ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

УДК 004.056

DOI: 10.21822/2073-6185-2024-51-3-42-53 Оригинальная статья/ Original article

Категорирование объектов критической информационной инфраструктуры учреждения высшего образования

Е.В. Бурькова, А.А. Рычкова, Л.А. Гриценко
Оренбургский государственный университет,
460018, г. Оренбург, просп. Победы, д. 13, Россия

Резюме. Цель. В настоящее время актуализируется задача обеспечения безопасности национальных информационных ресурсов России как важное направление политики государства в информационной сфере. Целью исследования является описание методики определения критичности процессов в научно-исследовательской деятельности высшего образовательного учреждения для решения вопроса присвоения ему категории критической информационной инфраструктуры и в соответствии с этой категорией - обеспечение требований к системе защиты информации. **Метод.** В качестве метода решения поставленной задачи используется метод экспертных оценок, моделирование бизнес-процессов BPMN. **Результат.** Представлен обзор подходов к категорированию объектов критической информационной инфраструктуры научной деятельности учреждения высшего образования. Проведен анализ и сопоставление нормативных документов регуляторов, их адаптация для сферы науки, определены основные этапы проведения категорирования, локальные нормативные документы, позволяющие проводить категорирование в соответствии с требованиями нормативно-правовой базы. Для проведения процесса категорирования вуза разработана схема этапов категорирования, рассмотрен регламент анализа объектов организации на предмет выявления критичности с последующим присвоением категории значимости или отказа от категории. **Вывод.** Научная деятельность учреждения высшего образования подлежит анализу на выявление критических процессов, инвентаризации объектов с выявлением возможных последствий в результате реализации угроз безопасности, определения субъектов и объектов критической информационной инфраструктуры, оценки категории значимости. Для повышения достоверности полученных результатов разработан регламент работы специальной комиссии по категорированию, проекты локальных документов по инвентаризации объектов и формализации процессов.

Ключевые слова: категорирование, объектов КИИ, этапы категорирования, метод моделирования бизнес-процессов

Для цитирования: Е.В. Бурькова, А.А. Рычкова, Л.А. Гриценко. Категорирование объектов критической информационной инфраструктуры учреждения высшего образования. Вестник Дагестанского государственного технического университета. Технические науки. 2024; 51(3):42-53. DOI:10.21822/2073-6185-2024-51-3-42-53.

Categorization of objects of critical information infrastructure of higher education institutions

E.V. Burkova, A.A. Rychkova, L.A. Gritsenko
Orenburg State University,
13 Pobeda Ave., Orenburg 460018, Russia

Abstract. Objective. Currently, the task of ensuring the security of Russia's national information resources is being updated as an important area of state policy in the information sphere. The purpose of the article is to describe a methodology for determining the criticality of processes in the research activities of a higher educational institution in order to solve the issue of assigning it the category of critical information infrastructure and, in accordance with this category, ensuring the requirements for the information security system. **Method**. The method

of expert assessments and BPMN business process modeling are used. **Result**. An overview of approaches to categorizing objects of critical information infrastructure of scientific activity of higher education institutions is presented. The analysis and comparison of regulatory documents of regulators, their adaptation for the field of science, the main stages of categorization, local regulatory documents allowing categorization in accordance with the requirements of the regulatory framework are determined. To carry out the categorization process of the university, a scheme of categorization stages has been developed, the rules of analysis of the organization's objects for the purpose of identifying criticality with subsequent assignment of a category of significance or rejection of a category have been considered. **Conclusion**. The scientific activity of a higher education institution is subject to analysis to identify critical processes, inventory of objects with identification of possible consequences as a result of the implementation of security threats, identification of subjects and objects of critical information infrastructure, assessment of the category of significance. To increase the reliability of the results obtained, the rules of procedure of the special commission on categorization, drafts of local documents on the inventory of objects and the formalization of processes have been developed.

Keywords: categorization of objects of critical information infrastructure in the field of science, stages of categorization, business process modeling method, BPMN.

For citation: E.V. Burkova, A.A. Rychkova, L.A. Gritsenko. Categorization of objects of critical information infrastructure of higher education institutions. Herald of the Daghestan State Technical University. Technical Sciences. 2024; 51(3):42-53 DOI:10.21822/2073-6185-2024-51-3-42-53

Введение. Обеспечение непрерывного функционирования объектов критической информационной инфраструктуры в современных условиях возрастающего количества и опасности кибератак становится важной и трудоемкой задачей. По данным компании Cortel типовые цели и векторы атак направлены на серверы и сетевую инфраструктуру организации (рис. 1.)

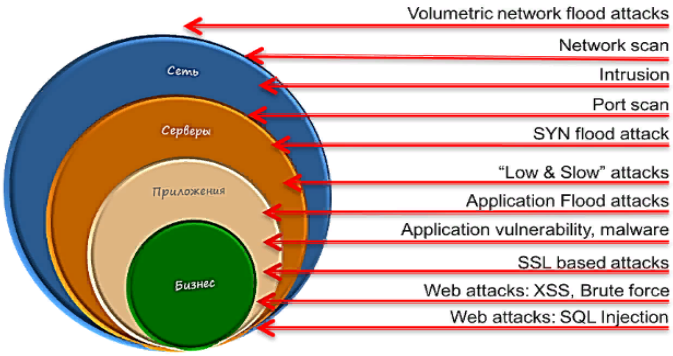

Рис. 1. Типовые цели и векторы атак
Fig. 1. Typical targets and attack vectors

Типичные уязвимости: слабо защищенные и низкопроизводительные маршрутизаторы и коммутаторы; DNS-серверы используют для перенаправления трафика и отказа в обслуживании критичных сервисов; серверы аутентификации; серверы приложений перегружают запросами для снижения производительности и отказа в обслуживании; BGP Hijacking (хищение BGP-маршрутов, используют для перехвата и хищения данных, либо для блокирования целевого ресурса). Ежедневно появляются новые «мишени».

Во II квартале 2023 года обнаружили более 7,5 тыс. уязвимостей, что на 7% больше, чем в начале года. Эксплуатируют и старые, поскольку некоторые системы остаются не обновленными [1]. Последствия реализации атак могут быть значительными: утечка персональных данных, приостановление предоставления образовательных услуг, нарушение работы сети организации, размещение на сайте организации компрометирующих записей, носящих противозаконный характер т.д. В конечном итоге организация может

понести финансовые и репутационные потери, поэтому необходима комплексная система защиты информации.

Постановка задачи. В качестве исследуемой организации мы рассматриваем учебное заведение высшего образования, государственный университет. В федеральном законе от 26.07.2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» определены сферы экономики, для субъектов которых необходимо провести категорирование КИИ и реализовать соответствующую защиту. Правила категорирования КИИ устанавливаются Постановлением Правительства РФ от 8 февраля 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений». Необходимо отметить, что в процессе категорирования объектов учитываются и информационные системы персональных данных, которые принадлежат субъекту КИИ, и должна быть реализована защита этих систем на основании требований законодательства России [2].

Сфера образования не входит в этот перечень, однако высшие учебные заведения осуществляют научную деятельность, следовательно, могут иметь в своем распоряжении объекты КИИ: информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры. Научно-исследовательская деятельность университета содержит следующие компоненты: интеграция науки и образования, реализация взаимодействия университета с научными учреждениями Российской Академии наук; научные исследования в области естественных и технических наук; участие ученых вуза в федеральных целевых программах, конкурсах и грантах, объявленных государственными научными фондами; развитие партнерства с предприятиями и другими хозяйствующими субъектами региона. Научные подразделения университета оснащены компьютерной техникой, имеют выход в локальную и глобальную сети, в них созданы база данных проводимых исследований, следовательно, реализуется множество информационных процессов, которые могут быть критичными и встает вопрос присвоении университету категории КИИ [3].

Задача категорирования объектов КИИ рассматривалась многими учеными. В статье [3] представлено содержание этапов процесса категорирования объектов КИИ организации сферы здравоохранения, а также представлен пример определения критичных процессов в конкретной организации.

В научной работе [4] проведен обзор существующих отечественных и зарубежных методик, приведена методика определения критических процессов предприятия в сфере химической промышленности. В статье [5] рассматривается методика оценки защищённости автоматизированной системы управления критической информационной инфраструктуры АСУ ТП от DDoS-атак на основе имитационного моделирования методом Монте-Карло.

Вопросы категорирования высшего учебного заведения как Вуз как субъекта законодательства о безопасности КИИ, рассматривались в работах [6, 19-20]. В статье [6] автор провел анализ научной деятельности вуза, считает, что основой процесса категорирования объектов КИИ является анализ уязвимостей и актуальных угроз, которые могут привести к значительным негативным последствиям. В статье приведен алгоритм действий по созданию перечней потенциальных уязвимостей и угроз, представлены применимые показатели критериев значимости объектов КИИ вуза.

Многие методики категорирования объектов КИИ базируются на основании экспертных данных, которые подвергаются дальнейшему анализу, процесс осложняется необходимостью учета взаимосвязи между объектами и их процессами, имеющими влияние на величину рисков, возникновение множественных сбоев из-за компьютерных атак [7-10, 16, 21]. Нами была разработана схема этапов категорирования объектов КИИ в сфере науки, представленная на рис.2.

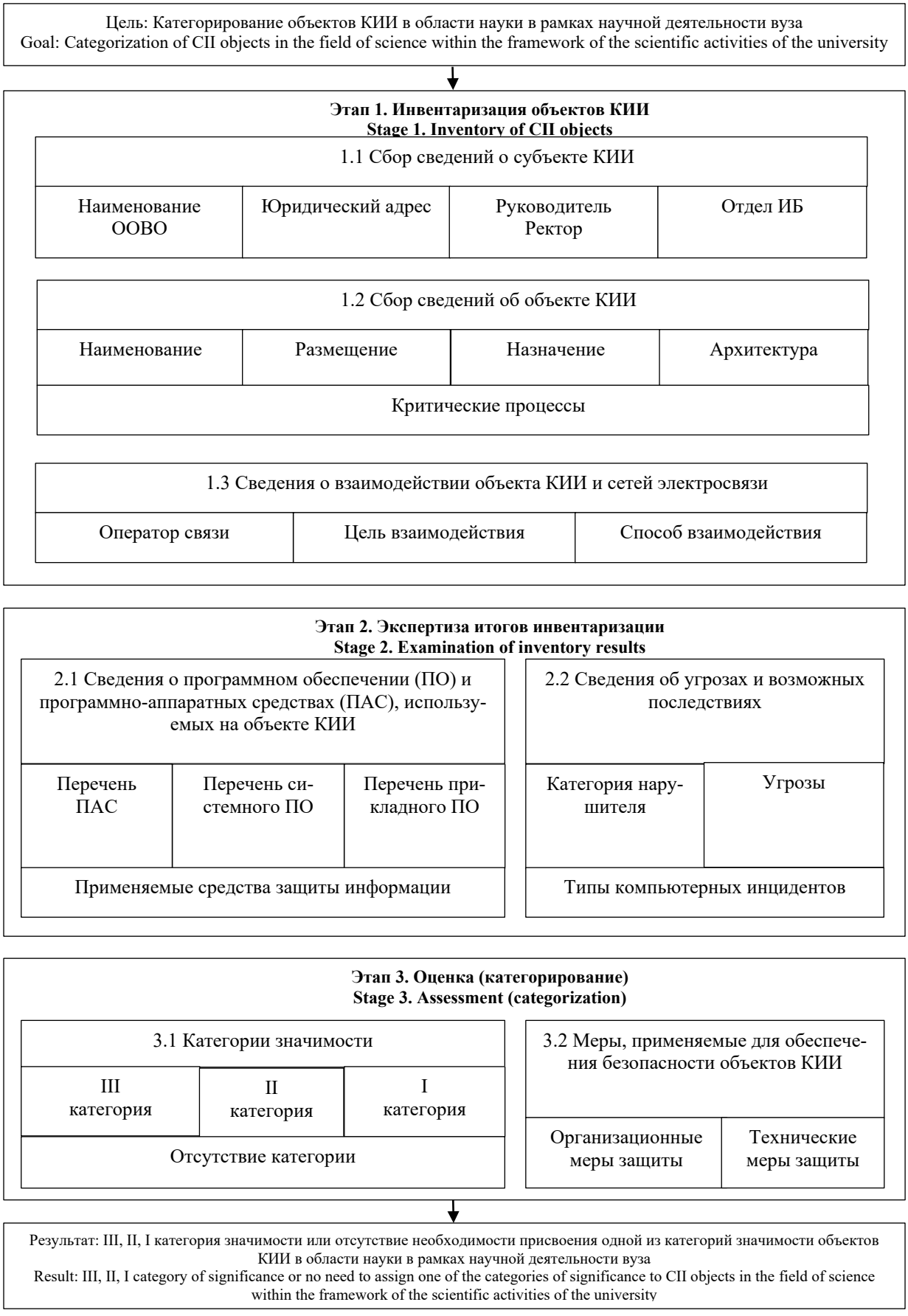

Рис. 2. Схема этапов категорирования объектов КИИ в сфере науки
Fig. 2. Scheme of stages of categorization of CII objects in the field of Science

Порядок категорирования объектов КИИ представлен в Постановлении Правительства № 127 и включает в себя:

1. Инвентаризацию объектов КИИ, таких как автоматизированные информационные системы управления, используемых при проведении научно-исследовательских работ с целью определения их критичности.

2. Экспертизу итогов инвентаризации на уровне специально созданной комиссии и утверждение перечня объектов КИИ.

3. Оценка - категорирование выделенных объектов КИИ с целью установления их значений показателей значимости и присвоение каждому из них одной из соответствующей категории либо отказ от присвоения.

В конечном итоге целью является создание адекватной системы информационной безопасности, снижение рисков, обеспечение бесперебойной работы инфраструктуры университета. Инвентаризация объектов КИИ в рамках научной деятельности университета является важным этапом процесса категорирования. В результате выполнения этого этапа формируется список всех информационных систем и информационно-телекоммуникационных сетей, их описание и указание месторасположения, принадлежность к субъекту КИИ, вовлеченность в деятельность научных организаций университета.

Не менее важным является этап анализа угроз информационной безопасности, категорий нарушителей, выявление инцидентов безопасности. Всестороннее и системное изучение угроз безопасности, в том числе угроз несанкционированного доступа на объектах КИИ, является сложной задачей. Для решения данной задачи используют количественные методы оценки на основе вероятностного подхода, а именно метрики вероятности проявления угроз [11].

Особое внимание необходимо уделять требованиям к структурным подразделениям обеспечения безопасности значимых объектов КИИ. Риск ущерба для субъектов КИИ от компьютерных атак на критические процессы имеет тяжелые последствия, начиная от потери репутации и до приостановления работы организации [12].

На основе экспертных данных, полученных в результате обследования информационной структуры университета, ставится задача определения критических процессов в научной деятельности, на основе которых может быть сделано заключение о необходимости присвоения университету категории КИИ. Сфера науки в ФЗ-187 недостаточно проработана и требует дополнительных уточнений, что конкретно относится к сфере науки. Если использовать классический подход, то необходимо проверить Общероссийский классификатор видов экономической деятельности (ОКВЭД) в документах организации. В большинстве университетах присутствует номер 72.19 и/или 72.20, что относится к научным исследованиям. Исходя из данных ОКВЭД университет является субъектом критической информационной инфраструктуры (далее – КИИ). И ставится задача определить критические процессы и значимость объектов КИИ.

Методы исследования. Реализация научной деятельности подразумевает использование информационных технологий и телекоммуникационных сетей. Данный фактор осложняет выявление отдельных управленческих, технологических, производственных, финансово-экономических и (или) иных процессов с целью анализа их на предмет критичности [13].

Для выполнения всех этапов категорирования применяют методы экспертных оценок, для анализа процессов научной деятельности применяют методы моделирования бизнес-процессов. В нашем исследовании рассмотрен метод моделирования бизнес-процессов BPMN.

В качестве объекта исследования рассмотрим научную деятельность Оренбургского государственного университета. В рамках выполнения функций (полномочий) или осуществления научно-исследовательской деятельности в университете функционирует Управление научной и инновационной деятельностью (УНИД), которое взаимодействует со всеми научно-исследовательскими институтами (НИИ), лабораториями и другими под-

разделениями науки в университете. На основании данных, полученных от УНИД можно сформировать перечень НИИ, центров коллективного пользования, лабораторий и центров вуза, в которых необходимо провести инвентаризацию ресурсов и определить процессы для дальнейшего анализа на критичность [14].

На рис. 3 представлен порядок формирования перечня критических процессов в области науки в нотации BPMN.

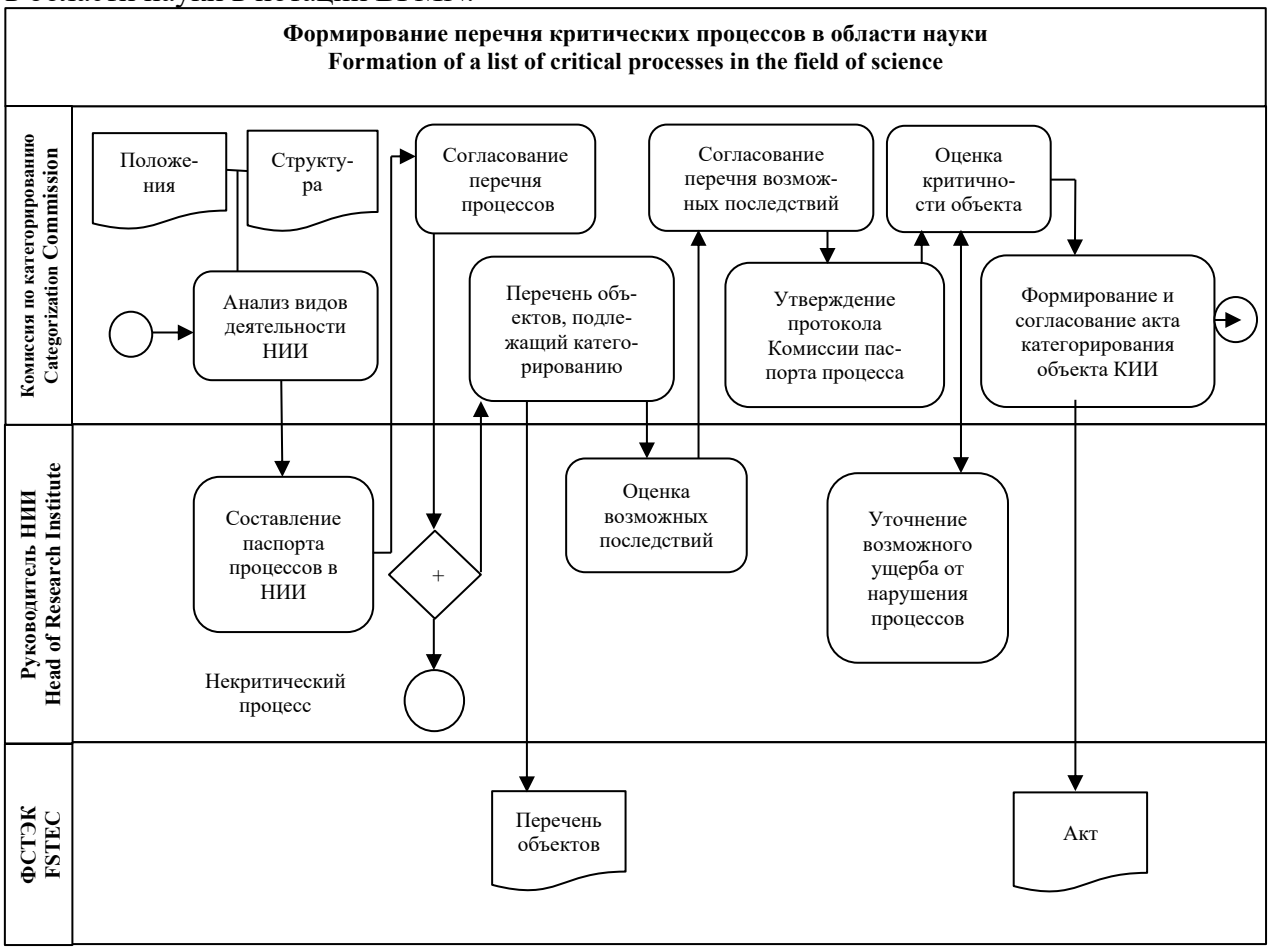

Рис. 3. Порядок формирования перечня процессов в области науки
Fig. 3. The procedure for creating a list of processes in the field of science

Обсуждение результатов. На первом этапе был проведен анализ деятельности НИИ, используемых информационных систем, испытательного оборудования, программного обеспечения с целью выяснения специфики проводимых работ и влияния результатов работ на возникновение негативных последствий [15].

Сложность возникает при выявлении самих критических процессов, так как в комиссию необходимо включать представителей НИИ. Поэтому для унификации каждого процесса в области науки был подготовлен регламент для описания процессов в области науки, в ходе которого формируется паспорт процесса научной деятельности, определяются задействованные объекты, пример заполнения синтетическими данными представлен в табл. 1.

Процесс научного исследования в ОГУ кроме основного процесса исследования и разработки включает в себя еще сопутствующие и обеспечивающие, а также управляющие процессы, такие как бухгалтерское сопровождение, закупки, кадровое обеспечение, выпуск приказов и распоряжений и т.д.

С целью сокращения трудозатрат на описание обеспечивающих процессов разработан и представлен в регламенте типовой процесс. Если описываемый процесс существенно отличается от типового, требуется внесение изменений в схему процесса.

Таблица 1. Описание процесса научного исследования (пример)
Table 1. Description of the scientific research process (example)

Наименование процесса исследования **Name of the research process**	**Подпроцесс(ы), в котором(ых) используется оборудование процесса** **Sub-process(es) in which process equipment is used**
Разработка комплексной системы оценки устойчивости моделей машинного обучения Грант РНФ № 123	Процесс экспериментальных исследований
Контролируемые параметры подпроцесса **Controlled subprocess parameters**	**Метод измерения параметров подпроцесса** **Method for measuring subprocess parameters**
- количество параметров обучающей модели - время расчета модели на оборудовании - точность предсказаний моделей -соответствие результатов эксперимента теоретическим результатам	Расчетные, сравнительные, экспертные
Бизнес-процесс верхнего уровня/Top level business process	
Научные исследования в НИИ ЦиНТ	
Вложенные процессы/ Nested Processes	
нет	
Задействованные Объекты (оборудование, информационные системы, сети, устройства, установки, программы) с инвентарным номером (при наличии) и степень влияния их отказа на весь процесс (низкая, средняя, высокая, краткое описание)/ Involved Objects	
сервер машинного обучения ASUS, инвентарный номер №111 – средняя, при отказе исследование нарушение сроков исполнения гранта, недостаточно публикаций по результатам; компьютеры инв. № 222 – низкая, продолжение работы на другом компьютере; маршрутизатор инв. № 333 – низкая, задействован только при первичном запуске модели, можно заменить на другой аналогичный; система хранения данных инв. №444 – средняя, при отказе будет снижена скорость расчетов модели; передатчик беспроводной многозонный инв. №2222– высокая, при отказе невозможно продолжение экспериментальных исследований; датчики беспроводные инв. № «б/н» - высокая, при отказе невозможно продолжение экспериментальных исследований; ПО Matlab 2008 – среднее, при отказе возможно использовать другие инструменты анализа.	
Текстовое описание подпроцесса и использования оборудования (и ПО) в нем **Text description of the subprocess and the use of equipment (and software) in it**	
Планирование эксперимента и подготовка наборов данных производится в ПО Keras (с открытым исходным кодом) на компьютерах инв. № 222 Экспериментальное исследование моделей проводится путем компьютерного моделирования на созданном программном обеспечении при использовании аппаратных ресурсов сервера инв. № 111на ПО tensorflow (с открытым исходным кодом). При запуске модели через маршрутизатор инв. № 333 скачиваются данные с системы хранения данных инв. № 444, после чего запускается серия расчетов. Результаты помещаются обратно в систему хранения данных. Эксперимент на оборудовании проводится после помещения рассчитанных на модели параметров в передатчик беспроводной инв. № 2222, после чего с помощью датчиков беспроводных инв. № «б/н 222» снимаются показания. После этого производится сравнение выборок результатов. Сравнение результатов модельных и натурных исследований производятся в ПО Matlab 2008R на компьютерах инв. № 222	
Руководитель процесса исследования	с.н.с., к.т.н., доц. лаборатории ПнП НИИ ЦиНТ Иванов И.И.

Функции процесса Process functions		
№	**Наименование функции**	**Исполнитель**
1	Составление плана эксперимента	с.н.с. Петров П.П.
2	Выгрузка наборов данных	с.н.с. Петров П.П.
3	Тестирование наборов данных	с.н.с. Сидоров С.С.
4	Запуск прогона моделей	с.н.с. Сидоров С.С.
5	Сбор и анализ данных моделей	с.н.с. Петров П.П.
6	Запуск натурного эксперимента	с.н.с. Петров П.П.
7	Сбор и анализ данных натурного эксперимента	с.н.с. Иванов И.И.

Перечень регламентирующих документов **List of regulatory documents**		
№	**Наименование документа**	**Источник документа**
	отсутствует	

Перечень подразделений и должностей, участвующих в процессе **List of departments and positions involved in the process**
Лаборатория ПнП НИИ ЦиНТ: *с.н.с. Иванов И.И.* *с.н.с. Петров П.П.*

Далее необходимо заполнить Паспорт процесса в соответствии со следующим алгоритмом:

1. Заполнить поля с указанием названия исследований, руководителей, подразделений.

2. Описать оборудование, программное обеспечение, с указанием степени критичности влияния работоспособности на процесс исследования.

3. Описать сам процесс исследования с использованием этого оборудования (где, и в какой мере оно используется).

4. По каждому объекту заполнить по форме возможные последствия от компьютерных инцидентов (атак, взломов, заражений) по форме табл. 2.

5. При наличии хотя бы одного возможного инцидента в форме оценке, необходимо предоставить расчеты значения критериев значимости процесса научного исследования, указанного в Паспорте процесса.

В регламенте устанавливаются обязанности сотрудников управления научной и инновационной деятельностью, ответственных за научное исследование, отдела информационной безопасности.

Процессу описания должно быть подвергнуто каждое научное исследование, проводимое в ОГУ и затрагивающее Объекты (оборудование, информационные системы, сети, устройства, установки), в которых используются компьютерные системы управления, контроллеры с возможностью удаленного перепрограммирования или системы автоматизированного управления с возможностью внешнего воздействия.

Основным критерием необходимости описания процесса по данному Регламенту является наличие в составе процесса научного исследования Объектов (оборудования, устройств, установок), которые имеют какие-либо информационные системы, подключаются к сети (локальной или к Интернет), имеют в составе компьютер, взаимодействуют с другими информационными технологиями.

При описании процесса для каждого используемого Объекта (оборудования, информационной системы, сети, устройства, установки) требуется провести оценку возможных последствий от нарушения процесса (в том числе технологического) через информационные технологии (например от воздействия вируса или хакерской атаки) – выход из строя Объекта (например, из-за нештатных режимов работы или отключения защиты), кража закрытых или конфиденциальных данных, потеря данных, угроза возгорания, угроза жизни и здоровью людей, экологические риски.

В конце табл. 1 указываются сведения, участвующих в заполнении паспорта процесса, так как данный материал используется членами комиссии для проведения категорирования.

Исходя из наличия в научных процессах программного обеспечения и оборудования необходимо по ПП-127 составить перечень показателей критериев значимости, предварительно участникам научного процесса оценить информационные риски, заполнив следующую табл. 2.

Итоговая форма расчета значения критериев значимости процесса научного исследования представлена в табл. 3.

Сформировав, таким образом, паспорт процесса, коллегиально на комиссии с приглашенными руководителями научных процессов проходит оценка, является ли процесс критическим.

В рассматриваемом университете большая часть НИИ используют компьютеры автономно, не подключая их даже к локальной сети вуза, вся информация о грантах университета и их краткое описание является открытой информацией и представлена на сайте университета [15].

Таблица 2. Оценка возможных последствий (пример синтетических данных)
Table 2. Assessment of possible consequences (synthetic data example)

Объект/ значимость Object/ importance	**Возможные последствия, связанные с инцидентами (взломами, атаками, сбоями) в сфере информационных технологий на оборудовании Possible consequences associated with incidents (break-ins, attacks, failures) in the field of information technology on equipment**				
	Социальная значимость Social significance		Экономическая значимость Economic importance		Экологическая значимость Ecological significance
	Нештатный режим работы и, вследствие этого, поломки или физическое разрушение объекта	Угрозы жизни и здоровья людей при нештатных режимах работы	Потеря (уничтожение), кража получаемых данных (в том числе через сеть)	Угрозы имуществу ОГУ (возгорание, затопление и т.д.)	Угрозы экологии (выбросы, сливы и т.д.)
сервер инв.№ 111	Нет	Нет	**Да**	Нет	Нет
маршрутизатор инв № 333	Нет	Нет	Нет	Нет	Нет
система хранения данных инв № 444	Нет	Нет	**Да**	Нет	Нет
передатчик беспроводной многозонный инв №2222	Нет	Нет	Нет	Нет	Нет
датчики беспроводные инв № «б/н»	Нет	Нет	Нет	Нет	Нет
ПО Matlab	Нет	Нет	Нет	Нет	Нет

Таблица 3. Итоговая обобщенная форма расчета значения критериев значимости процесса научного исследования
Table 3. Final generalized form for calculating the value of criteria for the significance of the scientific research process

Критерии значимости Significance criteria	**Значение критерия Criterion value**
Социальная значимость Social significance	Отсутствует Absent
Политическая значимость Political significance	Отсутствует Absent
Экономическая значимость Economic importance $Ущерб = \frac{Потери\ вуза}{Бюджет\ РФ\ усредн.} * 100\%$	Отсутствует Absent
Экологическая значимость Ecological significance	Отсутствует Absent
Значимость для обеспечения обороны страны, безопасности государства и правопорядка Significance for ensuring national defense, state security and law and order	Отсутствует Absent

На текущий момент критических процессов, которые могли бы попасть под критерии ПП-127 в вузе не было установлено. При появлении новых грантов, проектов или открытии новых НИИ и других подразделений в области науки, УНИД проводит уведомление комиссии по категорированию КИИ для проведения опроса, составления паспорта научного процесса и проведения оценки.

Проведенный обзор нормативно-правовых документов в сфере КИИ, методических разработок и подходов в области категорирования объектов критической информационной инфраструктуры учреждений высшего образования позволил определить этапы, формализовать процессы, определить всех участников:

- одним из видов деятельности высшего учебного заведения является научная деятельность, относящаяся к сферам субъектов КИИ;
- отсутствие в настоящий момент единых методических указаний по категорированию объектов КИИ в сфере науки и необходимость выполнения требований

регуляторов предписывает вузам разрабатывать локальные нормативные акты для проведения соответствующих процедур;

– в основе категорирования объектов КИИ лежит экспертный подход. В качестве экспертной комиссии выступают компетентные специалисты соответствующих научных направлений и специалисты информационной безопасности.

Вывод. Разработанный в Оренбургском государственном университете регламент описания процессов научных исследований соответствует требованиям Федерального закона № 187-ФЗ, включает методические рекомендации описания процессов в научной сфере, организацию работ с паспортами процессов, рекомендации подразделениям, занимающимся научной деятельностью.

Схема этапов категорирования, порядок формирования перечня процессов в области науки в высшем учебном заведении и регламент описания процессов являются методологической основой для дальнейшей работы по декомпозиции процессов теоретического и экспериментального исследований с помощью моделей IDEF0.

Входными данными для описания процессов научного исследования является информация о способах и методах проведения конкретных научных исследований, а также перечень оборудования (информационных систем, сетей, устройств, установок). Выходными данными является описание процесса в виде оценки возможных последствий от компьютерных инцидентов, а также (опционально) типовой процесса в нотации IDEF0.

Библиографический список:

1. Защита от DDoS в 2023: проблемы, опыт, лучшие практики URL: https://blog.cortel.cloud/category/Informaczionnaya-bezopasnost (дата обращения 10.02.2024)
2. Козырева А.А., Тарасов Д.А. Современное состояние государственной политики в сфере информационной безопасности / Вестник Воронежского института МВД России. 2018; № 4. С. 243–247.
3. Бурькова Е.В., Рычкова А.А. Некоторые аспекты категорирования высшего учебного заведения как субъекта критической информационной инфраструктуры / Научно-технический вестник Поволжья. 2022. № 4. С. 207-209.
4. Голубев Д.А., Прохорова Д.И. Категорирование объектов критической информационной инфраструктуры сферы здравоохранения / В сборнике: Актуальные вопросы современной науки и образования. сборник статей VIII Международной научно-практической конференции. Пенза, 2021. С. 129-136.
5. Салкуцан А.А., Гавдан Г.П., Полуянов А.А. Методика определения критических процессов на объектах информационной инфраструктуры / Безопасность информационных технологий. 2020. Т. 27. № 2. С. 18-34.
6. Воеводин В.А., Черняев В.С., Буренок Д.С., Виноградов И.В. Методика оценки защищённости автоматизированной системы управления критической информационной инфраструктуры от DDoS-атак на основе имитационного моделирования методом Монте-Карло / Вестник Дагестанского государственного технического университета. Технические науки. 2023. № 50(1). С. 62-74.
7. Вавичкин А.Н., Горбатов В.С., Дураковский А.П., Чжен Д.А. К вопросу категорирования объектов критической информационной инфраструктуры высших учебных заведений / Безопасность информационных технологий. 2019. Т. 26. № 2. С. 44-57.
8. Фисун В.В. Методика оценки защищенности в интеллектуальной системе управления информационной безопасностью объектов критической информационной инфраструктуры/ Информационная безопасность - актуальная проблема современности. Совершенствование образовательных технологий подготовки специалистов в области информационной безопасности. 2019. № 2 (11). С. 43-50.
9. Краснов А.Е., Мосолов А.С., Феоктистова Н.А. Оценивание устойчивости критических информационных инфраструктур к угрозам информационной безопасности / Безопасность информационных технологий. 2021. Т. 28. № 1. С. 106-120.
10. Смирнов Е.В. Методика оценки политической значимости угроз объекту критической информационной инфраструктуры на примере объекта инфокоммуникаций / Экономика и качество систем связи. 2020. № 2 (16). С. 49-56.
11. Скрыль С.В., Ицкова А.А., Хасин Е.В. О возможности совершенствования процедур количественной оценки угроз несанкционированного доступа к информации объектов критической информационной инфраструктуры / Безопасность информационных технологий. 2023. Т. 30. № 4. С. 61-73.
12. Гавдан Г.П., Иваненко В.Г., Салкуцан А.А. Обеспечение безопасности значимых объектов критической информационной инфраструктуры / Безопасность информационных технологий. 2019. Т. 26. № 4. С. 69-82.
13. Абраменко Г.Т., Лансере Н.Н., Фадеев И.И. Анализ особенностей субъектов критической информационной инфраструктуры российской федерации, функционирующих в сфере науки. В сборнике: Актуальные

проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). XI Международная научно-техническая и научно-методическая конференция. Санкт-Петербург, 2022. С. 49-54.
14. Методические рекомендации Категорирование объектов критической информационной инфраструктуры. ООО «СТЭП ЛОДЖИК». URL: https://step.ru/news/?code=2046 (дата обращения 15.02.2024).
15. Сайт Оренбургского государственного университета. [Электронный ресурс]. URL: http://www.osu.ru/doc/5419 - 15.02.2024 (дата обращения 02.02.2024).
16. Харланов Р.Л. Правовые основы обеспечения безопасности критической информационной инфраструктуры в России / Современная наука: Актуальные проблемы теории и практики. Серия: Экономика и право, 2022. № 3-2. С. 98-103
17. Котов А.А., Куринная В.С., Шлыков М.С. Алгоритм категорирования объектов критической информационной инфраструктуры / REDS: Телекоммуникационные устройства и системы, 2018. Т. 8. № 4. С.34-37
18. Сидак А.А., Корниенко А.А., Глухова В.А. Категорирование и оценка значимости объектов критической информационной инфраструктуры железнодорожного транспорта / Двойные технологии, 2019. № 1 (86). С.88-93.
19. Солдатов А.Ю., Солдатов Е.Ю., Скориков В.С. Вуз как объект критической информационной инфраструктуры / ИНТЕР ЭКСПО ГЕО СИБИРЬ, 2022. Т. 7. № 2. С. 93-96.
20. Мазепин П.С., Гришин Н.А., Бочаров М.В. Подход к категорированию высших учебных заведений в рамках категорирования объектов критической информационной инфраструктуры / Инновации. Наука. Образование, 2021. № 34. С. 879-883.
21. Заколдаев Д.А., Швед В.Г., Копырулина О.А. Автоматизация процессов категорирования объектов критической информационной инфраструктуры. Защита информации. Инсайд, 2021. № 3 (99). С. 37-43

References:

1. DDoS protection in 2023: problems, experience, best practices URL: https://blog.cortel.cloud/category/Informaczionnaya-bezopasnost (accessed 02/10/2024) (In Russ)
2. Kozyreva A.A., Tarasov D.A. The current state of state policy in the field of information security. *Herfld of the Voronezh Institute of the Ministry of Internal Affairs of Russia*. 2018; 4: 243-247. (In Russ)
3. Burkova E.V., Rychkova A.A. Some aspects of categorizing a higher educational institution as a subject of critical information infrastructure. *Scientific and Technical Bulletin of the Volga region*. 2022; 4:207-209. (In Russ)
4. Golubev D.A., Prokhorova D.I. Categorization of objects of critical information infrastructure in the healthcare sector. In the collection: Topical issues of modern science and education. collection of articles of the VIII International Scientific and Practical Conference. Penza, 2021;129-136. (In Russ)
5. Salkutsan A.A., Gavdan G.P., Poluyanov A.A. Methodology for determining critical processes at information infrastructure facilities. *Information technology security*. 2020; 27(2):18-34. (In Russ)
6. Voevodin V.A., Chernyaev V.S., Burenok D.S., Vinogradov I.V. Methodology for assessing the security of an automated control system of critical information infrastructure from DDoS attacks based on Monte Carlo simulation. *Herfld of the Daghestan State Technical University. Technical Sciences*. 2023; 50(1):62-74. (In Russ)
7. Vavichkin A.N., Gorbatov V.S., Durakovsky A.P., Zheng D.A. On the issue of categorization of objects of critical information infrastructure of higher educational institutions. *Information technology security*. 2019; 26(2): 44-57. (In Russ)
8. Fisun V.V. Methodology for assessing security in an intelligent information security management system for critical information infrastructure facilities/ Information security is an urgent problem of our time. Improvement of educational technologies for training specialists in the field of information security. 2019;2 (11):43-50. (In Russ)
9. Krasnov A.E., Mosolov A.S., Feoktistova N.A. Assessment of the stability of critical information infrastructures to threats to information security. *Information technology security*. 2021; 28(1):106-120. (In Russ)
10. Smirnov E.V. Methodology for assessing the political significance of threats to the object of critical information infrastructure on the example of an infocommunication object. *Economics and quality of communication systems.* 2020;2 (16):49-56 (In Russ)
11. Skryl S.V., Itskova A.A., Khasin E.V. On the possibility of improving procedures for quantifying threats of unauthorized access to information of critical information infrastructure facilities. *Information Technology Security*. 2023;30(4):61-73 (In Russ)
12. Gavdan G.P., Ivanenko V.G., Salkutsan A.A. Ensuring the security of significant objects of critical information infrastructure. *Information technology security*. 2019; 26(4):69-82. (In Russ)
13. Abramenko G.T., Lancere N.N., Fadeev I.I. Analysis of the features of the subjects of the critical information infrastructure of the Russian Federation operating in the field of science. In the collection: Current problems of infotelecommunications in science and education (APINO 2022). XI International Scientific-technical and scientific-methodical Conference. St. Petersburg, 2022; 49-54 (In Russ)

14. Methodological recommendations Categorization of objects of critical information infrastructure. STEP LOGIC LLC. URL: https://step.ru/news/?code=2046 (accessed 02/15/2024). (In Russ)
15. Website of Orenburg State University. [electronic resource]. URL: http://www.osu.ru/doc/5419 - 02/15/2024 (accessed 02/02/2024). (In Russ)
16. Kharlanov R.L. The legal foundations of ensuring the security of critical information infrastructure in Russia. *Modern science: Actual problems of theory and practice. Series: Economics and Law,* 2022; 3-2:98-103 (In Russ)
17. Kotov A.A., Kurinnaya V.S., Shlykov M.S. Algorithm for categorizing objects of critical information infrastructure. *REDS: Telecommunication devices and systems*. 2018; 8(4):34-37 (In Russ)
18. Sidak A.A., Kornienko A.A., Glukhova V.A. Categorization and assessment of the importance of objects of critical information infrastructure of railway transport. *Dual technologies*. 2019; 1 (86):88-93. (In Russ)
19. Soldatov A.Yu., Soldatov E.Yu., Skorikov V.S. University as an object of critical information infrastructure. *INTER EXPO GEO SIBERIA*, 2022; 7(2): 93-96 (In Russ)
20. Mazepin P.S., Grishin N.A., Bocharov M.V. Approach to categorization of higher educational institutions within the framework of categorization of objects of critical information infrastructure. *Innovations. Science. Education.* 2021;34:879-883 (In Russ)
21. Zakoldaev D.A., Shved V.G., Kopyrulina O.A. Automation of categorization processes of objects of critical information infrastructure. *Information protection. Inside*, 2021; 3 (99):37-43 (In Russ)

Сведения об авторах:

Бурькова Елена Владимировна, кандидат педагогических наук, доцент, кафедра вычислительной техники и защиты информации; tulpan63@bk.ru

Рычкова Анастасия Александровна, кандидат педагогических наук, доцент, кафедра вычислительной техники и защиты информации; rnansy@yandex.ru; ORCID: 0000-0003-0734-5071

Гриценко Любовь Андреевна, ассистент, кафедра вычислительной техники и защиты информации; lubaizvekova@gmail.com

Information about authors:

Elena V. Burkova, Cand. Sci. (Pedagog.), Assoc. Prof., Department of Computer Technology and Information Security; tulpan63@bk.ru

Anastasia A. Rychkova, Cand. Sci. (Pedagog.), Assoc. Prof., Department of Computer Technology and Information Security; rnansy@yandex.ru; ORCID: 0000-0003-0734-5071

Lyubov A. Gritsenko, Assistant, Department of Computer Technology and Information Security; lubaizvekova@gmail.com

Конфликт интересов/Conflict of interest.

Авторы заявляют об отсутствии конфликта интересов/The authors declare no conflict of interest.

Поступила в редакцию/Received 01.03.2024.

Одобрена после/рецензирования Reviced 29.03.2024.

Принята в печать/ Accepted for publication 29.03.2024.