информационные *ограничения*, обусловленные осведомляющей информацией о потенциальных информационных, радиоэлектронных и др. угрозах безопасности эргасистемы и источниках дестабилизирующих факторов.

Дальнейшую разработку рациональной совокупности информационных показателей эффективности эргасистем целесообразно осуществлять согласно принципу *информационной ценности* [6, 7, 9, 13], что позволит учесть ценность информации, в частности, той, которая содержится в эргасистеме и которой система оперирует в соответствии с целевой задачей, а также учесть затраты информационного ресурса при определении эффективности функционирования эргасистемы как информационной системы. Учет ценности информации, в свою очередь, позволит обеспечить своевременное и качественное регулирование, координацию и оптимизацию информационных процессов в эргасистеме.

Рецензент: ***Запольский Сергей Васильевич,*** *доктор юридических наук, профессор, заслуженный юрист Российской Федерации, главный научный сотрудник Института государства и права Российской академии наук, Российская Федерация, г. Москва.*
E-mail: zpmoscow@mail.ru

Литература

1. Ващекин А.Н., Дзедзинский А.В. Правовое регулирование отношений в цифровом пространстве // Правосудие. 2020. № 2. С. 108—114.
2. Голоскоков Л. В. Теория сетевого права. М. : МПСУ, 1912. 216 с.
3. Ершов В. В. Правовое и индивидуальное регулирование общественных отношений: Монография. М. : РГУП, 2018. 628 с. ISBN 978-5-93916-631-7.
4. Кутузов В. И., Раимова А. Т. Основы информационного законодательства. М. : УРСС, 2004. 336 с.
5. Ловцов Д. А. Теория информационного права: базисные аспекты // Государство и право. 2011. № 11. С. 43—51. ISSN 0132-0769.
6. Ловцов Д. А. Концепция комплексного «ИКС»-подхода к исследованию сложных правозначимых явлений как систем // Философия права. 2009. № 5. С. 40—45.
7. Ловцов Д. А. Информационная теория эргасистем: Тезаурус. М. : Наука, 2005. 248 с. ISBN 5-02-033779-X.
8. Ловцов Д. А. Основы технологии эффективного двухуровневого правового регулирования информационных отношений в инфосфере // Правовая информатика. 2018. № 2. С. 4—14. DOI: 10.21681/1994-1404-2018-2-4-14.

9. Ловцов Д. А. Информационная теория эргасистем: основные положения // Правовая информатика. 2019. № 3. С. 4—20. DOI: 10.21681/1994-1404-2019-3-4-16.
10. Ловцов Д. А. Системология правового регулирования информационных отношений в инфосфере: архитектура и состояние // Государство и право. 2012. № 8. С. 16—25. ISSN 0132-0769.
11. Ловцов Д. А. Система принципов эффективного правового регулирования информационных отношений в инфосфере // Информационное право. 2017. № 1. С. 13—18.
12. Ловцов Д. А., Ниесов В. А. Актуальные проблемы создания и развития единого информационного пространства судебной системы России // Информационное право. 2013. № 5. С. 13—18.
13. Ловцов Д. А., Сергеев Н. А. Управление безопасностью эргасистем : монография / Под ред. Д. А. Ловцова. М. : РАУ — Университет, 2001. 224 с. ISBN 5-86014-131-9.
14. Осипов М. Ю. Правовое регулирование как динамическая система // Право и политика. 2006. № 11. С. 17—31.
15. Теория государства и права / Под ред. В. М. Корельского, В. Д. Перевалова. М. : Норма, 2002. 616 с.
16. Тихомиров Ю. А. Правовое регулирование: теория и практика. М. : Формула права, 2008. 400 с.
17. Chobanyan V. A., Glazov B. I., Lovtsov D. A. Observability and Controllability of Projects under Conflict Conditions of Information Vagueness, Proceedings of 14th World Congress on Project Management IPMA “Strategy Start-Up”, vol. 2, Ljubljana : ZPM-Slovenija, 1998, pp. 668-670.

EFFICIENCY OF LEGAL ERGASYSTEMS IN THE INFOSPHERE

Dmitrii Lovtsov, *Doctor of Science (Technology), Professor, Meritorious Scientist of the Russian Federation, Deputy Director for Research of Lebedev Institute of Precision Mechanics and Computer Engineering of the Russian Academy of Sciences, Head of the Department of Information Technology Law, Informatics and Mathematics of the Russian State University of Justice, Moscow, Russian Federation.*
E-mail: dal-1206@mail.ru

Keywords: *legal ergasystem, legal regulation, target and technological efficiency, level, information indicators, problem, legal methods, principles, information, infosphere, information and digital space, information technology law.*

Abstract.
Purpose of the work: *improving the scientific and methodological basis of the legal informatics theory.*
Method used: *system analysis and formal logical development of relevant information and mathematical indicators of efficiency of legal regulation systems.*
Results obtained: *the state of the problem of support of legal ergasystems efficiency in the infosphere and ways for solving it based on the scientific and methodological basis of the modern theory of information technology law are studied. Principles-postulates taking into account the specific features of the information technology law branch are considered. A justification is given for the transition to the Information Code of the Russian Federation. General and special methods of legal science studies in the subject area of information technology law are determined. Pragmatic information indicators of target and technological efficiency of legal ergasystems are formalised, their use will allow to provide for a rational level of information efficiency of real systems. A justification is given for creating a single information space of legal ergasystems based on a integrative plan of aggregation of automated information systems of law enforcement authorities with government systems and services in the sphere of support of legal regulation for productive monitoring (including quantitative estimates) and ensuring an efficient functioning of national legal ergasystems in the infosphere including the information and digital spaces.*

References

1. Vashchekin A.N., Dzedzinskii A.V. Pravovoe regulirovanie otnoshenii v tsifrovom prostranstve. Pravosudie, 2020, No. 2, pp. 108-114.
2. Goloskokov L. V. Teoriia setevogo prava. M. : MPSU, 1912, 216 pp.
3. Ershov V. V. Pravovoe i individual’noe regulirovanie obshchestvennykh otnoshenii : monografiia. M. : RGUP, 2018, 628 pp., ISBN 978-5-93916-631-7.
4. Kutuzov V. I., Raimova A. T. Osnovy informatsionnogo zakonodatel’stva. M. : URSS, 2004, 336 pp.
5. Lovtsov D. A. Teoriia informatsionnogo prava: bazisnye aspekty. Gosudarstvo i pravo, 2011, No. 11, pp. 43-51, ISSN 0132-0769.
6. Lovtsov D. A. Kontseptsiia kompleksnogo “IKS”-podkhoda k issledovaniiu slozhnykh pravoznachimykh iavlenii kak sistem. Filosofiia prava, 2009, No. 5, pp. 40-45.
7. Lovtsov D. A. Informatsionnaia teoriia ergasistem: tezaurus. M. : Nauka, 2005, 248 pp., ISBN 5-02-033779-X.

8. Lovtsov D. A. Osnovy tekhnologii effektivnogo dvukhurovnevogo pravovogo regulirovaniia informatsionnykh otnoshenii v infosfere. Pravovaia informatika, 2018, No. 2, pp. 4-14, DOI: 10.21681/1994-1404-2018-2-4-14.
9. Lovtsov D. A. Informatsionnaia teoriia ergasistem: osnovnye polozheniia. Pravovaia informatika, 2019, No. 3, pp. 4-20, DOI: 10.21681/1994-1404-2019-3-4-16.
10. Lovtsov D. A. Sistemologiia pravovogo regulirovaniia informatsionnykh otnoshenii v infosfere: arkhitektura i sostoianie. Gosudarstvo i pravo, 2012, No. 8, pp. 16-25, ISSN 0132-0769.
11. Lovtsov D. A. Sistema printsipov effektivnogo pravovogo regulirovaniia informatsionnykh otnoshenii v infosfere. Informatsionnoe pravo, 2017, No. 1, pp. 13-18.
12. Lovtsov D. A., Niesov V. A. Aktual'nye problemy sozdaniia i razvitiia edinogo informatsionnogo prostranstva sudebnoi sistemy Rossii. Informatsionnoe pravo, 2013, No. 5, pp. 13-18.
13. Lovtsov D. A., Sergeev N. A. Upravlenie bezopasnost'iu ergasistem : monografiia. Pod red. D. A. Lovtsova. M. : RAU - Universitet, 2001, 224 pp., ISBN 5-86014-131-9.
14. Osipov M. Iu. Pravovoe regulirovanie kak dinamicheskaia sistema. Pravo i politika, 2006, No. 11, pp. 17-31.
15. Teoriia gosudarstva i prava. Pod red. V. M. Korel'skogo, V. D. Perevalova. M. : Norma, 2002, 616 pp.
16. Tikhomirov Iu. A. Pravovoe regulirovanie: teoriia i praktika. M. : Formula prava, 2008, 400 pp.
17. Chobanyan V. A., Glazov B. I., Lovtsov D. A. Observability and Controllability of Projects under Conflict Conditions of Information Vagueness. Proceedings of 14th World Congress on Project Management IPMA "Strategy Start-Up", vol. 2, Ljubljana : ZPM-Slovenija, 1998, pp. 668-670.

АРХИТЕКТУРА ГИБРИДНОЙ ИНТЕЛЛЕКТУАЛЬНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ АНАЛИЗА СУДЕБНОЙ АРБИТРАЖНОЙ ПРАКТИКИ

*Таран М.О., Гапанюк Ю.Е.**

Ключевые слова: *арбитражный суд, гибридная интеллектуальная система, гибридная интеллектуальная информационная систем, сознание информационной системы, подсознание информационной системы, анализ текстов, многоагентная система, граф, метаграф, метавершина, метаребро, метаграфовый процесс, метаграфовый агент, активный узел метаграфа.*

Аннотация.

Цель работы: *совершенствование научно-методической базы информационного обеспечения системы судебной практики арбитражных судов.*

Методы: *методы проектирования гибридных интеллектуальных информационных систем на основе моделей сложных сетей.*

Результаты: *рассмотрен подход к разработке гибридных интеллектуальных информационных систем (ГИИС), основанный на использовании модулей сознания, подсознания и коммуникации; исследован подход на основе сложных сетей для реализации ГИИС; показано, что метаграфовая модель позволяет описывать данные, знания и процессы, как составные части ГИИС; исследована структура метаграфового агента, обеспечивающего обработку метаграфовой модели; показано, что метаграфовый агент можно представить в виде метаграфовой модели, что позволяет агентам верхнего уровня модифицировать структуру агентов нижнего уровня; введено понятие активного узла метаграфа как комбинации метаграфовой модели данных и знаний, и метаграфовых агентов; на основе активного узла метаграфа введено понятие метаграфового процесса; обоснована архитектура ГИИС анализа судебной практики арбитражных судов.*

DOI: 10.21681/1994-1404-2020-1-15-25

Введение

Защита законных прав и интересов предпринимателей не обходится без взаимодействия с судебной системой. В арбитражные суды обращаются как индивидуальные предприниматели, так и юридические лица. Судебный процесс состоит из этапов, каждый из которых сопровождается документальным оформлением. В завершение процесса суды принимают судебный акт, который может называться поразному, в зависимости от инстанции и сути принятого решения. В соответствии с ч. 1 ст. 15 АПК РФ к судебным актам относят: судебный приказ, решение, постановление, определение.

Хотя судебная система России не является прецедентной, судебные решения играют ключевую роль при подготовке к судебному процессу. Из-за законодательных коллизий или отсутствия регулирующих норм большинство судебных решений основывается на правовых позициях Пленумов Верховного Суда РФ (и/или Высшего Арбитражного Суда РФ до упразднения в 2014 г.).

Представители как истцов, так и ответчиков в обязательном порядке начинают подготовку к делу с изучения судебной практики, поиска похожих дел, определения схожих обстоятельств и обоснований своих позиций. Мотивированный судебный акт может занимать от 4 до 15 страниц. При этом таких решений нужно изучить достаточно много, чтобы составить более полное представление о возможном исходе судебного процесса.

* ***Таран Мария Олеговна,*** *аспирант Московского государственного технического университета им. Н. Э. Баумана, Российская Федерация, г. Москва.*

E-mail: gapyu@bmstu.ru

Гапанюк Юрий Евгеньевич, *кандидат технических наук, доцент Московского государственного технического университета им. Н. Э. Баумана, Российская Федерация, г. Москва.*

E-mail: gapyu@bmstu.ru

По информации сайта «Электронное правосудие», за девять месяцев 2019 г. в арбитражных судах России было выпущено более 1 300 000 документов[1]. Обработать, обобщить и сделать какие-либо выводы из такого массива документов в ручном режиме достаточно сложно.

В соответствии с ч. 4 ст. 19 Федерального конституционного закона от 31 декабря 1996 г. № 1-ФКЗ «О судебной системе Российской Федерации», Верховный суд РФ в целях обеспечения единообразного применения законодательства РФ дает судам разъяснения по вопросам судебной практики. Это выражается в подготовке *обзоров судебной практики* по разным отраслям, а иногда и конкретным статьям. Такие обзоры представляют собой краткое изложение дел и позиции суда по нему. Иногда в рамках одного вопроса рассматриваются сразу несколько однотипных споров, по которым делается обобщенный вывод.

Для совершенствования законодательства также необходимо изучать судебную практику. При этом можно заметить единообразные решения, которые вынуждены принимать суды из-за несовершенства законодательного акта. Примером такой ситуации может служить отсутствие четкого закрепления сроков подачи искового заявления после отмены судебного приказа в делах о взыскании финансовых санкций с организации. Данный пример включен в обзор № 2 (2019)[2] судебной практики Верховного Суда Российской Федерации. В этих ситуациях судам приходится принимать решения по аналогии, каждый раз указывая одни и те же причины, а также ссылаясь на позицию Верховного Суда РФ.

Подобные дела оборачиваются высокой экономической неэффективностью. Государство оплачивает расходы судов и других органов, сотрудники тратят большое количество времени на судебные процессы, которых могло и не быть, хотя достаточно было бы внести соответствующие технико-правовые нормы в законодательство, чтобы прервать череду подобных процессов, снизить нагрузку на суды по аналогичным делам [3].

Для продуктивного использования судебной практики представляется целесообразным ускорить процесс её изучения и обобщения [4]. Это возможно, в частности, на основе применения разработанной *автоматизированной системы*, архитектура которой рассматривается в данной статье. В результате использования системы вместо текста в несколько страниц юристы могут получить краткое содержание текста с наиболее значимой информацией, которую можно использовать для принятия решения о необходимости подробного изучения документа или в каких-то других целях. Юристам будет также предоставлен граф связей между извлеченными концептами, ассоциативные связи между ними и статистическая информация.

[1] Сайт «Электронное правосудие». URL: http://ras.arbitr.ru

[2] Обзор судебной практики Верховного Суда Российской Федерации. URL: http://www.supcourt.ru/documents/ practice/?year=2019 .

Гибридные интеллектуальные информационные системы

В настоящее время для построения интеллектуальных систем используется большое количество подходов: продукционные правила, нейронные сети, нечеткая логика, эволюционные методы и др. При этом можно отметить явную тенденцию к совместному использованию разных методов для решения различных классов задач. Это привело к появлению такого направления, как «гибридные интеллектуальные системы» (ГИС) [1, 2].

Ключевым вопросом является вопрос о том, каким образом реализовать принцип гибридности. Ответ на этот вопрос предлагается, в частности, в работе [6]. В ней сформулирован следующий принцип гибридности [6, с. 20—21]: «В литературе встречаются схемы гибридизации нейроинформатики и искусственного интеллекта, построенные по следующему принципу: правое полушарие — нейрокомпьютер; левое полушарие — основанная на знаниях система, а вопрос лишь в их взаимодействии или балансе право- и лево-полушарности. В реальном поведении человека невозможно разделить восприятие и логическую обработку, поэтому более успешной представляется схема глубинной интеграции».

В настоящее время интеллектуальные системы, как правило, не разрабатываются отдельно, но встраиваются в виде модулей в традиционные информационные системы для решения задач, связанных с интеллектуальной обработкой данных и знаний. Такую комбинированную систему в соответствии с [12] назовем гибридной интеллектуальной информационной системой (ГИИС), которая обладает следующими особенностями:

- сочетает различные методы, используемые для построения интеллектуальных систем, и в этом смысле является ГИС;
- сочетает интеллектуальные методы с традиционными методами, используемыми для разработки данных в информационных системах, и в этом смысле является комбинацией ГИС и информационной системы, предназначенной для обработки данных.

Таким образом, под ГИИС будем понимать информационную систему, которая использует комбинацию традиционных методов обработки данных и интеллектуальных методов, что полностью соответствует концепции [6]. Однако, по мнению авторов статьи, вместо право- и лево-полушарности скорее сто́ит говорить о «подсознании» и «сознании» ГИИС. «Подсознание» строится на основе методов мягких вычислений, а «сознание» — на основе традиционных методов обработки данных и знаний. На рис. 1 представлена обобщенная архитектура ГИИС, построенная на основе «сознания» и «подсознания».

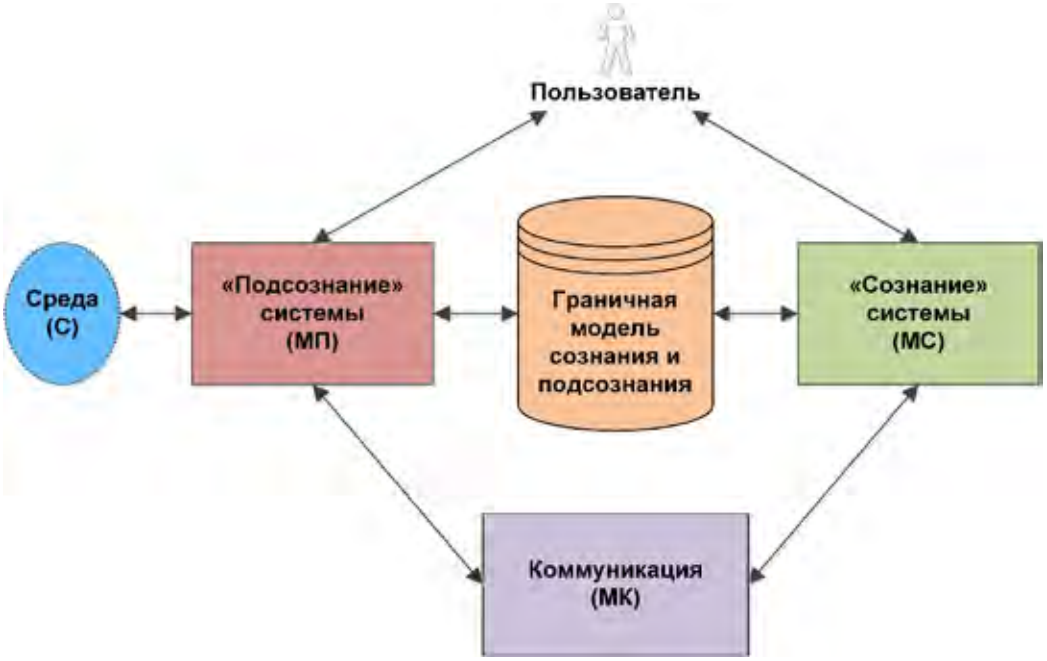

Рис. 1. Обобщенная архитектура ГИИС

Основой системы являются «подсознание» (модуль подсознания — МП) и «сознание» системы (модуль сознания — МС). «Подсознание» связано со средой, в которой функционирует ГИИС.

Основной задачей МП является обеспечение взаимодействия ГИИС со «средой», или «выживание» ГИИС в среде.

Поскольку среда может быть представлена в виде набора непрерывных сигналов, то в качестве методов обработки данных «подсознания» хорошо подходят методы, основанные на нейронных сетях и нечеткой логике, в том числе и комбинированные нейронечеткие методы.

Модель данных «подсознания» максимально приближена к «понятийной системе» среды, представляет собой набор данных, который позволяет максимально эффективно взаимодействовать со средой. Часть этих данных может не иметь «физического смысла» с точки зрения МС, однако позволяет МП взаимодействовать со средой с нужной производительностью.

«Сознание» ГИИС строится на принципах обработки данных и знаний. Обработка данных в МС может вестись на основе традиционных языков программирования или известной технологии «потока работ» (англ. *"workflow"*). Однако в последнее время все большую популярность приобретает подход на основе продукционных правил. Раньше данный подход использовался для принятия решения в *экспертных системах* [5], но в настоящее время на основе правил пишутся обычные программы. Такой подход называется программированием на основе правил (англ. *"rule-based programming"*). К достоинствам подхода на основе правил можно отнести гибкость, так как в этом случае программа не кодируется жестко, а фактически «выводится» из правил на основе данных. К недостаткам можно отнести возможность зацикливания правил, а также сложность обработки большого объема правил.

Заметим, что задача хранения требуемых данных решается отдельно на уровне МС и на уровне МП. Мы предполагаем, что на уровне обобщенной архитектуры соответствующие хранилища «встроены» в МС и МП, поэтому на рис. 1 хранилища явно не представлены.

Модуль сознания воспринимает понятийную систему как целостную модель «онтологического» класса и может «осознанно» обрабатывать элементы данной модели на основе правил.

Модуль подсознания воспринимает понятийную систему в виде отдельных (возможно, несвязанных) признаков. Требование «осознания» целостности модели не предъявляется. Основным критерием является эффективность взаимодействия системы со средой.

С точки зрения коммуникации в ГИИС возможны следующие варианты или их комбинации:

Коммуникация осуществляется через среду. МП читает данные из среды, преобразует и передает в МС. МС осуществляет логическую обработку и возвращает результаты обработки в МП. МП записывает результирующие данные в среду, откуда они могут быть прочитаны другими ГИИС.

Для коммуникации с другими ГИИС используется модуль коммуникации (МК). В зависимости от решаемых задач с МК может взаимодействовать МС (что характерно для традиционных информационных систем) или МП (что более характерно для систем на основе мягких вычислений).

Взаимодействие с пользователем также может осуществляться через МС (что характерно для традиционных информационных систем) или через МП (что может быть использовано, например, в автоматизированных тренажерах).

Граничная модель сознания и подсознания предназначена для глубинной интеграции модулей сознания и подсознания и представляет собой интерфейс между этими модулями с функцией хранения данных. В качестве данных выступает комплексная онтология, которая используется как сознанием, так и подсознанием. Основной задачей подсознания является распознавание из среды элементов онтологии. Если рассматривать сознание как разновидность экспертной системы, то распознанные элементы онтологии могут рассматриваться в качестве элементов операционной памяти экспертной системы, которые приводят к срабатыванию соответствующих правил. В зависимости от целей системы, правила могут формировать выходную информацию для пользователя или сигналы для модуля подсознания, которые оказывает требуемое воздействие на среду.

Предложенная архитектура рассматривается как основа обобщенного подхода, который должен быть адаптирован для создания информационных систем в конкретных предметных областях.

Использование подхода на основе сложных сетей для реализации ГИИС

В современных информационных системах традиционно используются разнородные информационные модели данных, знаний и процессов. Эта ситуация сложилась исторически, потому что раньше мощность вычислительных систем была невысока и во главу угла ставилась производительность обработки информационной модели. Вопросы интеграции информационных систем и унификации информационных моделей оставались на втором плане.

В настоящее время ситуация изменилась. Появление и активное развитие технологий обработки *больших данных* [10], расширение круга информационно-аналитических задач привело к тому, что в качестве обрабатываемых данных вполне могут выступать знания, ситуации, процессы. Это требует новых подходов к интеграции систем, к информационным моделям.

Сервис-ориентированный подход (в том числе в его современном микросервисном варианте) до определенной степени решает задачу интеграции информационных систем, но при этом каждая система функционирует как «черный ящик». Интеграция возможна только на уровне элементов, которые вынесены в интерфейс сервиса. Например, если в целях решения информационно-аналитических задач мы хотим использовать *OLAP*-куб для хранения и агрегации не чисел, а ситуаций или процессов, то использование сервис-ориентированного подхода не поможет; потребуется интеграция на уровне единой информационной модели.

В качестве интеграционной модели для реализации ГИИС мы предлагаем использовать *метаграфовую* модель [13].

На кафедре «Системы обработки информации и управления» МГТУ им. Н.Э. Баумана в рамках в рамках развития данного направления метаграфовую модель предлагается применять как средство для описания: сложных сетей [11], семантики и прагматики информационных систем [7], гибридных интеллектуальных информационных систем [12].

Для обработки метаграфовой модели предлагается использовать подход на основе многоагентной системы (МАС). В соответствии с [9], под программным агентом будем понимать программный модуль, который выполняется в виде автономной задачи (не зависит от других агентов), способен обмениваться информацией со средой и другими агентами. Под МАС будем понимать систему однородных или разнородных агентов, функционирующих в среде.

Для реализации ГИИС наиболее интересным представляется подход на основе холонической многоагентной системы (холонической МАС). В соответствии с [9, с. 234], холон — это «целое, рассматриваемое в то же время как часть целого». С точки зрения данного подхода, рассмотренные компоненты, такие как МП, МС, МК, являются агентами. В то же время они являются частями системы, которая, в свою очередь, является агентом.

При этом МП является сложной структурой, которая включает агенты нижнего уровня, каждый из которых может, в свою очередь, включать МП, МС, МК, предназначенные для решения конкретных задач данного агента. Несмотря на то, что агент нижнего уровня находится в составе МП, он может включать в свою структуру МС, предназначенный для решения задач МП более высокого уровня. Поэтому с точки зрения данного подхода нет ничего удивительного в том, что в МС могут использоваться нечеткие продукционные правила, а в МП входят «классические» модули обработки данных.

Метаграфовая модель описания данных, знаний и процессов в ГИИС

Под метаграфом будем понимать следующую структуру:

$$MG = \langle V, MV, E, ME \rangle,$$

где MG — метаграф; V — множество вершин метаграфа; MV — множество метавершин метаграфа; E — множество ребер метаграфа; ME — множество метаребер метаграфа.

Вершина метаграфа характеризуется множеством атрибутов:

$$v_i = \{atr_k\}, v_i \in V,$$

где v_i — вершина метаграфа; atr_k — атрибут.

Ребро метаграфа характеризуется множеством атрибутов, исходной и конечной вершиной и признаком направленности:

$$e_i = \langle v_S, v_E, eo, \{atr_k\} \rangle, e_i \in E, eo = true \mid false,$$

где e_i — ребро метаграфа; v_S — исходная вершина (метавершина) ребра; v_E — конечная вершина (метавершина) ребра; eo — признак направленности ребра ($eo=true$ — направленное ребро, $eo=false$ — ненаправленное ребро); atr_k — атрибут.

Фрагмент метаграфа:

$$MG_i = \{ev_j\}, ev_j \in (V \cup E \cup MV \cup ME),$$

где MG_i — фрагмент метаграфа; ev_j — элемент, принадлежащий объединению множеств вершин (метавершин) и ребер (метаребер) метаграфа.

Отсюда, фрагмент метаграфа в общем виде может содержать произвольные вершины (метавершины) и ребра (метаребра) без ограничений. Ограничения вводятся на фрагменты метаграфа, входящие в метавершину и метаребро.

Метавершина метаграфа является основным элементом предлагаемой модели:

$$mv_i = \langle \{atr_k\}, \{ev_j\} \rangle, mv_i \in MV, ev_j \in \in (V \cup E^{eo=false} \cup MV \cup ME^{eo=false}),$$

где mv_i — вершина метаграфа; atr_k — атрибут, ev_j — элемент, принадлежащий объединению множеств вершин (метавершин) и ребер (метаребер) метаграфа.

Следовательно, метавершина в дополнение к свойствам вершины включает вложенный фрагмент метаграфа. При этом ребра и метаребра этого фрагмента могут быть только ненаправленными, $eo=false$.

Метаребро метаграфа:

$$me_i = \langle v_S, v_E, eo, \{atr_k\}, \{ev_j\} \rangle, e_i \in E, eo = = true \mid false,$$

где me_i — метаребро метаграфа; v_S — исходная вершина (метавершина) ребра; v_E — конечная вершина (метавершина) ребра; eo — признак направленности метаребра ($eo=true$ — направленное метаребро, $eo=false$ — ненаправленное метаребро); atr_k — атрибут; ev_j — элемент, принадлежащий объединению множеств вершин (метавершин) и ребер (метаребер) метаграфа.

Отсюда, метаребро в дополнение к свойствам ребра включает вложенный фрагмент метаграфа. При этом ребра и метаребра этого фрагмента могут быть только направленными, $eo=true$.

Определения метавершины и метаребра являются рекурсивными, так как элементы ev_j могут быть, в свою очередь, метавершинами и метаребрами. Метавершина является формализмом описания данных, а метаребро — формализмом описания процессов.

Наличие у метавершин собственных атрибутов и связей с другими вершинами является важной особенностью метаграфов. Это соответствует принципу эмерджентности, т. е. приданию понятию нового качества, несводимости понятия к сумме его составных частей. Фактически, как только вводится новое понятие в виде метавершины, оно «получает право» на собственные свойства, связи и др., так как в соответствии с принципом эмерджентности новое понятие обладает новым качеством и не может быть сведено к подграфу базовых понятий.

Таким образом, метаграф можно охарактеризовать как «сеть с эмерджентностью», т. е. фрагмент сети, состоящий из вершин и связей, который может выступать как отдельное целое.

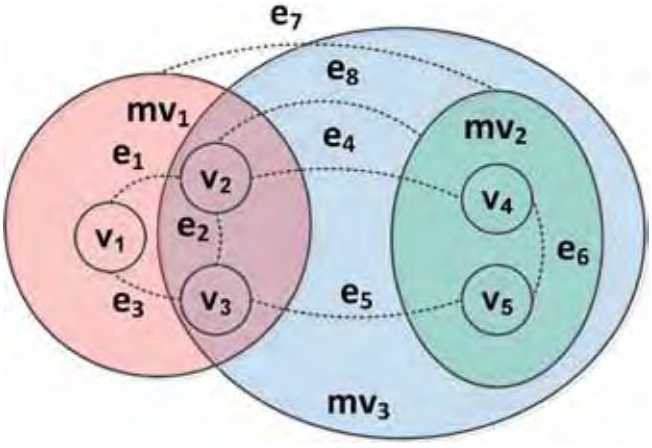

Рис. 2. Пример описания метавершины метаграфа

Пример описания метавершины метаграфа показан на рис. 2. Данный метаграф содержит вершины, метавершины и ребра. На рис. 2 показаны три метавершины: mv_1, mv_2 и mv_3. Метавершина mv_1 включает вершины v_1, v_2, v_3 и связывающие их ребра e_1, e_2, e_3. Метавершина mv_2 включает вершины v_4, v_5 и связывающее их ребро e_6. Ребра e_4, e_5 являются примерами ребер, соединяющих вершины v_2-v_4 и v_3-v_5, включенные в различные метавершины mv_1 и mv_2. Ребро e_7 является примером ребра, соединяющего метавершины mv_1 и mv_2. Ребро e_8 является примером ребра, соединяющего вершину v_2 и метавершину mv_2. Метавершина mv_3 включает метавершину mv_2, вершины v_2, v_3 и ребро e_2 из метавершины mv_1, а также ребра e_4, e_5, e_8, что показывает холоническую структуру метаграфа.

Если метавершины предназначены прежде всего для описания данных и знаний, то метаребра предназначены в большей степени для описания процессов.

Пример описания метаребра метаграфа представлен на рис. 3. Метаребро содержит метавершины v_S,

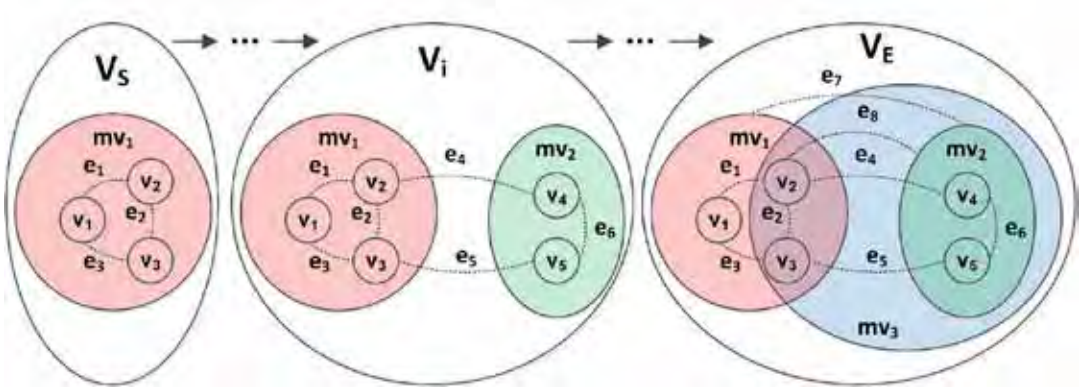

Рис. 3. Пример описания метаребра метаграфа

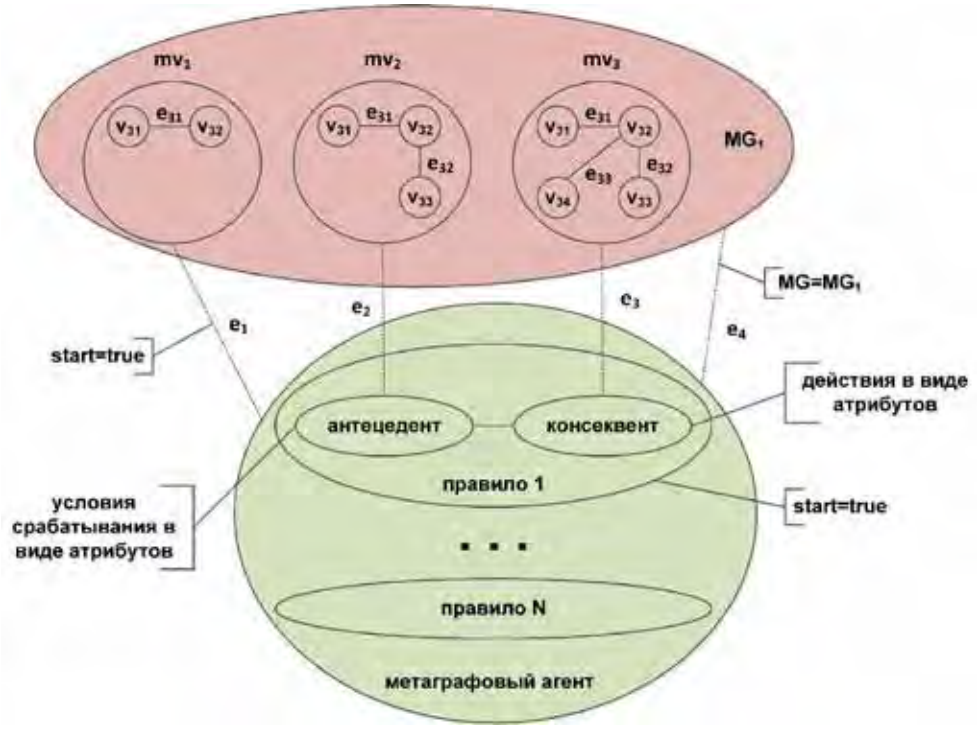

Рис. 4. Представление метаграфового агента в виде фрагмента метаграфа

… v_i, … v_E и связывающие их ребра. Исходная метавершина содержит фрагмент метаграфа. В процессе преобразования исходной метавершины v_S в конечную метавершину v_E происходит дополнение содержимого метавершины, добавляются новые вершины, связи, вложенные метавершины.

В целом, метаграфовая модель позволяет в рамках единой модели описывать данные, знания и процессы.

Обработка метаграфовой модели с использованием метаграфовых агентов

Для обработки метаграфовой модели используются два вида агентов: агент-функция и метаграфовый агент.

Определим агент-функцию следующим образом:

$$ag^F = \langle MG_{IN}, MG_{OUT}, AST \rangle,$$

где ag^F — агент-функция; MG_{IN} — метаграф, который выполняет роль входного параметра агента-функции; MG_{OUT} — метаграф, который выполняет роль выходного параметра агента-функции; AST — абстрактное синтаксическое дерево агента-функции, которое можно представить в виде метаграфа.

Определим метаграфовый агент следующим образом:

$$ag^M = \langle MG_D, R, AG^{ST} \rangle, R = \{r_j\},$$

где ag^M — метаграфовый агент; MG_D — метаграф данных и знаний, на основе которого выполняются правила агента; R — набор правил (множество правил r_j); AG^{ST} — стартовое условие выполнения агента (фрагмент метаграфа, который используется для стартовой проверки правил, или стартовое правило).

Структура правила метаграфового агента:

$$r_i : MG_j \rightarrow OP^{MG},$$

где r_i — правило; MG_j — фрагмент метаграфа, на основе которого выполняется правило; OP^{MG} — множество операций, выполняемых над метаграфом.

Антецедентом правила является фрагмент метаграфа, консеквентом правила является множество операций, выполняемых над метаграфом.

Пример представления метаграфового агента в виде фрагмента метаграфа приведен на рис. 4.

Метаграфовый агент представлен в виде метавершины метаграфа. В соответствии с определением, он связан с метаграфом MG_1, на основе которого выполняются правила агента. Данная связь показана с помощью ребра e_4.

Метаграфовый агент содержит множество вложенных метавершин, соответствующих правилам (*правило* 1 — *правило N*). Каждая метавершина правила содержит вершины антецедента и консеквента. В данном примере с антецедентом правила связана метавершина данных mv_2, что показано ребром e_2, а с консеквентом правила связана метавершина данных mv_3, что показано ребром e_3. Условия срабатывания антецедента и множество действий консеквента задаются в виде атрибутов соответствующих вершин.

Стартовое условие выполнения агента задается с помощью атрибута «start=true». Если стартовое условие задается в виде стартового правила, то данным атрибутом помечается метавершина соответствующего правила, в данном примере это *правило* 1. Если стартовое условие задается в виде стартового фрагмента метаграфа, который используется для стартовой проверки правил, то атрибутом «start=true» помечается ребро, которое связывает стартовый фрагмент

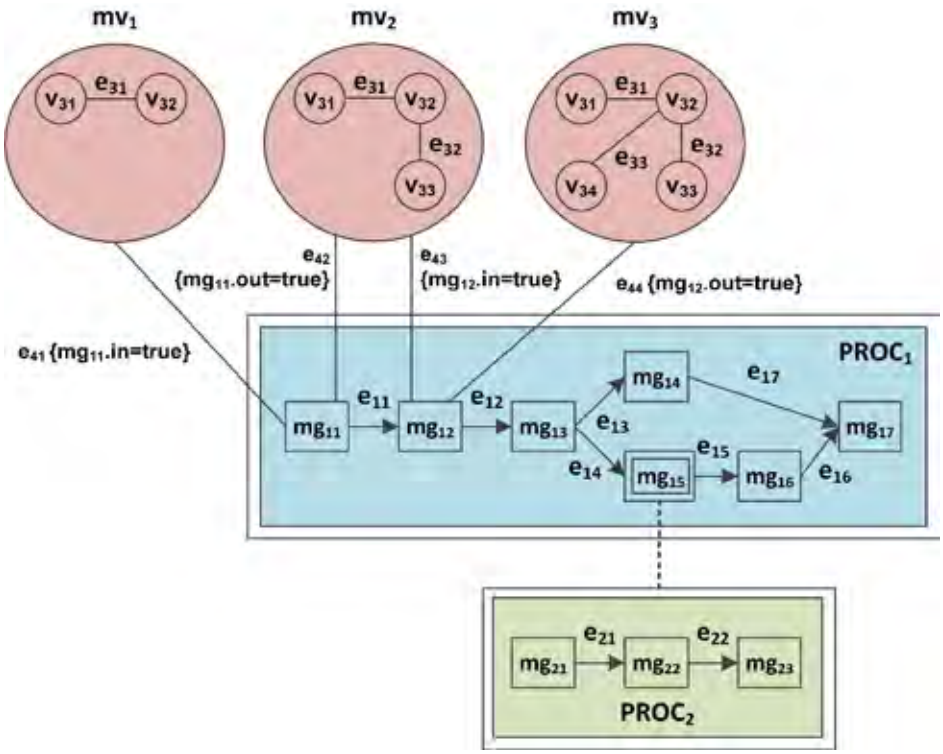

Рис. 5. Пример метаграфового процесса

метаграфа с метавершиной агента, в данном примере это ребро e_1.

Под «активным узлом метаграфа» mv_{node}^{ACTIVE} будем понимать вершину или метавершину метаграфа, с которой связаны программные агенты, выполняющие определенные функции. Под «метаграфовым процессом» (рис. 5) будем понимать метаребро, базирующееся на активных узлах:

$$PROC_i = \left\langle v_S, v_E, \{atr_k\}, MG_j \left[mv_{node} \equiv mv_{node}^{ACTIVE} \right] \right\rangle,$$
$$mv_{node} \in (V \cup MV),$$

где $PROC_i$ — метаграфовый процесс; v_S — исходная вершина (метавершина) процесса; v_E — конечная вершина (метавершина) процесса; atr_k — атрибут; MG_j — фрагмент метаграфа, такой, что каждая его вершина или метавершина mv_{node} является активным узлом метаграфа.

На рис. 5 окружностями показаны вершины и метавершины, используемые для описания данных. Прямоугольниками показаны метавершины или метаребра, соответствующие элементам процесса. Метаграфовые процессы $PROC_1$ и $PROC_2$ показаны двойными прямоугольниками. Ненаправленными связями показаны ненаправленные ребра (eo=false), а направленными стрелками показаны направленные ребра (eo=true). Пунктирной связью показана вложенность фрагмента метаграфа.

Процесс состоит из элементов процесса v_{1*} (под «*» понимается произвольное значение второго индекса). Элементы процесса соединены направленными ребрами e_{1*}. В качестве примера для элемента процесса v_{15} показаны элементы вложенного подпроцесса. Таким образом, элемент v_{15} одновременно является и элементом процесса me_1, и метаребром, которое содержит вложенный процесс.

Данные, поступающие на вход элемента v_{11}, показаны в виде метавершины mv_1, которая содержит вложенные вершины данных v_{31} и v_{32} и ненаправленную связь между ними e_{31}. Связь метавершины mv_1 с элементом процесса v_{11} осуществляется с помощью ребра e_{41}. Признак того, что метавершина mv_1 содержит входные данные процесса v_{11}, моделируется с помощью атрибута ребра e_{41} (вершины и ребра могут иметь атрибуты, так как используется модель атрибутивного метаграфа). В данном случае используется атрибут v_{11}. $in{=}true$. Аналогично с использованием ребер e_{42}, e_{43}, e_{44} производится привязка метавершин mv_2 и mv_3 к элементам процесса v_{11} и v_{12} в качестве входных-выходных данных.

На рис. 5 показан случай, когда выходные данные предыдущего процесса являются входными данными следующего процесса. Однако предлагаемая модель связи метавершин данных с элементами процесса носит более гибкий характер и позволяет моделировать передачу данных как через входные-выходные метавершины данных, так и другими способами, например, через представленный метавершиной общий контекст.

Архитектура системы анализа арбитражной практики

Рассмотрим предлагаемую архитектуру информационной системы анализа судебной практики арбитражных судов, построенную на основе подхода ГИИС (рис. 6).

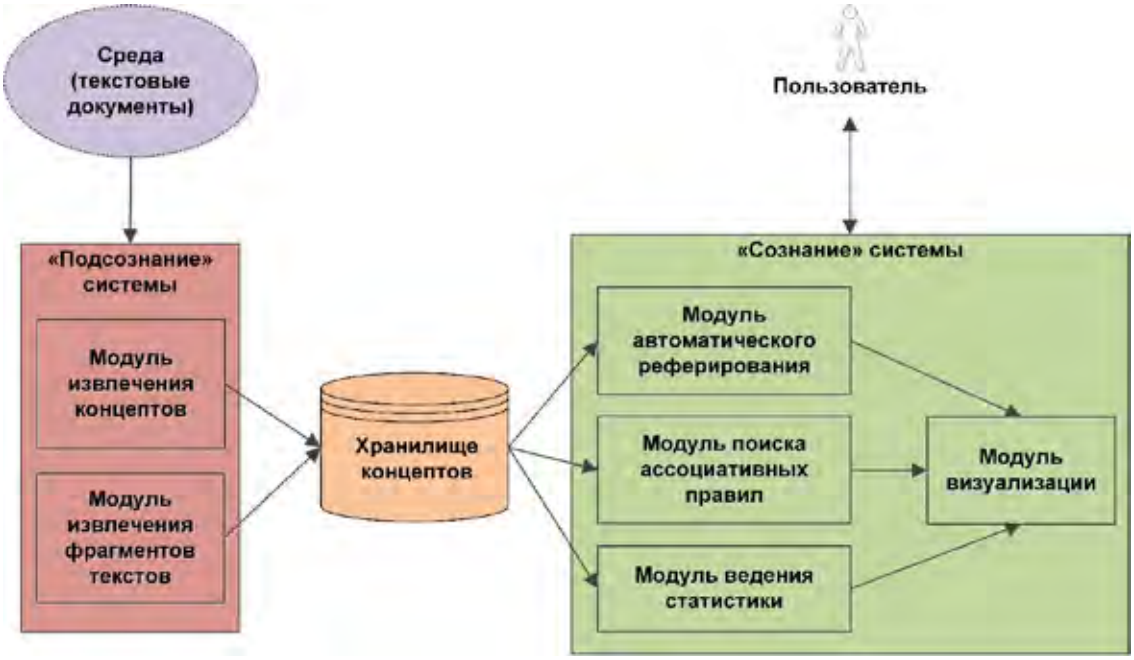

Рис. 6. Архитектура системы анализа арбитражной практики

Классическая архитектура практически любой аналитической информационной системы включает подсистему сбора данных и подсистему обработки данных. В классической архитектуре при проектировании подсистемы сбора рассматриваются в основном аспекты сбора данных из различных источников, меньшее значение уделяется унификации семантики данных. Подсистема обработки формирует аналитику на основе собранных данных.

Напротив, в архитектуре ГИИС основной упор делается на семантику данных. В концепции ГИИС подсистеме сбора можно сопоставить подсознание, а подсистеме обработки сопоставить сознание, но такое сопоставление достаточно условно. Основная задача подсознания — формирование концептов, используемых для принятия решения. Основная задача сознания — принятие решения на основе выделенных концептов.

Средой в данной системе являются исходные текстовые документы юридической направленности.

Подсознание системы включает модуль извлечения концептов и модуль извлечения фрагментов текстов, при этом фрагменты текстов могут рассматриваться как укрупненные концепты, используемые при формировании аналитики.

Извлеченные концепты и фрагменты текстов помещаются в хранилище концептов, которое соответствует граничной модели сознания и подсознания.

Сознание системы включает модули автоматического реферирования, визуализации, ведения статистики, поиска ассоциативных правил.

Модули «подсознания» системы

В модуле извлечения концептов из текста извлекаются основные данные: имя или название истца и ответчика; имя или название заявителя (в жалобах); суть дела; цена иска; решение суда и др.

Модуль строится на гибридном подходе, сочетая в себе как подход на основе правил, так и использование машинного обучения. Отметим, что такой подход хорошо зарекомендовал себя в обработке текстов [16]. Для тривиальных случаев используются правила. Например, тип документа, цена иска, решение суда и др. Остальной текст анализируются нейросетевыми моделями на основе фреймворка *TensorFlow* [14].

В зависимости от извлекаемых данных, требуется решить различные задачи машинного обучения, а именно: извлечение именованных сущностей; извлечение фактов; извлечение временных данных.

Для каждой задачи создается свой подмодуль с нейросетью и/или правилами. Для обучения моделей можно использовать датасеты не только на основе судебной практики, так как извлечение именованных сущностей и временных данных носят универсальный характер. Однако, специальный размеченный датасет со специализированными текстами может дать более высокое качество.

Модуль извлечения фрагментов текстов отвечает за отбор текстовых блоков, которые могут быть использованы в реферате. Для решения этой задачи используются методы машинного обучения [15].

С точки зрения машинного обучения предсказание подходящего текстового блока можно отнести к задаче обучения с учителем (по прецедентам), а именно многоклассовой классификации. У каждого объекта есть определенный набор признаков. В нашем случае это абзац и некоторые дополнительные данные, которые извлекаются на предыдущем шаге. Ответом является метка класса, к которому отнесен блок.

После классификации остаются только блоки, отнесенные к полезным. В хранилище концептов передается уже частично сжатый текст.

Модули «сознания» системы

Модуль автоматического реферирования является основным инструментом, который значительно ускоряет для юриста обработку документов. В [8] отмечается, что методы автоматического реферирования можно разделить на две большие группы:

- *экстракция* (извлечение предложений, *Sentence Extraction*, квазиреферирование) — извлечение из исходного текста наиболее важных и существенных информационных блоков (абзацев, предложений);
- *абстракция* (извлечение содержания, *Content Extraction*) — генерация реферата с порождением нового текста, содержательно обобщающего первичный документ или документы.

Для методов, основанных на абстракции, в большей степени подходят концепты, извлеченные с помощью модуля извлечения концептов. Для методов, основанных на экстракции, могут быть использованы фрагменты текстов, полученные на выходе модуля извлечения фрагментов текстов. Следует заметить, что методы, основанные на абстракции, вызывают все больший интерес, а для решения задачи реферирования используются методы на основе графов.

Сформированный граф документа может быть представлен юристу с использованием модуля визуализации.

Сокращение объема текста — далеко не единственная задача, которую должна решать информационная система; не менее важной задачей является выявление причин принятия судебных решений. Здесь на помощь приходит модуль поиска ассоциативных правил, который позволяет понять, какие факторы привели к принятию конкретного судебного решения. Необходимо отметить, что практически все существующие алгоритмы поиска ассоциативных правил предполагают работу с концептами, поэтому очень важно то, что подсознание ГИИС выделяет не просто текст, а концепты, которые поступают на вход данного модуля.

Ассоциативные правила также могут быть представлены в виде графов с использованием модуля визуализации.

Модуль ведения статистики позволяет хранить и обрабатывать количественную информацию: сколько дел было обработано в том или ином суде за определенный временной период и др. Для реализации этого модуля может быть использована *OLAP*-система, в этом случае она может иметь собственной хранилище. Хранилище концептов может быть использовано для формирования и иерархической организации измерений *OLAP*-системы.

Статистические данные в графическом представлении также отображаются с использованием модуля визуализации.

Выводы

Обоснованная архитектура информационной системы анализа судебной практики арбитражных судов базируется на концепции ГИИС. Средой в данной системе являются исходные текстовые документы юридической направленности.

Обобщенную структуру ГИИС предлагается строить на основе модулей «сознания» и «подсознания». На основе обобщенной структуры могут быть построены частные случаи структуры ГИИС, которым соответствуют конкретные ГИИС. Подсознание системы включает модуль извлечения концептов и модуль извлечения фрагментов текстов, при этом фрагменты текстов могут рассматриваться как укрупненные концепты, используемые при формировании аналитики. Извлеченные концепты и фрагменты текстов помещаются в хранилище концептов, которое соответствует граничной модели сознания и подсознания. Сознание системы включает модули автоматического реферирования, визуализации, ведения статистики, поиска ассоциативных правил.

Для реализации ГИИС предполагается использовать холоническую многоагентную систему. Структура такой МАС может быть описана с использованием метаграфового подхода. Метаграфовый подход является одним из вариантов описания «сетей с эмерджентностью». Эмерджентность обеспечивается за счет использования метавершин. С использованием метаграфовой модели возможно унифицированное представление архитектуры разрабатываемой системы. Для обработки метаграфовой модели используются два вида агентов: агент-функция и метаграфовый агент. С активным узлом метаграфа связаны программные агенты, выполняющие определенные функции обработки метаграфовой модели. Под «метаграфовым процессом» понимается метаребро, базирующееся на активных узлах.

Рецензент: ***Сухов Андрей Владимирович,*** *доктор технических наук, профессор, профессор кафедры радиоэлектроники, телекоммуникаций и нанотехнологий Московского авиационного института (национального исследовательского университета), Российская Федерация, г. Москва.*
E-mail: avs57@mail.ru

Литература

1. Колесников А. В. Гибридные интеллектуальные системы. Теория и технология разработки. СПб. : СПбГТУ, 2001. 137 с.

2. Колесников А. В., Кириков И. А., Листопад С. В. Гибридные интеллектуальные системы с самоорганизацией: координация, согласованность, спор. М. : ИПИ РАН, 2014. 189 с.
3. Ловцов Д. А., Ниесов В. А. Модернизация информационной инфраструктуры судопроизводства — ключевое направление оптимизации нагрузки на судебную систему // Российское правосудие. 2014. № 9. С. 30—40.
4. Ловцов Д. А., Ниесов В. А. Актуальные проблемы создания и развития единого информационного пространства судебной системы России // Информационное право. 2013. № 5. С. 13—18.
5. Ловцов Д. А., Сергеев Н. А. Информационно-математическое обеспечение управления безопасностью эргатических систем. III. Экспертная информационная система // НТИ. Сер. 2. Информ. процессы и системы. 2001. № 11. С. 23—30.
6. Прикладные интеллектуальные системы, основанные на мягких вычислениях / Под ред. Н. Г. Ярушкиной. Ульяновск : УлГТУ, 2004. 139 с.
7. Самохвалов Э. Н., Ревунков Г. И., Гапанюк Ю. Е. Использование метаграфов для описания семантики и прагматики информационных систем // Вестник МГТУ им. Н.Э. Баумана. Сер. «Приборостроение». 2015. Вып. № 1. С. 83—99.
8. Тарасов С. Д. Современные методы автоматического реферирования // Научно-технические ведомости СПбГПУ. 2010. Вып. № 6. С. 59—74.
9. Тарасов В. Б. От многоагентных систем к интеллектуальным организациям: философия, психология, информатика. М. : Эдиториал УРСС, 2002. 352 с.
10. Федосеев С. В. Применение современных технологий больших данных в правовой сфере // Правовая информатика. 2018. № 4. С. 50—58.
11. Черненький В. М., Терехов В. И., Гапанюк Ю. Е. Представление сложных сетей на основе метаграфов // Труды XVIII Всеросс. науч.-техн. конф. «Нейроинформатика-2016». Ч. 1 / НИЯУ МИФИ. М. : МИФИ, 2016. С. 173—178.
12. Черненький В. М., Терехов В. И., Гапанюк Ю. Е. Структура гибридной интеллектуальной информационной системы на основе метаграфов // Нейрокомпьютеры: разработка, применение. 2016. Вып. № 9. С. 3—14.
13. Basu A., Blanning R. Metagraphs and their applications. Springer, 2007. 174 pp.
14. Geron A. Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow. Concepts, Tools, and Techniques to Build Intelligent Systems. O'Reilly, 2019. 856 pp.
15. Kulkarni A., Shivananda A. Natural Language Processing Recipes. Unlocking Text Data with Machine Learning and Deep Learning using Python. Apress, 2019. 234 pp.
16. Taran M., Revunkov G., Gapanyuk Yu. The Hybrid Intelligent Information System for Poems Generation. Neuroinformatics 2019: Advances in Neural Computation, Machine Learning, and Cognitive Research III. Pp. 78-86.

THE ARCHITECTURE FOR A HYBRID INTELLIGENT INFORMATION SYSTEM FOR ANALYSING COMMERCIAL COURTS PRACTICE

Mariia Taran, *Ph.D. student at the Bauman Moscow State Technical University, Russian Federation, Moscow.*
E-mail: gapyu@bmstu.ru

Iurii Gapaniuk, *Ph.D. (Technology), Associate Professor at the Bauman Moscow State Technical University, Russian Federation, Moscow.*
E-mail: gapyu@bmstu.ru

Keywords: *commercial court, hybrid intelligent system, hybrid intelligent information system, information system conscious, information system subconscious, text mining, multiagent system, graph, metagraph, metavertex, metaedge, metagraph process, metagraph agent, active metagraph node.*

Abstract.

Purpose of the work: *improving the scientific and methodological basis of information support for the commercial courts practice system.*

Methods used: *methods of hybrid intelligent information systems design based on complex networks models.*

Results obtained: *an approach to the development of Hybrid Intelligent Information Systems (HIIS) based on the use of modules of conscious, subconscious and communication is considered. An approach for HIIS implementation based on complex networks is studied. It is shown that a metagraph model allows describing data, knowledge, and processes as HIIS*

components. The structure of a metagraph agent providing for the processing of the metagraph model is studied, and it is shown that a metagraph agent can be represented by a metagraph model, which allows top-level metagraph agents to modify the structure of lower-level metagraph agents. The concept of an active metagraph node is introduced as a combination of a metagraph data & knowledge model and metagraph agents. The concept of a metagraph process based on the active metagraph node concept is introduced, and a justification is given for an architecture of a HIIS for analysing commercial courts practice.

References

1. Kolesnikov A. V. Gibridnye intellektual'nye sistemy. Teoriia i tekhnologiia razrabotki. SPb. : SPbGTU, 2001, 137 pp.
2. Kolesnikov A. V., Kirikov I. A., Listopad S. V. Gibridnye intellektual'nye sistemy s samoorganizatsiei: koordinatsiia, soglasovannost', spor. M. : IPI RAN, 2014, 189 pp.
3. Lovtsov D. A., Niesov V. A. Modernizatsiia informatsionnoi infrastruktury sudoproizvodstva -- kliuchevoe napravlenie optimizatsii nagruzki na sudebnuiu sistemu. Rossiiskoe pravosudie, 2014, No. 9, pp. 30-40.
4. Lovtsov D. A., Niesov V. A. Aktual'nye problemy sozdaniia i razvitiia edinogo informatsionnogo prostranstva sudebnoi sistemy Rossii. Informatsionnoe pravo, 2013, No. 5, pp. 13-18.
5. Lovtsov D. A., Sergeev N. A. Informatsionno-matematicheskoe obespechenie upravleniia bezopasnost'iu ergaticheskikh sistem. III. Ekspertnaia informatsionnaia sistema, NTI, ser. 2. Inform. protsessy i sistemy, 2001, No. 11, pp. 23-30.
6. Prikladnye intellektual'nye sistemy, osnovannye na miagkikh vychisleniiakh. Pod red. N. G. Iarushkinoi. Ul'ianovsk : UlGTU, 2004, 139 pp.
7. Samokhvalov E. N., Revunkov G. I., Gapaniuk Iu. E. Ispol'zovanie metagrafov dlia opisaniia semantiki i pragmatiki informatsionnykh sistem. Vestnik MGTU im. N.E. Baumana, ser. "Priborostroenie", 2015, vyp. No. 1, pp. 83-99.
8. Tarasov S. D. Sovremennye metody avtomaticheskogo referirovaniia. Nauchno-tekhnicheskie vedomosti SPbGPU, 2010, vyp. No. 6, pp. 59-74.
9. Tarasov V. B. Ot mnogoagentnykh sistem k intellektual'nym organizatsiiam: filosofiia, psikhologiia, informatika. M. : Editorial URSS, 2002, 352 pp.
10. Fedoseev S. V. Primenenie sovremennykh tekhnologii bol'shikh dannykh v pravovoi sfere. Pravovaia informatika, 2018, No. 4, pp. 50-58.
11. Chernen'kii V. M., Terekhov V. I., Gapaniuk Iu. E. Predstavlenie slozhnykh setei na osnove metagrafov. Trudy XVIII Vseross. nauch.-tekhn. konf. "Neiroinformatika-2016", ch. 1, NIIaU MIFI, M. : MIFI, 2016, pp. 173-178.
12. Chernen'kii V. M., Terekhov V. I., Gapaniuk Iu. E. Struktura gibridnoi intellektual'noi informatsionnoi sistemy na osnove metagrafov. Neirokomp'iutery: razrabotka, primenenie, 2016, vyp. No. 9, pp. 3-14.
13. Basu A., Blanning R. Metagraphs and their applications. Springer, 2007, 174 pp.
14. Geron A. Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow. Concepts, Tools, and Techniques to Build Intelligent Systems. O'Reilly, 2019. 856 pp.
15. Kulkarni A., Shivananda A. Natural Language Processing Recipes. Unlocking Text Data with Machine Learning and Deep Learning using Python. Apress, 2019. 234 pp.
16. Taran M., Revunkov G., Gapanyuk Yu. The Hybrid Intelligent Information System for Poems Generation. Neuroinformatics 2019: Advances in Neural Computation, Machine Learning, and Cognitive Research III. Pp. 78-86.

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ МОДЕЛИРОВАНИЯ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Большаков А.С., Раковский Д.И.*

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

Аннотация.

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

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

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

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

Введение

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

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

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

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

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

E-mail: alexbol57@mail.ru

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

E-mail: dimitor1998@mail.ru

Таблица 1

Сравнение действующего программного обеспечения[5]

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

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

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

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

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

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

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

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

Постановка задачи

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

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

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

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

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

Исходные данные, поступающие на вход ПО, представляют собой:

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

*Таблица **2***

Описание параметров угроз, представленных в банке данных угроз

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

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

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

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

*Таблица **3***

Описание параметров уязвимостей, представленных в банке данных уязвимостей

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

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

Особенности разработанного программного обеспечения

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

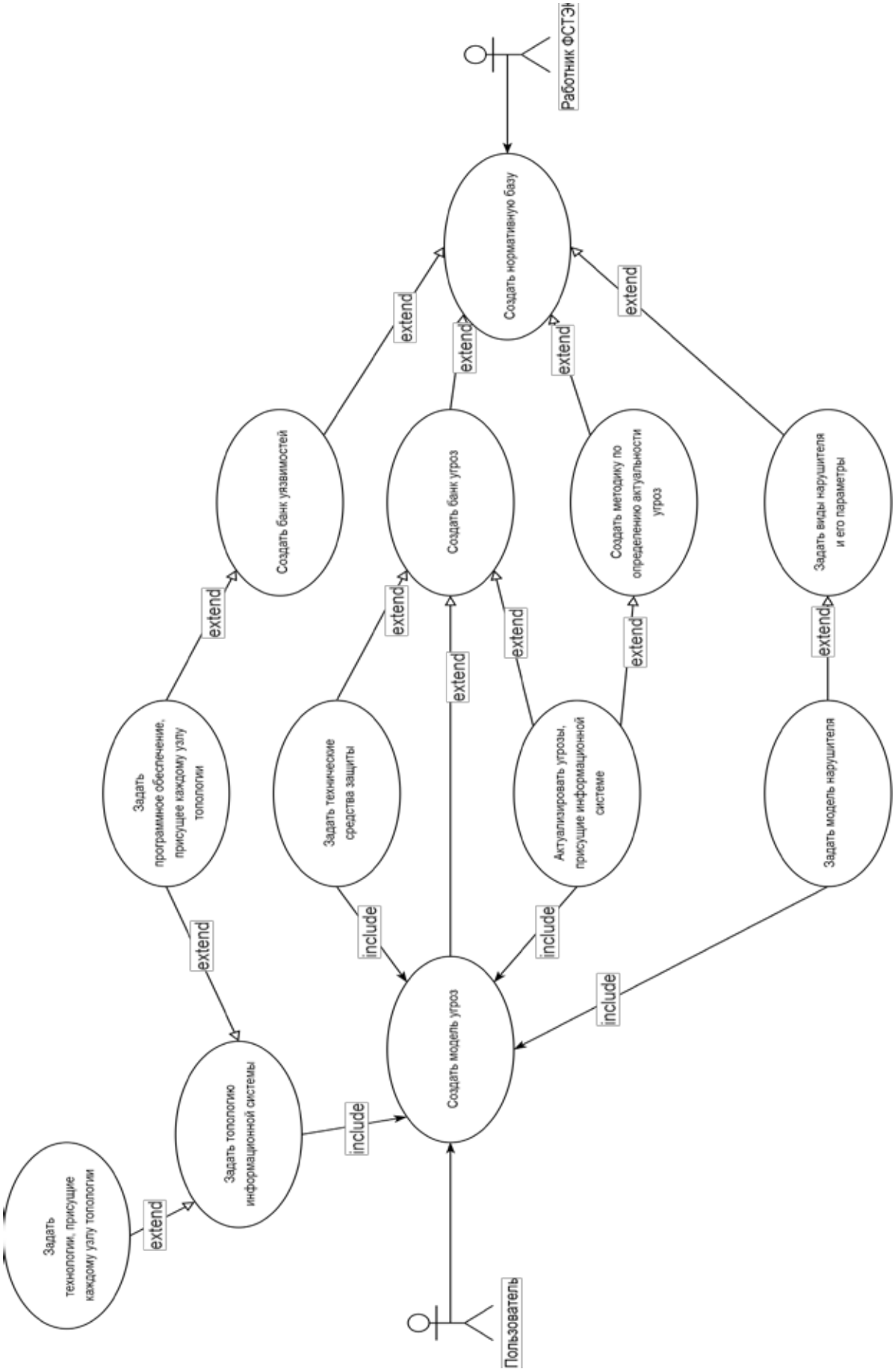

Рис. 1. Диаграмма вариантов использования программного обеспечения

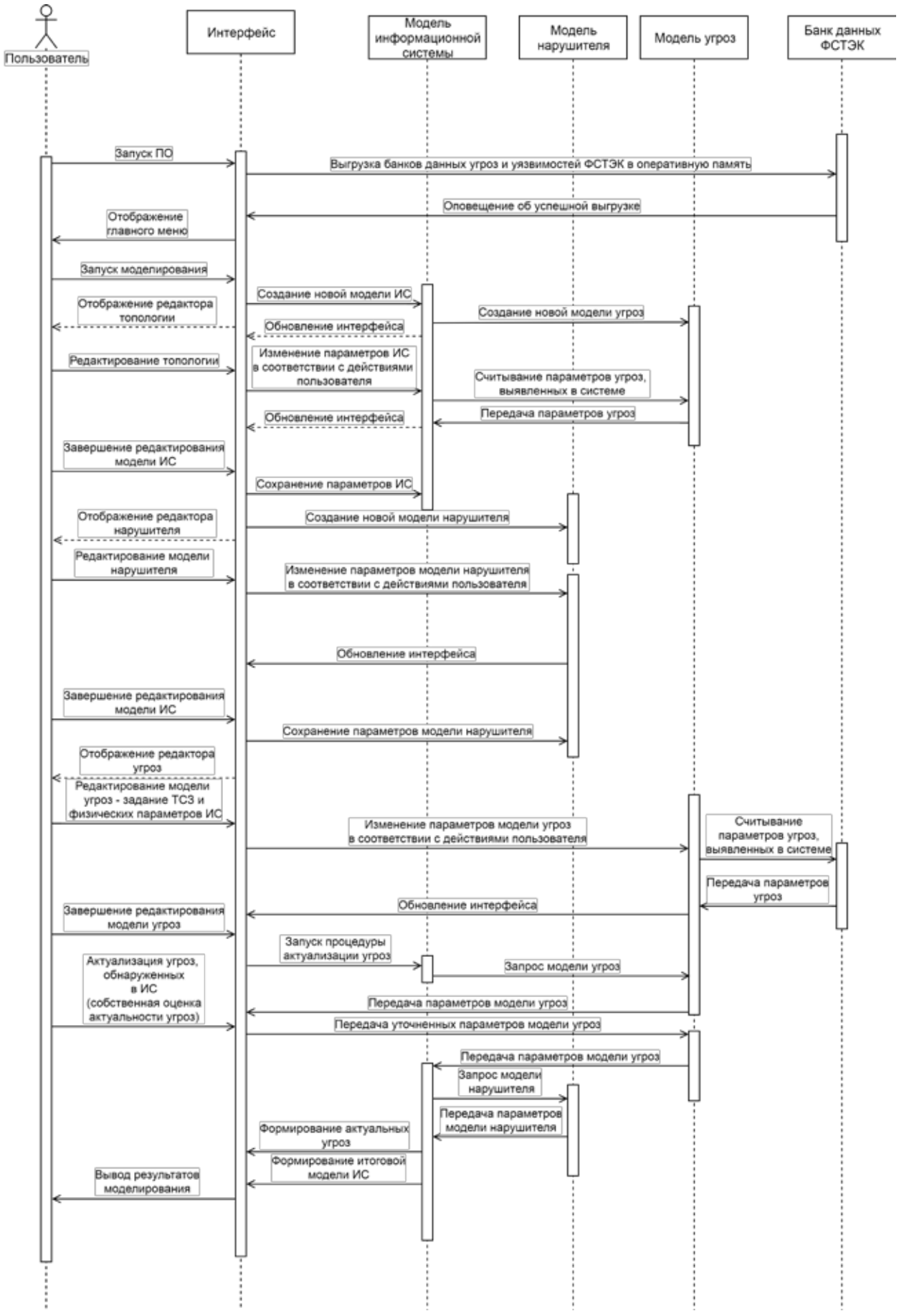

Рис. 2. Диаграмма последовательности создания модели угроз

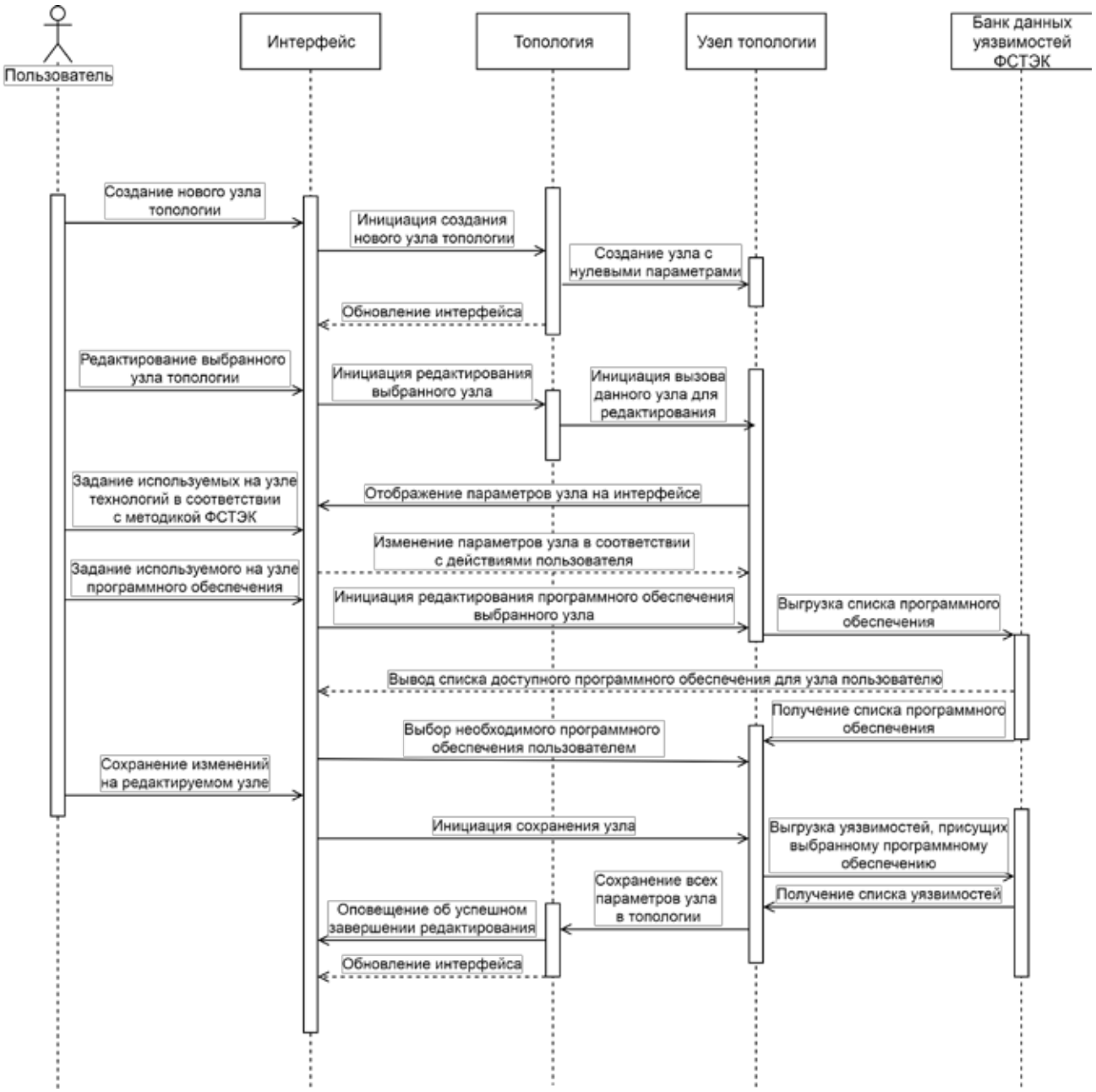

Рис. 3. Диаграмма последовательности задания топологии инфосистемы

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

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

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

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

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

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

ся в разработанном программном обеспечении согласно следующему алгоритму ФСТЭК:

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

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

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

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

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

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

Таблица 4

Определение возможности реализации j-й угрозы инфосистеме

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

Таблица 5

Определение актуальности j-й угрозы инфосистеме

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

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

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

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

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

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

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

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

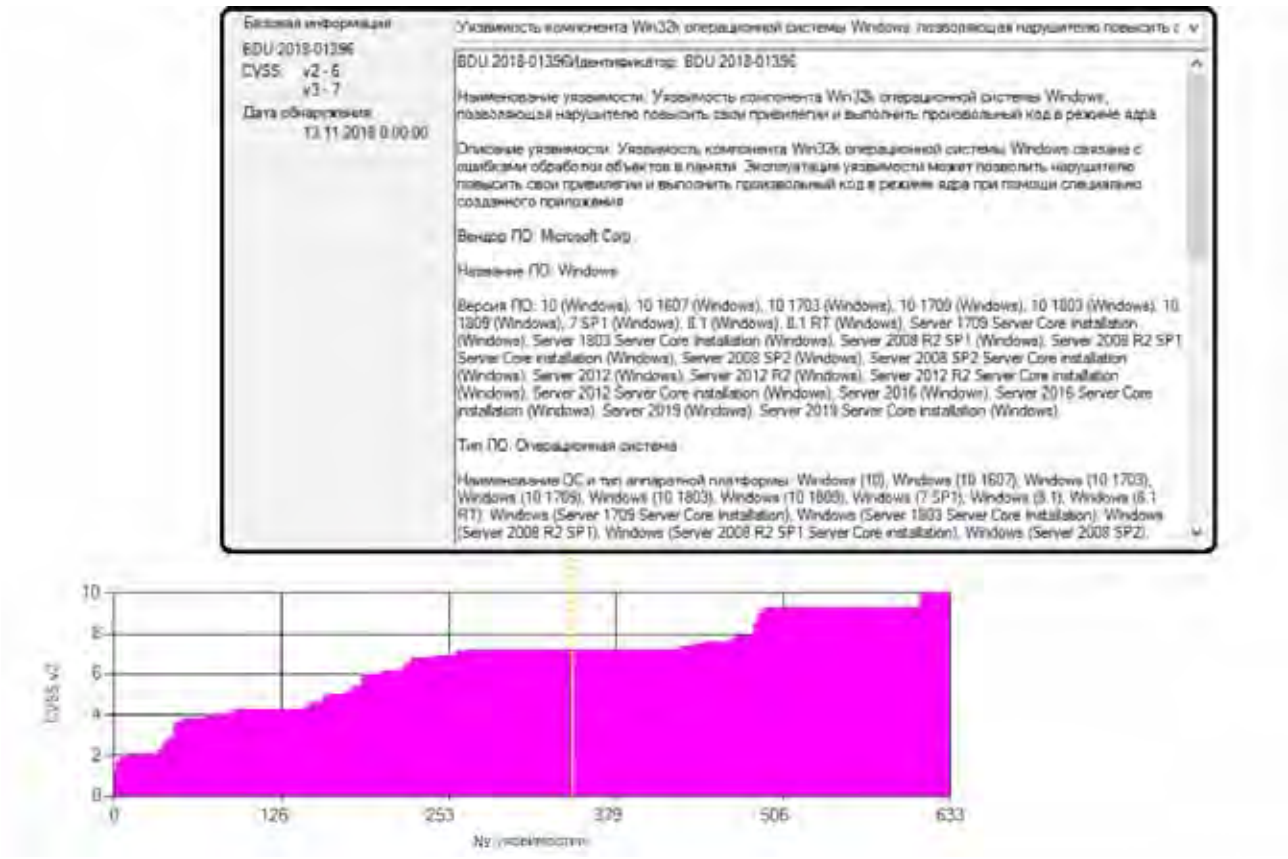

Рис. 4. Распределение уязвимостей по оценкам их опасности для узла «файловый сервер» инфосистемы (иллюстрация анализа выбранной пользователем уязвимости)

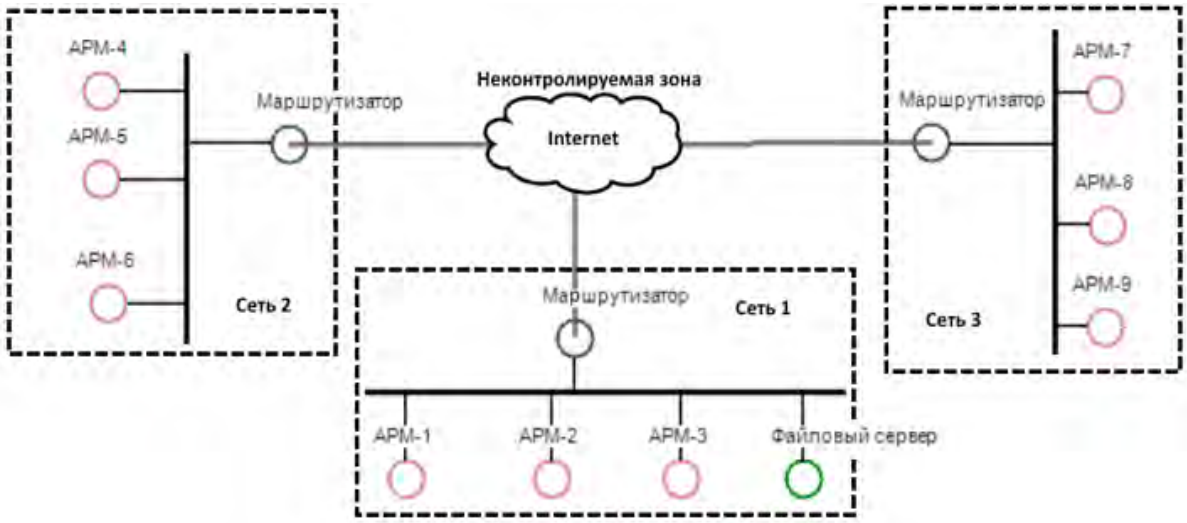

Рис. 5. Моделируемая топология распределенной сети

Адекватность полученных результатов моделирования

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

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

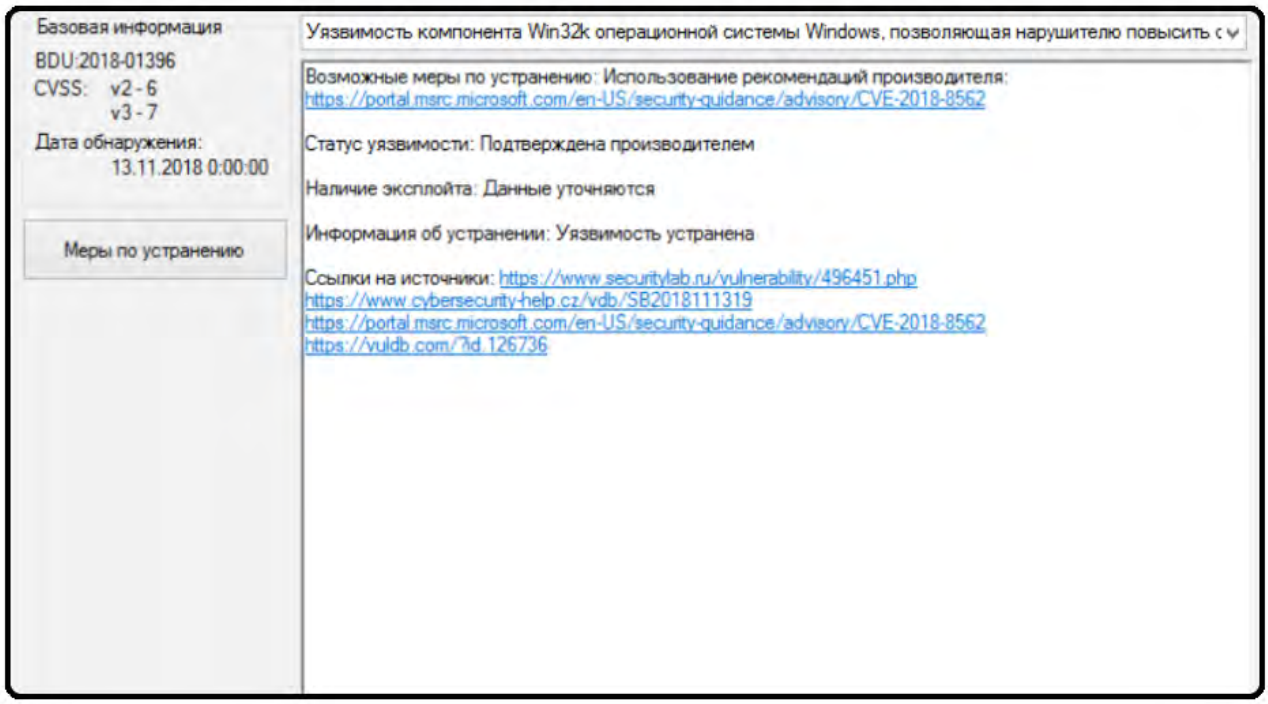

Рис. 6. Демонстрация взаимодействия пользователя с программным обеспечением

Рис. 7. Пояснение к определению адекватности моделирования угроз

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

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

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

Таблица 6

Сравнение результатов работы программного обеспечения и экспертной оценки

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

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

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

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

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

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

Заключение

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

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

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

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

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

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

Литература

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

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

SOFTWARE FOR MODELLING INFORMATION SECURITY THREATS IN INFORMATION SYSTEMS

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

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

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

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

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

References

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

МНОГОФАКТОРНАЯ МОДЕЛЬ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ

*Минаков В.Ф., Шепелёва О.Ю., Лобанов О.С.**

Ключевые слова: *угрозы, опасности, несанкционированный доступ, модель, эффективность.*

Аннотация.

Цель работы: *разработка математической модель и интегральной оценки вероятности обеспечения безопасного состояния информационных ресурсов компании в условиях угроз и опасностей несанкционированного доступа к коммерческой конфиденциальной информации.*

Методы: *комплексные аналитические и экспертные методы систематизации и математическое моделирование экономических отношений в цифровой экономике.*

Результаты: *представленная модель отличается учетом влияния ресурсных факторов обеспечения информационной безопасности, а также фактора времени. На основе предложенной математической модели построена зависимость вероятности обеспечения защищенного состояния информационных ресурсов компании в заданном диапазоне временных и ресурсных показателей. Установлена высокая эффективность совместного использования факторов времени и ресурсов для повышения вероятности безубыточной работы компании посредством снижения рисков возникновения ущербов в результате несанкционированного доступа к конфиденциальной коммерческой информации. Обоснована возможность использования модели в задачах стратегического управления деятельностью компании.*

DOI: 10.21681/1994-1404-2020-1-40-46

Введение

Современные процессы цифровизации распространяются не только на локальные технологические операции предприятий, но и на взаимодействие субъектов экономики [1—3]. Это процедуры формирования предложений товаров, работ и услуг производителями, их выбор потребителями и формирование запросов на их приобретение. Таким образом, посредством цифровых ресурсов обеспечивается управление потоками материальных и трудовых ресурсов [4, 5]. Оплата товаров и услуг также производится чаще по безналичному расчету (электронными платежами). Для этого используются как банковские услуги: платежные системы, дистанционное банковское обслуживание в системах «клиент-банк», посредством банковских карт и т. д., так и сервисы замкнутых платежных систем «Яндекс-Деньги», Web-Money и др. Доля безналичных расчетов примерно равна доле наличных, причем у обладателей банковских карт эта доля составляет 90% (по данным Центробанка России). Важно также, что цифровые технологии трансформировали экономические процессы. Информационно-коммуникационные технологии (ИКТ) играют системообразующую роль. Так, финансовые, транспортные, маркетинговые агрегаторы стали фактором сближения и конвергенции участников экономических процессов. Именно цифровые платформы агрегаторов обеспечивают согласование интересов потребителей и производителей товаров и услуг, обеспечивая принятие и исполнение решений о сделках, запуске бизнес-процессов, управлении ресурсами хозяйственной деятельности [6, 7].

В таких условиях растут возможности несанкционированного доступа к материальным и финансовым ресурсам, и, соответственно, число компьютерных

* ***Минаков Владимир Фёдорович,*** *доктор технических наук, профессор кафедры информатики, Санкт-Петербургский государственный экономический университет, Российская Федерация, г. Санкт-Петербург.*
E-mail: m-m-m-m-m@mail.ru

Шепелёва Ольга Юрьевна, *ассистент кафедры информатики, Санкт-Петербургский государственный экономический университет, Российская Федерация, г. Санкт-Петербург.*
E-mail: shepeleva-olga@list.ru

Лобанов Олег Сергеевич, *кандидат экономических наук, доцент кафедры информатики, Санкт-Петербургский государственный экономический университет, Российская Федерация, г. Санкт-Петербург.*
E-mail: thelobanoff@gmail.com

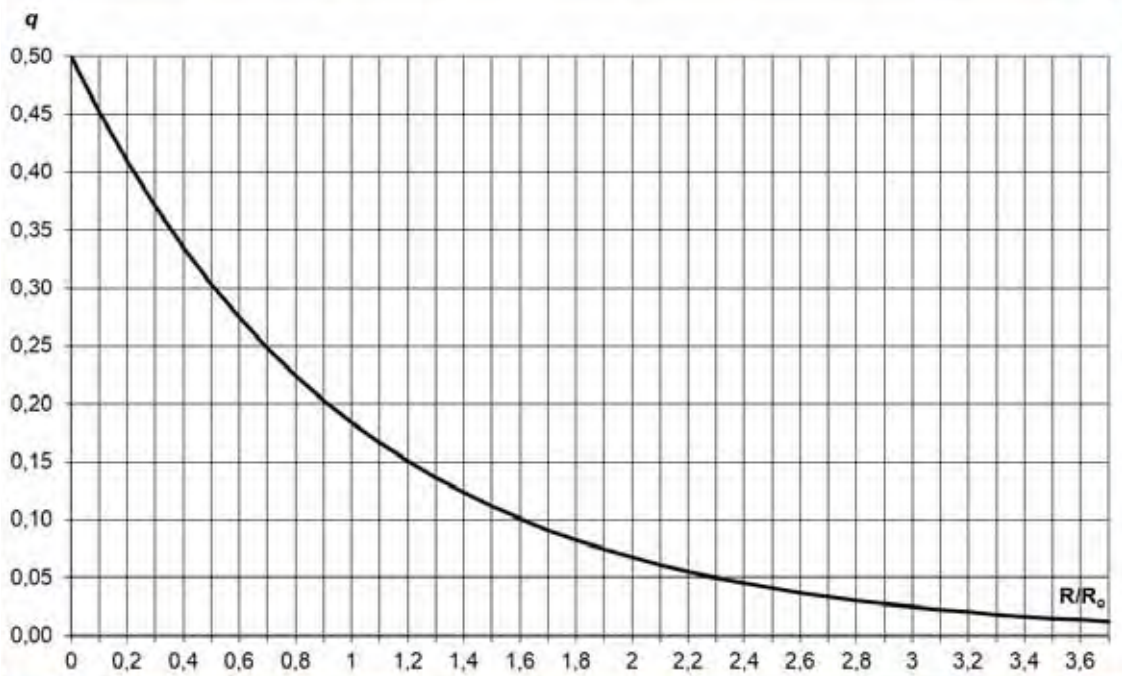

Рис. 1. Зависимость вероятности компьютерных преступлений от затрат на средства обеспечения информационной безопасности

преступлений в отношении управления перечисленными ресурсами [8—10]. Только прямой финансовый ущерб от компьютерных преступлений за 2018 год, по расчетам специалистов компании McAfee, составил свыше 600 миллиардов долларов США, а ущерб с учетом потерь репутации, срыва сделок и, соответственно, упущенной выгоды — 3 триллиона долларов США. Следовательно, актуальность обеспечения информационной безопасности в экономике возрастает [11, 12]. Не случайно так растет интерес к прорывным информационным технологиям: например, распределенным реестрам (блокчейн) и криптовалютам, их эмитентам и платежам с их использованием. Аналогичные процессы наблюдаются в системах смарт-контрактов.

Целью данного исследования стала разработка модели ресурсного динамического обеспечения безопасности в цифровой экономике. Надежность системы безопасности информационных ресурсов экономических объектов предопределяется функционированием средств защиты в условиях угроз и опасностей несанкционированного доступа. Анализ таких средств [8—14] позволяет установить, что они направлены на решение задач a) выявления; b) предотвращения; c) нейтрализации; d) пресечения; e) локализации; f) уничтожения; g) отражения; h) локализации последствий. Каждая из функциональных информационных систем, решающая названный класс задач, требует от предприятия затрат на приобретение, внедрение и сопровождение средств компьютерной безопасности.

Следовательно, для решения каждой задачи необходимы инвестиции. Очевидно, класс средств защиты снижает вероятность q компьютерного преступления в *k* раз:

$$q_1(R) = q_0/k(R_1), q_2(R) = q_0/k(R_1)/k(R_2)\ldots \quad (1)$$

где R-стоимость средств безопасности.

Для средневзвешенного значения затрат

$$R = (R_1 + R_2 + \ldots + R_n)/N\ , \quad (2)$$

имеем среднее значение k и, следовательно, получаем в общем виде

$$q(R) = q_0/k^R = q_0 \cdot k^{-R} \quad (3)$$

Выразим кратность через фиксирование основание натурального логарифма e через соотношение

$$k^{-R} = e^{-R/R_o} \quad (4)$$

где R_o — численное значение затрат, обеспечивающее снижение вероятности q в e раз:

$$q(R) = q_0 \cdot e^{-R/R_o} \quad (5)$$

Характер зависимости $q(R)$ представлен на рис. 1.

Рисунок 1 показывает, что затраты на информационную безопасность асимптотически снижают вероятность киберпреступлений. Действительно, добиться абсолютной безопасности с нулевым значением вероятности совершения злоумышленных действий в виртуальном пространстве невозможно [15].

Учитывая, что сумма вероятностей безопасной работы информационных ресурсов p и вероятности реализации компьютерных преступлений q:

$$q(R) + p(R) = 1\ , \quad (6)$$

получаем

$$p(R) = 1 - q(R), \quad (7)$$

Таким образом, показатель надежности — вероятность безотказной работы системы защиты — описывается зависимостью от объема ресурсного обеспечения средствами безопасности: программным и аппаратным обеспечением, разработкой новых методов, организационными механизмами и пр. [16]. Это можно выразить формулой:

$$p(R) = p_{max1} \cdot \left(1 - e^{-R/R_0}\right), \quad (8)$$

где $e \approx 2{,}71828$,

p, p_{max1} — вероятности (текущее и максимально возможное значение) успешного противодействия угрозам и опасностям совершения компьютерного преступления и, соответственно, вызванного им экономического ущерба при базовом варианте обеспечения информационной безопасности.

Очевидно, что использование дополнительных средств защиты в виде инновационных решений, для которых не созданы средства взлома в силу неизвестности принципа действия и характеристик нововведений, повышает вероятность состояния защищенности на некоторую величину p_{max2}, причем $p_{max1} + p_{max2} = p_{max}$. Иначе: $p_{max} = p_{max} \cdot (a_1 + a_2)$. В [14, с. 54] получена «зависимость вероятности обеспечения защиты» во времени в форме сигмоиды. Представим сигмоиду вероятностей функцией вида

$$p(t) = \frac{p_{max2}}{1 + e^{d - t/T}} \quad (9)$$

где T постоянная времени изменения эффекта защиты в условиях эксплуатации средства безопасности;

$e \approx 2{,}71828$,

d — число постоянных времени смещения медианного значения сигмоиды относительно начала времени отсчета.

Теперь с учетом одновременного влияния ранее использованных средств защиты и инновационных решений получим результирующую вероятность обеспечения защиты в виде суммы компонент (в качестве примера использованы: постоянная времени T=2 года как средний период между обновлениями программного обеспечения в системе информационной безопасности, R_0=4, $a_1 = 0{,}5$; $a_2 = 0{,}5$):

$$p(t,R) = \frac{0{,}5}{1 + e^{4 - t/2}} + 0{,}5 \cdot \left(1 - e^{-R/4}\right), \quad (10)$$

На рис. 1 визуализирован эффект повышения вероятности противодействия ущербам от несанкционированных доступов к коммерческой конфиденциальной информации. Как видно из рисунка, рост вероятности защищенности цифровых ресурсов существенно зависит от соотношения времени и ресурсного обеспечения информационной безопасности. Это позволяет закладывать проектные решения на основе решения задачи обеспечения требуемого уровня рисков, определяя такое соотношение ресурсов (а следовательно, и затрат) и времени реализации проекта, которое в наибольшей степени отвечает целям компании, возможностям реализации проекта в соответствии со стратегией ее деятельности [17—19]. Более того, полученная зависимость является инструментом построения поля сценариев для принятия управленческих решений по обеспечению безопасного состояния не только информационных, но и финансовых, а также материальных ресурсов компании [20—22]. Очевидно, что соотношение между эффектами повышения вероятности предотвращения несанкционированного доступа a_1 и a_2 может на основе полученной модели выбираться и оптимизационным путем, когда модель может использоваться в интегральных показателях деятельности компании в течение определенного времени.

Важно отметить, что развитие парадигмы ресурсно-затратного вида на обеспечение информационной безопасности фактором влияния времени приводит

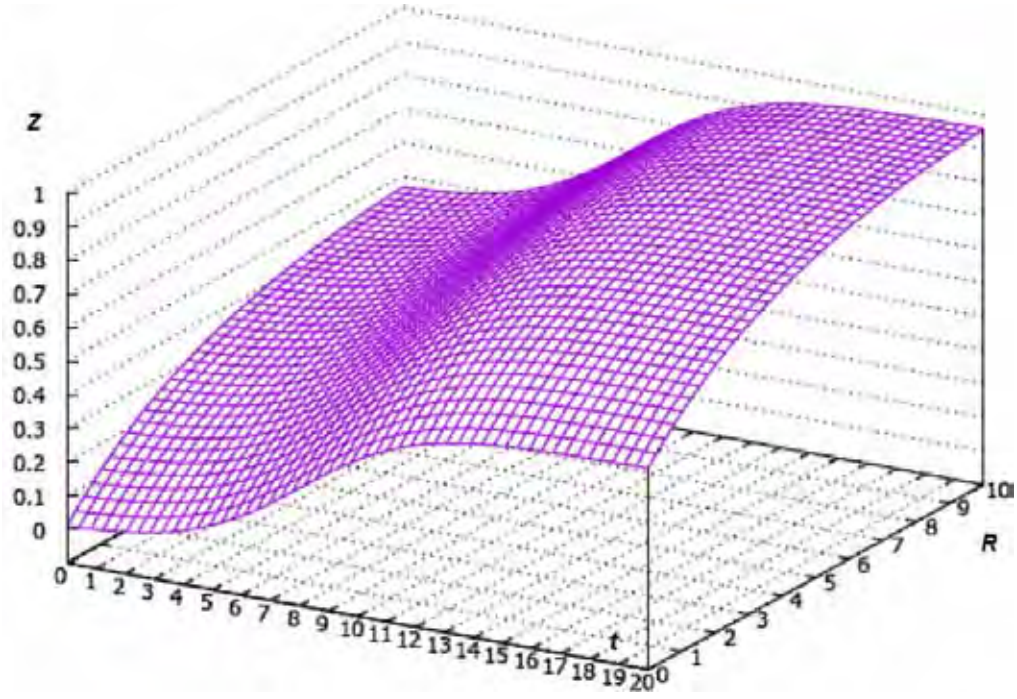

Рис. 2. Влияние ресурсов (R) ***и времени*** (t) ***на вероятность обеспечения безопасного состояния***

к обобщенной модели. Действительно, подстановка в предложенную модель единственного численного значения времени (например, текущего момента времени) приводит к частному случаю решения задачи обеспечения информационной безопасности, например, при оперативном управлении. Для задач тактического управления в среднесрочной перспективе задаются интервалы времени, определяемые тактическими целями. Для разработки стратегии развития системы безопасности предприятия модель может быть использована на длительных временных интервалах, в течение которых требуется достижение долгосрочный целей.

Кроме того, фиксируя расчетный момент времени, получаем модель вариативных решений в части выбора целесообразных инвестиций в ресурсы информационной безопасности, — например, для выбора альтернативных проектов, предлагаемых аутсорсерами информационной безопасности [16].

Модель аналитического вида выгодно отличается от представления процессов управления информационной безопасностью системами дифференциальных уравнений, во-первых, возможностью ее практического использования. Действительно, офисные приложения (включая облачные) позволяют любому пользователю выполнить расчеты, используя стандартные функции, например, табличных процессоров, и на их основе оценить альтернативные варианты решений проблемы обеспечения информационной безопасности. Важно, что, независимо от вида средств защиты, используемых в них методов, конечным показателем, оцениваемым моделью, является результат в форме оценки достигаемой вероятности безопасной работы информационных ресурсов предприятий, их объединений, органов государственной власти и многих других структур. Модель инвариантна к видам их деятельности, отраслям экономики, формам собственности и прочим особенностям.

Свойство инвариантности расширяет границы применимости предложенной модели. Она остается справедливой к новым, не представленным на современном рынке, разработкам. Это свойство имеет особую ценность в связи с беспрецедентной динамикой рынка информационно-коммуникационных систем и технологий. Во-первых, согласно закономерности, установленной Гордоном Муром применительно к концентрации активных ключей в аппаратной части микропроцессоров и дополненной Давидом Хаусом наблюдениями за динамикой роста производительности вычислительных средств, каждые 18 и 24 месяца вдвое возрастают соответственно первый и второй показатели. Следовательно, использование злоумышленниками более мощных вычислительных мощностей даже на основе метода простого перебора снижает вероятность сохранения защищенного состояния информационных систем предприятий. Во-вторых, сформировались и стремительно развиваются инновационные направления цифровизации экономики на основе смарт-технологий, обработки больших объемов данных, технологий M2M, интеллектуальных систем, облачных сервисов, платформ и инфраструктур и ряд других. Эволюция таких информационных технологий делает непредсказуемыми новые критические для экономических процессов места уязвимостей. Вместе с тем разработки адекватных методов и средств защиты информации и цифровых бизнес-процессов ведутся с учетом новых видов угроз и опасностей информационной безопасности в режиме реального времени. Компании-разработчики таких средств всегда делают предложения потребителям с указанием сроков разработки и внедрения средств защиты информации, а также ценой продуктов. Названные показатели и являются исходными данными для разработанной модели. А ее использование позволяет на основе прямых расчетов получить количественные оценки достигаемого результата в части информационной безопасности.

Модель также может быть использована в дополнение к методам анализа иерархий, деревьев решений и многих других в системах поддержки принятия решений. Важно, что развитие названных методов существенно развивает принципы обоснованного принятия управленческих решений учетом фактора времени. Данное обстоятельство имеет решающее значение для обеспечения устойчивости предприятий, их развития.

Очевидно, что фактор времени играет решающую роль в управлении изменениями. Его количественный учет позволяет изменить парадигму тактического и стратегического управления деятельностью предприятия. Вместо отслеживания происходящих изменений и следования им с лагом по времени, представляется возможность формирования изменений, обеспечивая предприятию конкурентные преимущества за счет первенства осуществления изменений. Не менее важно, что данная парадигма хорошо согласуется с методологиями проектного управления. Отметим, что традиционная парадигма проектного управления приводит, как показывает практика, к низкой реализуемости проектов. А инвестиции в разработку и реализацию проектов в хозяйственной деятельности предприятий существенно превосходят инвестиции в средства обеспечения информационной безопасности.

Выводы

Предложена модель интегральной оценки вероятности обеспечения безопасного состояния информационных ресурсов компании в условиях угроз и опасностей несанкционированного доступа к коммерческой конфиденциальной информации. Отличительной особенностью модели является учет фактора времени при использовании инновационных решений обеспечения информационной безопасности в дополнение к ресурсным факторам ее повышения, основанных на повышении затрат. Установлена достаточно высокая степень повышения вероятности безубыточной работы компании, превышающая в конкретном рассмо-

тренном примере эффект от ресурсного подхода к снижению рисков. Показана возможность использования модели в задачах стратегического управления деятельностью компании, управления проектами обеспечения информационной безопасности, а также оптимизации издержек. Достоверность предложенной модели подтверждается доказательством справедливости модели и строгими математическими выкладками.

Рецензент: ***Марков Алексей Сергеевич****, доктор технических наук, старший научный сотрудник, МГТУ им. Н.Э. Баумана, г. Москва, Россия.*
E-mail: a.markov@bmstu.ru

Литература

1. Бочков С.И., Макаренко Г.И., Федичев А.В. Об Окинавской хартии глобального информационного общества и задачах развития российских систем коммуникации // Правовая информатика. 2018. № 1. С. 4—14.
2. Минаков В.Ф., Шепелёва О.Ю., Шепелёв П.Ю. Феномен конвергенции информационных и материальных потоков в экономических процессах // Правовая информатика. 2018. № 3. С. 70—74.
3. Petrenko S.A., Makoveichuk K.A., Chetyrbok P.V., Petrenko A.S. About Readiness for Digital Economy. In: Proceedings of the 2017 IEEE II International Conference on Control in Technical Systems, IEEE, CTS, 2017, pp. 96-99. DOI: 10.1109/CTSYS.2017.8109498.
4. Kravchenko N.A., Glinskiy V.V., Serga L.K., Anokhin N.V. Sources of high-tech business financing: experience of empirical research. Academy of Accounting and Financial Studies Journal, 2017, v. 21, No. 3, pp. 12-14.
5. Ивантер В.В., Белоусов Д.Р., Блохин А.А. и др. Структурно-инвестиционная политика в целях модернизации экономики России // Проблемы прогнозирования. 2017. № 4 (163). С. 3—16.
6. Glinskiy V., Serga L., Khvan M. Assessment of environmental parameters impact on the level of sustainable development of territories. In: Procedia CIRP 13. Ser. 13th Global Conference on Sustainable Manufacturing -- Decoupling Growth from Resource Use, 2016, pp. 626-631.
7. Glinskiy V., Serga L., Chemezova E., Zaykov K. Clusterization economy as a way to build sustainable development of the region. In: Procedia CIRP 13. Ser. 13th Global Conference on Sustainable Manufacturing -- Decoupling Growth from Resource Use, 2016, pp. 324-328.
8. Дорофеев А.В., Марков А.С. Структурированный мониторинг открытых персональных данных в сети Интернет // Мониторинг правоприменения. 2016. № 1 (18). С. 41—53.
9. Карцхия А.А., Макаренко Г.И., Сергин М.Ю. Современные тренды киберугроз и трансформация понятия кибербезопасности в условиях цифровизации системы права // Вопросы кибербезопасности. 2019. № 3 (31). С. 18—23.
10. Степанов О.А. Правовое регулирование отношений в сфере безопасного функционирования и развития систем искусственного интеллекта: доктринальные аспекты // Правовая информатика. 2019. № 1. С. 56—63.
11. Dorofeev A.V., Markov A.S., Tsirlov V.L. Social media in identifying threats to ensure safe life in a modern city. Communications in Computer and Information Science, 2016, v. 674, pp. 441-449.
12. Maximov R., Krupenin A., Sharifullin S., Sokolovsky S. Innovative development of tools and technologies to ensure the Russian information security and core protective guidelines. Voprosy kiberbezopasnosti [Cybersecurity issues], 2019, No. 1 (29), pp. 10-17, DOI: 10.21681/2311-3456-2019-1-10-17.
13. Астраханцев Р.Г., Лось А.Б., Мухамадиева Р.Ш. Анализ современных тенденций развития технологии «блокчейн» и цифровых валют // Вопросы кибербезопасности. 2019. № 5 (33). С. 57—62.
14. Мальцев Г.Н., Панкратов А.В., Лесняк Д.А. Исследование вероятностных характеристик изменения защищенности информационной системы от несанкционированного доступа нарушителей // Информационно-управляющие системы. 2015. № 1 (74). С. 50—58. DOI: 10.15217/issn1684-8853.2015.1.50.
15. Probabilistic Modeling in System Engineering. By ed. A. Kostogryzov, London: IntechOpen, 2018. 278 p.
16. Минаков В.Ф., Шепелёва О.Ю., Лобанов О.С. Ресурсно-временная модель повышения защищенности конфиденциальных данных // Сборник трудов Десятой международной научно-технической конференции «Безопасные информационные технологии» (Москва, 3—4 декабря 2019 г.). М. : МГТУ им. Н.Э. Баумана, 2019. С. 301—304.
17. Glinskiy V., Serga L., Zaykov K. Identification method of the russian federation arctic zone regions statistical aggregate as the object of strategy development and a source of sustainable growth. Procedia Manufacturing, 2017, v. 8, pp. 308-314.
18. Litvintseva G.P., Glinskiy V.V., Stukalenko E.A. Interregional differentiation of population incomes in the Russian Federation in the post-crisis period. Academy of Strategic Management Journal, 2017, v. 16, No. 4.
19. Glinskiy V., Serga L., Novikov A., Bulkina A., Litvintseva G. Investigation of correlation between the regions sustainability and territorial differentiation. Procedia Manufacturing, 2017, v. 8, pp. 323-329.

20. Borisov V.N., Kuvalin D.B., Pochukaeva O.V. Improving the factor efficiency of machinery in the regions of the Russian Federation. Studies on Russian Economic Development, 2018, v. 29, No. 4, pp. 377-386.
21. Borisov V.N., Pochukaeva O.V. Investment and innovative technological efficiency: Case study of the Arctic project. Studies on Russian Economic Development, 2017, v. 28, No. 2, pp. 169-179.
22. Ivanter V.V., Belkina T.D., Belousov D.R., Blokhin A.A., Borisov V.N. et al. Recovery of economic growth in Russia. Studies on Russian Economic Development, 2016, v. 27, No. 5, pp. 485-494.

A MULTI-FACTOR MODEL FOR ENSURING CONFIDENTIAL DATA SECURITY

Vladimir Minakov, *Dr.Sc. (Technology), Professor at the Department of Informatics, Saint Petersburg State University of Economics, Saint Petersburg, Russian Federation.*
E-mail: m-m-m-m-m@mail.ru

Ol'ga Shepeleva, *Assistant Professor at the Department of Informatics, Saint Petersburg State University of Economics, Saint Petersburg, Russian Federation.*
E-mail: shepeleva-olga@list.ru

Oleg Lobanov, *Ph.D. (Economics), Associate Professor at the Department of Informatics, Saint Petersburg State University of Economics, Saint Petersburg, Russian Federation.*
E-mail: thelobanoff@gmail.com

Keywords: *threats, dangers, unauthorised access, model, efficiency.*

Abstract.

Purpose of the work: *working out a mathematical model and integrated estimate of the probability of ensuring a safe state of the company's information resources under the condition of threats and danger of unauthorised access to commercial confidential information.*

Method used: *complex analytical and expert methods of systematisation and mathematical modelling of economic relations in digital economy.*

Results obtained: *the presented model is notable for taking into account the influence of resource factors for ensuring information security as well as the time factor. Based on the proposed mathematical model, the relationship of the probability of ensuring a protected state of the company's information resources in a given range of time and resource indicators is built. A high efficiency of the joint use of time and resource factors for increasing the probability of the company's profitable operation by means of reducing the risk of damages arising from unauthorised access to confidential commercial information is established. A justification is given for the feasibility of using the model in tasks of strategic management of the company.*

References

1. Bochkov S.I., Makarenko G.I., Fedichev A.V. Ob Okinavskoi khartii global'nogo informatsionnogo obshchestva i zadachakh razvitiia rossiiskikh sistem kommunikatsii. Pravovaia informatika, 2018, No. 1, pp. 4-14.
2. Minakov V.F., Shepeleva O.Iu., Shepelev P.Iu. Fenomen konvergentsii informatsionnykh i material'nykh potokov v ekonomicheskikh protsessakh. Pravovaia informatika, 2018, No. 3, pp. 70-74.
3. Petrenko S.A., Makoveichuk K.A., Chetyrbok P.V., Petrenko A.S. About Readiness for Digital Economy. In: Proceedings of the 2017 IEEE II International Conference on Control in Technical Systems, IEEE, CTS, 2017, pp. 96-99. DOI: 10.1109/CTSYS.2017.8109498.
4. Kravchenko N.A., Glinskiy V.V., Serga L.K., Anokhin N.V. Sources of high-tech business financing: experience of empirical research. Academy of Accounting and Financial Studies Journal, 2017, v. 21, No. 3, pp. 12-14.
5. Ivanter V.V., Belousov D.R., Blokhin A.A. i dr. Strukturno-investitsionnaia politika v tseliakh modernizatsii ekonomiki Rossii. Problemy prognozirovaniia, 2017, No. 4 (163), pp. 3-16.
6. Glinskiy V., Serga L., Khvan M. Assessment of environmental parameters impact on the level of sustainable development of territories. In: Procedia CIRP 13. Ser. 13th Global Conference on Sustainable Manufacturing -- Decoupling Growth from Resource Use, 2016, pp. 626-631.
7. Glinskiy V., Serga L., Chemezova E., Zaykov K. Clusterization economy as a way to build sustainable development of the region. In: Procedia CIRP 13. Ser. 13th Global Conference on Sustainable Manufacturing -- Decoupling Growth from Resource Use, 2016, pp. 324-328.

8. Dorofeev A.V., Markov A.S. Strukturirovannyi monitoring otkrytykh personal'nykh dannykh v seti Internet. Monitoring pravoprimeneniia, 2016, No. 1 (18), pp. 41-53.
9. Kartskhiia A.A., Makarenko G.I., Sergin M.Iu. Sovremennye trendy kiberugroz i transformatsiia poniatiia kiberbezopasnosti v usloviiakh tsifrovizatsii sistemy prava. Voprosy kiberbezopasnosti, 2019, No. 3 (31), pp. 18-23.
10. Stepanov O.A. Pravovoe regulirovanie otnoshenii v sfere bezopasnogo funktsionirovaniia i razvitiia sistem iskusstvennogo intellekta: doktrinal'nye aspekty. Pravovaia informatika, 2019, No. 1, pp. 56-63.
11. Dorofeev A.V., Markov A.S., Tsirlov V.L. Social media in identifying threats to ensure safe life in a modern city. Communications in Computer and Information Science, 2016, v. 674, pp. 441-449.
12. Maximov R., Krupenin A., Sharifullin S., Sokolovsky S. Innovative development of tools and technologies to ensure the Russian information security and core protective guidelines. Voprosy kiberbezopasnosti [Cybersecurity issues], 2019, No. 1 (29), pp. 10-17, DOI: 10.21681/2311-3456-2019-1-10-17.
13. Astrakhantsev R.G., Los' A.B., Mukhamadieva R.Sh. Analiz sovremennykh tendentsii razvitiia tekhnologii "blokchein" i tsifrovykh valiut. Voprosy kiberbezopasnosti, 2019, No. 5 (33), pp. 57-62.
14. Mal'tsev G.N., Pankratov A.V., Lesniak D.A. Issledovanie veroiatnostnykh kharakteristik izmeneniia zashchishchennosti informatsionnoi sistemy ot nesanktsionirovannogo dostupa narushitelei. Informatsionno-upravliaiushchie sistemy, 2015, No. 1 (74), pp. 50-58, DOI: 10.15217/issn1684-8853.2015.1.50.
15. Probabilistic Modeling in System Engineering. By ed. A. Kostogryzov, London: IntechOpen, 2018. 278 pp.
16. Minakov V.F., Shepeleva O.Iu., Lobanov O.S. Resursno-vremennaia model' povysheniia zashchishchennosti konfidentsial'nykh dannykh. Sbornik trudov Desiatoi mezhdunarodnoi nauchno-tekhnicheskoi konferentsii "Bezopasnye informatsionnye tekhnologii" (Moskva, 3-4 dekabria 2019 g.), M. : MGTU im. N.E. Baumana, 2019, pp. 301-304.
17. Glinskiy V., Serga L., Zaykov K. Identification method of the russian federation arctic zone regions statistical aggregate as the object of strategy development and a source of sustainable growth. Procedia Manufacturing, 2017, v. 8, pp. 308-314.
18. Litvintseva G.P., Glinskiy V.V., Stukalenko E.A. Interregional differentiation of population incomes in the Russian Federation in the post-crisis period. Academy of Strategic Management Journal, 2017, v. 16, No. 4.
19. Glinskiy V., Serga L., Novikov A., Bulkina A., Litvintseva G. Investigation of correlation between the regions sustainability and territorial differentiation. Procedia Manufacturing, 2017, v. 8, pp. 323-329.
20. Borisov V.N., Kuvalin D.B., Pochukaeva O.V. Improving the factor efficiency of machinery in the regions of the Russian Federation. Studies on Russian Economic Development, 2018, v. 29, No. 4, pp. 377-386.
21. Borisov V.N., Pochukaeva O.V. Investment and innovative technological efficiency: Case study of the Arctic project. Studies on Russian Economic Development, 2017, v. 28, No. 2, pp. 169-179.
22. Ivanter V.V., Belkina T.D., Belousov D.R., Blokhin A.A., Borisov V.N. et al. Recovery of economic growth in Russia. Studies on Russian Economic Development, 2016, v. 27, No. 5, pp. 485-494.

ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ПРАВОВОГО РЕГУЛИРОВАНИЯ ФИНАНСОВЫХ ОТНОШЕНИЙ В ЦИФРОВОЙ ЭКОНОМИКЕ

Бачурин Д.Г.*

Ключевые слова: *цифровая экономика, правовое регулирование, финансовые отношения, финансовые услуги, цифровое право, информационная безопасность, специализированные принципы, информационная инфраструктура, компьютерные технологии, платежные платформы.*

Аннотация.

Цель: *совершенствование научно-методической базы теории правового регулирования финансовых отношений в условиях цифровой экономики.*

Методы: *системный и сравнительно-правовой анализ природы информационного обеспечения финансово-правовых институтов в условиях цифровой экономики.*

Результаты: *исследованы правовые аспекты формирования инфраструктурной среды цифровой экономики, перевода сервисного обслуживания финансовых операций в полностью автоматизированный режим выполнения, обеспечения информационной безопасности и устойчивости финансовых учреждений в условиях цифровой экономики; обоснована трёхкомпонентная система специализированных принципов правового регулирования финансовых отношений в условиях цифровой экономики; обоснован вывод о необходимости синхронизации развития процессов цифровизации и соответствующего правового регулирования; сформулированы рекомендации по совершенствованию финансово-правового регулирования: определение правовых принципов и процедур цифрового взаимодействия; юридическая регламентация электронного документа и цифрового архива; разработка правовых статусов машин с искусственным интеллектом и лиц, ответственных за функционирование таких объектов (производителей, владельцев, управляющих машинами).*

DOI: 10.21681/1994-1404-2020-1-47-56

Введение

Наибольшие сложности в регулировании финансово-правовых отношений, пронизывающих все сферы социальной деятельности, возникают в моменты качественных изменений в общественной жизни. Среди таких изменений, существенным образом трансформирующих социально-экономические отношения, следует выделить распространение *компьютерных* («*цифровых*») *технологий* [5] в совокупности с расширением доступа к интернету и мобильной связи. Эти изменения служат материальной базой перехода от традиционного индустриального хозяйства к новой информационной экономике, в которой создание и продажа услуг и товаров основаны на принципиально иных методах кодирования, накопления, обработки и передачи информации. По этой причине цифровую экономику можно рассматривать как *системно-структурированную совокупность экономических отношений*, развивающуюся на основе компьютерных технологий. Основное внимание в ней направлено не на совершенствование программного обеспечения, а на товары и услуги, реализуемые посредством электронных продаж.

Привлекательность новых технологий для финансово-кредитных учреждений довольно очевидна. Упрощение операционной интеграции, расширение возможностей интерактивного маркетинга и предложение онлайн-банкинга позволяют объединять предоставляемые услуги в единые пакеты, тем самым увеличивая число клиентов и размер прибыли.

Выгоды владельцев финансовых организаций лежат в плоскости снижения операционных издержек при замене персонала, действующего по заранее установленным правилам, на машинные алгоритмы. Уже сегодня можно наблюдать активное внедрение *новых форм работы*: через создание банковских площадок без сотрудников, где финансовые услуги предоставляются путем цифрового самообслуживания; расширение дистанционных сервисов (онлайн-банкинг) в сети интернет с применением стационарных и мобильных персональных компьютеров [2, 3].

* ***Бачурин Дмитрий Геннадьевич,*** *кандидат юридических наук, ведущий научный сотрудник сектора банковского, финансового, налогового и конкурентного права Института государства и права Российской академии наук, Российская Федерация, г. Москва.*

E-mail: 01ter@mail.ru

1. Правовое регулирование цифрового банкинга

С 2001 г. подавляющее большинство (80%) банков США практикуют электронный банкинг, а *Bank of America* переводит на эти услуги 3 *млн* клиентов (20% его клиентской базы)[1]. В 2009 г. 47% взрослых в США и 30% в Англии имеют активные цифровые (онлайн и мобильные) счета [18]. Согласно опросу, проведенному Японской ассоциацией банкиров (*JBA*) в 2012 г., 65,2% клиентов финансовых учреждений являются пользователями интернет-банкинга[2]. К 2013 г. объем мирового рынка информационных технологий оценивался в 1,7 *трлн долларов США*[3]. На начало 2020 г. услугами цифрового банкинга охвачено примерно 75% клиентов в более чем 95% от общего числа банков США, Англии и стран ЕС.

Важно, что в цифровом формате выполняются все международные расчеты. Они осуществляются через международную межбанковскую систему *SWIFT* (212 стран-участников системы), систему платежей США *Fedwire*, платежную платформу Европейского ЦБ *TARGET* 2 и интегрированные с ними национальные системы платежей отдельных стран.

Предоставление банковских сервисов и услуг практически всегда обслуживается интернет-сетями. По этой причине «цифровой банкинг» еще называют «интернет-банкингом» (*i-banking*). Если провести сравнение традиционной банковской деятельности с цифровым банковским учреждением, то можно выделить следующие характерные черты новых банковских сервисов:

- предоставление банковских услуг с использованием сетей электронных коммуникаций, дополняющих традиционные способы коммуникаций;
- виртуализация самого интернет-банка, материальным воплощением которого становится не банковский офис с мебелью, оргтехникой, денежными хранилищами и сотрудниками, а компьютерный сервер, выполняющий функции сбора, передачи, обработки и хранения информации о клиентах и проводимых ими операциях;
- визуализация цифровых банковских услуг осуществляется не путем живого общения с персоналом банка, а через выполнение клиентом цифрового банка алгоритмической последовательности действий, предлагаемых веб-сайтом такого виртуального банка;
- предоставление не только всего спектра традиционных банковских услуг (услуги по оплате счетов и переводу денежных средств; получение и обслуживание кредитов; ведение инвестиционных проектов; торговля на фондовом рынке; получение сопутствующих финансовых сервисов, дополняющих и обеспечивающих основной перечень банковских услуг), которые выполняются с применением кредитных карт, банкоматов (в том числе и принадлежащих другим организациям)[4], но и предложение разнообразных и постоянно совершенствующихся комплексных «финтех-продуктов», несущих в себе черты и финансов, и технологий (одноранговое кредитование (*P2P*), в том числе с применением кредитных платформ; краудфандинг и дистанционное управление капиталом, в том числе управление личными финансами, онлайн-фондами, электронными кошельками; брокерские онлайн-услуги);
- применение искусственного интеллекта и финансовых технологий, развитие которых идет на основе математических концепций, например, таких, как «облачные вычисления» (*cloud computing*) [4] и «большие данные» (*Big Data*) [14];
- цифровой *i-banking* активно трансформирует рынок финансовых услуг, с явно проявляющейся тенденцией к его децентрализации, со снижением роли традиционных банков и страховых организаций.

В США юридическое регулирование в области цифрового банкинга осуществляется с применением законодательных актов и судебных прецедентов. До начала 2010-х гг. такое регулирование выполняется в основном на основе правовых актов, относящихся к традиционной банковской деятельности.

В ряду ныне действующих актов специализированного законодательства, предусматривающего гарантии защиты прав клиентов финансовых учреждений, выделяется Закон Додда-Франка, принятый в 2009 г. (Dodd-Frank Act), согласно которому учреждается Бюро финансовой защиты потребителей, и Закон об экономическом росте, нормативно-правовом регулировании и защите прав потребителей (Economic Growth, Regulatory Relief, and Consumer Protection Act — EGRRCPA)[5], принятый в 2018 г. Закон EGRRCPA обязывает федеральные банковские агентства всемерно содействовать экономическому росту, делая финансовые услуги более справедливыми для потребителя.

В настоящее время в ряде других стран, в частности, в Китае, Индии, Южной Корее, осуществляются плановые работы по развитию индустрии искусственного интеллекта нового поколения, но практически нет всеобъемлющей правовой базы для защиты данных. Комитет экспертов правительства Индии 27 июля 2018 г. опубликовал проект закона о защите личных данных[6].

---

[1] См.: *Veeraghanta M.* Is Your Digital Banking Vendor Hurting Adoption Rates? The Financial Brand, 2017, URL: https://thefinancialbrand.com/68577/optimal-digital-banking-vendor-selection/ .

[2] URL: http://www.kokusen.go.jp/pdf/n-20001005_3.pdf .

[3] Распоряжение Правительства РФ от 01.11.2013 № 2036-р «Об утверждении Стратегии развития отрасли информационных технологий в Российской Федерации на 2014—2020 годы и на перспективу до 2025 года» // Собрание законодательства РФ. 2013. № 46. Ст. 5954.

[4] См.: *Banerjee R.* Internet Banking — Legal Issues. URL: http://rajdeepandjoyeeta.com/internet-banking-legal-issues/

[5] Economic Growth, Regulatory Relief, and Consumer Protection Act, URL: https://www.congress.gov/bill/115th-congress/senate-bill/2155/text .

[6] Personal Data Protection Bill, 2018, URL: http://meity.gov.in/writereaddata/files/Personal_Data_Protection _Bill,2018.pdf .

Индийский законопроект предусматривает специальную группу прав, связанных с правом протеста против автоматического принятия решений и доступа к логике, стоящей за ним. Эти права связаны с большими данными, поступающими в распоряжение систем искусственного интеллекта, и имеют законное обоснование. Они нацелены на ограничение вреда, возникающего в связи с возможными предубеждениями и дискриминацией в выходных данных из-за оценочных определений без анализа человеком. Решение может состоять в том, чтобы просто включить этап человеческого анализа, который сам по себе не защищен от предрассудков. Такое изменение может потребоваться при условии, что оно тщательно адаптировано к конкретным организациям и характеру их деятельности по обработке данных.

На наш взгляд, этого лучше достичь с помощью системы подотчетности, которая требует определенных фидуциариев данных, которые могут принимать оценочные решения с помощью автоматизированных средств, для организации процессов, которые отсеивают дискриминацию. Этот регулирующий механизм является составным элементом конфиденциальности, который должен быть введен в действие заблаговременно, периодически проверяться и контролироваться.

Представляется, что необходимо предусмотреть возможность юридических ограничений практики некорректной обработки данных. Очевидно, что наиболее действенным способом такой защиты может быть механизм *судебной защиты* нарушенного права [11]. В то же время такая модель не вполне обнажает сущность негативного воздействия. Например, если дискриминация субъекта цифровых отношений возникла в результате, по сути, законной, но дискриминационной по результату автоматической обработки данных.

2. Информационная безопасность и устойчивость финансовых учреждений

В процессе постепенной реорганизации банковской отрасли, связанном с развитием информационных технологий, распространением персональных компьютеров среди домашних хозяйств, интернет-банкингом, телефонным банковским обслуживанием, выявляется необходимость в принятии мер *предосторожности* при использовании новых услуг. С середины 2000-х гг. отмечается, что онлайн-банкинг не может работать вне режима безопасности клиентской информации, напрямую связанного с репутационными рисками самих банков[7].

Атаки на онлайн-банкинг в основном основаны на обмане пользователя с целью кражи данных для входа и действительных *TAN (Transaction authentication number)*. Среди наиболее известных способов кражи регистрационной информации следует выделить:

фишинг (англ. *phishing* — «рыбная ловля») — проведение массовых рассылок электронных писем от имени популярных брендов для получения доступа к конфиденциальным данным пользователей (логинам и паролям);

фарминг (англ. *pharming*) — скрытное перенаправление жертвы на ложный сайт (или *IP*-адрес);

межсайтовый скриптинг (англ. *Cross-Site Scripting*, *XSS*) — внедрение страницы вредоносного кода в компьютер пользователя и взаимодействие этого кода с веб-сервером злоумышленника для получения авторизованных данных пользователя или расширенного доступа. Вредоносный код проникает через уязвимость в веб-сервере или через уязвимость на компьютере пользователя;

кейлоггер (от англ. *keylogger*, *key* — клавиша и *logger* — регистрирующее устройство) — программное обеспечение или аппаратное устройство, отмечающее нажатие клавиш на клавиатуре компьютера и манипуляции с мышью;

троянские вирусные программы — вредоносные программы, внедряемые в компьютер под видом легального программного обеспечения с целью сбора, изменения и удаления информации о пользователе, а также использования ресурсов компьютера для майнинга или нелегальной торговли;

атаки на основе сигнатур, которые состоят в применении программного обеспечения так, чтобы на экране отображались правильные транзакции, а фактически проводимые сфальсифицированные транзакции подписывались в фоновом режиме.

Компьютерные вторжения, осуществляемые на основе перечисленных и вновь разработанных приемов, имеют тенденцию к постоянному увеличению убытков банков и ущерба их клиентов. В 2008 г. в американских банках выявлено 536 случаев компьютерного вторжения во время онлайн-банкинга со средней потерей 30 *тыс. долл.* на один инцидент. В 80% случаев источник вторжения неизвестен [17]. Исследователи Кембриджского университета указывают на удвоение за период с 2011 г. по 2017 г. объемов мошенничества в сфере онлайн-банкинга Англии[8].

Вопросы обеспечения *информационной безопасности* [7, 8, 10] и устойчивости финансовых учреждений в условиях цифровой экономики трудно переоценить. Они должны оперативно решаться по мере расширения информатизации процессов общественной жизни. Особое внимание необходимо уделять «болевым точкам» критично важной инфраструктуры электронного накопления, обработки и обмена информацией.

Среди них следует особо выделить следующие *проблемы*: нарушение финансовой стабильности в деятельности финансово-кредитных учреждений в ре-

[7] См.: Werani T. Business-to-Business-Marketing. Praxisorientiertes Business-to-Business-Marketing. Gabler, 2006, pp. 3-13.

[8] См.: *Kundaliya D.* Online banking fraud has doubled since 2011. Cambridge University, 2019, 31 May, URL: https://www.computing.co.uk/news/3076586/online-banking-frauds-doubled-in-the-seven-year-period-from-2011-to-2017-study-finds .

зультате компьютерных атак на их информационные ресурсы; удержание доверия контрагентов кредитных организаций к надежности предлагаемых электронных сервисов; обеспечение достоверности сведений о фактах нарушений защиты информации при осуществлении банковских операций; снижение непосредственного финансового ущерба клиентов банковских организаций в связи с несанкционированными финансовыми транзакциями (денежные переводы средств без распоряжения клиента).

Формирование инфраструктурной среды *информационной экономики*, развитие цифровых платформ, перевод сервисного обслуживания финансовых операций в полностью автоматизированный режим, применение открытых стандартов и протоколов обусловливает резкое возрастание информационных *рисков* и требует соответствующего развития правового регулирования. По этой причине органы государственной власти сосредотачивают свое внимание на важности решения вопросов регулирования в данной сфере общественных отношений [1].

Начало данного направления в нашей стране было оформлено в 2008 г. с утверждением Стратегии развития информационного общества, которая нацеливает на признание постиндустриальных информационных и телекоммуникационных технологий в качестве ключевых факторов увеличения добавленной стоимости в экономике и общей конкурентоспособности Российской Федерации[9].

Последующее принятие актов правового регулирования[10] в сфере цифровых технологий выделяет основные магистральные направления ее развития: создание современной информационно-телекоммуникационной инфраструктуры и развитие сервисов на основе информационно-телекоммуникационных технологий; обеспечение прав и основных свобод человека в информационном обществе; развитие технологий защиты информации, способных обеспечивать неприкосновенность частной жизни и безопасность информации ограниченного доступа; осуществление юридически значимых действий в электронном формате и др.

В концентрированном виде на решение указанных задач нацелен один из 17 национальных проектов, реализуемых по инициативе Президента Российской Федерации. В частности, национальная программа «Цифровая экономика Российской Федерации» содержит определение ключевых *целей* проекта в виде «создания устойчивой и безопасной информационно-телекоммуникационной инфраструктуры высокоскоростной передачи, обработки и хранения больших объемов данных, доступной для всех организаций и домохозяйств»[11]. Не случайно авторы программы в качестве двух ее базовых направлений (кроме обеспечения технических и кадровых условий) определяют нормативное регулирование и информационную безопасность.

Следует указать, что вопросы правового регулирования практически полностью охватывают юридическую составляющую регламентации информационной безопасности, выстраиваемой во взаимодействии с развивающимися правовыми институтами идентификации личности, персональных данных, электронной подписи, передачи цифровой информации, различных видов защищаемой законом тайны в системе конфиденциальной информации.

Принимая во внимание комплексный характер современного *информационного права* [6], развитие которого происходит на основе публично-правовых и частноправовых методов регулирования, специалисты ведут речь о необходимости выделения юридических вопросов цифровизации в отдельную подотрасль права [15] с оформлением соответствующих специализированных институтов, а также принятием необходимых норм других отраслей права.

Это предложение нашло законодательное подкрепление в 2019 г., когда в Гражданский кодекс (ГК) РФ были внесены базовые нормы юридического регулирования экономических отношений в цифровой среде[12]. В частности: «цифровые права» отнесены к объектам гражданских прав (ст. 128 ГК РФ); закреплено определение «цифровых прав», дана характеристика и определен субъект правоотношений (ст. 141.1 ГК РФ); идентифицированы дистанционные сделки, осуществляемые с помощью электронных технических средств (ст. 434 ГК РФ); предусмотрены ограничения для использования электронных средств (ст. 1124 ГК РФ); уточнено понятие «самоисполняемой сделки», выполняемой путем применения информационных технологий, определенных условиями такой сделки (ст.309 ГК РФ). Например: смарт-контракты, банковские автоматические платежи.

Важно заметить, что законодатель и регулятор достаточно своевременно среагировали на активное на-

[9] Стратегия развития информационного общества в Российской Федерации (утв. Президентом РФ 7 февраля 2008 г. № Пр-212) // РГ. 2008. № 34. 16 фев.

[10] Постановление Правительства РФ от 15 апреля 2014 г. № 313 «Об утверждении государственной программы Российской Федерации «Информационное общество (2011—2020 годы)» // Собрание законодательства РФ. 2014. № 18 (часть II). Ст. 2159; Распоряжение Правительства РФ от 1 ноября 2013 г. № 2036-р «Об утверждении Стратегии развития отрасли информационных технологий в Российской Федерации на 2014—2020 годы и на перспективу до 2025 года» // Собрание законодательства РФ. 2013. № 46. Ст. 5954; Распоряжение Правительства РФ от 8 декабря 2011 г. № 2227-р «Об утверждении Стратегии инновационного развития Российской Федерации на период до 2020 года» // Собрание законодательства РФ. 2012. № 1. Ст. 216; Распоряжение Правительства РФ от 17 ноября 2008 г. № 1662-р «О Концепции долгосрочного социально-экономического развития Российской Федерации на период до 2020 года» // Собрание законодательства РФ. 2008. № 47. Ст. 5489; Указ Президента РФ от 7 мая 2012 г. № 596 «О долгосрочной государственной экономической политике» // РГ. 2012. 9 мая.

[11] URL: http://government.ru/projects/selection/741/35675/ (дата обращения: 10.12.2019).

[12] Федеральный закон от 18 марта 2019 г. № 34-ФЗ «О внесении изменений в части первую, вторую и статью 1124 части третьей Гражданского кодекса Российской Федерации» // Собрание законодательства РФ. 2019. № 12. Ст. 1224.

растание информационных угроз в финансовой сфере Российской Федерации. В условиях расширения объемов платежных операций за 2017 г. с использованием платежных карт было совершено 317 тыс. несанкционированных операций на сумму 961,3 *млн руб*., а за 2018 г. 417 тыс. таких операций на общую сумму 1384,7 *млн руб*.[13].

При решении задач обеспечения и контроля информационной безопасности (ИБ), противодействия информационным угрозам в кредитно-финансовой сфере основные усилия были направлены на реализацию требований Федерального закона от 27 июня 2018 г. № 167-ФЗ[14] и Федерального закона от 27 июня 2011 г. № 161-ФЗ[15].

С этой целью Банком России были приняты экстренные меры. Введено в действие Указание Банка России № 4926-У1 от 8 октября 2018 г.[16], определяющее специальные процедуры и формы для ведения информационного обмена сообщениями о попытках осуществления переводов денежных средств без согласия клиента. Стандартом СТО БР БФБО-1.5-20182 с 1 ноября 2018 г.[17] уточнены рамки взаимодействия Банка России с субъектами системы информационного обмена в целях выявления инцидентов нарушений защиты информации.

К началу 2019 г. к базе информационного обмена (АСОИ ФинЦЕРТ[18]) подключены все кредитные организации Российской Федерации. С момента начала работы 26 сентября 2018 г. до конца 2018 г. АСОИ ФинЦЕРТ зафиксировано 15 607 финансовых операций без согласия клиента, выполнены мероприятия по приостановлению и блокировке платежей на общую сумму более 40 *млн руб*.

Сформирована первичная правовая база по обеспечению защиты прав человека и гражданина при обработке его биометрических персональных данных при проведении идентификации. В соответствии с частью 14 ст. 14.1 Федерального закона от 27 июля 2006 г. № 149-ФЗ[19] принято совместное Указание Банка России и Публичного акционерного общества «Ростелеком» № 4859-У/01/01/782-184 от 9 июля 2018 г.[20], регламентирующее ответственный сбор, хранение и обработку персональных данных в единой информационной системе.

Вместе с этим законодатель предпринимает меры по повышению эффективности уголовной ответственности за правонарушения в сфере цифровой экономики[21]. В частности, за хищение средств с банковского счета (ч.3 ст.158 УК РФ) и совершение мошенничества с использованием электронных средств платежа (ст. 159.6 УК РФ) предусмотрена ответственность до 6 лет лишения свободы.

3. Система принципов правового регулирования финансовых отношений в цифровой экономике

Сложность правового регулирования в сфере цифровой экономики в целом и финансовых услуг в частности обусловлена достаточно длительными параллельно протекающими процессами:

распространения цифровизации: по горизонтали — через рост числа пользователей, по вертикали — через охват властных и вертикально-интегрированных структур, по глубине — через создание новых электронных сервисов и услуг;

развития юридических конструкций, внедряемых в цифровые отношения;

адаптации основных элементов правовой системы под электронные реалии социально-экономических отношений.

Цифровая экономика через расширенные электронные сети предоставляет инструменты преобразования отраслей услуг и отдельных экономических структур для открытого и подотчетного сотрудничества[22]. О масштабах этого явления свидетельствует тот

---

[13] URL: http://www.cbr.ru/analytics (дата обращения: 10.12.2019).

[14] Федеральный закон от 27 июня 2018 г. № 167-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части противодействия хищению денежных средств» // Собрание законодательства РФ. 2018. № 27. Ст. 3950.

[15] Федеральный закон от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе» // Собрание законодательства РФ. 2011. № 27. Ст. 3872.

[16] Указание Банка России от 8 октября 2018 г. № 4926-У «О форме и порядке направления операторами по переводу денежных средств, операторами платежных систем, операторами услуг платежной инфраструктуры в Банк России информации обо всех случаях и (или) попытках осуществления переводов денежных средств без согласия клиента и получения ими от Банка России информации, содержащейся в базе данных о случаях и попытках осуществления переводов денежных средств без согласия клиента, а также о порядке реализации операторами по переводу денежных средств, операторами платежных систем, операторами услуг платежной инфраструктуры мероприятий по противодействию осуществлению переводов денежных средств без согласия клиента».

[17] Стандарт Банка России СТО БР БФБО-1.5-2018 «Безопасность финансовых (банковских) операций. Управление инцидентами информационной безопасности. О формах и сроках взаимодействия Банка России с участниками информационного обмена при выявлении инцидентов, связанных с нарушением требований к обеспечению защиты информации», введенный в действие Приказом Банка России от 14 сентября 2018 г. № ОД-2403.

[18] Автоматизированная система обработки инцидентов Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Департамента информационной безопасности Банка России.

[19] Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

[20] Указание Банка России и Публичного акционерного общества «Ростелеком» от 09.07.2018 № 4859-У/01/01/782-18 «О перечне угроз безопасности, актуальных при обработке, включая сбор и хранение, биометрических персональных данных, их проверке и передаче информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации в государственных органах, банках и иных организациях, указанных в абзаце первом части 1 статьи 14.1 Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», в единой информационной системе» // Собрание законодательства РФ, 2006. № 31 (1 ч.), ст. 3448.

[21] Федеральный закон от 23 апреля 2018 г. №111-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации» // Собрание законодательства РФ. 2018. № 18. Ст. 2581.

[22] URL: http://www.ericsson.com/res/thecompany/docs/publications/business-review/2014/mastering-digital-transformation-a-policy-makers-guide.pdf .

Таблица

Классификация принципов правового регулирования финансовыми отношениями в цифровой экономике

Факторы влияния	Специализированные принципы
Публично-правовой (общесоциальный)	Принцип учета общественных интересов при проектировании правового регулирования цифровых услуг
	Принцип учета мнений всех заинтересованных общественных групп при принятии решений о правовом регулировании отношений в области цифровых услуг
	Принцип координации действий федеральных и региональных органов исполнительной власти, местного самоуправления и гражданского общества по развитию цифровой экономики
Частноправовой	Принцип обеспечения потребителей услуг предсказуемыми уровнями защиты
	Принцип приоритета прав потребителей цифровых услуг
	Принцип цифрового резидентства физических и юридических лиц
Технико-правовой	Принцип тщательности и всесторонности анализа предлагаемых сервисов и услуг
	Принцип неразрывности в обеспечении характеристик эффективности, надежности и безопасности цифрового управления
	Принцип последовательного совершенствования правового регулирования
	Принцип применения преимущественно национального (российского) технического оборудования, программного обеспечения и технологий защиты информации
	Принцип комплексной оценки влияния рисков

факт, что сегодня более 82% потенциальных потребителей в мировой экономике движутся к сетевому образу жизни[23].

Очевидно, что подобное развитие предполагает достаточную гибкость, ясность и широкое распространение соответствующих режимов регулирования, которые объективно должны быть сосредоточены на важнейших социальных задачах и общественно принимаемых правилах их достижения посредством предоставления цифровых услуг и новых возможностей для потребителей[24].

Стратегическим приоритетом здесь выступает разработка *нормативной правовой базы* [11, 12], которая должна отражать базовые ценности, связывающие структуры цифровых услуг, четко определять нормативно-закрепляемые цели и учитывать весь спектр исторических, текущих и вновь возникающих рисков [17].

При проектировании нормативной правовой базы цифровых услуг следует руководствоваться четкими правовыми ориентирами, базирующимися на системе обоснованных принципов [9]. Формализация наиболее важных из них позволяет выделить следующую группу специализированных норм-принципов (см. таблицу), выявленных в ходе системного анализа развития цифровых технологий, искусственного интеллекта, робототехники и отдельных особенностей их юридического положения в ряде зарубежных стран.

Принцип учета и согласования общественных интересов при проектировании правового регулирования цифровых услуг. Данный принцип заключается в том, что никакие правила не должны быть навязаны участникам цифровых правоотношений без свидетельства явно выраженного общественного интереса. Этот принцип особенно важен, когда выясняется, что приоритеты социальной политики или политики безопасности воплощаются в более широком контексте, чем этого требуют коммерческие интересы.

Принцип учета мнений всех заинтересованных общественных групп при принятии решений о правовом регулировании цифровых услуг. Консультации со всеми заинтересованными сторонами важны, чтобы избежать непреднамеренных последствий, возникающих в связи с принятием новой политики или новых правил. Опыт зарубежных стран свидетельствует, что максимально репрезентативные консультации помогают достигать эффективной результативности в определении уровней защиты потребителей при одновременном развитии конкуренции.

Принцип координации действий федеральных и региональных органов исполнительной власти, местного самоуправления и гражданского общества по развитию цифровой экономики. Данный принцип подчеркивает важность тесного взаимосогласованного сотрудничества в решении вопросов развития цифровой экономики всеми заинтересованными участниками отношений. В числе вопросов, разрешаемых на основе применения данного принципа, в частности, могут быть следующие: определение источников бюджетного и внебюджетного финансирования мероприятий (исследований и разработок) технического и норма-

[23] URL: http://www.ericsson.com/res/docs/2015/consumerlab/ericsson-consumerlab-the-network ed-life.pdf .

[24] URL: http://www.iccwbo.org/Advocacy-Codes-and-Rules/Document-centre/2012/ICC-policy-statement-on-business-views-on-regulatory-aspects-of-cloud-computing/ .

тивно-правового оснащения цифровой экономики; выработка и описание ключевых компетенций действующих в ней субъектов; описание регламентов и стандартов регулирования; организация фундаментальных и прикладных исследований, пилотных проектов и экспертных оценок и др.

Принцип приоритета прав потребителей цифровых услуг предполагает опору на существующее законодательство о защите прав потребителей, положения которого должны иметь очевидное предпочтение перед новыми предписаниями.

Принцип обеспечения потребителей услуг предсказуемыми уровнями защиты. С целью обеспечения защиты потребителей и сохранения стимулов для дальнейшего развития законодатель должен учитывать широкий круг преднамеренных и непреднамеренных последствий применения новых правил. Например, такие угрозы могут быть связаны с построением сложных иерархических информационных и компьютерных систем [16], применяющих виртуализацию, удаленные (облачные) хранилища данных личности, объединений граждан и организаций бизнеса.

Принцип цифрового резидентства физических и юридических лиц. Важность данного принципа обусловлена ранее неизвестными угрозами и вызовами, которые способны к проникновению и активному действию в пространстве цифровой экономики. Не случайно в программе «Цифровая экономика Российской Федерации», утвержденной распоряжением Правительства РФ от 28 июля 2017 г. № 1632-р (*утратило силу*), особо отмечены проблемы обеспечения прав человека в цифровом мире, в том числе при его идентификации, выступающей в виде процедуры соотнесения человека с его цифровым образом или фрагментарными его характеристиками. В данном контексте должны также рассматриваться задачи сохранности цифровых данных пользователей и обеспечения доверия граждан к цифровой среде. Можно также обоснованно предположить, что в уже в ближайшей перспективе возможна постановка вопроса о «резидентстве» машинных систем. Обзоры зарубежной литературы по данной тематике свидетельствуют о том, что он уже перешел из области научной фантастки в число актуальных для исследователей США, Южной Кореи и Японии.

Принцип комплексной оценки влияния рисков. Внедрение такой оценки должно предусматривать максимально полный и четкий анализ всей совокупности возможных рисков принимаемых нововведений.

Принцип тщательности и всесторонности анализа предлагаемых сервисов и услуг. Необходимо определить, какие услуги являются конкурирующими, заменяемыми или аналогичными уже имеющимся на современных финансовых рынках. Особенное внимание следует сосредоточить на выявлении и воспрепятствовании применению так называемых «недопустимых инноваций». Эксперты Международной торговой палаты относят к ним такие технологии и бизнес-модели, которые могут привести к разрушительным последствиям для экономики или нанесению ущерба отдельным потребителей финансовых услуг[25].

Принцип неразрывности в обеспечении характеристик эффективности, надежности и безопасности цифрового управления приобретает особую значимость в контексте неуклонного нарастания враждебного технического воздействия на критично значимую информационную инфраструктуру и стремительное увеличение возможностей международной компьютерной преступности.

Принцип применения преимущественно национального (российского) технического оборудования, программного обеспечения и технологий защиты информации. Совершенно ясно, что без создания собственной элементной базы информационной инфраструктуры не представляется возможным достижение полноценной и устойчивой работы отечественной цифровой экономики. Это вдвойне очевидно, если приходится выстраивать такую сложную систему в достаточно агрессивном окружении [7, 8].

Принцип последовательного совершенствования правового регулирования. Юридические рамки не должны существенно отставать от стремительно развивающихся технологий. Модернизация [12, 13] нормативного обеспечения предполагает систематическое обновление с целью принятия регламентов, которые должны соответствовать новым фактам цифровой экономики, или отказа от правил, которые более не являются обоснованными.

Исследование предлагаемой группы специализированных принципов обнаруживает, что они могут быть классифицированы по отдельным видовым признакам. Например: системно-факторный анализ позволяет выделить три основные взаимосвязанные группы принципов, обусловленные воздействием соответствующих трех основных факторов (см. таблицу): публично-правового (общесоциального), частноправового и технико-правого характера.

Представленная классификация является условной. Фактор *неопределенности*, приобретающий доминирующее влияние в условиях глобальной социально-экономической турбулентности, не позволяет в деталях описать юридические характеристики не только самого здания, но даже несущего каркаса цифровой экономики.

В таких условиях необходимо не только тщательно развивать функцию соответствующего правового регулирования, но и своевременно упорядочивать и систематизировать процессы цифровизации современной экономики.

Достаточно часто эти процессы требуют тщательно выверенной *синхронизации*. В частности, в данной плоскости находится решение вопросов определения *правового статуса*: специализированных роботов и в целом машин с искусственным интеллектом, а также лиц, ответственных за функционирование таких объектов (произ-

[25] ICC policy statement on Regulatory Modernization in the Digital Economy. URL: https://iccwbo.org/publication/icc-policy-statement-on-regulatory-modernization-in-the-digital-economy/ .

водителей, владельцев, управляющих машинами и др.). Этот принципиально важный уже в самой ближайшей перспективе вопрос не может решаться в отрыве от нарождающейся практики применения таких объектов, потому что нельзя заранее предвидеть всех нюансов правового поля складывающейся цифровой реальности.

В деле совершенствования юридического инструментария, применяемого при цифровизации финансовых услуг, представляется необходимым также отметить важность разработки, в частности, таких категорий, институтов и понятий цифрового права, как: правовые процедуры и принципы цифрового взаимодействия, юридическая регламентация электронного документа и цифрового архива.

В этой связи существенным ресурсом проектирования российского цифрового законодательства могут стать сравнительно-правовые исследования современного зарубежного опыта правового регулирования в данной сфере отношений. Многие из вышеназванных вопросов уже находят свое юридическое воплощение в актах законодательства и судебных прецедентах США, Южной Кореи, Японии, Сингапура и других зарубежных стран.

Заключение

Искусственный интеллект и робототехника подрывают системы, которые люди приводили в действие на протяжении тысячелетий, включая производство, гражданские свободы, образование, социальные услуги, научный прогресс и саму природу знаний. Отношения человечества с компьютерами кардинально меняются, но перспективы влияния искусственного интеллекта на общество и экономику остаются неясными.

В этой связи существенным ресурсом проектирования российского цифрового законодательства могут стать дальнейшие исследования современного зарубежного опыта правового регулирования в данной сфере отношений. Многие из вышеназванных вопросов уже находят свое юридическое воплощение в актах законодательства и судебных прецедентах США, Южной Кореи, Новой Зеландии, Китая, Индии, Японии, Сингапура, Индонезии и других зарубежных стран.

Большинство зарубежных стран в 2017—2018 гг. вступили в стадию правового проектирования. Именно в этот период можно наблюдать активное формирование ответственных организационных структур, обсуждения и консультации с экспертным и предпринимательским сообществом, выражение мнений со стороны потребителей, разработку нормативных актов, имеющих преимущественно предварительный характер, как по содержанию, так и времени действия. В таких условиях необходимо не только тщательно развивать функцию соответствующего правового регулирования, но и своевременно упорядочивать и систематизировать процессы цифровизации современной экономики.

Рецензент: ***Запольский Сергей Васильевич,*** *доктор юридических наук, профессор, заслуженный юрист Российской Федерации, главный научный сотрудник Института государства и права Российской академии наук, Российская Федерация, г. Москва.*
E-mail: zpmoscow@mail.ru

Литература

1. Андреев В. К. О понятии цифровых прав и их оборотоспособности // Журнал предпринимательского и корпоративного права. 2018. № 8. С. 38—41.
2. Ващекин А. Н., Ващекина И. В. Противодействие преступной деятельности в условиях развития цифровых технологий дистанционного банковского обслуживания // Правовая информатика. 2019. № 4. С. 86—95. DOI: 10.21681/1994-1404-2019-4-86-95.
3. Ващекин А.Н., Ващекина И. В. Структурная особенность банковской системы РФ и динамика основных показателей ее функционирования // Научное обозрение. Экономические науки. 2019. № 1. С. 5—10.
4. Ефименко А. А., Федосеев С. В. Организация инфраструктуры облачных вычислений на основе SDN сети // Экономика, статистика и информатика. Вестник УМО. 2013. № 5. С. 185—187.
5. Ловцов Д. А. Основы технологии эффективного двухуровневого правового регулирования информационных отношений в инфосфере // Правовая информатика. 2018. № 2. С. 4—14. DOI: 10.21681/1994-1404-2018-2-04-14.
6. Ловцов Д. А. Теория информационного права: базисные аспекты // Государство и право. 2011. № 11. С. 43—51.
7. Ловцов Д. А. Обеспечение информационной безопасности в российских телематических сетях // Информационное право. 2012. № 4. С. 3—7.
8. Ловцов Д. А. Проблема гарантированного обеспечения информационной безопасности крупномасштабных автоматизированных систем // Правовая информатика. 2017. № 3. С. 66—74. DOI: 10.21681/1994-1404-2017-3-66-74.
9. Ловцов Д. А. Система принципов эффективного правового регулирования информационных отношений в инфосфере // Информационное право. 2017. № 1. С. 13—18.
10. Ловцов Д. А., Верхоглядов А. А. Информационная безопасность судебных автоматизированных информационных систем: правовое регулирование и юрисдикция // Российское правосудие. 2008. № 8. С. 55—64.

11. Ловцов Д. А., Ниесов В. А. Обеспечение единства судебной системы России в инфосфере: концептуальные аспекты // Российское правосудие. 2006. № 4. С. 35—40.
12. Ловцов Д. А., Ниесов В. А. Модернизация информационной инфраструктуры судопроизводства — ключевое направление оптимизации нагрузки на судебную систему // Российское правосудие. 2014. № 9. С. 30—40.
13. Ловцов Д. А., Ниесов В. А. Проблемы и принципы системной модернизации «цифрового» судопроизводства // Правовая информатика. 2018. № 2. С. 15—22. DOI: 10.21681/1994-1404-2018-2-15-22.
14. Федосеев С. В. Применение современных технологий больших данных в правовой сфере // Правовая информатика. 2018. № 4. С. 50—58. DOI: 10.21681/1994-1404-2018-4-50-58.
15. Хабриева Т.Я., Черногор Н.Н. Право в условиях цифровой реальности // Журнал российского права. 2018. № 1. С. 85—102.
16. Черных А. М. Основные направления интеграции федеральных государственных информационных систем и пространственных данных // Правовая информатика. 2018. № 2. С. 47—56. DOI: 10.21681/1994-1404-2018-2-47-56.
17. Deighton-Smith R., Erbacci A., Kauffmann C. Promoting inclusive growth through better regulation: The role of regulatory impact assessment. OECD Regulatory Policy Working Papers. Paris: OECD Publishing, 2016, No. 3, DOI: http://dx.doi.org/10.1787/5jm3tqwqp1vj-en .
18. Rishi P. Maximizing Business Performance and Efficiency Through Intelligent Systems. Hershey, 2017, 255 pp.

INFORMATION SUPPORT FOR LEGAL REGULATION OF FINANCIAL RELATIONS IN DIGITAL ECONOMY

Dmitrii Bachurin, *Ph.D. (Law), Leading Researcher at the Sector of Banking, Financial, Tax, and Competition Law of the Institute of State and Law of the Russian Academy of Sciences, Russian Federation, Moscow.*
E-mail: 01ter@mail.ru

Keywords: *digital economy, legal regulation, financial relations, financial services, digital law, information security, specialised principles, information infrastructure, computer technologies, payment platforms.*

Abstract.
Purpose of the paper: *improving the scientific and methodological basis of the theory of legal regulation of financial relations under the conditions of digital economy.*
Methods used: *a system and comparative law analysis of the nature of information support of financial and legal institutions under the conditions of digital economy.*
Results obtained: *legal aspects of formation of the infrastructure environment of digital economy, transfer of financial transactions servicing to a fully automated execution mode, ensuring information security and stability of financial institutions under the conditions of digital economy are studied. A justification is given for a three-component system of specialised principles of legal regulation of financial relations in digital economy as well as for a conclusion that digitalisation processes development and corresponding legal regulations need to be synchronised. The following recommendations for improving the financial and legal regulation are given: determination of legal principles and procedures for digital interaction; legal regulation of electronic documents and digital archives; development of the legal status of machines with artificial intelligence and persons responsible for the operation of such objects (manufacturers, owners, machine operators).*

References

1. Andreev V. K. O poniatii tsifrovykh prav i ikh oborotosposobnosti. Zhurnal predprinimatel'skogo i korporativnogo prava, 2018, No. 8, pp. 38-41.
2. Vashchekin A. N., Vashchekina I. V. Protivodeistvie prestupnoi deiatel'nosti v usloviiakh razvitiia tsifrovykh tekhnologii distantsionnogo bankovskogo obsluzhivaniia. Pravovaia informatika, 2019, No. 4, pp. 86-95, DOI: 10.21681/1994-1404-2019-4-86-95.
3. Vashchekin A.N., Vashchekina I. V. Strukturnaia osobennost' bankovskoi sistemy RF i dinamika osnovnykh pokazatelei ee funktsionirovaniia. Nauchnoe obozrenie, Ekonomicheskie nauki, 2019, No. 1, pp. 5-10.
4. Efimenko A. A., Fedoseev S. V. Organizatsiia infrastruktury oblachnykh vychislenii na osnove SDN seti. Ekonomika, statistika i informatika, Vestnik UMO, 2013, No. 5, pp. 185-187.
5. Lovtsov D. A. Osnovy tekhnologii effektivnogo dvukhurovnevogo pravovogo regulirovaniia informatsionnykh otnoshenii v infosfere. Pravovaia informatika, 2018, No. 2, pp. 4-14, DOI: 10.21681/1994-1404-2018-2-04-14.

6. Lovtsov D. A. Teoriia informatsionnogo prava: bazisnye aspekty. Gosudarstvo i pravo, 2011, No. 11, pp. 43-51.
7. Lovtsov D. A. Obespechenie informatsionnoi bezopasnosti v rossiiskikh telematicheskikh setiakh. Informatsionnoe pravo, 2012, No. 4, pp. 3-7.
8. Lovtsov D. A. Problema garantirovannogo obespecheniia informatsionnoi bezopasnosti krupnomasshtabnykh avtomatizirovannykh sistem. Pravovaia informatika, 2017, No. 3, pp. 66-74, DOI: 10.21681/1994-1404-2017-3-66-74.
9. Lovtsov D. A. Sistema printsipov effektivnogo pravovogo regulirovaniia informatsionnykh otnoshenii v infosfere. Informatsionnoe pravo, 2017, No. 1, pp. 13-18.
10. Lovtsov D. A., Verkhogliadov A. A. Informatsionnaia bezopasnost' sudebnykh avtomatizirovannykh informatsionnykh sistem: pravovoe regulirovanie i iurisdiktsiia. Rossiiskoe pravosudie, 2008, No. 8, pp. 55-64.
11. Lovtsov D. A., Niesov V. A. Obespechenie edinstva sudebnoi sistemy Rossii v infosfere: kontseptual'nye aspekty. Rossiiskoe pravosudie, 2006, No. 4, pp. 35-40.
12. Lovtsov D. A., Niesov V. A. Modernizatsiia informatsionnoi infrastruktury sudoproizvodstva -- kliuchevoe napravlenie optimizatsii nagruzki na sudebnuiu sistemu. Rossiiskoe pravosudie, 2014, No. 9, pp. 30-40.
13. Lovtsov D. A., Niesov V. A. Problemy i printsipy sistemnoi modernizatsii "tsifrovogo" sudoproizvodstva. Pravovaia informatika, 2018, No. 2, pp. 15-22, DOI: 10.21681/1994-1404-2018-2-15-22.
14. Fedoseev S. V. Primenenie sovremennykh tekhnologii bol'shikh dannykh v pravovoi sfere. Pravovaia informatika, 2018, No. 4, pp. 50-58, DOI: 10.21681/1994-1404-2018-4-50-58.
15. Khabrieva T.la., Chernogor N.N. Pravo v usloviiakh tsifrovoi real'nosti. Zhurnal rossiiskogo prava, 2018, No. 1, pp. 85-102.
16. Chernykh A. M. Osnovnye napravleniia integratsii federal'nykh gosudarstvennykh informatsionnykh sistem i prostranstvennykh dannykh. Pravovaia informatika, 2018, No. 2, pp. 47-56, DOI: 10.21681/1994-1404-2018-2-47-56.
17. Deighton-Smith R., Erbacci A., Kauffmann C. Promoting inclusive growth through better regulation: The role of regulatory impact assessment. OECD Regulatory Policy Working Papers. Paris, OECD Publishing, 2016, No. 3, DOI: http://dx.doi.org/10.1787/5jm3tqwqp1vj-en .
18. Rishi P. Maximizing Business Performance and Efficiency Through Intelligent Systems. Hershey, 2017, 255 pp.

КОНЦЕПТУАЛЬНО-ЛОГИЧЕСКОЕ МОДЕЛИРОВАНИЕ ИНФОРМАЦИОННЫХ ПРАВООТНОШЕНИЙ В РАЙОННОМ СУДЕ

*Коваленко А.О.**

Ключевые слова: *информация в районном суде (входящая, исходящая, внутренняя), переработка информации, модель информационных правоотношений в районном суде, участники, права и обязанности, связи и взаимоотношения, правовой протокол, предварительное судебное заседание, закрытое судебное заседание, информация ограниченного доступа.*

Аннотация.

Цель работы: *совершенствование научно-методической базы обеспечения рациональной переработки судебной информации.*

Метод: *информационно-правовой и системный анализ прав и обязанностей субъектов-участников информационных правоотношений, концептуально-логическое моделирование.*

Результаты: *разработана комплексная модель информационных правоотношений в районном суде общей юрисдикции, характеризующая порядок и особенности движения информации, поступающей в районный суд, и предназначенная для оптимизации информационного взаимодействия участников судопроизводства; выявлены особенности правового статуса субъектов-участников; введено новое обобщенное понятие «лицо, обращающееся в суд»; раскрыты особенности взаимоотношений среди участников, выделены их права и обязанности, определено их правовое регулирование; разработаны правовой протокол и классификация этапов переработки судебной информации, для каждого из которых определены права и обязанности субъектов; выделены варианты реализации этапов обработки обращения граждан в районном суде.*

DOI: 10.21681/1994-1404-2020-1-57-66

Введение

Согласно Федеральной целевой программе «Развитие судебной системы России на 2013—2020 годы»[1] судебная система как механизм государственной защиты имеет большое значение в любом правовом государстве. Исполняя роль общественного арбитра, она защищает одновременно все сферы деятельности, регулируемые правом. Система судебных органов обеспечивает незыблемость основ конституционного строя, охраняя правопорядок, единство экономического пространства, имущественные и неимущественные права граждан и юридических лиц, а также гарантирует свободу экономической деятельности.

Применение электронных технологий и средств, с помощью которых участники правоотношений осуществляют взаимодействие, привело к возникновению новых — *целевых* информационных отношений [7], требующих специального правового регулирования.

Целевые информационные правоотношения — это урегулированные нормами права информационные отношения, т. е. общественные отношения, возникающие в связи с информацией либо юридически значимыми результатами действий (бездействия) в отношении этой информации (передача, получение, преобразование, предоставление, неразглашение) и др. [7]. Субъектами такого правоотношения считаются его правосубъектные участники — носители субъективных юридических прав (управомоченные) и обязанностей (правообязанные)[2] [8].

Системы (модели) правового регулирования во многом сопряжены с задачами, которые представляются людям (государству, законодателям, гражданам) в отношении определенной сферы жизни общества. Характером задачи, ее содержанием предопределяются

[1] Постановление Правительства РФ от 27 декабря 2012 г. № 1406 «О федеральной целевой программе «Развитие судебной системы России на 2013—2020 годы» // Собрание законодательства РФ. 2013. № 1. Ст. 13.

[2] Теория государства и права : учебник / Под ред. В.М. Корельского, В.Д. Перевалова. М. : Норма, 2002. С. 616.

* ***Коваленко Анна Олеговна,*** *аспирант кафедры информационного права, информатики и математики Российского государственного университета правосудия, Российская Федерация, г. Москва.*

E-mail: ans16@yandex.ru

и особенности правовых средств, при помощи которых она решается [1].

Федеральной целевой программой «Развитие судебной системы России на 2013—2020 годы» предусмотрено создание мобильного правосудия, электронного правосудия, внедрение программных средств аналитического обеспечения деятельности и осуществление сканирования всех поступающих в суды документов, а также формирование электронных дел и формирование электронного архива судебных дел.

В идеале, внедрение и эксплуатация автоматизированных систем должны сократить и оптимизировать нагрузку на районные суды, однако поскольку продолжается использование информации на бумажных носителях, происходит снижение оперативности и качества переработки судебной информации [9].

Для повышения скорости и качества переработки судебной информации, поступающей как на бумажном носителе, так и в электронном виде, создан наглядный функциональный протокол рациональной переработки судебной информации [5]. Однако для его использования необходимо создание концептуально-логической модели информационных правоотношений [4] участников протокола, которая раскрывала бы правовой статус субъектов-участников, их связи и роль.

1. Концептуальная организация взаимоотношений субъектов информационных правоотношений в районном суде

Районный суд является основным звеном судов общей юрисдикции российской судебной системы. Анализ действующего законодательства позволяет сделать *вывод* о том, что районные суды обладают очень широкой компетенцией: они рассматривают гражданские, уголовные дела и дела об административных правонарушениях, осуществляют контроль за законностью и обоснованностью решений мировых судей [10].

Исходя из специфики правоотношений, возникающих в районном суде, целесообразно выделить следующие их *субъекты*: судья, аппарат районного суда (сотрудники суда) и лицо, обращающееся в суд. Выделение субъектов рассматриваемых правоотношений необходимо для обеспечения конкретизации юридического статуса каждого из них, закрепления прав и обязанностей, определения их юридических связей.

Судья и аппарат суда находятся в одной связке, поскольку их работа взаимосвязана и направлена на достижение одних и тех же целей. Кроме того, их деятельность по документообороту в суде регулируется общими для судьи и аппарата суда нормативными правовыми актами.

Так, помимо правовых (нормативных) актов, распространяющихся на все органы государственной власти, включая, в частности: «ГОСТ Р 7.0.97-2016. Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу…»[3], «Типовая инструкция по делопроизводству федеральных органах исполнительной власти»[4], «Методические рекомендации по разработке инструкций по делопроизводству в федеральных органах исполнительной власти»[5], Федеральный закон «О порядке рассмотрения обращений граждан Российской Федерации»[6] и др., имеются специализированные нормативные правовые акты: Федеральный закон «Об обеспечении доступа к информации о деятельности судов в Российской Федерации»[7], приказы Судебного департамента при Верховном Суде РФ «Об утверждении Инструкции по судебному делопроизводству в районном суде»[8] и «Об утверждении Инструкции о порядке организации комплектования, хранения, учета и использования документов (электронных документов) в архивах федеральных судов общей юрисдикции»[9] и др. [11].

Районный суд формируется в составе председателя районного суда, его заместителя (заместителей) и судей районного суда (ст. 33 ФКЗ «О судах общей юрисдикции в Российской Федерации»[10]).

Судья — должностное лицо, уполномоченное осуществлять правосудие (п. 54 ст. 5 УПК РФ[11]). Согласно Закону «О статусе судей»[12] (ст. 1) судья является должностным лицом государственной власти, который в конституционном порядке наделен полномочиями осуществлять правосудие и выполнять свои обязанности на профессиональной основе. Судьи независимы и под-

---

[3] ГОСТ Р 7.0.97-2016. Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Организационно-распорядительная документация. Требования к оформлению документов (утв. Приказом Росстандарта от 08 декабря 2016 г. № 2004-ст). // М. : Стандартинформ. 2017. 15 с.

[4] Приказ Росархива от 27 ноября 2000 г. № 68 «Об утверждении Типовой инструкции по делопроизводству в федеральных органах исполнительной власти» (зарегистрировано в Минюсте РФ 26 декабря 2000 г. № 2508) // Российская газета. 2006. 07 фев.

[5] Приказ Федерального архивного агентства от 23 декабря 2009 г. № 76 «Об утверждении Методических рекомендаций по разработке инструкций по делопроизводству в федеральных органах исполнительной власти» // Документ опубликован не был. URL: http://www.consultant.ru/document/cons_doc_LAW_96081 (дата обращения: 05.08.2019).

[6] Федеральный закон от 02 мая 2006 г. № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации» // Российская газета. 2006. 5 мая.

[7] Федеральный закон от 22 декабря 2008 г. № 262-ФЗ «Об обеспечении доступа к информации о деятельности судов в Российской Федерации» // Российская газета. 2008. 26 дек.

[8] Приказ Судебного департамента при Верховном Суде РФ от 29 апреля 2003 г. № 36 «Об утверждении Инструкции по судебному делопроизводству в районном суде» // Российская газета. 2004. 05 ноя.

[9] Приказ Судебного департамента при Верховном Суде РФ от 19 марта 2019 г. № 56 «Об утверждении Инструкции о порядке организации комплектования, хранения, учета и использования документов (электронных документов) в архивах федеральных судов общей юрисдикции» // Бюллетень актов по судебной системе. 2019. № 5.

[10] Федеральный конституционный закон от 07 февраля 2011 г. № 1-ФКЗ «О судах общей юрисдикции в Российской Федерации» // Собрание законодательства РФ. 2011. № 7. Ст. 898.

[11] Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ // Российская газета. 2001. 22 дек. № 249.

[12] Закон РФ от 26 июня 1992 г. № 3132-1 «О статусе судей в Российской Федерации»// Ведомости СНД и ВС РФ. 1992. № 30. Ст. 1792.

чиняются только Конституции РФ и закону. В своей деятельности по осуществлению правосудия они никому не подотчетны. Требования и распоряжения судей при осуществлении ими полномочий обязательны для всех без исключения государственных органов, общественных объединений, должностных лиц, других юридических лиц и физических лиц. *Информация, документы и их копии,* необходимые для осуществления правосудия, представляются по требованию судей безвозмездно. Неисполнение требований и распоряжений судей влечет установленную законом ответственность.

Сотрудник суда — должностное лицо, которое в соответствии со ст. 38 ФКЗ «О судах общей юрисдикции в Российской Федерации» осуществляет организационное обеспечение деятельности федерального суда общей юрисдикции по осуществлению правосудия. Согласно Приказу Судебного департамента при Верховном Суде РФ «Об утверждении Положения об аппарате федерального суда общей юрисдикции»[13] аппарат суда состоит из соответствующих структурных подразделений — отделов, не входящих в их состав должностей: «помощник председателя суда», «помощник судьи», а также должностей, не относящихся к должностям федеральной государственной гражданской службы.

Представляется, что структуру аппарата районного суда следует представить как совокупность государственных гражданских служащих, так как именно для них характерно осуществление должностных полномочий в тесном взаимодействии друг с другом [14]. Единые цели и задачи, стоящие перед государственными гражданскими служащими, и общие принципы организации и деятельности аппарата районного суда гарантируют постоянное и непрерывное выполнение функции аппарата районного суда по обеспечению судебной деятельности.

Таким образом, термин «аппарат районного суда» можно определить как совокупность работников районного суда — государственных гражданских служащих, осуществляющих свои полномочия на основе общих принципов организации и функционирования районного суда в целях обеспечения его деятельности.

Должностные обязанности, права, квалификационные требования и ответственность работников аппарата суда определяются соответствующими должностными регламентами (инструкциями), утверждаемыми председателем соответствующего федерального суда общей юрисдикции (п. 2.10 Положения). Основными функциями сотрудника суда являются следующие (ст. 39 ФКЗ «О судах общей юрисдикции в Российской Федерации»): принимает и выдает документы; удостоверяет копии судебных документов; производит вручение документов, уведомлений и вызовов; контролирует уплату пошлин и сборов; осуществляет организационно-подготовительные действия в связи с назначением дел к слушанию; оказывает помощь судьям в привлечении присяжных заседателей к осуществлению правосудия; обеспечивает ведение протоколов судебных заседаний; ведет учет движения дел и сроков их прохождения в суде; обеспечивает обращение к исполнению судебных решений; осуществляет хранение дел и документов; участвует в обобщении данных судебной практики, ведет судебную статистику, информационно-справочную работу по законодательству Российской Федерации и иную работу; осуществляет прием граждан.

Вся деятельность сотрудника суда регламентируется «Инструкцией по судебному делопроизводству в районном суде». Таким образом, помимо технической работы сотрудники суда в большей или меньшей степени задействованы в выполнении и процессуальных функций [16].

Лицо, обращающееся в суд — физическое лицо или представитель юридического лица, обращающееся в суд за защитой нарушенных либо оспариваемых прав, свобод или законных интересов. В соответствии со ст. 5 ч. 58 УПК РФ участники уголовного судопроизводства — лица, принимающие участие в уголовном процессе (участники со стороны обвинения и участники со стороны защиты). В соответствии со ст. 34 ГПК РФ[14] лицами, участвующими в деле, являются стороны, третьи лица, прокурор, лица, обращающиеся в суд за защитой прав, свобод и законных интересов других лиц или вступающие в процесс в целях дачи заключения, заявители и другие заинтересованные лица по делам особого производства.

В соответствии со ст. 37 КАС РФ[15] лицами, участвующими в деле, являются: 1) стороны; 2) заинтересованные лица; 3) прокурор; 4) органы, организации и лица, обращающиеся в суд в защиту интересов других лиц или неопределенного круга лиц.

В соответствии с гл. 25 КоАП РФ[16] участниками производства по делам об административных правонарушениях могут быть: лицо, в отношении которого ведется производство по делу об административном правонарушении; потерпевший; законный представитель физического лица; законный представитель юридического лица; защитник, представитель, свидетель, понятой, специалист, эксперт, переводчик, прокурор и др.

Лицо, обращающееся в суд, вступает в правоотношение с сотрудником суда, при этом у них возникают взаимные права и обязанности. Одновременно сотрудник суда вступает в правоотношения с судьей, являясь как бы посредником между лицом, обращающимся в суд, и судьей. Но несмотря на то, что судья

[13] Приказ Судебного департамента при Верховном Суде РФ от 21 декабря 2012 г. № 238 «Об утверждении Положения об аппарате федерального суда общей юрисдикции» // Бюллетень актов по судебной системе. 2013. № 6.

[14] Гражданский процессуальный кодекс Российской Федерации от 14 ноября 2002 г. № 138-ФЗ // Российская газета. 2002. 20 ноя.

[15] Кодекс административного судопроизводства Российской Федерации от 08 марта 2015 г. № 21-ФЗ // Российская газета. 2015. 11 мар.

[16] Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ // Собрание законодательства РФ. 2002. № 1 (ч. 1). Ст. 1.

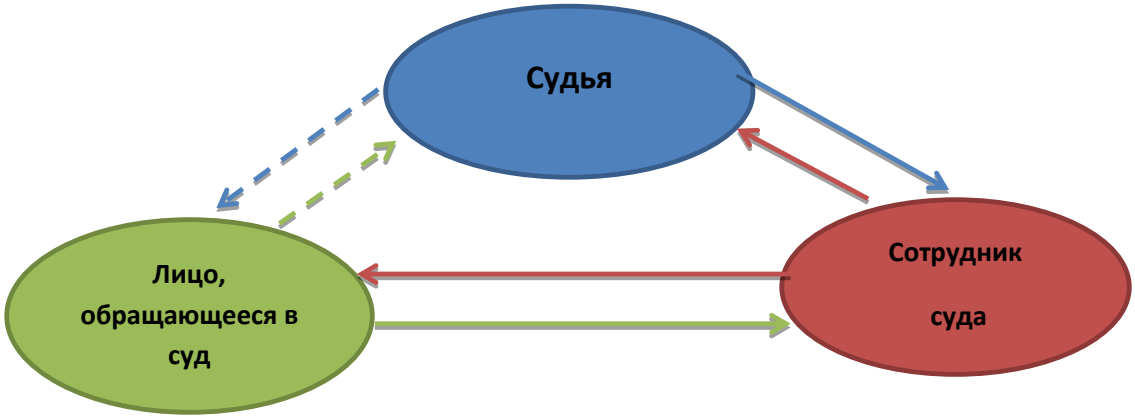

Рис. 1. Концептуальная организация взаимоотношений субъектов информационных правоотношений в районном суде

и лицо, обращающееся в суд, фактически не контактируют, между ними все равно возникают правоотношения, поскольку они друг перед другом несут определенные обязанности и имеют соответствующие права (рис. 1).

Таким образом, правоотношения, возникающие в районном суде, чаще всего являются трехсторонними, поскольку между судьей и лицом, обращающимся в суд, есть сотрудник суда, который занимается организационным обеспечением судебной деятельности. Это необходимо для изоляции чьего-либо вмешательства в деятельность судьи для реализации *принципа беспристрастности*.

2. Комплексная модель информационных правоотношений, возникающих в районном суде

Права и обязанности участников судопроизводства по каждой категории и виду дел (административное, уголовное, гражданское), содержатся в процессуальном законодательстве.

Важно рассмотреть общие права и обязанности, возникающие в районном суде, которые характерны для любого рода и вида дела, т. е. «обобщенные», присущие любому участнику (рис. 2).

Определяя содержание правоотношения, необходимо исходить из того, что всякое правоотношение состоит из прав и обязанностей его участников, что в правоотношении правам одних лиц соответствуют обязанности других и наоборот [13]. Данное правило на рис. 2 обозначается стрелками, которые группируют права и порождающие их обязанности либо обязанности и порождающие их права. Права и обязанности каждого субъекта обозначены определенным цветом (рис. 1 и 2): права и обязанности судьи — голубым; сотрудника суда — красным; лица, обращающегося в суд — зеленым. При этом стрелками соответствующего цвета показаны юридические связи, т. е. «право — обязанность» одного субъекта связано с «обязанностью — правом» другого субъекта. Цвет и направление стрелок формируется исходя из значимости прав и обязанностей.

На основе специфики рассматриваемых правоотношений разработан рациональный *правовой протокол* обработки обращений граждан в районном суде, в котором выделено 4 группы (шага) правоотношений, характерных для каждой стадии движения информации.

Протокол обработки обращений граждан в районном суде состоит в следующем:

Шаг 1. Поступление информации ($Q_{вх}$).

Лицо, обращающееся в суд, имеет право обратиться в суд путем подачи информации $Q_{вх}$ (входящая информация) на любом виде носителя ($Q_{вх}$ — поступившая в районный суд информация по средствам использования электронной формы $Q_{вх.эл}$ или на бумажном носителе $Q_{вх.бум}$) (п. 1.1). Оно порождает у сотрудника суда обязанность принять и зарегистрировать поступившую информацию как входящую $Q_{вх}$ (п. 1.2).

Помимо права на обращение, у лица, обращающегося в суд, есть обязанность, которая заключается в том, что информация, подаваемая в суд, должна соответствовать установленным законом требованиям (п. 1.3). В связи с этим у сотрудника суда есть право отклонить документ, поданный в электронном виде без заполнения специальных форм, как поданный в нарушении порядка (п. 1.4).

Шаг 2. Обработка и рассмотрение, поступившей информации, направление ответа ($Q_{вн}$, $Q_{исх}$).

Судья обязан рассмотреть поступивший документ (п. 2.2); лицо, обращающееся в суд, вправе требовать его рассмотрения (п. 2.1).

Судья вправе принять к производству документ либо отказать в принятии в случае нарушения требований, предусмотренных законодательством (п. 2.3); лицо, обращающееся в суд, обязано соблюдать процессуальный порядок (п. 2.4).

Судья обязан дать соответствующий ответ на поступивший документ по существу принятого решения (п. 2.6). В свою очередь лицо, обращающееся в суд, вправе требовать получения компетентного ответа (п. 2.5). Поскольку у сотрудника суда возникает обязанность направить ответ (п. 2.7), лицо, обращающее в суд, вправе требовать получение компетентного ответа (п. 2.5).

Лицо, обращающееся в суд		Судья		Сотрудник суда	
Права	*Обязанности*	*Права*	*Обязанности*	*Права*	*Обязанности*

Шаг 1. Поступление информации ($Q_{вх}$)

1.1 Обратиться путем подачи информации на любом виде носителя ($Q_{вх.эл}$,$Q_{вх.бум.}$)	1.3 Направить $Q_{вх}$, соответствующую установленным требованиям			1.4 Отклонить $Q_{вх.эл}$, поступившее без заполнения специальных форм	1.2 Принять и зарегистрировать $Q_{вх}$, передать на рассмотрение судье

Шаг 2. Обработка и рассмотрение, поступившей информации, направление ответа ($Q_{вн}$, $Q_{исх}$)

2.1 Требовать рассмотрения $Q_{вх}$ 2.5 Получить компетентный ответ $Q_{исх}$	2.4 Соблюдать порядок, предусмотренный процессуальным законодательством	2.3 $Q_{вх}$ → принять к производству $Q_{вн}$	2.3 $Q_{вх}$ → отказать в принятии при нарушении требований $Q_{исх}$	2.2 Рассмотреть поступивший документ $Q_{вх} \Rightarrow Q_{вн}$ 2.6 Дать соответствующий ответ по существу принятого решения $Q_{вн}$	2.8 Использовать установленный законом срок для направления ответа	2.7 Направить ответ по существу принятого решения $Q_{вн} \rightarrow Q_{исх}$

Шаг 3. Назначение и проведение судебного заседания, вынесение и направление судебного акта ($Q_{вн}$, $Q_{исх}$)

3.3 Своевременно получать информацию о ходе рассмотрения дела	3.5Соблюдать порядок, предусмотренный процессуальным законодательством 3.7 Не разглашать информацию, в отношении которой введен режим тайны	3.6 Провести закрытое судебное заседание при наличии оснований, предусмотренных законодательством	3.1 Назначить и провести судебное заседание, по результату которого вынести судебный акт	3.4Использовать установленный законом срок для направления извещения	3.2 Направить извещение о дате суд. заседания/ копию суд. акта 3.7 Взять подписку о неразглашении сведений, в отношении которых введен режим тайны

Шаг 4. Обжалование результата рассмотрения

4.1 Обжаловать вынесенный судебный акт 4.8 Получать информацию о ходе рассмотрения жалобы	4.6 Соблюдать процессуальную форму	4.4 Вернуть жалобу	4.3 Рассмотреть жалобу	4.5Использовать установленный законом срок для направления возвращенной жалобы	4.2 Принять жалобу 4.7 Подготовить, направить дело в вышестоящую инстанцию для обжалования

Рис. 2. Комплексная модель информационных правоотношений в районном суде

При этом сотрудник суда вправе направить ответ в срок, установленный законодательством, а лицо, обращающееся в суд, обязано соблюдать порядок, предусмотренный процессуальным законодательством (п. 2.4). Судья вправе принять к производству заявление либо отказать в принятии в случае нарушения требований, установленных законодательством, для соответствующего вида документа (п. 2.3), поскольку у лица, обращающегося в суд, есть обязанность соблюдать порядок, предусмотренный процессуальным законодательством (п. 2.4).

Шаг 3. Назначение и проведение судебного заседания, вынесение и направление судебного акта ($Q_{вн}$, $Q_{исх}$).

При принятии заявления к производству судья обязан назначить и провести судебное заседание, по результату которого вынести судебный акт (п. 3.1), в рамках чего сотрудник суда обязан направить извещение о дате судебного заседания или копию судебного акта в случае его вынесения (п. 3.2). Лицо, обращающееся в суд, вправе своевременно получать информацию о ходе рассмотрения дела, быть извещённым о дате судебного заседания (п. 3.3). Сотрудник суда вправе использовать установленный законом срок для направления извещения или судебного акта (п. 3.4), а лицо, обращающееся в суд, обязано соблюдать порядок, предусмотренный процессуальным законодательством (п. 3.5). Судья вправе в случаях, предусмотренных законодательством, провести закрытое судебное заседание (п. 3.6), при этом сотрудник суда обязан взять подписку о неразглашении сведений, ставших известными в ходе проведения судебного заседания, если они носят конфиденциальный характер, сокрыты в режиме тайны (п. 3.7). Лицо, обращающееся в суд, в свою очередь, обязано не разглашать информацию, в отношении которой введен режим тайны (п. 3.8).

Шаг 4. Обжалование результата рассмотрения.

Лицо, обращающееся в суд, вправе обжаловать вынесенный судебный акт (п. 4.1); сотрудник суда обязан принять такую жалобу и передать судье для рассмотрения (п. 4.2), а судья обязан рассмотреть поступившую жалобу (п. 4.3). Судья вправе вернуть жалобу (п. 4.4), в случае если она не соответствует требованиям, установленным законодательством, поскольку при подаче жалобы лицо, обращающееся в суд, обязано соблюдать процессуальную форму, предусмотренную законодательством (п. 4.6), а сотрудник суда вправе использовать установленный законом срок для возврата жалобы (п. 4.5).

В случае принятия жалобы (п. 4.3), сотрудник суда обязан подготовить и направить дело в вышестоящую инстанцию для рассмотрения такой жалобы по существу (п. 4.7), а лицо, обращающееся в суд, вправе получать информацию о ходе рассмотрения жалобы (в том числе о дате рассмотрения дела в вышестоящей инстанции) (п. 4.8).

Рассмотрим данный протокол обработки обращения граждан в районном суде более подробно.

Так, *первая* группа правоотношений (*Шаг 1*) возникает при первичном поступлении информации (на рис. 2 отмечена коричневым цветом). При обращении в суд у лица, обращающегося в суд, есть право обратиться в суд (п. 1.1). Данное право является неотъемлемым и гарантируется ст. 46 Конституции РФ[17] — «каждому гарантируется судебная защита его прав и свобод». Это может быть подача: заявления, искового заявления, ходатайства, обращения, жалобы, письма, сообщения и др. При этом подача информации возможна на любом виде носителя (бумажном или электронном). Оно порождает у сотрудника суда обязанность принять и зарегистрировать поступившую информацию как входящую (п. 1.2). При этом сотрудником проводится ее первичный анализ, в случае необходимости такая информация распечатывается на бумажном носителе, ей присваивается уникальный штрих-код, она проходит процедуру сканирования. После совершения указанных действий информация передается судье для рассмотрения.

Помимо права на обращение, у лица, обращающегося в суд, есть обязанность, которая заключается в том, что информация, подаваемая в суд, должна соответствовать установленным законом требованиям (п. 1.3). В связи с этим у сотрудника суда есть право отклонить документ, поданный в электронном виде без заполнения специальных форм, как поданный в нарушении порядка (п. 1.4). Это право предусмотрено Инструкцией по судебному делопроизводству в районном суде (п. 2.1.1 Инструкции). При этом сотрудник суда не имеет рава отклонить или не принять любой другой входящий документ (за исключением случая, указанного выше), поскольку сотрудник суда передает входящие документы на рассмотрение судье.

На данном этапе лицо, обращающееся в суд, контактирует только с сотрудником суда, поэтому правоотношение возникает только между ними и являются *двухсторонними*.

Вторая группа правоотношений (*Шаг 2*) возникает при переработке и рассмотрении $Q_{вх}$. Результатом переработки такой информации становится $Q_{вн}$ (если $Q_{вх}$ соответствует всем установленным законом требованиям, предъявляемых к данному виду документов, то она принимается к производству) либо $Q_{исх}$ (если $Q_{вх}$ не соответствует требованиям, предъявляемым к данному виду документов, то она покидает районный суд) (на рис. 2 отмечена серым цветом). Судья обязан рассмотреть поступивший документ (п. 2.2); лицо, обращающееся в суд, вправе требовать его рассмотрения (п. 2.1). Поскольку это обобщенная модель правоотношений, возникающих в районном суде, под «документом» понимается: любое поступившее в суд исковое заявление, заявление, связанное с уже рассмотренным или рассматриваемым делом; административный ма-

[17] Конституция Российской Федерации» (принята всенародным голосованием 12.12.1993) // Собрание законодательства РФ. 2014. 04 авг. № 31. Ст. 4398.

териал; дело, поступившее по подсудности, или дело, направленное для рассмотрения в апелляционную инстанцию или вернувшееся с апелляционного рассмотрения, ходатайство по делу, обращение, жалоба и др. Судья вправе принять к производству документ либо отказать в принятии в случае нарушения требований, предусмотренных законодательством (п. 2.3); лицо, обращающееся в суд, обязано соблюдать процессуальный порядок (п. 2.4).

Судья обязан дать соответствующий ответ на поступивший документ по существу принятого решения (п. 2.6). В свою очередь, лицо, обращающееся в суд, вправе требовать получения компетентного ответа (п. 2.5). Однако, исходя из специфики отношений, судья поручает направление ответа на поступивший документ по существу принятого решения сотруднику суда. Тем самым правоотношения, возникающие на данном этапе, становятся *трехсторонними*. Поскольку у сотрудника суда возникает обязанность направить ответ (п. 2.7), лицо, обращающее в суд, вправе требовать получение компетентного ответа (п. 2.5). При этом сотрудник суда вправе направить ответ в срок, установленный законодательством, т. е. в любой момент, когда будет удобно сотруднику в пределах течения этого срока, а лицо, обращающееся в суд, обязано соблюдать порядок, предусмотренный процессуальным законодательством (п. 2.4).

«Использование установленного законом срока» возможно рассматривать и как право сотрудника суда, и как его обязанность не нарушать установленный законом срок. Но значимее отнести его к правам, поскольку сотрудник суда сам, по своему усмотрению, в рамках течения этого срока решает, когда следует направить ответ, исходя из своей загруженности и первоочередности дел.

Судья вправе принять к производству заявление либо отказать в принятии в случае нарушения требований, установленных законодательством, для соответствующего вида документа (п. 2.3), поскольку у лица, обращающегося в суд, есть обязанность соблюдать порядок, предусмотренный процессуальным законодательством (п. 2.4).

Для *третьей* группы правоотношений (*Шаг 3*) характерно дальнейшее рассмотрение и переработка информации $Q_{вн}$. В рамках данной группы происходит проведение судебного заседания, вынесение соответствующего судебного акта (отмечено голубым цветом на рис. 2). Некоторая информация, поступившая в районный суд, не проходит данную стадию. Так, это касается жалоб, обращений, некоторого рода заявлений, для рассмотрения которых назначение судебного заседания не требуется. Кроме того, в случаях, предусмотренных процессуальным законодательством, возможно назначение предварительного судебного заседания в рамках гражданского процесса. Предварительное судебное заседание имеет двоякую природу [2]: *с одной стороны*, оно проходит при подготовке дела к судебному разбирательству, т. е. является этапом стадии подготовки, а *с другой стороны*, это судебное заседание, в котором судья согласно ст. 152 ГПК РФ принимает решение, которое является актом правосудия [12].

В рамках уголовного процесса возможно назначение предварительного слушания. Так, поводом для проведения предварительного слушания является ходатайство стороны или собственная инициатива судьи (ч. 1 ст. 229 УПК РФ). При этом по инициативе суда может быть проведено предварительное слушание только для решения вопроса о возвращении уголовного дела прокурору, решения вопроса о приостановлении или прекращении уголовного дела. По остальным основаниям предварительное слушание проводится только при наличии ходатайства сторон [3].

В рамках данной группы правоотношений возможно появление так называемой *информации ограниченного доступа* [8]. В соответствии со ст. 5 Федерального закона «Об обеспечении доступа к информации о деятельности судов в Российской Федерации»[18] доступ к информации о деятельности судов ограничивается, если указанная информация отнесена в установленном федеральным законом порядке к сведениям, составляющим государственную или иную охраняемую законом тайну [5, 6].

Основным способом защиты привилегированной информации от доступа к ней третьих лиц является сокрытие ее в режиме тайны. Необходимость обеспечения *сохранности* определенных сведений, в отношении которых введен режим тайны, может быть инициирована в рамках судебного разбирательства двумя категориями субъектов: либо непосредственно судом, либо лицом, участвующим в судебном процессе [15]. По результатам рассмотрения ходатайства суд выносит определение (постановление) о проведении закрытого судебного заседания либо об отклонении ходатайства о проведении закрытого судебного заседания. Закрытая форма рассмотрения дела предполагает реализацию ряда процедурных запретов, которые необходимы для гарантии защиты информации ограниченного доступа.

При принятии судьей заявления к производству и назначении судебного заседания, сотрудник суда обязан направить извещение о дате судебного заседания, а после вынесения судебного акта и копию судебного акта. Поскольку лицо, обращающееся в суд, вправе своевременно получать информацию о ходе рассмотрения дела и быть извещенным о дате судебного заседания, возникающее правоотношение является также *трехсторонним*.

Для *четвертой группы* правоотношений (*Шаг 4*) характерным признаком является то, что на данном этапе судебный акт (решение, постановление, приговор) обжалуется в случаях, предусмотренных процессуальным законодательством (на рис. 2 отмечено фиолетовым цветом).

[18] Федеральный закон от 22 декабря 2008 г. № 262-ФЗ «Об обеспечении доступа к информации о деятельности судов в Российской Федерации» // Собрание законодательства РФ. 2008. № 52 (ч.1). Ст. 6217.

Рис. 3. Варианты реализации этапов обработки обращений граждан в районном суде

3. Варианты реализации этапов обработки обращений граждан в суде общей юрисдикции

Информация, поступившая в районный суд, проходит 4 этапа (шага) ее переработки (см. рис. 2, 3):

- поступление информации;
- обработка и рассмотрение поступившей информации, направление ответа;
- назначение и проведение судебного заседания, вынесение и направление судебного акта;
- обжалование результата рассмотрения.

Исходя из вида и содержания поступившей информации, представляется возможным при ее переработке прохождение не всех рассмотренных шагов (рис. 3). При этом возможны следующие четыре варианта:

I вариант — поступление информации, её переработка и рассмотрение, направление ответа, обжалование результата рассмотрения. Это тот случай, когда, например, поступило заявление, судья его рассмотрел и отказал в принятии, поскольку имеются нарушения требований процессуального законодательства, а лицо, обращающееся в суд, обжаловало такой отказ.

II вариант — поступление информации, её переработка и рассмотрение, направление ответа. Например, поступило заявление, судья его рассмотрел и отказал в принятии, но такой отказ не обжаловался.

III вариант — поступление информации, её переработка и рассмотрение, назначение и проведение судебного заседания, вынесение и направление судебного акта, обжалование результата рассмотрения. Например, поступило исковое заявление, судья его рассмотрел, принял к производству, назначил судебное заседания, по результатам судебного заседания вынес решение, которое обжаловалось.

IV вариант — поступление информации, её переработка и рассмотрение, назначение и проведение судебного заседания, вынесение и направление судебного акта. Например, поступило исковое заявление, судья его рассмотрел, принял к производству, назначил судебное заседания, по результатам судебного заседания вынес решение, которое не обжаловалось.

Заключение

Разработана обобщенная комплексная модель информационных правоотношений в районном суде, позволяющая составить общее представление о ходе движения информации, поступающей в районный суд. Для ее создания необходимо было выделение субъектов,

которые вступают в информационные правоотношения, возникающие при переработке информации в районном суде. К ним относятся: судья, сотрудник суда и лицо, обращающееся в суд. В данной модели рассмотрены права и обязанности субъектов, а также выявлена концептуальная организация их взаимоотношений. Кроме того, определены возможные варианты реализации этапов обработки обращений граждан в районном суде.

Обобщенную комплексную модель информационных правоотношений целесообразно использовать в районном суде для оптимизации информационного взаимодействия участников судопроизводства, для формирования общего представления движения информации у лиц, обращающихся в суд, а также для понимания задач своей работы у вновь пришедших кадров в аппарате суда. Внедрение данной комплексной модели и правового протокола обработки обращений граждан обсуждалось и получило одобрение на совещании судей Чертановского районного суда г. Москвы. Кроме того, разработанные модель и протокол прошли апробацию на IX Международной научно-практической конференции «Правовое и индивидуальное регулирование общественных отношений: проблемы теории и практики» (г. Москва, 25 апреля 2018 г.) и X Всероссийской научно-практической конференции аспирантов, соискателей и молодых ученых «Толкование и конкретизация права: проблемы теории и практики» (г. Москва, 23 апреля 2019 г.).

*Рецензент: **Полякова Татьяна Анатольевна,** доктор юридических наук, профессор, главный научный сотрудник, заведующая сектором информационного права ИГП РАН, г. Москва, Россия.*
E-mail: polyakova_ta@mail.ru

Литература

1. Алексеев С. С. Право. Азбука. Теория. Философия. Опыт комплексного исследования. М. : Статут, 1999. 456 с.
2. Бороздина М. О. Предварительное судебное заседание как новелла ГПК РФ // Проблемы гражданской юрисдикции в свете нового законодательства. Саратов : СГАП, 2003. С. 20—31.
3. Долгих Т. Н. Проблемные вопросы процессуального порядка проведения предварительных слушаний по уголовному делу // Вестник Томского гос. пед. ун-та. 2006. № 11. С. 85—87.
4. Коваленко А. О. Модель информационного правоотношения участников гражданского, административного и уголовного судопроизводства // Тр. IV Всеросс. науч.-практ. конф. «Современное непрерывное образование и инновационное развитие» (23 апреля 2014 г.) / ФГАУ «ФИРО». Серпухов : МОУ «ИИФ», 2014. С. 732—736.
5. Коваленко А. О. Протокол рациональной переработки и правовые режимы судебной информации // Правовая информатика. 2019. № 2. С. 49—56. DOI: 10.21681/1994-1404-2019-2-49-56.
6. Ловцов Д. А. Концептуально-логическое моделирование юридического понятия «тайна» // Информационное право. 2009. № 2. С. 12—14.
7. Ловцов Д. А. Теория информационного права: базисные аспекты // Государство и право. 2011. № 11. С. 43—51.
8. Ловцов Д. А., Коваленко А. О. Разработка национального классификатора правовых режимов информации ограниченного доступа // Тр. VI Всеросс. науч.-прак. конф. «Современное непрерывное образование и инновационное развитие» (20 апреля 2016 г.) / ФГАУ «ФИРО». Серпухов : МОУ «ИИФ», 2016. С. 706—709.
9. Ловцов Д. А., Ниесов В. А. Обеспечение единства судебной системы России в инфосфере: концептуальные аспекты // Российское правосудие. 2006. № 4. С. 35—40.
10. Лукоянов Д. Н. Совершенствование правового регулирования статуса председателя районного суда // Вестник Костромского гос. ун-та. 2011. № 5-6. С. 265—268.
11. Медведева О. В. Нормативная база управления документацией в государственных организациях // Ученые записки Тамбовского отделения Российского союза молодых ученых : сб. науч. ст. № 11. Тамбов, 2018. С. 179—184.
12. Некрасов К. О. Предварительное судебное заседание // Вопросы науки и образования. 2017. № 11(12). С. 169—174.
13. Проблемы общей теории государства и права / Под общ. ред. В. С. Нерсесянца. М. : Норма, 2001. 832 с.
14. Прокудина Л. А. Участие аппарата суда в осуществлении судебной деятельности // Право. Журнал Высшей школы экономики. 2009. № 3. С. 50—56.
15. Сальникова О. Ю. Институт закрытого судебного заседания как гарантия информационной защищённости участников арбитражного судопроизводства // Информационная безопасность регионов. 2014. № 2 (15). С. 90—93.
16. Смирнова Е. В. Проблемы определения правовой природы термина «аппарат районного суда» // Вестник Костромского гос. ун-та. 2011. № 3. С. 359—362.

CONCEPTUAL AND LOGICAL MODELLING OF INFORMATIONAL LEGAL RELATIONS IN DISTRICT COURTS

Anna Kovalenko, *Ph.D. student at the Department of Information Technology law, Informatics and Mathematics of the Russian State University of Justice, Moscow, Russian Federation.*
E-mail: ans16@yandex.ru

Keywords: *district court information (incoming, outgoing, internal); information processing; model of informational legal relations in a district court; participants; rights and obligations; communications and relationships; legal protocol; preliminary court session; closed court session; restricted access information.*

Abstract.

Purpose of the work: *improving the scientific and methodological basis of ensuring rational processing of judicial information.*

Method used: *information technology law and system analysis of rights and obligations of participants of informational legal relations, conceptual and logical modelling.*

Results obtained: *an integrative model of informational legal relations in a general jurisdiction district court describing the procedure and specific features of the incoming information flow to the district court and designed to optimise the information interaction of participants of proceedings is worked out. Features of the legal status of the participants are identified. A new generalised concept of the 'person applying to the court' is introduced. Features of relations between the participants are expounded upon, their rights and obligations are highlighted, and their legal regulation is determined. The legal protocol and a classification of stages of judicial information are worked out, the rights and obligations of subjects for each of these stages are determined. Variants of implementing the stages of processing citizens' applications to a district court are highlighted.*

References

1. Alekseev S. S. Pravo. Azbuka. Teoriia. Filosofiia. Opyt kompleksnogo issledovaniia. M. : Statut, 1999, 456 pp.
2. Borozdina M. O. Predvaritel'noe sudebnoe zasedanie kak novella GPK RF. Problemy grazhdanskoi iurisdiktsii v svete novogo zakonodatel'stva, Saratov : SGAP, 2003, pp. 20-31.
3. Dolgikh T. N. Problemnye voprosy protsessual'nogo poriadka provedeniia predvaritel'nykh slushanii po ugolovnomu delu. Vestnik Tomskogo gos. ped. un-ta, 2006, No. 11, pp. 85-87.
4. Kovalenko A. O. Model' informatsionnogo pravootnosheniia uchastnikov grazhdanskogo, administrativnogo i ugolovnogo sudoproizvodstva. Tr. IV Vseross. nauch.-prakt. konf. "Sovremennoe nepreryvnoe obrazovanie i innovatsionnoe razvitie" (23 aprelia 2014 g.), FGAU "FIRO", Serpukhov : MOU "IIF", 2014, pp. 732-736.
5. Kovalenko A. O. Protokol ratsional'noi pererabotki i pravovye rezhimy sudebnoi informatsii. Pravovaia informatika, 2019, No. 2, pp. 49-56, DOI: 10.21681/1994-1404-2019-2-49-56.
6. Lovtsov D. A. Kontseptual'no-logicheskoe modelirovanie iuridicheskogo poniatiia "taina". Informatsionnoe pravo, 2009, No. 2, pp. 12-14.
7. Lovtsov D. A. Teoriia informatsionnogo prava: bazisnye aspekty. Gosudarstvo i pravo, 2011, No. 11, pp. 43-51.
8. Lovtsov D. A., Kovalenko A. O. Razrabotka natsional'nogo klassifikatora pravovykh rezhimov informatsii ogranichennogo dostupa. Tr. VI Vseross. nauch.-prak. konf. "Sovremennoe nepreryvnoe obrazovanie i innovatsionnoe razvitie" (20 aprelia 2016 g.), FGAU "FIRO", Serpukhov : MOU "IIF", 2016, pp. 706-709.
9. Lovtsov D. A., Niesov V. A. Obespechenie edinstva sudebnoi sistemy Rossii v infosfere: kontseptual'nye aspekty. Rossiiskoe pravosudie, 2006, No. 4, pp. 35-40.
10. Lukoianov D. N. Sovershenstvovanie pravovogo regulirovaniia statusa predsedatelia raionnogo suda. Vestnik Kostromskogo gos. un-ta, 2011, No. 5-6, pp. 265-268.
11. Medvedeva O. V. Normativnaia baza upravleniia dokumentatsiei v gosudarstvennykh organizatsiiakh. Uchenye zapiski Tambovskogo otdeleniia Rossiiskogo soiuza molodykh uchenykh : cb. nauch. st., No. 11, Tambov, 2018, pp. 179-184.
12. Nekrasov K. O. Predvaritel'noe sudebnoe zasedanie. Voprosy nauki i obrazovaniia, 2017, No. 11(12), pp. 169-174.
13. Problemy obshchei teorii gosudarstva i prava. Pod obshch. red. V. S. Nersesiantsa. M. : Norma, 2001, 832 pp.
14. Prokudina L. A. Uchastie apparata suda v osushchestvlenii sudebnoi deiatel'nosti. Pravo, Zhurnal Vysshei shkoly ekonomiki, 2009, No. 3, pp. 50-56.
15. Sal'nikova O. Iu. Institut zakrytogo sudebnogo zasedaniia kak garantiia informatsionnoi zashchishchennosti uchastnikov arbitrazhnogo sudoproizvodstva. Informatsionnaia bezopasnost' regionov, 2014, No. 2 (15), pp. 90-93.
16. Smirnova E. V. Problemy opredeleniia pravovoi prirody termina "apparat raionnogo suda". Vestnik Kostromskogo gos. un-ta, 2011, No. 3, pp. 359-362.

АНАЛИЗ МЕТОДОВ РАСПОЗНАВАНИЯ КОМПЬЮТЕРНЫХ АТАК

Добкач Л.Я.*

Ключевые слова: *обнаружение вторжений, поведенческие методы, методы на основе знаний, сигнатуры атак, деревья решений, искусственные нейронные сети, гибридные методы.*

Аннотация.

Цель статьи: *изучение существующих методов обнаружения вторжений с позиций их достоинств и недостатков, а также с учетом их классификации.*

Методы исследования: *компаративный анализ, статистический анализ, сигнатурный анализ, теория графов, байесовский метод.*

Результаты: *методы обнаружения вторжений можно условно разделить на четыре группы: поведенческие методы (подходят для поиска аномалий), методы на основе знаний (подходят для поиска злоупотреблений), методы интеллектуального анализа данных (подходят для обоих направлений поиска), причем последние разветвляются на методы машинного обучения и методы вычислительного интеллекта. Перспективной группой методов выступают гибридные методы, сочетающие в себе элементы различных «чистых» методов, и на основе соотнесения наиболее значимых недостатков разобранных методов предлагается гибридный метод, использующий преимущества как искусственных нейронных сетей, так и сигнатурных методов.*

DOI: 10.21681/1994-1404-2020-1-67-75

Введение

Информационные активы стали неотъемлемой частью современной жизни и, как следствие, представляют интерес для злоумышленников. Чтобы заполучить доступ к защищаемым сведениям, они пробуют осуществить атаку на систему, где хранятся нужные им данные. Чтобы верно разобрать проблему распознавания атак и найти лучший способ их пресечения, необходимо понять, что собой представляют компьютерные атаки, какие они бывают и к каким последствиям могут привести в случае успешного вторжения.

Существует множество различных классификаций разного уровня подробности и проработанности, из которых становится очевидным широкое разнообразие путей реализации угроз информационной безопасности. Так, в труде Питера Мелла «Компьютерные атаки: что это и как им противостоять»[1] классификация основывается на возможных действиях злоумышленника (к примеру, удаленное и локальное проникновение, отказы в обслуживании, опробование портов, анализ сетевого трафика). Но данная классификация почти не освещает такую важную характеристику любой атаки, как сегмент системы, подвергаемый злонамеренному воздействию.

Компания *Internet Security Systems* предлагает две классификационные нотации, одна из которых представляет более компактное представление версии Мелла из пяти типов атак, а вторая вводит ранжирование по степени риска, местоположению субъекта атаки, подвергаемому атаке программному обеспечению (ПО) и характеру действий («черные ходы», атаки типа «отказ в обслуживании» (*DoS и DDoS*), потенциально незащищенная операционная система, неавторизованный доступ). Здесь теряется цель атаки, а также ее последствия.

Все классификации так или иначе предлагают деление многообразия атак на несколько типов. Если их окажется мало, система обнаружения вторжений (СОВ) не сможет предложить конкретный сценарий действий, поскольку факт злонамеренного воздействия (в котором еще надо убедиться) не дает сам по себе ключ к пресечению такового. Обратная ситуация, когда типов так много, представляет собой скорее набор будто бы не связанных между собой частных случаев, нежели стандартный алгоритм реагирования на схожие по какому-то признаку вторжения.

«Золотой серединой» будет небольшое количество типов атак, которые позволят средству защиты информации и администратору информационной безопасности совершить определенные заранее действия за минимальное время и, таким образом, обеспечить защиту информационных активов.

[1] *См.:* Аграновский А. В., Хади Р. А. Новый подход к защите информации — системы обнаружения компьютерных угроз // Jet Info: Информ. бюл. 2007. 4(167). 24 с.

* ***Добкач Леонид Яковлевич,*** *аспирант Московского государственного технического университета им. Н. Э. Баумана, Российская Федерация, г. Москва.*

E-mail: dobkachleo@mail.ru

В качестве классификации разнообразных атак мы будем пользоваться совокупностью из 4 классов (удаленные атаки *R2L*, повышение полномочий *U2R*, отказы в обслуживании *DOS* и зондирующие атаки *Probe*), введенной в базе данных *KDD Cup* 1999. Каждый из этих классов имеет особенности, позволяющие обеспечить верное реагирование на атаку.

Но чтобы это сделать, ее необходимо распознать, изучить и проанализировать существующие методы обнаружения вторжений, а также предложить, исходя из сопоставления их преимуществ и недостатков, новый эффективный метод обнаружения вторжений.

Сформулируем задачи: установить классификационную схему методов выявления атак; сформировать метод распознавания атак по данной классификации; формализовать полученный метод.

Теоретическая значимость исследования заключается в выявлении эффективного метода распознавания атак и его формализации; практическая — в реализации метода в системе обнаружения вторжений, что позволит лучше выявлять атаки, а значит, и защищать информационные активы пользователей и предприятий.

1. Классификация методов распознавания атак

Утверждения об особенностях классификации компьютерных атак в равной мере применимы к классификации методов их распознавания, как и для любой сложной системы. Однако на этот раз справедливым, хотя и предварительным, будет разбиение на две пары подходов:

а) ***Сигнатурные и адаптивные (интеллектуальные) методы.***

Многие СОВ основаны на сличении текущих событий сетевого трафика с базой известных сигнатур или, в более общем случае, с правилами на их основе. Это безусловно гарантирует уверенность, что выделенное событие представляет именно злонамеренное действие, однако плохо распознает необычные атаки [1]. В качестве примеров можно выделить открытые системы обнаружения вторжений *Snort* и *Suricata* [2].

Адаптивные методы связаны с интеллектуальной обработкой или предобработкой событий и стремительно набирают популярность, но им присуща вероятностная природа. При обучении средства защиты информации можно установить точность распознавания, и она едва ли окажется равной 100%. Нивелирование этого недостатка представляется нам неотъемлемой частью поиска наилучшего метода распознавания атак ввиду возможности с помощью методов этой группы выявлять те атаки, которые будут пропущены сигнатурной системой обнаружения вторжений.

б) ***Методы обнаружения аномалий и злоупотреблений.***

Можно провести взаимосвязь между этой парой подходов и первой, но здесь во главу угла ставится совершенно иная природа методов. Начнем с того, что аномалии можно искать, когда сформирован профиль «нормального» функционирования системы, и отклонения от нормы фиксируются и выдаются за попытку вторжения [1].

Злоупотребления, напротив, предполагают знания о таких цепочках событий, которые ведут к эксплуатированию уязвимостей и другому вреду информационной системы. Тут можно провести явную связь с сигнатурными методами, хотя ими возможности распознавания атак не ограничиваются.

С позиции обнаружения аномалий или злоупотреблений оказываются общими методы интеллектуального анализа данных, такие как нейронные сети, деревья решений, генетические алгоритмы и др. Отличие лишь в том, что рассматривается по умолчанию как главное, а что — как цель для выявления [3]. Если сравнивать с вышеописанной парой подходов, данная пара дает больше вариаций методов выявления атак[2].

Забегая вперед, заметим, что неменьшую популярность набирают не чисто адаптивные методы, а комбинации различных подходов, т. е. там, где вероятность распознавания атак недостаточна для уверенного принятия решения, помогают более строгие правила из сигнатурных методов и им подобных.

2. Поведенческие методы

Важную роль в обнаружении аномалий играют поведенческие методы [1, 4]. К ним можно отнести вейвлет-анализ, спектральный, статистический анализ, анализ энтропии, фрактальный анализ[3] и др. Объединяет их сравнение параметров наблюдаемого поведения с нормальным профилем системы. Здесь присутствует вероятностный фактор, из-за которого СОВ не всегда реагирует только на аномалии. Повышение точности сопряжено со значительными временными затратами, хотя на этот фактор можно закрыть глаза, сочтя его за подготовку к работе. Гораздо хуже, если на этом этапе злоумышленник планомерно внесет злонамеренные действия в нормальный профиль системы, тогда средство защиты информации будет воспринимать аномалии как должное.

Кратко рассмотрим перечисленные выше поведенческие методы. Итак, начнем с ***вейвлет-анализа*** [5]. Основывается он, как подсказывает название, на вейвлет-преобразовании, что придает вес наиболее полезной информации. Для этого вычисляются коэффициенты, использующиеся в разложении исходного сигнала по базисным функциям. Сам же сигнал представляет, к примеру, интенсивность сетевого трафика. Достоинства «приоритизации» затеняются неоднозначностью

[2] См.: *Корниенко А. А., Слюсаренко И. М.* Системы и методы обнаружения вторжений: современное состояние и направления совершенствования // *CIT Forum*, 2009. 16 с.

[3] См.: *Басараб М. А., Строганов И. С.* Обнаружение аномалий в информационных процессах на основе мультифрактального анализа // Вопросы кибербезопасности. 2014. № 4 (7). С. 30—40.

выбора базисных функций, большой вычислительной сложностью при расчете коэффициентов разложения сигнала и правильным заданием размера скользящего окна, в котором ищется аномалия [3].

Недалеко от вейвлет-анализа отстоит спектральный анализ. Метод основан на предположении, что компоненты аномального трафика отличаются от компонентов обычного трафика. Главные компоненты должны отражать наибольшую изменчивость исходного процесса, остальные рассматриваются как составляющие шума. Тогда при изменении размерности исходного пространства признаков путем анализа ковариационной матрицы элементов исследуемого процесса, например, методом главных компонентов, можно выделить наиболее информативные составляющие этого процесса [3].

Статистический анализ — это целая группа методов, куда входят цепи Маркова, метод среднеквадратичных отклонений, анализ временных рядов, пороговый анализ и др. Их чаще всего применяют для поиска аномалий, ведь они способны учитывать изменения поведения пользователя и выявлять измененные атаки. В то же время следует верно выбирать контролируемые параметры, чтобы лучше отличать аномалии от нормального трафика, что, впрочем, не гарантирует избавления от ложноположительных срабатываний. Некоторым методам также присущи рост занимаемой памяти, «злонамеренное» переобучение, отсутствие стационарности (для временных рядов) и др.

Одна из разновидностей статистического анализа приводится в [6]. Исходя из распределения нулевых значений признаков базы данных *KDD Cup* 1999, выводится классификатор глубокого автокодировщика. Метод дает общую корректность в 87%, при этом точность распознавания *R2L*-атак и отклик на зондирующие атаки оставляют желать лучшего.

В теории информации важным понятием является энтропия. Она взята на вооружение в следующем рассматриваемом методе — ***анализе энтропии***. Атаки воспринимаются как точки, принадлежащие какому-то аномальному классу, для чего требуются заметные затраты памяти. Энтропия множества X вычисляется по формуле:

$$H(X) = -\sum_{x \in X} P(x) \cdot \log_2 P(x), \qquad (1)$$

где $P(x)$ — вероятность попадания события x в множество X.

Затраты памяти — вынужденная необходимость, обусловленная тем утверждением, что чем больше уникальных записей, тем равномернее их распределение относительно заданных классов множества X, отчего энтропия увеличивается [3].

3. Методы на основе знаний

Методы из данной группы чаще применяются для обнаружения злоупотреблений, т. е. на основе известных данных об атаках. Самыми распространенными среди них выступают ***сигнатурные методы***. По известным сигнатурам атак, составленных в виде регулярных выражений или правил на основе образца, проверяются текущие события, и становится точно известно, какое из них характеризует вторжение. Однако незнакомые сценарии вторжений и попросту неизвестные атаки останутся незамеченными. Помимо проблем с адаптивностью, подобным СОВ из-за больших баз сигнатур присуща низкая производительность [7].

Большей гибкостью обладают ***языки описания сценариев атак***, но из-за вычислительной сложности быстродействующими эти методы назвать нельзя. Эта проблема в меньшей степени серьезна для ***анализа систем состояний***, когда функционирование системы представляется в виде ориентированного графа с недопустимыми путями с опасными конечными состояниями[4]. Достаточно построить часть графа, чтобы выявить известные недопустимые пути, и это приводит к тому же недостатку, что и у сигнатурных методов — отсутствию адаптивности [3].

Еще один наглядный метод обнаружения злоупотреблений — анализ переходов состояний на основе раскрашенных ***сетей Петри***. Он реализован в СОВ *IDIOT* (англ. *Intrusion Detection In Our Time*). Сценарии вторжений преобразуются в шаблоны, с которыми сравниваются поступающие события безопасности. Достоинство метода — упреждение атаки, существенный недостаток — сложность реализации [3].

Система обнаружения вторжений *Snort* с открытым исходным кодом, считающаяся де-факто стандартом сигнатурных СОВ, также нередко называется ***экспертной системой***. Для таких реализаций характерны правила, которые называются продукционными. По сути, они представляют действие по условию, что приводит к быстродействию и точности работы. Однако перед началом применения необходимо набрать достаточно примеров, на основе которых и будут созданы искомые правила. Этот подход приводит к такому описанному выше недостатку, как адаптивность к неизвестным атакам [3].

Последним из методов обнаружения злоупотреблений рассмотрим ***метод проверки на модели***. Поскольку атака состоит из ряда отдельных операций, а также предпосылок, целей и ожидаемых результатов, можно сформировать поведенческие сценарии. От поведенческих методов он отличается, *во-первых*, стороной рассмотрения (злоупотребления вместо аномалий), а *во-вторых*, поиском подмножеств указанных сценариев атак. Другими словами, если в записях аудита обнаружится искомое подозрительное подмножество, так называемый антисипатор («предвосхититель») определяет, какие действия со стороны злоумышленника возможны следующими. Их планировщик более вни-

[4] См.: *Гамаюнов Д. Ю.* Обнаружение компьютерных атак на основе анализа поведения сетевых объектов : дисс. … канд. физ.-мат. наук: 05.13.11. М., 2007. 88 с.

мательно «высматривает» в записях аудита, предварительно преобразовав варианты поведения в системно-аудитозависимые выражения. Подозрения могут как оправдаться, так и быть опровергнуты, что влияет на вероятность наличия атаки в системе.

Благодаря тому, что «предвосхититель» начинает с обобщенных записей аудита, проверять все подряд необязательно — повышается быстродействие и точность. Планировщик обеспечивает независимость представления от формы данных аудита, т. е. универсальность. Однако все это хорошо лишь в теории, а практическая реализация сопряжена с проблемами отбора содержательных и точных количественных характеристик для разных частей графического представления модели и трудностями создания эффективного программного прототипа. Также метод нельзя назвать самостоятельным, не требующим применения других, он лучше работает вместе с подсистемой обнаружения аномалий [3].

4. Методы машинного обучения

Вышеперечисленные методы основаны, вне зависимости от стороны рассмотрения, на каких-то данных или знаниях, отчего большинству из них характерны значительные временные затраты, низкая производительность и (или) отсутствие гибкости, адаптивности [3]. Начиная с появления первого перцептрона, нейронные сети переживали то периоды подъема интереса к ним, то упадка. Сейчас мы наблюдаем очередную волну популярности, что подстегивается развитием вычислительных технологий. Методы машинного обучения и вычислительного интеллекта нашли применение и в области информационной безопасности.

Методы интеллектуального анализа могут в равной мере применяться для распознавания и аномалий, и злоупотреблений. Совершенно не важно, какой подход реализуется: искусственные нейронные сети (ИНС) и им подобные алгоритмы справятся с выявлением обоих типов подозрительной деятельности, обеспечивая бóльшую гибкость, нежели, к примеру, сигнатурные методы или экспертные системы [3].

Нейронные сети — лишь один из методов решения проблемы выявления атак. Наряду с ними существует еще множество других алгоритмов. Среди них: генетические и роевые алгоритмы, использование нечеткой логики, алгоритмы кластеризации, байесовские сети и метод, иммунные сети, деревья решений и др. Рассмотрим некоторые из них, и начнем с методов именно машинного обучения.

Метод ***деревьев решений*** может напомнить продукционные правила экспертных систем, но ему присуща адаптивность, повышение быстродействия, точность и верифицируемость[5]. Тем не менее, будучи вероятностным методом, стопроцентной точности обнаружения вторжений он не дает, причем чем меньше исходных данных для обучения, тем хуже результат [3]. Случайный лес, как ансамблевый алгоритм на основе деревьев решений, дает высокую точность (от 97%) распознавания атак и подтверждает свою эффективность в условиях, близких к реальным [8]. Деревья решений могут выступать в качестве метода обучения с учителем для обнаружения аномалий [9].

Следующими рассмотрим *байесовскую сеть* и ее частный случай — ***байесовский метод***. Они основаны на известной теореме Байеса, позволяя, таким образом, оценить апостериорную вероятность принадлежности события тому или иному классу. Для этого создается модель, где кодируются вероятностные отношения между событиями-переменными, а затем вычисляются условные вероятности их наступления. Байесовский метод иначе называется наивным байесовским классификатором, и его особенность — в предположении, что входные переменные независимы друг от друга. Из достоинств следует отметить возможность работы в режиме реального времени и обнаружение конкретных аномалий. Однако необходимо учитывать влияние измерений друг на друга, что сильно усложняет сам метод [3].

5. Методы вычислительного интеллекта

Именно к методам вычислительного интеллекта относится применение искусственных нейронных и иммунных сетей, генетических и роевых алгоритмов, опорных векторов и другие подходы к решению проблемы распознавания вторжений. Всем им, за исключением разве что метода опорных векторов, присуще «подглядывание» цепочки действий у живых существ (отдельного организма либо целой популяции) в переложении на язык математики.

Другими словами, машина реализует алгоритм, имитирующий явления живой природы, более гибкий в плане реакции на окружающий мир и при этом вычислительно более быстрый по сравнению с ней же. Так, ***нейронные сети*** способны по неполным данным делать выводы о новых объектах, в данном случае — относить их к тому или иному классу атак. При этом, как и живые существа, они могут ошибаться, а могут и верно догадываться. Все зависит от того, насколько хорошо они обучились и на какой обучающей выборке [10]. Возможность самообучения избавляет подобные системы от постоянного обновления сигнатур, уменьшает время реакции СОВ на аномалию сетевого трафика и позволяет увеличить объемы пропускаемого трафика, что ведет к обеспечению более высокого уровня защищенности информации [7].

Сети Кохонена [8], рекуррентные нейронные сети или сети глубокого доверия с применением классификатора с памятью способны эффективно распознавать

[5] См.: Брюховецкий А. А. Скатков А. В., Березенко П. О. Обнаружение уязвимостей в критических приложениях на основе решающих деревьев // Радиоэлектронные и компьютерные системы. № 5 (64). Харьков: Изд-во ХАИ, 2013. С. 18—23

низкоинтенсивные *DDoS*-атаки. Если обучить систему на нормальном трафике с небольшой примесью аномальных событий, что имитирует поведение реальных информационных систем, количество ошибок первого рода будет сведено до минимума [11].

Более сложным, хотя и похожим, методом выступают ***искусственные иммунные сети*** (ИИС), основанные на иммунной системе человека[6]. В основе их обучения лежат, как правило, такие алгоритмы, как отрицательный отбор и клональная селекция [3]. Первый отвечает за обнаружение только внешних антигенов, а значит, они способны отличить свои элементы от чужеродных. При этом генерируемые антитела рассматриваются как правила, описываемые формулой:

$$R^k: if\ x_1 \in \left[\min_1^k, \max_1^k\right] \wedge \ldots \wedge x_n \in \left[\min_n^k, \max_n^k\right] then\ anomaly, \quad (2)$$

где R^k — k-е правило, которое можно воспринимать как n-мерный гиперкуб с ребрами и $\min_1^k$, а $\max_1^k$, а $\{x_1, \ldots, x_n\}$— параметры подозрительного трафика (антигена).

Второй метод представляет собой эволюционный алгоритм для решения задач оптимизации[7]. В нем используется клональная селекция, а в качестве обучающей и тестовой выборок — данные базы данных *KDD Cup* 1999, что широко распространено в теоретических трудах. Результаты ИИС выявили достаточно высокую оценку распознавания, от 79,40% для *R*2L-атак (удаленных) до 93,42% для нормальных событий сетевого трафика.

Еще одним «биологическим» методом являются генетические алгоритмы (ГА). Если искусственные иммунные сети берут за основу иммунную систему человека, то ГА имитируют биологические принципы естественного отбора, математически представляя скрещивание и мутации в ходе эволюции генов. Нередко генетические алгоритмы применяют вместе с другими моделями классификации данных, например, с элементами нечеткой логики, рассмотренными выше деревьями решений, иммунными сетями и др. Эксперименты показали бóльшую эффективность обнаружения шаблонов атак и меньшее ресурсопотребление по сравнению с СОВ *Snort* [3].

Рассмотрим также метод опорных векторов (*SVM*, от англ. *support vector machine*), который часто применяется для классификации элементов из двух линейно разделимых множеств. Все множество разбивается гиперплоскостью, задаваемой линейной комбинацией нескольких опорных векторов из обучающей выборки. Если элемент оказался по одну сторону разделителя, значит, он в таком-то классе, иначе — в другом. Возможна линейная неразделимость на два множества, что влечет за собой условие для минимизации ошибки распознавания (так называемый штраф), либо же применяется линейное, полиномиальное или гауссовское ядро (отображение) для перехода к спрямляющим пространствам. Возникает сложность интерпретации параметров модели, а также невозможность калибровки вероятности попадания в определенный класс [3].

Для выявления удаленных атак и атак, направленных на повышение полномочий, можно взять за основу линейный дискриминант Фишера[8], а в качестве источника данных использовать базу данных *KDD Cup* 1999, из которой убрать признаки, наименее существенные для каждого отдельно взятого класса атак. Хотя для *U2R* результаты оказываются равны 99,9%, такой подход показал себя довольно посредственно (73,2% против 99,981% с помощью нейронных сетей на базе метода главных компонентов) в случае *R2L*.

Следует заметить, что *метод главных компонентов* часто используют для отбора значимых данных, но порой необходимо аннулировать корреляции между координатами, откуда берутся альтернативные способы избавления от избыточности [12]. Важность отбора признаков, наиболее полезных для распознавания образов, показана в [13], где сравнивались показатели точности выявления компьютерных атак без метода многофакторного анализа *ANOVA* и с ним. Улучшение стало наиболее заметным для класса *R2L*-атак (почти 22%), наименьшим — для нормальных событий сетевого трафика (0,49%).

Из приведенных характеристик следует вывод о неточности распознавания методами интеллектуального анализа. Такова цена за привнесение адаптивности в процесс распознавания атак. Многое упирается, как и в других методах, в затраты памяти (впрочем, в *радиально-базисных нейронных сетях* они не столь значительны для больших объемов входных данных обучающей выборки, как для ИНС *прямого распространения*) или в снижение производительности из-за вычислительной сложности алгоритма.

6. Гибридные методы

Решение проблемы с устранением недостатков различных методов лежит на поверхности: надо соединить два и более метода в один, гибридный, чтобы взять от обоих их преимущества, а недостатки оставить «оригинальным» алгоритмам [1]. Практическая реализация, безусловно, сложнее, однако можно достичь высоких показателей выявления вторжений путем нахождения наилучшего совмещения нескольких методов. Например, в [3] описан ансамбль из трех нейронных сетей, обученных разными алгоритмами, чьи выходные зна-

[6] См.: *Аграновский А.В., Хади Р.А.* Новый подход к защите информации — системы обнаружения компьютерных угроз // Jet Info: Информ. бюл. 2007. 4(167). 24 с.

[7] См.: *Брюховецкий А.А., Скатков А.В.* Адаптивная модель обнаружения вторжений в компьютерных сетях на основе искусственных иммунных систем // Электротехнические и компьютерные системы. № 12 (88). Одесса : ОНПУ, 2013. С. 102—111.

[8] См.: *Jeya P.G., Ravichandran M., Ravichandran C.S.* Efficient Classifier for R2L and U2R Attacks. International Journal of Computer Applications, vol. 45, 21, NY: Foundation of Computer Science, 2012, pp. 28-32.

чения подавали на вход процедуры взвешенного голосования и голосования по большинству (метод опорных векторов), и добились точности более 99%.

Приведенный пример как нельзя лучше подкрепляет утверждение о более высокой эффективности гибридных методов и подсказывает направление дальнейших изысканий. Теоретически мы допускаем, что ансамбль нейронных сетей, прошедших различное обучение, в совокупности с еще одной, «суммирующей» ИНС, обеспечат лучшие показатели как для выявления нормальных событий сетевого трафика, так и попыток вторжений.

Применение нейросетевого метода описано, например, в [14—16] для обнаружения низкоинтенсивных *DDoS*-атак на *web*-сервисы. В отличие от вышеприведенного классификатора с памятью [16], в качестве метода используется ансамбль одинаковых нейронных сетей для каждого сервиса (порта), величина окна задается в зависимости от данных, размерность уменьшают за счет кластеризации векторов самоорганизующейся картой, а вектора подают на вход многослойному перцептрону. Результаты даны с позиций ошибок первого и второго рода, которые не превышают 12% и 84%, соответственно, на одном и том же эксперименте с недостаточными данными, в основном же величина ошибки первого рода не превышает 6%, а второго рода — 10%. С учетом трудностей выявления низкоинтенсивных *DDoS*-атак, подобные результаты также подтверждают перспективность использования гибридных методов.

Не все «чистые» методы можно объединить так, чтобы получилась эффективная система защиты информации. Не имеет смысла использовать два и более метода, если их общие недостатки не компенсируются, а наоборот, усугубляются. Поэтому соберем все выделенные отрицательные стороны рассмотренных методов в табл. 1.

Таблица 1

Недостатки методов распознавания атак

Метод	Группы недостатков				
	Затраты времени	Затраты памяти	Сложность реализации	Нет адаптивности	Неточность (на известных данных)
1. Поведенческие методы					
Вейвлет-анализ	+		+		
Спектральный анализ	+		+		
Статистический анализ		+			+
Анализ энтропии		+			+
2. Методы на основе знаний					
Сигнатурные методы	+	+		+	
Языки описания сценариев атак	+		+		
Анализ систем состояний				+	
Сети Петри			+		
Экспертные системы		+		+	
Метод проверки на модели			+		
3. Методы машинного обучения					
Деревья решений					+
Байесовские сети			+		
Байесовский метод			+		
4. Методы вычислительного интеллекта					
Нейронные сети					+
Иммунные сети					+
Генетические алгоритмы	+		+		+
Метод опорных векторов			+		

В табл. 1 не учитываются некоторые специфические недостатки, такие, как, например, применимость метода опорных векторов только для двух классов. Также следует заметить, что приведенными методами их многообразие не ограничивается. Нейронные сети в совокупности с методами на основе знаний (допустим, сигнатурными методами) потенциально могут дать высокие результаты с позиции точности, так как ИНС способны обучаться на базе данных сигнатур известных атак и делать выводы о принадлежности незнакомых событий сетевого трафика к конкретному классу, не имея жесткой зависимости от базы сигнатур [17].

Ввиду приведенных выше примеров дополнительную точность могут придать ансамблевые структуры [3, 8, 15]. Однако чрезмерное употребление этого подхода может привести, напротив, к затратам как времени, так и памяти. В рамках задачи распознавания компьютерных атак необходимо снизить количество ошибок *второго рода* (пропуски цели), а также получить, по возможности, малое число ошибок *первого рода* (ложные тревоги).

С учетом изложенного теоретически эффективным гибридным методом представляется ансамбль нейронных сетей, не только обученных на множестве известных сигнатур различных событий сетевого трафика, но и учитывающих их непосредственно при принятии решения, что можно описать формулой:

$$K(x) = \begin{cases} \left[\frac{\sum_{i=1}^{n} \frac{T_i SK^2(x)}{P_i(x)}}{n}\right], SK(x) \neq 0 \\ \left[\frac{\sum_{i=1}^{n} T_i P_i(x)}{n}\right], SK(x) = 0 \end{cases} \quad (3)$$

где x — событие сетевого трафика; n — количество ИН; $K(x)$ — класс события x; T_i — точность i-й ИНС (уровень ложной тревоги); $P_i(x)$ — вероятный класс события x для i-й ИНС; $SK(x)$ — класс события x (если известна его сигнатура).

Пример с несколькими вариантами распределения значений класса (от 0 — для незнакомых событий и от 1 до 5 — для известных) приведен в табл. 2. Там же приведены результаты вычисления класса по формуле (3): округленные и приведенные с точностью до одного знака после запятой. Можно видеть, что в данном случае правила округления вынуждены отличаться от обычных, так как, например, 6 класса не существует, а 0 класс предназначен для незнакомых событий сетевого трафика.

Таблица 2

Теоретический эксперимент

$SK(x) \setminus T_i$	0,7	0,3	0,9	
1	4	3	2	1 (0,2)
3	2	2	2	3 (2,8)
0	3	4	1	1 (1,4)
5	5	1	4	5 (5,5)
3	1	2	5	3 (3,1)

Заключение

Таким образом, рассмотрено около двадцати существующих подходов, которые можно условно разделить на четыре группы, а также два направления поисков:

1. **Для поиска аномалий:**
1.1. Поведенческие методы.
1.2. Методы интеллектуального анализа данных.
2. **Для поиска злоупотреблений:**
2.1. Методы на основе знаний.
2.2. Методы интеллектуального анализа данных.

Методы интеллектуального анализа данных, в свою очередь, делятся на методы машинного обучения и *методы вычислительного интеллекта* (при этом, например, искусственные нейронные сети иногда относят к методам машинного обучения, поэтому представленное деление условно).

Также выделяются *гибридные методы*, представляющие интерес для перспективных исследований задачи распознавания компьютерных атак. К гибридным методам еще относятся *ансамблевые*, которые могут состоять как из нескольких реализаций одного подхода (так, в предлагаемом методе ансамбль состоит как минимум из трех ИНС, обученных на различных выборках образцов), так и различных подходов одной из вышеописанных групп.

Рассмотренные методы проанализированы с точки зрения преимуществ и недостатков. Последние были подвергнуты сравнительному анализу, на основе которого предложен *гибридный метод*, использующий адаптивность нейронных сетей и точность сигнатурных методов.

Теоретический эксперимент (см. табл. 2) удостоверяет целесообразность применения предложенного метода в несигнатурных системах обнаружения вторжений, что может обеспечить более высокий уровень защищенности информационных систем и сетей.

Рецензент: ***Цирлов Валентин Леонидович,*** *кандидат технических наук, доцент Московского государственного технического университета им. Н.Э. Баумана, г. Москва, Россия.*
E-mail: v.tsirlov@npo-echelon.ru

Литература

1. Ананьин Е. В., Кожевникова И. С., Лысенко А. В., Никишова А. В. Методы обнаружения аномалий и вторжений // Проблемы современной науки и образования. № 34 (76). Иваново : Олимп, 2016. С. 48—50.
2. Добкач Л. Я. Анализ эффективности систем обнаружения вторжений // Труды Всеросс. студ. конф. «Студенческая научная весна», посвященная 165-летию со дня рождения В. Г. Шухова» / Росмолодежь, МГТУ им. Н.Э. Баумана, СНТО им. Н.Е. Жуковского. М. : Изд. дом «Научная библиотека», 2018. С. 314—315.
3. Браницкий А. А., Котенко И. В. Анализ и классификация методов обнаружения сетевых атак // Труды СПИИРАН. № 2 (45). СПб. : ФГБУН «СПИИРАН», 2016. С. 207—244.
4. Вишневский А. С. Обманная система для выявления хакерских атак, основанная на анализе поведения посетителей веб-сайтов // Вопросы кибербезопасности. 2018. №3 (27). С. 54—62. DOI:10.21681/2311-3456-2018-3-54-62.
5. Микова С. Ю., Оладько В. С. Результат исследования алгоритмов выявления сетевых аномалий // Вопросы кибербезопасности. 2015. № 4(12). С. 38—41. DOI: 10.21681/2311-3456-2015-4-38-41.
6. Ieracitano C., Adeel A., Gogate M. [etc.] Statistical Analysis Driven Optimized Deep Learning System for Intrusion Detection. Proc. of the 9th International Conference on Brain Inspired Cognitive Systems (BICS 2018), Cham: Springer, 2018, pp. 759-769.
7. Кусакина Н. М. Методы анализа сетевого трафика как основа проектирования системы обнаружения сетевых атак // Труды XLI Междунар. науч.-прак. конф. "International Scientific Review of the Problems and Prospects of Modern Science and Education". Boston: Problems of Science, 2018. С. 28—31.
8. Кочетов Д. А., Лукащик Е.П. Нейросетевая технология обнаружения сетевых вторжений // Прикаспийский журнал: Управление и высокие технологии. 2018. № 2 (42). С. 104—112.
9. Шелухин О. И., Рябинин В. С., Фармаковский М. А. Обнаружение аномальных состояний компьютерных систем средствами интеллектуального анализа данных системных журналов // Вопросы кибербезопасности. 2018. № 2 (26). С. 33—43. DOI: 10.21681/2311-3456-2018-2-33-43.
10. Добкач Л. Я. Создание модуля распознавания атак для систем обнаружения вторжений // Труды Всеросс. студ. конф. «Студенческая научная весна», посвященная 85-летию Ю.А. Гагарина» / МГТУ им. Н.Э. Баумана, СНТО им. Н.Е. Жуковского. М. : Изд. дом «Научная библиотека», 2019. С. 36—37.
11. Чисоходова А. А., Сидоров И. Д. Модернизированный метод обнаружения низкоинтенсивных распределенных атак типа «отказ в обслуживании» // Успехи современной науки. 2017. Т. 1. С. 169—175.
12. Петрова В. И., Платонов В. В. Исследование методов сокращения размерности для обнаружения сетевых атак // Труды студ. науч. конф. «Информатика и кибернетика (COMCON-2016)» / Институт компьютерных наук и технологий. СПб. : СПбПУ им. Петра Великого, 2016. С. 210—213.
13. Марков Р. А., Бухтояров В. В., Попов А. М., Бухтоярова Н. А. Подход к выявлению инцидентов информационной безопасности // Научно-технический вестник Поволжья. 2016. № 1. С. 78—80.
14. Тарасов Я. В. Исследование применения нейронных сетей для обнаружения низкоинтенсивных DDoS-атак прикладного уровня // Вопросы кибербезопасности. 2017. № 5 (24). С. 23—29. DOI: 10.21681/2311-3456-2017-5-23-29.
15. Абрамов Е. С., Тарасов И.В. Применение комбинированного нейросетевого метода для обнаружения низкоинтенсивных DDoS-атак на web-сервисы // Инженерный вестник Дона. 2017. № 3 (46). С. 59.
16. Слесарчик К. Ф. Метод обнаружения низкоинтенсивных распределенных атак отказа в обслуживании со случайной динамикой характеристик фрагментации и периодичности // Вопросы кибербезопасности. 2018. № 1 (25). С. 19—27. DOI: 10.21681/2311-3456-2018-1-19-27.
17. Modorskiy A. M., Minzov A. S., Baronov O. R., Nevskiy A. Y. LAN Abnormalities Threat Detection: An Outlook and Applicability Analysis // Вопросы кибербезопасности. 2018. № 1(25). С. 11—18. DOI: 10.21681/2311-3456-2018-1-11-18.

AN ANALYSIS OF METHODS FOR IDENTIFYING COMPUTER ATTACKS

Leonid Dobkach, *Ph.D. student at the Bauman Moscow State Technical University, Russian Federation, Moscow.*
E-mail: dobkachleo@mail.ru

Keywords: *intrusion detection, behavioural methods, knowledge-based methods, attack signatures, decision trees, artificial neural networks, hybrid methods.*

Abstract.

Purpose of the paper: *studying the existing intrusion detection methods from the perspective of their advantages and drawbacks, as well as considering their classification.*

Methods of study: *comparative analysis, statistical analysis, signature-based analysis, graph theory, Bayesian method.*

Results obtained: *intrusion detection methods can be loosely divided into four groups: behavioural methods (suitable for searching anomalies), knowledge-based methods (suitable for searching abuses), and data mining methods (suitable for both search directions), the latter splitting into machine learning methods and computational intelligence methods. A promising group of such methods are hybrid methods combining elements of different 'pure' methods, and based on a comparison of the most significant weaknesses of analysed methods, a hybrid method using the strengths of artificial neural networks as well as of signature-based methods is put forth.*

References

1. Anan'in E. V., Kozhevnikova I. S., Lysenko A. V., Nikishova A. V. Metody obnaruzheniia anomalii i vtorzhenii. Problemy sovremennoi nauki i obrazovaniia, No. 34 (76), Ivanovo : Olimp, 2016, pp. 48-50.
2. Dobkach L. Ia. Analiz effektivnosti sistem obnaruzheniia vtorzhenii. Trudy Vseross. stud. konf. "Studencheskaia nauchnaia vesna", posviashchennaia 165-letiiu so dnia rozhdeniia V. G. Shukhova", Rosmolodezh', MGTU im. N.E. Baumana, SNTO im. N.E. Zhukovskogo, M. : Izd. dom "Nauchnaia biblioteka", 2018, pp. 314-315.
3. Branitskii A. A., Kotenko I. V. Analiz i klassifikatsiia metodov obnaruzheniia setevykh atak. Trudy SPIIRAN, No. 2 (45), SPb. : FGBUN "SPIIRAN", 2016, pp. 207-244.
4. Vishnevskii A. S. Obmannaia sistema dlia vyiavleniia khakerskikh atak, osnovannaia na analize povedeniia posetitelei veb-saitov. Voprosy kiberbezopasnosti, 2018, No.3 (27), pp. 54-62, DOI: 10.21681/2311-3456-2018-3-54-62.
5. Mikova S. Iu., Olad'ko V. S. Rezul'tat issledovaniia algoritmov vyiavleniia setevykh anomalii. Voprosy kiberbezopasnosti, 2015, No. 4(12), pp. 38-41, DOI: 10.21681/2311-3456-2015-4-38-41.
6. Ieracitano C., Adeel A., Gogate M. [etc.] Statistical Analysis Driven Optimized Deep Learning System for Intrusion Detection. Proc. of the 9th International Conference on Brain Inspired Cognitive Systems (BICS 2018), Cham: Springer, 2018, pp. 759-769.
7. Kusakina N. M. Metody analiza setevogo trafika kak osnova proektirovaniia sistemy obnaruzheniia setevykh atak. Trudy XLI Mezhdunar. nauch.-prak. konf. "International Scientific Review of the Problems and Prospects of Modern Science and Education", Boston: Problems of Science, 2018, pp. 28-31.
8. Kochetov D. A., Lukashchik E.P. Neirosetevaia tekhnologiia obnaruzheniia setevykh vtorzhenii. Prikaspiiskii zhurnal: Upravlenie i vysokie tekhnologii, 2018, No. 2 (42), pp. 104-112.
9. Shelukhin O. I., Riabinin V. S., Farmakovskii M. A. Obnaruzhenie anomal'nykh sostoianii komp'iuternykh sistem sredstvami intellektual'nogo analiza dannykh sistemnykh zhurnalov. Voprosy kiberbezopasnosti, 2018, No. 2 (26), pp. 33-43, DOI: 10.21681/2311-3456-2018-2-33-43.
10. Dobkach L. Ia. Sozdanie modulia raspoznavaniia atak dlia sistem obnaruzheniia vtorzhenii. Trudy Vseross. stud. konf. "Studencheskaia nauchnaia vesna", posviashchennaia 85-letiiu Iu.A. Gagarina", MGTU im. N.E. Baumana, SNTO im. N.E. Zhukovskogo, M. : Izd. dom "Nauchnaia biblioteka", 2019, pp. 36-37.
11. Chistokhodova A. A., Sidorov I. D. Modernizirovannyi metod obnaruzheniia nizkointensivnykh raspredelennykh atak tipa "otkaz v obsluzhivanii". Uspekhi sovremennoi nauki, 2017, t. 1, pp. 169-175.
12. Petrova V. I., Platonov V. V. Issledovanie metodov sokrashcheniia razmernosti dlia obnaruzheniia setevykh atak. Trudy stud. nauch. konf. "Informatika i kibernetika (COMCON-2016)", Institut komp'iuternykh nauk i tekhnologii, SPb. : SPbPU im. Petra Velikogo, 2016, pp. 210-213.
13. Markov R. A., Bukhtoiarov V. V., Popov A. M., Bukhtoiarova N. A. Podkhod k vyiavleniiu intsidentov informatsionnoi bezopasnosti. Nauchno-tekhnicheskii vestnik Povolzh'ia, 2016, No. 1, pp. 78-80.
14. arasov Ia. V. Issledovanie primeneniia neironnykh setei dlia obnaruzheniia nizkointensivnykh DDoS-atak prikladnogo urovnia. Voprosy kiberbezopasnosti, 2017, No. 5 (24), pp. 23-29, DOI: 10.21681/2311-3456-2017-5-23-29.
15. Abramov E. S., Tarasov I.V. Primenenie kombinirovannogo neirosetevogo metoda dlia obnaruzheniia nizkointensivnykh DDoS-atak na web-servisy. Inzhenernyi vestnik Dona, 2017, No. 3 (46), pp. 59.
16. Slesarchik K. F. Metod obnaruzheniia nizkointensivnykh raspredelennykh atak otkaza v obsluzhivanii so sluchainoi dinamikoi kharakteristik fragmentatsii i periodichnosti. Voprosy kiberbezopasnosti, 2018, No. 1 (25), pp. 19-27, DOI: 10.21681/2311-3456-2018-1-19-27.
17. Modorskiy A. M., Minzov A. S., Baronov O. R., Nevskiy A. Y. LAN Abnormalities Threat Detection: An Outlook and Applicability Analysis. Voprosy kiberbezopasnosti, 2018, No. 1(25), pp. 11-18, DOI: 10.21681/2311-3456-2018-1-11-18.

Над номером работали:

Начальник РИО	*Ю.В. Матвиенко*
Шеф-редактор	*Г.И. Макаренко*
Редактор-переводчик	*Т.В. Галатонов*
Дизайн обложки	*И.Г. Колмыкова*
Верстка	*Н.Г. Шабанова*