DOI: http://dx.doi.org/10.21686/2413-2829-2024-6-123-130



# УПРАВЛЕНИЕ РИСКАМИ КАК ЭЛЕМЕНТ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ В КОМПАНИЯХ, РАБОТАЮЩИХ В СФЕРЕ ЦИФРОВЫХ ТЕХНОЛОГИЙ

**С. П. Бурланков**
Российский экономический университет имени Г. В. Плеханова, Москва, Россия
**К. О. Семёнов**
Московский финансово-юридический университет МФЮА, Москва, Россия
**Е. В. Галактионова**
Научно-исследовательский институт гуманитарных наук
при Правительстве Республики Мордовия,
Саранск, Республика Мордовия, Россия
**В. А. Комаров**
Национальный исследовательский Мордовский государственный университет
им. Н. П. Огарёва, Саранск, Республика Мордовия, Россия

В статье показана сущность экономической безопасности с выделением ее основных компонентов; дана общая классификация угроз экономической безопасности. Особо выделена информационная безопасность как ключевая составляющая экономической безопасности в ИТ-компаниях. Авторы рассматривают понятие цифровой инфраструктуры компании, выделяя ключевые угрозы сферы информационной безопасности и задачи по ее обеспечению. Исследователями особое внимание акцентировано на необходимости использования комплексного и системного подходов при обеспечении информационной безопасности. Проведен анализ основных методов обеспечения информационной безопасности, включая правовые, технические, организационные, а также отмечены современные продвинутые технологии защиты информации: блокчейн, большие данные, искусственный интеллект, машинное обучение, нейронные сети.
*Ключевые слова*: ИТ-компании, цифровизация, информационная безопасность, технологии защиты информации.

# RISK MANAGEMENT AS ELEMENT OF ECONOMIC SECURITY IN COMPANIES WORKING WITH DIGITAL TECHNOLOGIES

**Stepan P. Burlankov**
Plekhanov Russian University of Economics, Moscow, Russia
**Kirill O. Semenov**
Moscow University of Finance and Law MFUA, Moscow, Russia
**Ekaterina V. Galaktionova**
Research Institute of Humanities by the Government of the Republic of Mordovia,
Saransk, Republic of Mordovia, Russia
**Vladimir A. Komarov**
National Research Ogarev Mordovia State University,
Saransk, Republic of Mordovia, Russia

The article shows the essence of economic security and identifies its key elements, the general classification of threats to economic security is provided. Special attention is paid to information security as a key component of

economic security in IT companies. The authors study the notion of digital infrastructure in the company and highlight key threats to information security and ways of its provision. The researchers focus on necessity to use complex and systemic approaches to providing information security. Principle methods of providing information security were analyzed, including legal, technical and organizational. At the same time advanced technologies of information protection were mentioned, such as blockchain, big data, artificial intellect, computer learning, and neuron nets.
*Keywords*: IT companies, digitalization, information security, technologies of information protection.

В последние годы в нашей стране, как и во многих зарубежных странах, возрастает роль цифровых технологий. Эта отрасль включает компании, работающие в сфере телекоммуникаций, хранения и обработки данных, разработки и выпуска аппаратного и программного обеспечения. Цифровые технологии активно внедряются практически во все сферы народного хозяйства и образуют фундамент нового технологического уклада.

В современных условиях особую актуальность приобретает обеспечение экономической безопасности компаний, работающих в сфере цифровых информационных технологий (ИТ-компаний). Технологии непрерывно совершенствуются, в связи с чем постоянно возникают новые уязвимости информационных систем и угрозы для субъектов, работающих в цифровой среде. Поэтому ИТ-компании вынуждены проводить тщательный мониторинг угроз и принимать соответствующие меры по обеспечению собственной безопасности.

Одним из важнейших компонентов экономической безопасности компаний, работающих в сфере цифровых технологий (как и компаний многих других отраслей), в настоящее время стала информационная безопасность. От ее обеспечения зависят сохранность и нормальное использование не только информационных, но и всех прочих видов ресурсов компании: финансовых, материальных, кадровых.

Информация является стратегическим ресурсом ИТ-компаний. Она составляет основу их продуктов и услуг, а также ключевых внутренних бизнес-процессов. Таким образом, данный ресурс имеет критическое значение для экономической безопасности компаний рассматриваемой отрасли. Рациональное и безопасное оперирование информационными массивами и потоками – залог выживания, рыночной и финансовой устойчивости, а также прибыльности цифрового бизнеса в долгосрочном периоде. К настоящему моменту в научной среде не сложилось единого подхода к определению термина «экономическая безопасность». Это связано прежде всего с тем, что экономическая безопасность предприятия в значительной степени зависит от особенности его бизнеса, отраслевой, страновой и региональной специфики. На рисунке приведены наиболее распространенные подходы к определению рассматриваемого понятия.

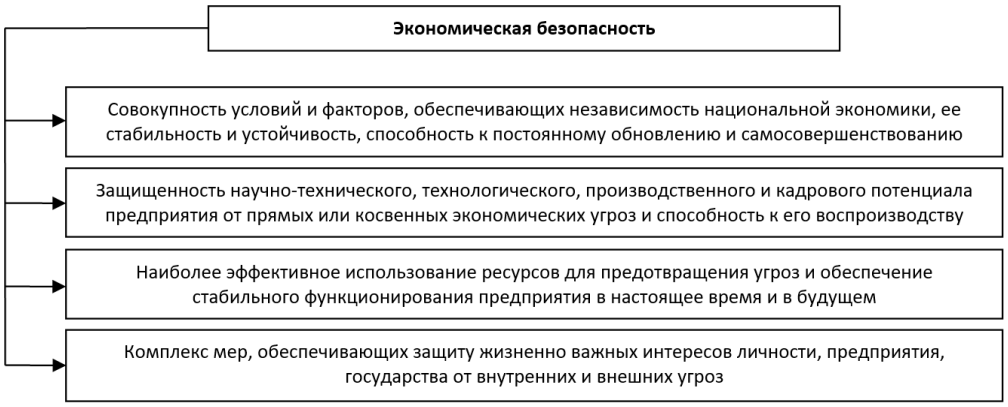


Рис. Подходы к трактовке термина экономическая безопасность [9]

По результатам анализа различных трактовок можно предложить следующее определение экономической безопасности предприятия: состояние хозяйствующего субъекта, характеризующееся его защищенностью от отрицательного воздействия внутренних и внешних факторов и эффективностью управления рисками, способными дестабилизировать финансово-экономическое положение предприятия.

Существуют две основные категории угроз экономической безопасности предприятия:

1. *Внутренние угрозы* (вредоносные действия (бездействия) персонала либо нештатное функционирование технических систем, обусловливающее риски для нормального функционирования предприятия).

2. *Внешние угрозы*, обусловленные воздействием различных факторов макро- и микросреды предприятия.

Для того чтобы противостоять этим угрозам, компания должна сформировать комплексную систему управления рисками экономической безопасности и разработать соответствующие стратегии и тактические планы работы в данной области.

К числу основных компонентов экономической безопасности относятся финансовый, кадровый, материально-технический, энергетический, информационный (в соответствии с видами используемых компанией ресурсов).

Для обеспечения безопасности по всем перечисленным компонентам необходимо задействовать штатных или привлеченных извне профильных специалистов, которые должны работать по следующим направлениям деятельности:

– обеспечение безопасности денежных потоков предприятия;

– безопасное управление персоналом;

– обеспечение сохранности материально-технических ресурсов;

– рациональное использование энергетических ресурсов;

– обеспечение сохранности и целостности используемой информации.

Деятельность компаний сферы цифровых технологий непосредственно связана с генерацией, хранением, обработкой и передачей на расстояние массивов данных. Речь идет о персональных данных клиентов, а также о служебной информации, обеспечивающей бизнес-процессы компаний. Эта информация является предметом повышенного интереса со стороны различного рода злоумышленников [4]. Кроме того, ИТ-компании эксплуатируют критически важную информационную инфраструктуру, поэтому их деятельность подвержена особому контролю со стороны государства.

Большую опасность для ИТ-компаний представляют кибератаки. Например, кибератака на оператора связи или оператора центра обработки данных может прервать нормальное обслуживание тысяч пользователей Интернета и телефонной связи, а атака на цифровую инфраструктуру банка или компании, специализирующейся на осуществлении электронных платежей, может привести к серьезным финансовым потерям. Кроме того, атаки на критическую информационную инфраструктуру могут нарушить нормальное функционирование экономики отдельных регионов и целой страны.

Количество кибератак постоянно растет. Согласно статистическим данным, за 2022 г. оно выросло на 54% по сравнению с 2021 г. Следует иметь в виду, что более 70% атак осуществляется в отношении субъектов малого и среднего бизнеса. При этом основной целью злоумышленников являются персональные и финансовые данные. В частности, в последние годы участились утечки персональных данных из телекоммуникационных компаний.

Таким образом, одна из ключевых задач в сфере экономической безопасности ИТ-компании – обеспечение защиты критически важной информации. Важность информационной безопасности тем выше, чем выше интенсивность использования компаниями цифровых систем и сложность этих систем. В связи с этим обеспе-

чение информационной безопасности чрезвычайно важно для компаний, работающих в сфере цифровых технологий.

Информационная безопасность компании – это состояние защищенности используемой информации, т. е. состояние, при котором обеспечиваются целостность, конфиденциальность, доступность и аутентичность данных [5].

Ключевой составляющей информационной безопасности ИТ-компании является безопасность цифровой инфраструктуры, которая включает:

– сетевые устройства и каналы связи;
– серверное оборудование;
– пользовательские компьютеры;
– пользовательские мобильные терминалы;
– центр обработки данных.

Необходимо поддерживать нормальное функционирование всех перечисленных компонентов цифровой инфраструктуры и обеспечивать их защиту от кибератак и физического вмешательства. С ростом сложности инфраструктуры (количества элементов и их взаимосвязей) растет и уровень рисков.

К числу наиболее серьезных угроз информационной безопасности современных ИТ- компаний можно отнести [8]:

– деятельность внешних злоумышленников, получающих несанкционированный доступ к информации компании, нарушающих ее целостность или использующих в противоправных целях;
– нарушение сотрудниками компании установленных правил сбора, обработки и обмена информацией в результате ошибок или халатности;
– умышленные действия сотрудников компании по отношению к информационным системам, направленные на причинение вреда бизнесу;
– ошибки при проектировании, внедрении и техническом обслуживании цифровых систем;
– поломки оборудования и сбои в работе программного обеспечения.

Отдельно следует выделить разновидности угроз для цифровых систем компании со стороны ее персонала:

– использование работниками служебного положения для доступа к конфиденциальной или критически важной информации, нарушение ее целостности или использование для нанесения вреда компании и получения личной выгоды;
– осуществление работниками вредоносных действий в обход существующих правил доступа к корпоративной информации;
– причинение вреда информационной инфраструктуре со стороны лиц, не находящихся в штате компании, но работающих по временным контрактам [7].

Внедрение в ИТ-компании каждого нового цифрового решения приводит к возникновению множества субъективных и объективных уязвимостей. Прогнозирование проблем такого рода является чрезвычайно сложной задачей, поэтому компания должна проводить регулярный мониторинг уязвимостей и своевременно перекрывать возможные пути утечки и порчи данных.

Существует множество задач обеспечения информационной безопасности компании. К их числу можно отнести:

– обеспечение безопасного хранения данных на различных носителях (в том числе в облачных хранилищах);
– защиту информации, передаваемой по телекоммуникационным каналам;
– управление правами доступа к различным информационным системам;
– резервное копирование данных;
– восстановление информации после аварий, сбоев, атак и т. д. [5].

Информационную безопасность компании необходимо обеспечивать на основе комплексного и системного подхода. Следует регулярно обновлять и пополнять базу данных угроз и принимать превентивные меры защиты.

В рамках системы информационной безопасности должен осуществляться постоянный контроль в реальном времени

всех ключевых состояний и событий, определяющих безопасность информации. Защиту цифровых систем необходимо осуществлять в режиме 24/7, при этом система информационной безопасности должна охватывать весь жизненный цикл данных: от их получения или генерации до архивирования или уничтожения.

На корпоративном уровне вопросы информационной и экономической безопасности курируют специальные подразделения (службы или отделы информационных технологий, персонала, безопасности и т. д.) [5].

Выделяют три категории методов обеспечения информационной безопасности: правовые, технические и организационные [6]. Все эти методы необходимо использовать комплексно с учетом их взаимосвязей. Необходимо четко регламентировать полномочия и ответственность различных подразделений компании в сфере информационной безопасности и организовать руководство из единого центра.

Правовые методы подразумевают организацию деятельности в сфере информационной безопасности в соответствии с действующей в стране и регионе законодательной базой, а также с внутренней нормативной документацией компании. Правовые акты позволяют не только эффективно регламентировать процессы, связанные с информационной безопасностью и протекающие внутри компании, но и организовать безопасный обмен информацией с клиентами, контрагентами, партнерами и государственными структурами. Отметим, что в России работает множество компаний, предлагающих услуги по правовому сопровождению защиты информации.

На практике применяется широкий арсенал технических методов обеспечения информационной безопасности:

– методы аутентификации и идентификации пользователей;
– криптографические методы;
– виртуальные частные сети;
– межсетевые экраны;
– методы фильтрации контента;
– методы проверки целостности данных на материальных носителях;
– антивирусы;
– средства анализа уязвимостей компьютерных систем.

Особую роль играют криптографические методы. В последнее время интерес компаний к ним значительно вырос в связи с учащением случаев перехвата коммерческой информации. Наибольшую популярность получили различные инструменты шифрования и кодирования данных. Также активно применяются методы сжатия информации. Для защиты передаваемых по сети аудиоданных используются инструменты аналогового скремблирования, а также инструменты цифрового шифрования.

В последнее время набирает популярность использование таких современных технологий обеспечения информационной безопасности, как блокчейн, большие данные, искусственный интеллект, технологии дистанционного обучения.

Блокчейн-технологии позволяют децентрализованно обрабатывать данные, контролировать их целостность и прозрачность. Они помогают предприятиям повысить свою информационную и экономическую безопасность, так как дают возможность организовать надежное хранение и обработку персональных данных, а также данных о транзакциях. Использование блокчейн-технологий подразумевает, что информация хранится не в единой базе данных, а на множестве узлов [2].

В российской предпринимательской среде большое значение при установлении партнерства имеет формирование доверительных отношений. Тем не менее многие компании предпочитают не полагаться исключительно на доверие, а дополнительно проверять своих контрагентов и использовать различные технологические инструменты, позволяющее повысить вероятность должного исполнения обязательств. К числу таких инструментов относится блокчейн.

Блокчейн-технологии дают возможность значительно повысить безопасность использования материальных, финансовых и трудовых ресурсов [1]. Преимуществами этих технологий являются прозрачность транзакций и отсутствие необходимости прибегать к услугам посредников. Это позволяет избежать искажения данных и снизить транзакционные издержки.

Следует отметить, что блокчейн-технологии позволяют защитить информацию и повысить прозрачность бизнес-процессов в значительно большей степени, чем любая существующая традиционная технология управления базами данных. Поэтому они используются в рамках корпоративных информационных систем при организации электронного нотариата. Кроме того, они интегрируются в различные цифровые торговые площадки.

Следующей важной технологией обеспечения информационной и экономической безопасности бизнеса является технология больших данных. Она позволяет применять специфические методы для анализа больших объемов информации, установления взаимосвязей и оценки их тесноты, построения имитационных моделей и решения многих других аналитических задач.

Особое место в современных системах обеспечения безопасности занимает искусственный интеллект. Данная технология позволяет значительно повысить эффективность анализа информации и разработки управленческих решений. Технология искусственного интеллекта непосредственно связана с машинным обучением и большими данными, а также с технологиями нейронных сетей [3].

Отдельного внимания заслуживают технологии дистанционного обучения. Они дают возможность значительно снизить издержки на обучение персонала и повысить его эффективность. Как известно, уровень профессиональных компетенций работников в значительной степени определяет состояние экономической безопасности предприятия.

В число организационных методов обеспечения информационной безопасности входят разработка внутренних регламентов работы с информацией, а также с аппаратным и программным обеспечением, документирование процедур сбора, обработки и передачи данных [5].

Комплексное использование описанных выше методов будет эффективным только в том случае, когда система информационной безопасности будет полностью интегрирована в систему экономической безопасности и в общий контур стратегического управления предприятием. Практика показывает, что большинство ИТ-компаний используют различные технические средства защиты информации (антивирусы, межсетевые экраны, средства шифрования и т. д.). Однако часто они не дают должного эффекта ввиду отсутствия системного подхода к обеспечению экономической безопасности. Более того, имея в своем распоряжении продвинутые аппаратные и программные средства защиты данных, многие компании не используют их возможности даже наполовину. Поэтому построение комплексной системы экономической безопасности в компании следует начинать с детальной формализации и оптимизации бизнес-процессов, четкого определения полномочий и ответственности сотрудников, а также с регламентирования всех процедур, имеющих отношение к обеспечению безопасности. Такой подход позволит минимизировать потери, связанные с нарушениями в работе информационных систем компании.

Список литературы

1. *Авраменко Г. М.* Блокчейн: новая информационная технология, меняющая парадигму экономического сознания // Медиаэкономика 21 века. – 2017. – № 4. – С. 17–20.

2. *Власов А. И., Карпунин А. А., Новиков И. П.* Системный анализ технологии обмена и хранения данных blockchain // Современные технологии. Системный анализ. Моделирование. – 2017. – № 3 (55). – С. 75–83.

3. *Галанов А. Э., Селюкова Г. П.* Нейронные сети и нейронные технологии // Актуальные вопросы науки и хозяйства: новые вызовы и решения : сборник материалов LIII Международной студенческой научно-практической конференции. – Ч. 2. – Тюмень, 2019. – С. 399–405.

4. Защита данных телекоммуникационных компаний: что такое угрозы и меры безопасности. – URL: https://rt-solar.ru/products/solar_dozor/blog/3525/ (дата обращения: 15.07.2023).

5. Обеспечение информационной безопасности предприятия. – URL: https://arinteg.ru/articles/informatsionnaya-bezopasnost-predpriyatiya-25799.html (дата обращения: 15.07.2023).

6. *Петрова Г. В.* Финансы и экономика «цифрового пространства»: правовые проблемы защиты и практика формирования международных и национальных норм // Проблемы экономики и юридической практики. – 2018. – № 1. – С. 118–122.

7. *Подледнов Д. Д.* Правовое и организационное обеспечение информационной безопасности: проблемы и решения // Аллея науки. – 2017. – Т. 2. – № 14. – С. 506–519.

8. *Северин В. А.* Концептуальные аспекты безопасности информации при производстве и реализации товаров // Безопасность бизнеса. – 2017. – № 1. – С. 30–35.

9. *Тимаев Р. А.* Понятие информационно-экономической безопасности предприятия // Проблемы материальной культуры. – 2018. – № 6. – С. 64–69.

References

1. Avramenko G. M. Blokcheyn: novaya informatsionnaya tekhnologiya, menyayushchaya paradigmu ekonomicheskogo soznaniya [Blockchain: Brand-New Information Technology Altering the Paradigm of Economic Consciousness]. *Mediaekonomika 21 veka* [Media-Economics of the 21st Century], 2017, No. 4, pp. 17–20. (In Russ.).

2. Vlasov A. I., Karpunin A. A., Novikov I. P. Sistemnyy analiz tekhnologii obmena i khraneniya dannykh blockchain [Systemic Analysis of Technology for Exchanging and Storing Data – Blockchain]. *Sovremennye tekhnologii. Sistemnyy analiz. Modelirovanie* [Advanced Technologies. Systemic Analysis. Modeling], 2017, No. 3 (55), pp. 75–83. (In Russ.).

3. Galanov A. E., Selyukova G. P. Neyronnye seti i neyronnye tekhnologii [Neuron Nets and Neuron Technologies]. *Aktualnye voprosy nauki i khozyaystva: novye vyzovy i resheniya: sbornik materialov LIII Mezhdunarodnoy studencheskoy nauchno-prakticheskoy konferentsii* [Acute Issues of Science and Economy: New Challenges and Solutions: collection of materials of the LIII International Students' Conference], part 2. Tyumen, 2019, pp. 399–405. (In Russ.).

4. Zashchita dannykh telekommunikatsionnykh kompaniy: chto takoe ugrozy i mery bezopasnosti [Protecting Data of Telecommunicating Companies: What do Threats and Security Measures Mean?]. (In Russ.). Available at: https://rt-solar.ru/products/solar_dozor/blog/3525/ (accessed 15.07.2023).

5. Obespechenie informatsionnoy bezopasnosti predpriyatiya [Providing Information Security to the Enterprise]. (In Russ.). Available at: https://arinteg.ru/articles/informatsionnaya-bezopasnost-predpriyatiya-25799.html (accessed 15.07.2023).

6. Petrova G. V. Finansy i ekonomika «tsifrovogo prostranstva»: pravovye problemy zashchity i praktika formirovaniya mezhdunarodnykh i natsionalnykh norm [Finance and Economy of 'Digital Space': Legal Problems of Protection and Practice of Designing International and National Standards]. *Problemy ekonomiki i yuridicheskoy praktiki* [Problems of Economics and Juridical Practice], 2018, No. 1, pp. 118–122. (In Russ.).

7. Podlednov D. D. Pravovoe i organizatsionnoe obespechenie informatsionnoy bezopasnosti: problemy i resheniya [Legal and Organizational Support of Information Security: Problems and Solutions]. *Alleya nauki* [Science Avenue], 2017, Vol. 2, No. 14, pp. 506–519. (In Russ.).

8. Severin V. A. Kontseptualnye aspekty bezopasnosti informatsii pri proizvodstve i realizatsii tovarov [Conceptual Aspects of Information Security in Manufacturing and Sale of Goods]. *Bezopasnost biznesa* [Business Security], 2017, No. 1, pp. 30–35. (In Russ.).

9. Timaev R. A. Ponyatie informatsionno-ekonomicheskoy bezopasnosti predpriyatiya [The Idea of Information and Economic Security of Enterprise]. *Problemy materialnoy kultury* [Issues of Material Culture], 2018, No. 6, pp. 64–69. (In Russ.).

**Сведения об авторах**

**Степан Петрович Бурланков**
доктор экономических наук, профессор,
профессор кафедры пищевых технологий
и биоинженерии РЭУ им. Г. В. Плеханова.
Адрес: ФГБОУ ВО «Российский экономический университет имени Г. В. Плеханова», 109992, Москва, Стремянный пер., д. 36.
E-mail: Burlankov.SP@rea.ru
ORCID: 0000-0001-9326-9006

**Кирилл Олегович Семёнов**
аспирант кафедры экономики
и государственного и муниципального управления МФЮА.
Адрес: АОЧУ ВО «Московский финансово-юридический университет МФЮА», 115191, Москва, ул. Серпуховский вал, д. 17, корп. 1.
E-mail: kirill_sem_1998@mail.ru

**Екатерина Владимировна Галактионова**
аспирантка НИИГН.
Адрес: Научно-исследовательский институт гуманитарных наук при Правительстве Республики Мордовия, 430005, Республика Мордовия, Саранск, ул. Л. Толстого, д. 3.
E-mail: frolova1@yandex.ru

**Владимир Александрович Комаров**
доктор технических наук, профессор,
профессор кафедры технического сервиса машин МГУ им. Н. П. Огарёва.
Адрес: ФГБОУ ВО «Национальный исследовательский Мордовский государственный университет им. Н. П. Огарёва» 430005, Республика Мордовия, Саранск, ул. Большевистская, д. 68.
E-mail: komarov.v.a2010@mail.ru
ORCID: 0000-0003-1910-2923

**Information about the authors**

**Stepan P. Burlankov**
Doctor of Economics, Professor,
Professor of the Department for Food Technology and Bioengineering of the PRUE.
Address: Plekhanov Russian University of Economics, 36 Stremyanny Lane, Moscow, 109992, Russian Federation.
E-mail: Burlankov.SP@rea.ru
ORCID: 0000-0001-9326-9006

**Kirill O. Semenov**
Post-Graduate Student of the Department for Economics and Public and Municipal Administration of the MFUA.
Address: Moscow University of Finance and Law MFUA, building 1, 17 Serpukhov Val Str., Moscow, 115191, Russian Federation.
E-mail: kirill_sem_1998@mail.ru

**Ekaterina V. Galaktionova**
Post-Graduate Student of the Research Institute of Humanities.
Address: Research Institute of Humanities by the Government of the Republic of Mordovia, 3 L. Tolstoy Str., Saransk, Republic of Mordovia, 430005, Russian Federation.
E-mail: frolova1@yandex.ru

**Vladimir A. Komarov**
Doctor of Technical Sciences,
Professor, Professor of the Department for Technical Service of Machines of the MRSU.
Address: National Research Ogarev Mordovia State University, 68 Bolshevistskaya Str., Saransk, Republic of Mordovia, 430005, Russian Federation.
E-mail: komarov.v.a2010@mail.ru
ORCID: 0000-0003-1910-2923