УДК 004.056.5(075.8)
DOI: 10.26102/2310-6018/2022.39.4.008

Системная классификация угроз информационной безопасности информационно-телекоммуникационной сети

А.В. Попов[1]✉, О.Н. Чопоров[2], Ю.П. Преображенский[3]

[1]Воронежский государственный технический университет, Воронеж, Российская Федерация
[2]Воронежский государственный медицинский университет, Воронеж, Российская Федерация
[3]Воронежский институт высоких технологий, Воронеж, Российская Федерация
otdelaaa@gmail.com✉

Резюме. Рассматриваемая проблема обеспечения информационной безопасности (ИБ) в вычислительных сетях находится в центре внимания специалистов уже около 40 лет, с момента появления интернет-протокола (англ. Internet Protocol, IP) в качестве стандартного сетевого протокола ARPANET с 1982 г. В настоящее время известны подходы и лучшие практики к обеспечению ИБ сетей, которые были взяты за отправную точку данной работы. Анализ показал, что в настоящее время проблема обеспечение информационной безопасности информационно-телекоммуникационной системы с применением современных интеллектуальных подходов остается до конца научно не решенной, а обеспечение информационной безопасности информационно-телекоммуникационной системы (ИБ ИТКС) на основе создания специализированного структурного элемента в составе ИТКС ранее не было темой специального комплексного научного исследования. Многочисленные ежегодные исследования по вопросам ИБ показывают, что стратегии обеспечения ИБ, которые традиционно были основаны на соблюдении нормативных и правовых требований и ограничивались лишь «защитой периметра» (англ. perimeter defense) компьютерных сетей, не успевают за растущим уровнем рисков ИБ в данной области. В работе поведена научно обоснованная структуризация понятий информационной защищенности и описания внутреннего и внешнего контекста деятельности организаций как единой таксономии, необходимой для конкретизации требований к ЦИУСБ, которая позволила бы получить научную систематизацию и совокупность классификаций сложноорганизованных иерархических взаимосвязанных сущностей (базовые понятия ИБ: «уязвимость», «угроза ИБ», «сетевая атака» и «инцидент ИБ»).

Ключевые слова: системная классификация, сети, телекоммуникация, безопасность, угрозы.

Для цитирования: Попов А.В., Чопоров О.Н., Преображенский Ю.П. Системная классификация угроз информационной безопасности информационно-телекоммуникационной сети. *Моделирование, оптимизация и информационные технологии*. 2022;10(4). Доступно по: https://moitvivt.ru/ru/journal/pdf?id=1156 DOI: 10.26102/2310-6018/2022.39.4.008

System classification of information security threats to the information and telecommunication network

A.V. Popov[1]✉, O.N. Choporov[2], Y.P. Preobrazhenskiy[3]

[1]Voronezh State Technical University, Voronezh, Russian Federation
[2]Voronezh State Medical University, Voronezh, Russian Federation
[3]Voronezh Institute of High Technologies, Voronezh, Russian Federation
otdelaaa@gmail.com✉

Abstract. The problem of cybersecurity protection has been in the focus of specialists' attention for about 40 years since the advent of the Internet Protocol (English Internet Protocol, IP) as the standard ARPANET network protocol since 1982. Currently, the approaches and best practices of cybersecurity protection are known, which were taken as the starting point of this research. The analysis showed that at present the problem of ensuring information security of an information and telecommunications system by means of modern intellectual approaches still remains not fully scientifically solved, and ensuring information security of an information and telecommunications system (ITCS) based on the creation of a specialized structural element in the ITCS previously has not been the subject of a special comprehensive scientific study. Numerous annual studies on information security issues demonstrate that information security strategies that have been traditionally based on compliance with the regulatory and legal requirements and were limited only to the "perimeter defense" of computer networks, do not cope with the growing level of information security risks in this area. The paper presents a scientifically grounded structuring of the information security concepts and the description of the internal and external context of an organization's activities as a single taxonomy necessary to specify the requirements for the center of network security intelligent control, which would help to obtain a scientific systematization and a set of complex hierarchical interconnected entity classifications (basic concepts of information security are "vulnerability", "information security threat", "network attack" and "information security incident").

Keywords: system classification, networks, telecommunications, security, threats.

For citation: Popov A.V., Choporov O.N., Preobrazhenskiy Y.P. System classification of information security threats to the information and telecommunication network. *Modeling, Optimization and Information Technology*. 2022;10(4). Available from: https://moitvivt.ru/ru/journal/pdf?id=1156 DOI: 10.26102/2310-6018/2022.39.4.008 (In Russ.).

Введение

Актуальность исследования заключается в том, что при проведении анализа всех предполагаемых угроз информационной безопасности, а также проведения оценки их влияния, важной задачей при создании системы обеспечения информационной безопасности (ИБ) является анализ информационно-телекоммуникационной системы (ИТКС), что позволит нанести данным угрозам вред. Сайт ФСТЭК РФ [https://bdu.fstec.ru] наиболее полно описывает угрозы информационной безопасности. По состоянию на 15.09.2021 г., в этом списке фигурировало двести семнадцать видов угроз. Из всех известных сейчас угроз ИБ самая актуальной для ИТКС является та, которую можно в ней реализовать, и которая способна нанести вред ее ресурсам. Компании должны осуществлять защиту своих ресурсов только от тех информационных угроз, которые являются для нее актуальными, но не от всех существующих. Как и при ситуации со списком уязвимостей, в данный момент угрозы ИБ не классифицированы.

Целью работы является системная классификация угроз ИБ ИТКС.

Для достижения поставленной цели необходимо решить следующие задачи:

1. Произвести описание классификации угроз ИБ ИТКС организации;
2. Разработать системные классификации уязвимостей и угроз ИБ.

Материалы и методы

Формируя представленную классификацию информационных угроз, применялось большое количество литературных тематических источников, способы нахождения этих угроз за рубежом, например, OCTAVE, разработанная Университетом Карнеги-Меллона в Соединенных Штатах в 2001-м году [1], с ее обновленной версией OCTAVE Allegro и Harmonized TRA (Канада, 2007-й год) [8]. В нашей стране также есть аналогичные разработки (к примеру, «ЭЛВИС+»), которые создавали различные исследовательские и консалтинговые фирмы. Кроме того, использовался ряд стандартов,

и методической документации. Например, Рекомендации по стандартизации работы Банка России РС БР ИББС-2.2-2009 «Обеспечение ИБ банковских учреждений РФ».

С учетом накопленного опыта изучения информационных угроз, выведены 5 основных условий к созданию их классификации:

1) классификация обязана хранить данные о том, каким образом проявляют себя информационные угрозы в ИБ ИТКС компаний, в ее ЦИУСБ, выступающий как главный компонент системы по обеспечению ИБ ИТКС компаний;

2) классификация обязана хранить данные, которые характеризуют жизненный цикл объекта, где появилась информационная угроза;

3) классификация обязана хранить данные о целях информационной угрозы (атака внешнего окружения, самой архитектуры сети, внутренней конфигурации, программного обеспечения и тому подобное);

4) не допускается расположение по одному уровню классификации, которые описывают значительный класс угроз с различной абстракцией, или же какую-либо неординарную ситуацию;

5) классификация обязана связывать информационные угрозы и уязвимости друг с другом, которые позволяют проводить атаки на компьютерное оборудование и сети. К понятию «информационная угроза» в ИБ ИТКС, относят также 2 определения, имеющее прямое отношение к информационной безопасности организаций.

1. Threat Intelligence [1]. Представляет собой свод аналитической информации об информационных угрозах, позволяющий определить предполагаемые угрозы. Это, к примеру, обозначение IP-адресов и доменов злоумышленников, вирусные сигнатуры, файлы, пользователи, E mail, инструменты, используемые хакерами.

По определению организации Gartner, Threat Intelligence является «основанными на реальной информации фактических знаниями, с содержанием контекста, способов, индикаторов, инструментов и практических советов о предполагаемых информационных угрозах в IT-сфере» [11]. Все это можно применить для того, чтобы действенно отреагировать на возникающие информационные угрозы. Интеллектуальный подход при решении проблем в информационной безопасности, давно зарекомендовал себя с самой лучшей стороны. В первую очередь, угроза должна быть исследована со всех сторон, затем определяются ее источники, возможность появления с ее помощью инцидентов в информационной безопасности, что затем позволит найти действенные способы для ликвидации этих угроз.

В информационно-телекоммуникационных сетях организаций данный интеллектуальный подход применяется особенно часто, поскольку в сетях этого типа постоянно присутствует большое количество хакерских атак, что позволяет правонарушителям оставаться незамеченными, если они сменили свое поведение, метод атаки или файлы. Использование системного интеллектуального подхода при использовании информации, предоставляемой разными источниками о возникновении информационных угроз в информационно-телекоммуникационных сетях, дает возможность изменить их в практические знания, которые будут иметь простую доступную структуру и позволят вовремя определить известные и новые информационные угрозы. Дальше, мы более тщательно осветим применение интеллектуального подхода в вопросах противодействия информационным угрозам. Платформы, работающие с применением Threat Intelligence, в реальном времени собирают информацию о предполагаемых угрозах, используя для этого самые разные источники любого типа, осуществляют ее классификацию, и производят с этой информацией разные действия, вместе с выгрузкой в системы СЗИ, а также SIEM. К этому можно отнести и такое понятие, как Threat Intelligence Feeds. Которое описывает

постоянные потоки информации об информационных угрозах, имеющих свою структуру, которая постоянно подвергается обновлению.

Данная информация получается при обработке аналитических данных и использования их в начально собранных данных, которые затем передаются подписанным на это компаниям. К ней можно отнести ряд бесплатных и коммерческих информационных каналов, выдающих информацию о компрометирующих индикаторах, бюллетенях, о внутренних разведывательных данных компаний.

Также информацию о известных в какой – либо сфере организаций, информацию от организаций закрытого типа, работающих в приоритетных сферах.

2. Threat Hunting [8]. Представляет собой планомерную «охоту за информационными угрозами», с работой на упреждение. Это постоянный поиск, определение, локализация, а также проведение анализа информационных угроз, которые способны обойти действующие средства защиты информации. Данные действия, как правило, исполняются в ручном режиме, при которых аналитиком, основываясь на собственных знаниях и квалификации, производится обработка информации, собираемая им при помощи различных средств, с целью выделить новые признаки хакерских атак, чтобы в дальнейшем распознавать их автоматически.

При получении откуда-либо данных Threat Intelligence о том, что произошла новая атака, аналитиком в первую очередь создается гипотеза, по которой предполагается наличие определенного инцидента по информационной безопасности, который средства информационной защиты пропустили. После чего, им осуществляется проверка этой гипотезы, с ее подтверждением или же опровержением. От того, насколько успешно данная гипотеза будет проверена, аналитик должен верно ее сформулировать, что зависит от его квалификации. Данный факт привносит в этот процесс определенный субъективизм, и его желательно было вообще убрать впоследствии. Применение интеллектуального подхода способно оказать помощь в этом вопросе. Общие итоги создания признаков классификации относительно информационных угроз ИБ ИТКС организаций, разрабатываемые изначально в [5], с продолжением в [4], представлены в таблице.

3. Главными признаками, позволяющими классифицировать виды информационных угроз, выступают: непосредственно источник информационной угрозы, его местоположение, цель информационной угрозы, ее направление. Кроме того, к ним относятся этапы жизненного цикла компонента ИБ ИТКС, подверженного угрозе, тип нарушений, которые вызвала угроза, характерность угрозы, ее происхождение, способ, с помощью которого она реализуется. Для того чтобы определить и оценить информационные угрозы, любой их класс разделяют по подклассам (если это нужно). К примеру, это осуществляется для определенных компонентов информационно-телекоммуникационной сети, что позволяет более наглядно их систематизировать и более детально описать информационную угрозу. Необходимо заметить, что классификационные параметры, показанные в Таблице 1, имеют довольно сложную взаимную связь. К примеру, источники, а также формы, по которым реализуются информационные угрозы, могут определить множественность их источников или же наоборот. В связи с этим, оценивая общую защиту информационно-телекоммуникационных сетей организаций, необходимо исследовать все предполагаемые последствия при наступлении информационной угрозы.

Результаты

Таблица 1 показывает, что и в параметрах классификаций говорится об уязвимостях вместе с источниками информационных угроз, и это еще раз доказывает, что они очень тесно взаимосвязаны.

Таблица 1 – Классификация информационных угроз в ИБ ИТКС
Table 1 – ITCS information security threat classification

Тип	Класс	Подкласс
Тип 1. Источник угрозы ИБ	Класс 1. Антропогенный (связанные с человеком)	Подкласс 1. Внешний
		Подкласс 2. Внутренний
	Класс 2. Техногенный	Подкласс 1. Внешний
		Подкласс 2. Внутренний
	Класс 3. Стихийный (естественный, связанный со средой)	Подкласс 1. Стихийные бедствия и природные катастрофы
		Подкласс 2. Нарушения внутриклиматических условий
		Подкласс 3. Форс-мажор и непредвиденные обстоятельства
Тип 2. Расположение угрозы ИБ	Класс 1. Внешнее	
	Класс 2. Внутреннее	
Тип 3. Цели реализации угрозы ИБ		
Тип 4. Направленность угрозы ИБ	Класс 1. Организация в целом	
	Класс 2. ИТКС	Подкласс 1. Уровень каналов связи и телекоммуникационного оборудования
		Подкласс 2. Уровень сетевой среды и ее отдельных элементов
		Подкласс 3. Общесистемное (общее), прикладное, специальное ПО
		Подкласс 4. Предоставление услуг
		Подкласс 5. Функционирование
Тип 5. Угрозы ИБ на стадиях жизненного цикла элементов ИТКС	Класс 1. Проектирование	Подкласс 1. Архитектура
		Подкласс 2. Технологии
		Подкласс 3. Протоколы
		Подкласс 4. Сервисы
	Класс 2. Реализация и программирование	
	Класс 3. Внедрение и использование	
	Класс 4. Снятие с эксплуатации	
Тип 6. Используемые угрозой ИБ уязвимости		
Тип 7. Виды нарушений, вызванных угрозой ИБ	Класс 1. Угроза нарушения свойств ИБ	Подкласс 1. Угроза нарушения конфиденциальности / приватности
		Подкласс 2. Угроза нарушения целостности
		Подкласс 3. Угроза нарушения доступности

Кроме того, при помощи данной классификации, можно обнаружить наиболее опасные информационные угрозы и выработать ряд мер, позволяющих снизить приносимый ими вред, или же уменьшить его.

Обсуждение

С большей наглядностью все виды информационных угроз, возникающих в ИБ ИТКС, показывает Рисунок 1.

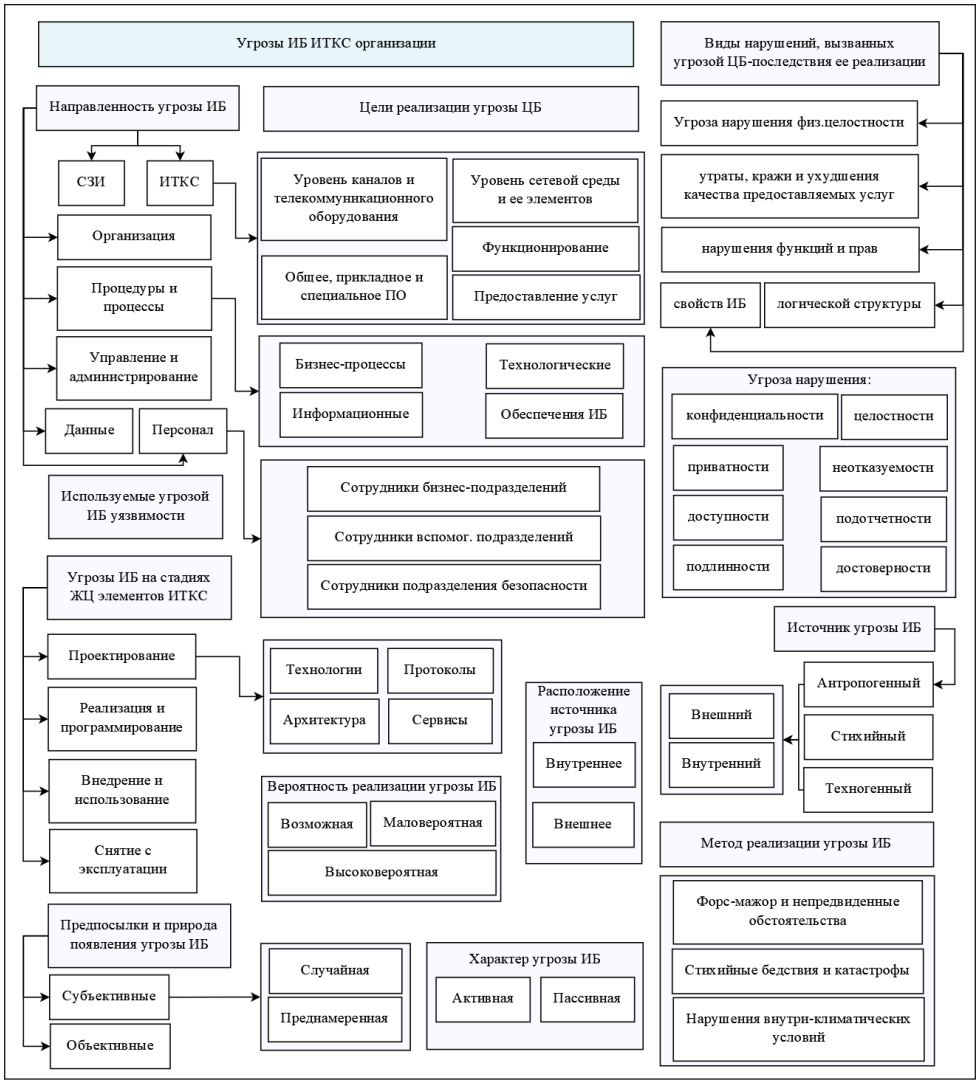

Рисунок 1 – Описание классификации угроз информационной безопасности в ИБ ИТКС организации

Figure 1 – Description of an organization’s ITCS information security threat classification

Также на их основе будет создаваться модель угроз ИБ ИТКС, а также модель нарушителей ИБ ИТКС, на основе которых будет формироваться, в первую очередь, Корпоративная Политика, обеспечивающая ИБ ИТКС в организациях (дальше – Политика информационной безопасности). После этого, каждая организация формирует собственную Политику ИБ, и список, в котором указаны возможные риски для ее информационно-телекоммуникационной сети, что позволит выбрать наиболее действенные меры для обеспечения информационной безопасности, основываясь на Модели информационных угроз.

В соответствии с [5 и 10], данной моделью является описание (обычно текстовое или таблицами):

1) защищаемых объектов защиты, а также объектов, в которых могут проявиться информационные угрозы;

2) предполагаемых источников информационных угроз;

3) уязвимостей и их классов, которыми пользуются источники информационных угроз;

4) способов и методик, при помощи которых реализуются информационные угрозы;

5) предполагаемых типов нарушения ИБ ИТКС (к примеру, неправомерное использование конфиденциальных данных, нарушение полноты и доступности информационных ресурсов);

6) масштабов возможного ущерба.

Исходя из вышеописанной системы классификации угроз, была разработана высокоуровневая диаграмма процесса управления инцидентами ИБ для организации.

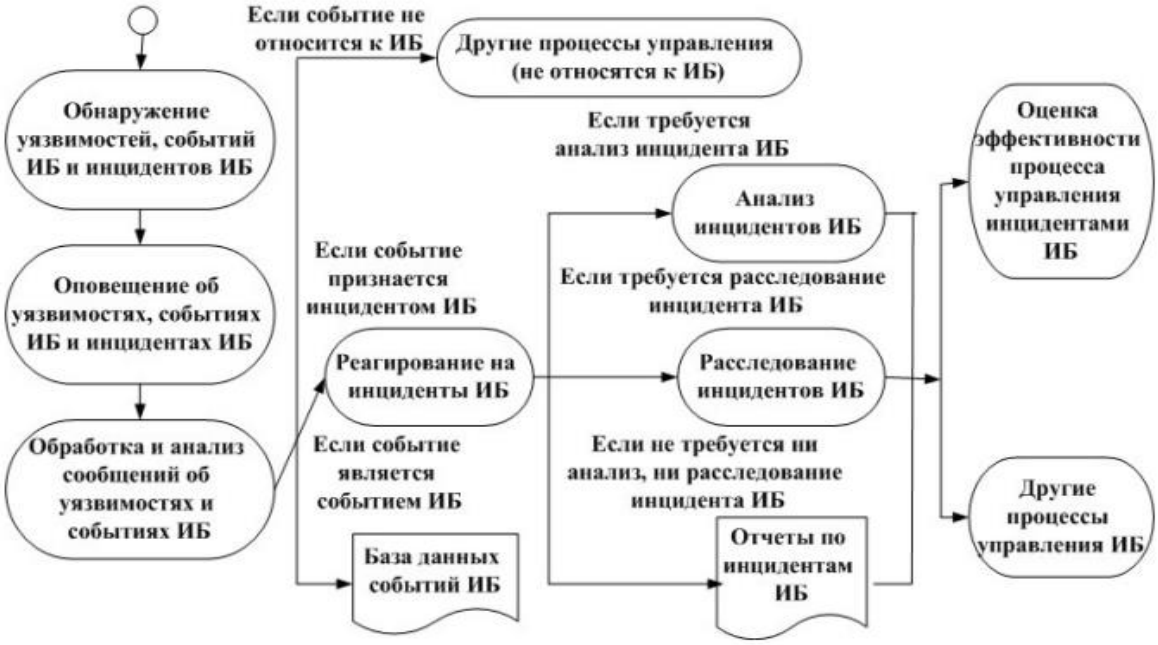

Рисунок 2 – Высокоуровневая диаграмма процесса управления инцидентами ИБ для организации

Figure 2 – High level diagram of managing information security incidents for an organization

Заключение

Разработанные системные классификации уязвимостей и угроз ИБ полностью согласованы между собой, что обеспечивает целостный взгляд на природу происхождения инцидентов ИБ для последующего понимания, какие уязвимости устранять и каких последствий от их реализации ожидать. Они необходимы для построения Модели угроз ИБ и Модели нарушителей ИБ, составляющих основу разработки положений сначала Корпоративной Политики ИБ.

Разработанная высокоуровневая диаграмма процесса управления инцидентами ИБ для организации акцентирует внимание на достижении поставленных целей, а также на затраченных для этого ресурсах.

СПИСОК ИСТОЧНИКОВ

1. Преображенский Ю.П., Чопоров О.Н., Ружицкий Е. Проблемы оценки характеристик пользователей в больших системах. *Вестник Воронежского института высоких технологий*. 2021;1(36):103–106.
2. Львович И.Я., Альтварг М.С., Абрамов М.И. Характеристики методов и средств управления программными проектами. *Вестник Воронежского института высоких технологий.* 2021;1(36):47–50.
3. Преображенский Ю.П., Чопоров О.Н., Ружицкий Е. Проблемы анализа жизненного цикла IT-продуктов. *Вестник Воронежского института высоких технологий.* 2021;1(36):66–69.
4. Преображенский Ю.П., Чопоров О.Н., Ружицкий Е. О проблемах защиты данных в информационных системах. *Вестник Воронежского института высоких технологий.* 2021;1(36):70-73.
5. Коростелева Н.А., Батищев П.А., Денисенко С.С. Проблемы оценки эффективности работы организаций. *Вестник Воронежского института высоких технологий.* 2021;1(36):101–103.
6. Львович Э.М., Чупринская Ю.Л., Кравцова Н.Е. Особенности типологии проектных рисков. *Вестник Воронежского института высоких технологий.* 2021;2(37):104–106.
7. Львович Э.М., Чупринская Ю.Л., Кравцова Н.Е. Способы оценки и анализа проектных рисков. *Вестник Воронежского института высоких технологий.* 2021;2(37):107–109.
8. Коростелева Н.А., Попова С.С., Новичкова А.А. О проблемах моделирования функционирования организаций. *Вестник Воронежского института высоких технологий.* 2021;2(37):31–33.
9. Преображенский Ю.П., Чопоров О.Н., Ружицкий Е. Об истории развития автоматизированных систем, связанных с управлением. *Вестник Воронежского института высоких технологий.* 2021;2(37):75–78.
10. Львович Я.Е., Львович И.Я., Волкова Н.В. Проблемы построения корпоративных информационных систем на основе web-сервисов. *Вестник Воронежского государственного технического университета.* 2021;7(6):8–10.
11. Комаристый Д.П., Агафонов А.М., Степанчук А.П., Коркин П.С. Использование информационных систем на предприятиях. *Вестник Воронежского института высоких технологий.* 2021;2(21):104–106.
12. Гостева Н.Н., Гусев А.В. Информационные системы в управлении производством. *Вестник Воронежского института высоких технологий.* 2017;20(1):58–60.
13. Шапаев А.В., Юдаков Д.А., Часовской А.А. Проблемы поиска текстовой информации в больших объемах данных. *Вестник Воронежского института высоких технологий.* 2019;1(28):113–115.
14. Львович И.Я., Кравцова Н.Е., Чупринская Ю.Л. Особенности решений для обработки текстовых данных. *Вестник Воронежского института высоких технологий.* 2019;1(28):89–92.

REFERENCES

1. Preobrazhensky Yu.P., Choporov O.N., Ruzhitsky E. Problems of assessing user characteristics in large systems. *Vestnik Voronezhskogo instituta vysokikh tekhnologiy = Bulletin of the Voronezh Institute of High Technologies.* 2021;1(36):103–106. (In Russ.).

2. Lvovich I.Ya., Altvarg M.S., Abramov M.I. Characteristics of methods and tools for managing software projects. *Vestnik Voronezhskogo instituta vysokikh tekhnologiy = Bulletin of the Voronezh Institute of High Technologies.* 2021;1(36):47–50. (In Russ.).
3. Preobrazhensky Yu.P., Choporov O.N., Ruzhitsky E. Problems of life cycle analysis of IT products. *Vestnik Voronezhskogo instituta vysokikh tekhnologiy = Bulletin of the Voronezh Institute of High Technologies.* 2021;1(36):66–69. (In Russ.).
4. Preobrazhensky Yu.P., Choporov O.N., Ruzhitsky E. About the problems of data protection in information systems. *Vestnik Voronezhskogo instituta vysokikh tekhnologiy = Bulletin of the Voronezh Institute of High Technologies.* 2021;1(36):70–73. (In Russ.).
5. Korosteleva N.A., Batishchev P.A., Denisenko S.S. Problems of evaluating the effectiveness of organizations. *Vestnik Voronezhskogo instituta vysokikh tekhnologiy = Bulletin of the Voronezh Institute of High Technologies.* 2021;1(36):101–103. (In Russ.).
6. Lvovich E.M., Chuprinskaya Y.L., Kravtsova N.E. Features of the typology of project risks. *Vestnik Voronezhskogo instituta vysokikh tekhnologiy = Bulletin of the Voronezh Institute of High Technologies.* 2021;2(37):104–106. (In Russ.).
7. Lvovich E.M., Chuprinskaya Y.L., Kravtsova N.E. Methods of assessment and analysis of project risks. *Vestnik Voronezhskogo instituta vysokikh tekhnologiy = Bulletin of the Voronezh Institute of High Technologies.* 2021;2(37):107–109. (In Russ.).
8. Korosteleva N.A., Popova S.S., Novichkova A.A. On the problems of modeling the functioning of organizations. *Vestnik Voronezhskogo instituta vysokikh tekhnologiy = Bulletin of the Voronezh Institute of High Technologies.* 2021;2(37):31–33. (In Russ.).
9. Preobrazhensky Yu.P., Choporov O.N., Ruzhitsky E. On the history of the development of automated systems related to management. *Vestnik Voronezhskogo instituta vysokikh tekhnologiy = Bulletin of the Voronezh Institute of High Technologies.* 2021;2(37):75–78. (In Russ.).
10. Lvovich Ya.E., Lvovich I.Ya., Volkova N.V. Problems of building corporate information systems based on web services. *Vestnik Voronezhskogo gosudarstvennogo tekhnicheskogo universiteta = Bulletin of the Voronezh State Technical University.* 2021;7(6):8–10. (In Russ.).
11. Komaristy D.P., Agafonov A.M., Stepanchuk A.P., Korkin P.S. The use of information systems in enterprises. *Vestnik Voronezhskogo instituta vysokikh tekhnologiy = Bulletin of the Voronezh Institute of High Technologies.* 2021;2(21):104–106. (In Russ.).
12. Gosteva N.N., Gusev A.V. Information systems in production management. *Vestnik Voronezhskogo instituta vysokikh tekhnologiy = Bulletin of the Voronezh Institute of High Technologies.* 2017;1(20):58–60. (In Russ.).
13. Shapaev A.V., Yudakov D.A., Chasovskoy A.A. Problems of searching for textual information in large volumes of data. *Vestnik Voronezhskogo instituta vysokikh tekhnologiy = Bulletin of the Voronezh Institute of High Technologies.* 2019;1(28):113–115. (In Russ.).
14. Lvovich I.Ya., Kravtsova N.E., Chuprinskaya Yu.L. Features of solutions for text data processing. *Vestnik Voronezhskogo instituta vysokikh tekhnologiy = Bulletin of the Voronezh Institute of High Technologies.* 2019;1(28):89–92. (In Russ.).

ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

Попов Андрей Вениаминович, аспирант Воронежского государственного технического университета, кафедра систем информационной безопасности
e-mail: otdelaaa@gmail.com

Andrey Veniaminovich Popov, Postgraduate student, Voronezh State Technical University, Department of Information Security Systems, Voronezh, Russian Federation.

Чопоров Олег Николаевич, доктор технических наук, профессор Воронежского государственного медицинского университета, Воронеж, Российская Федерация.
e-mail: choporov_oleg@mail.ru
ORCID: 0000-0002-3176-499X

Oleg Nikolaevich Choporov, Doctor of Technical Sciences, Professor at Voronezh State Medical University, Voronezh, Russian Federation.

Преображенский Юрий Петрович, кандидат технических наук, проректор по ИТ Воронежского института высоких технологий, Воронеж, Российская Федерация.
e-mail: petrovich@vivt.ru

Yuri Petrovich Preobrazhenskiy, Candidate of Technical Sciences, Vice Rector (IT) at Voronezh Institute of High Technologies, Voronezh, Russian Federation.

Статья поступила в редакцию 03.10.2022; одобрена после рецензирования 31.10.2022; принята к публикации 06.12.2022.

The article was submitted 03.10.2022; approved after reviewing 31.10.2022; accepted for publication 06.12.2022.