Управление рисками и безопасностью

Обеспечение безопасности при формировании планов НИОКР холдинга

А.Ю. Даниленко, Г.П. Акимова

Федеральный исследовательский центр «Информатика и управление» Российской академии наук, г. Москва, Россия

Аннотация. В статье рассмотрены особенности работы с документами, предназначенными для принятия решения о постановке научно-исследовательских и опытно-конструкторских работ, в том числе совместная обработка бумажных и электронных документов. Представлены варианты потенциальных угроз и способов действий потенциальных нарушителей, сформулированы способы построения системы защиты информации.

Ключевые слова: *научно-исследовательские и опытно-конструкторские работы, информационная безопасность, инвестиции в технологии, угрозы для бумажных и электронных документов.*
DOI: 10.14357/20790279250407 **EDN:** KLAUFH

Введение

Как правило, крупные компании, холдинги, объединяющие большое число подразделений, уделяют большое внимание и выделяют существенные ресурсы на проведение исследований, разработок и других инновационных работ. Эти научно-исследовательские и опытно-конструкторские работы (НИОКР) могут быть не связаны напрямую с основной деятельностью компании, т.е. не приносят непосредственный экономический эффект. Такие НИОКР – это работа на перспективу, их результаты должны в будущем, причем в большинстве случаев в ближайшем будущем, позволить усовершенствовать технологические процессы холдинга и принести существенную прибыль.

Например, ПАО «Аэрофлот» в 2021 году приняло Программу инновационного развития до 2026 года [1], в которой выделены следующие направления деятельности (технологические группы):

- технологии, направленные на повышение надежности, предотвращение авиакатастроф;
- технологии «озеленения» и эргономические системы;
- технологии энергосбережения и снижения ресурсоемкости;
- технологии, направленные на повышение физической и экономической доступности авиатранспорта, а также на рост удовлетворенности и лояльности клиентов;
- технологии оптимизации наземной авиационной инфраструктуры с использованием новейших информационных и логистических систем.

Документ [2] дает представление об объемах инвестиций ПАО «Аэрофлот» в исследования и разработки. В разделе «Нематериальные активы» указано, что на 31 декабря 2023 года первоначальная стоимость вложений в разработку ПО и НИ-

ОКР составляла 1.049 млрд руб., остаточная стоимость – 148 млн.

Как указано в [3], Сбербанк в 2024-2026 годах увеличит инвестиции в технологии в полтора раза – до 450 млрд рублей, сообщил вице-президент, руководитель блока «Финансы» Сбербанка Тарас Скворцов. Он отметил, что все эти инвестиции окупаются. Прибыль от применения технологий искусственного интеллекта в 2021-2023 годах составляет порядка 800 млрд рублей.

ПАО «НК «Роснефть» приняла Программу инновационного развития [4]. Результаты научного внедрения рассмотрены, в частности, в [5]. Подтвержденный экономический эффект по итогам года от технологий, внедренных за предшествующие три года, составил более 40 млрд рублей. Согласно Отчету в области устойчивого развития ПАО «НК «Роснефть» за 2020 год, компанией было подано 60 заявок на патенты и свидетельства на программное обеспечение. Что еще более важно, продолжается активное внедрение в производственную деятельность компании технологий, чей охранный статус подтвержден патентным ведомством. Так, по итогам прошлого года 172 технологии было испытано, 72 – внедрено и тиражировано.

Как указано в [6], Группа Газпром (ПАО «Газпром», ПАО «Газпром нефть», ООО «Газпром энергохолдинг» и другие дочерние общества) обладает развитой системой управления инновационной деятельностью. В ПАО «Газпром» на постоянной основе работает Комиссия по НИОКР, которая рассматривает вопросы целесообразности и организации выполнения НИОКР в ПАО «Газпром» и его дочерних обществах, руководствуясь принципами открытости, объективности и независимости. По результатам работы Комиссии в 2023 г. принято решение о выполнении 102 новых тематик НИОКР (на 32 % больше по сравнению с 2022 г.). Объем инвестиций в НИОКР и количество полученных патентов составляют:
2021 год: 24.60 млрд руб., 2 901 патент;
2022 год: 30.01 млрд руб., 3 119 патентов;
2023 год: 31.70 млрд руб., 3 397 патентов.

1. Формирование планов работ

Деловая логика организаций при формировании планов НИОКР имеет общие черты, обусловленные сложившейся практикой взаимодействия организаций, стоящих на разных ступенях иерархии. В данной работе рассмотрен вариант двухуровневой организации структуры холдинга: одно головное подразделение и несколько подчиненных. При этом головное подразделение является распорядителем финансовых активов, именно в нем принимается решение о начале новых работ (рис. 1).

Руководство подчиненного подразделения принимает решение о постановке НИОКР с целью совершенствования технологических процессов подразделения и увеличения объема прибыли. В связи с этим формируется заявка, описывающая требуемую разработку и объем финансирования в виде технико-экономического обоснования (ТЭО). Сформированный пакет документов поступает в головное подразделение, обработка в котором предусматривает несколько этапов.

Выявление похожих работ. На первом этапе обработки заявки выполняется поиск похожих работ, проводившихся ранее, т.е. работ, результаты которых соответствуют предполагаемым в заявке. Поиск таких работ, точнее их результатов, выполняется как по собственной базе данных прежних НИОКР (реализованных либо отклоненных), так и с использованием внешних источников в ходе па-

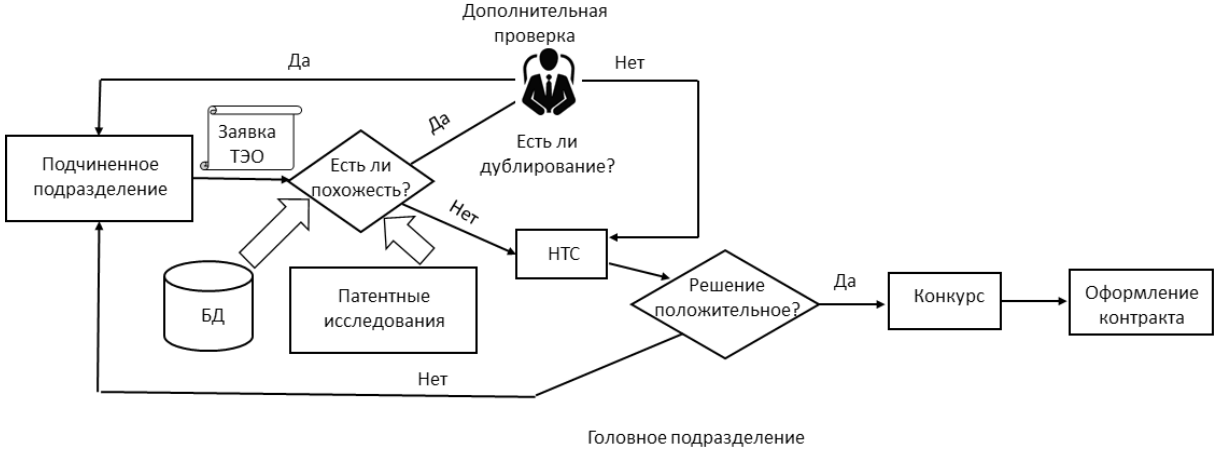

Рис. 1. Алгоритм принятия решения о постановке НИОКР

тентного поиска в соответствии с [7]. Этот стандарт предусматривает поиск по патентным базам данных и по общедоступным источникам. Дополнительно для поиска похожих работ может быть использовано специально разработанное программное обеспечение. Такие алгоритмы применены, в частности, в системе Антиплагиат [8], целесообразно и применение подхода [9].

Дополнительная проверка. В случае выявления похожих работ подключаются эксперты, которые должны дать ответ, действительно ли новая заявка предполагает работу, дублирующую полученные ранее результаты. В случае положительного решения работа отклоняется, а заявка возвращается в подчиненное подразделение. Если эксперты делают вывод о необходимости проведения данной работы, документы передаются на рассмотрение научно-технического совета (НТС).

Рассмотрение заявки на НТС. Задача научно-технического совета или другого коллегиального органа с аналогичными функциями при рассмотрении вопроса о постановке НИОКР не только подтвердить вывод экспертов об уникальности новой работы, но и определить ее необходимость для всего холдинга. При решении вопроса о целесообразности начала работы требуется также учесть финансовую составляющую, описанную в технико-экономическом обосновании (ТЭО), являющемся составной частью заявки.

В случае решения о целесообразности работы она запускается, то есть начинаются конкурсные процедуры для выбора исполнителя с последующим оформлением контракта. При отклонении работы документы возвращаются в подчиненное подразделение, инициировавшее рассмотрение предполагаемой НИОКР.

2. Обеспечение безопасности

При рассмотрении вопросов, связанных с обеспечением информационной безопасности, следует иметь в виду, что документы, которые создаются, хранятся и обрабатываются в ходе принятия решения о постановке новых НИОКР, могут быть как в электронном виде, так и на бумажных носителях. Если говорить об электронных версиях документов, то для них требуется обеспечить конфиденциальность, целостность и доступность. Однако обеспечение конфиденциальности выходит на первый план, поскольку целостность и доступность достаточно надежно достигаются аппаратными средствами: надежное оборудование и регулярное резервное копирование информации. В связи с этим далее будут рассмотрены способы обеспечения конфиденциальности электронных и бумажных документов.

2.1. Угрозы несанкционированного доступа для электронных и бумажных документов

Источниками угроз несанкционированного доступа (НСД) для электронных документов, обрабатываемых автоматизированными информационными системами (АИС) согласно [10], могут быть внешние и внутренние нарушители. Внешние нарушители не имеют доступа к АИС и реализуют угрозы из внешних сетей связи общего пользования, в том числе сетей международного информационного обмена. Внутренние нарушители имеют доступ к АИС, в том числе к ним относятся их пользователи.

Доступ внешних нарушителей к бумажным документам возможен только в результате сговора внешних и внутренних нарушителей. Для рассматриваемого случая постановки НИОКР актуальны внутренние нарушители и внешние, относящиеся к разведывательным службам и конкурентам. Доступ к охраняемой информации осуществляется с целью недобросовестной конкуренции, выраженной в преступных действиях и направленной на подрыв коммерческой деятельности конкурентоспособной компании, нелегальном получении и использовании сведений, составляющих коммерческую, налоговую или банковскую тайну (промышленный шпионаж, ст. 183 Уголовного кодекса России «Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну»).

Внешний нарушитель имеет возможность осуществлять несанкционированный доступ к каналам связи, выходящим за пределы служебных помещений, использовать специальные программные вирусы, вредоносные программы, алгоритмические или программные закладки.

Возможности внутреннего нарушителя существенным образом зависят от действующих в пределах контролируемой зоны режимных и организационно-технических мер защиты, в том числе по допуску сотрудников к обрабатываемой информации и контролю порядка проведения работ.

Внутренние потенциальные нарушители подразделяются в зависимости от способа доступа и полномочий доступа к АИС:

– лица, имеющие санкционированный доступ к АИС, но не имеющие доступа к обрабатываемой информации. К этому типу нарушителей относятся должностные лица, обеспечивающие нормальное функционирование АИС;

– зарегистрированные пользователи АИС, осуществляющие ограниченный доступ к ресурсам АИС с рабочего места;
– пользователи АИС с полномочиями администраторов различного уровня и полномочий (безопасности, системные, баз данных и т.д.);
– разработчики прикладного программного обеспечения и технических средств и лица, обеспечивающие их сопровождение.

К бумажным документам имеют доступ только специалисты, непосредственно работающие с документами, а также сотрудники, имеющие доступ в помещения, в которых документы хранятся и обрабатываются.

Все угрозы безопасности информации подразделяются на два класса:
– реализуемые за счет непреднамеренных воздействий и не являющиеся атаками;
– реализуемые за счет преднамеренных (злоумышленных) воздействий и являющиеся атаками (потенциальными или проводимыми).

К угрозам, не являющимся атаками, относятся:
– угрозы стихийного, техногенного и т. п. характера, не связанные с деятельностью лиц;
– угрозы, заключающиеся в ошибочных действиях и/или нарушениях, связанных с халатностью, некомпетентностью лиц, задействованных на разных этапах жизненного цикла АИС.

Все перечисленные угрозы актуальны для электронных документов, тогда как для документов на бумажных носителях могут быть реализованы угрозы стихийного и техногенного характера. Относительно угроз, связанных с халатностью и некомпетентностью, отметим, что такие действия могут способствовать атакам, заключающимся в несанкционированном ознакомлении и копировании информации на бумажных носителях.

2.2. Атаки внешних нарушителей

Атаки, то есть целенаправленные воздействия на АИС с целью несанкционированного доступа к обрабатываемой информации, могут совершаться как внешними, так и внутренними нарушителями. Основные категории атак, которые могут быть реализованы внешними нарушителями:
– анализ сетевого трафика;
– сканирование сети;
– подмена доверенного объекта сети;
– навязывание ложного маршрута;
– внедрение ложного объекта сети.

Все перечисленные категории атак направлены на сетевую инфраструктуру и позволяют, в случае успешной реализации, перехватывать передаваемые данные, а также навязывать ложную информацию. Противодействие атакам, основанным на использовании уязвимостей технических средств АИС и сетевой инфраструктуры, осуществляется общеобъектовыми мерами защиты, а также использованием надежного оборудования и защищенных каналов связи.

2.3. Атаки внутренних нарушителей

Атаки, реализуемые внутренними нарушителями, направлены, как правило, на нарушение конфиденциальности информации, т.е. представляют собой попытки несанкционированного доступа с целью ознакомления с документами и, возможно, их искажения или уничтожения. Для обеспечения конфиденциальности данных большое значение имеют организационные меры, определяемые внутренними нормативными актами предприятий и организаций. Так, согласно [11], при работе с бумажными документами требуется:
– печатать документы с информацией ограниченного доступа на выделенных компьютерах с последующим уничтожением черновиков;
– передавать их работникам под расписку;
– пересылать сторонним организациям фельдъегерской связью, заказными или ценными почтовыми отправлениями;
– размножать с письменного разрешения соответствующего руководителя с последующим поэкземплярным учетом;
– хранить в надежно запираемых и опечатываемых шкафах;
– передавать документы и дела с пометкой «Для служебного пользования» от одного работника другому с разрешения соответствующего руководителя;
– регулярно проводить проверку наличия документов специально формируемой комиссией.

Все перечисленные требования распространяются на порядок обращения с любыми носителями информации, включая машинные.

Меры, направленные на обеспечение конфиденциальности электронных документов, обрабатываемых АИС, перечислены в руководящих документах и приказах ФСТЭК России [12–14].

В частности, они предусматривают реализацию следующих мер:
– идентификация и аутентификация пользователей;
– управление учетными записями пользователей;
– реализация необходимых методов и правил разграничения доступа;
– разделение полномочий (ролей) пользователей и администраторов;
– назначение минимально необходимых прав и привилегий пользователям;

– разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации (организация или запрет гостевого доступа);
– установка только разрешенного к использованию программного обеспечения;
– сбор, запись и хранение информации о событиях безопасности в течении установленного времени хранения;
– учет машинных носителей информации и управление доступом к ним.

2.4. Управление доступом

Существенное значение для обеспечения конфиденциальности имеет политика управления доступом, которая реализуется в организации. Именно ею руководствуются руководители при передаче документов между работниками, причем это справедливо как при передаче материальных носителей, так и при предоставлении доступа к электронным документам, обрабатываемым в АИС.

В подчиненных подразделениях доступ ко всем документам, имеющим отношение к новым НИОКР, определяется должностными обязанностями сотрудников. Круг участников подготовки этих документов ограничен: руководство (утверждает документы), профильное подразделение (формирует заявку и обосновывает необходимость заказываемой НИОКР), экономический блок (подготовка ТЭО).

В головном подразделении заявки на постановку новых НИОКР рассматривает достаточно широкий круг сотрудников, кроме того, все они знакомы, причем многие весьма детально, со всеми работами холдинга. Это обстоятельство требует тщательного подхода к распределению полномочий между этими сотрудниками, а также серьезных мер по контролю их работы. На приведенном рисунке видно, что с заявками на постановку НИОКР работают следующие группы сотрудников:
– секретариат, получающий входящие и отправляющий исходящие документы (на рисунке не показан);
– патентный отдел, выполняющий патентные исследования;
– специалисты, выполняющие поиск работ, имеющих признаки похожести на работы, данные о которых есть в базе данных НИОКР, причем это могут быть работы как холдинга, так и внешних организаций;
– эксперты, выполняющие дополнительную проверку с целью окончательного решения о наличии дублирования работ, выполнявшихся ранее;
– члены НТС;
– сотрудники, готовящие конкурсные процедуры;
– подразделение, выполняющее подготовку и заключение контракта на выполнение работы.

Для обеспечения конфиденциальности информации сотрудники всех перечисленных подразделений должны строго соблюдать перечисленные выше требования в части обращения с документами, содержащими служебную информацию.

Для электронных документов, обрабатываемых средствами АИС целесообразно установить следующие правила разграничения доступа:
– создаются следующие группы пользователей АИС: все пользователи, работающие с новыми работами; группы по подразделениям, входящие в первую группу: секретариат, патентный отдел, НТС и т.д.
– с точки зрения информационной безопасности все сотрудники, входящие в группу, имеют равный доступ ко всем документам, связанным с новыми работами. Такое решение позволяет упростить процедуру сертификации АИС;
– средствами АИС реализуется технологическое разграничение доступа по следующим правилам:
  • сотрудники секретариата не могут читать документы, но могут их регистрировать, заполняя регистрационные карточки;
  • сотрудники патентного отдела и подразделения, выполняющего поиск похожих работ, читают документы, но не могут их редактировать. Создают свои документы – отчеты о проведенном поиске;
  • эксперты читают документы и создают свои отчеты о проделанной работе;
  • члены НТС читают все документы, как пришедшие из подчиненного подразделения, так и сформированные в головном подразделении. Решение НТС по рассматриваемой работе оформляется новым документом – заключением о целесообразности постановки НИОКР;
  • сотрудники, готовящие конкурсные процедуры и оформляющие контракт, читают все документы и готовят материалы для проведения конкурса;
  • каждый сотрудник имеет доступ к документу на время выполнения своей работы.
– таким образом, редактирование документов, пришедших из подчиненного подразделения сотрудниками головного подразделения запрещено;
– в АИС реализуется процедура утверждения документа, после выполнения которой редактирование документа запрещается. Утверждение выполняется руководителем сотрудника, создавшего документ;
– редактирование документа, созданного сотрудником, разрешается до момента утверждения документа.

Заключение

Широкое внедрение цифровых технологий во все отрасли народного хозяйства, образование, государственное управление, которое часто называют их цифровизацией, невозможно без надежного обеспечения безопасности обрабатываемой информации. Рассмотренные в статье особенности работы с документами, предназначенными для принятия решения о постановке НИОКР, предполагают подход к обеспечению безопасности, обусловленный совместной обработкой бумажных и электронных документов. Предложенные варианты потенциальных угроз и способов действий потенциальных нарушителей позволяют сформулировать способы построения системы защиты информации как с использованием технических средств, так и организационных мер.

Описанные способы обеспечения безопасности информации могут быть с успехом применены в различных областях народного хозяйства России.

Литература

1. Паспорт Программы инновационного развития. https://www.aeroflot.com/media/aflfiles/media/strategy/pasport_programmy_innovatsionnogo_razvitiia.pdf.
2. Публичное акционерное общество «Аэрофлот – российские авиалинии». Консолидированная финансовая отчетность в соответствии с международными стандартами финансовой отчетности за 2023 год. https://cdn.financemarker.ru/reports/2023/MOEX/A/AFLT_2023_12_Y_%D0%9C%D0%A1%D0%A4%D0%9E.pdf.
3. Сбер в 2024-2026 годах увеличит инвестиции в технологии в 1,5 раза. https://www.interfax.ru/business/934900.
4. Паспорт. Программы инновационного развития ПАО «НК «Роснефть». Москва 2021. https://www.rosneft.ru/upload/site1/document_file/passport-proginfr.pdf?ysclid=mfdxu2doq9155565532.
5. Научное внедрение. https://rapsinews.ru/incident_publication/20211220/307611054.html
6. Инновационное развитие. https://sustainability.gazpromreport.ru/2023/about-gazprom/innovative-development/?ysclid=mfdy6jwz4b720052440.
7. Интеллектуальная собственность. Патентные исследования. Содержание и порядок проведения. ГОСТ Р 15.011—2024.
8. *Ивахненко А.* Так устроен поиск заимствований в Антиплагиате. https://habr.com/ru/companies/antiplagiat/articles/429634/.
9. Извлечение признаков из текстовых данных с использованием TF-IDF. https://habr.com/ru/companies/otus/articles/755772/.
10. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена Заместителем директора ФСТЭК России 15 февраля 2008 г.
11. Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти… (утв. постановлением Правительства РФ от 3 ноября 1994 г. № 1233). С изменениями и дополнениями от: 20 июля 2012 г., 20 февраля, 18 марта 2016 г., 6 августа 2020 г.
12. Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Приказ ФСТЭК России от 11 февраля 2013 г. № 17.
13. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Руководящий документ ФСТЭК России. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.
14. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Руководящий документ ФСТЭК России. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.

Акимова Галина Павловна. Федеральный исследовательский центр «Информатика и управление» Российской академии наук, г. Москва, Россия. Старший научный сотрудник. Кандидат технических наук. Область научных интересов: системное программирование, системный анализ, информационные технологии, влияние человеческого фактора, информационно-аналитические системы, электронный документооборот, электронный архив. E-mail: akimova@isa.ru

Даниленко Андрей Юрьевич. Федеральный исследовательский центр «Информатика и управление» Российской академии наук, г. Москва, Россия. Старший научный сотрудник. Кандидат физико-математических наук. Область научных интересов: системное программирование, системный анализ, информационные технологии, электронный документооборот, информационная безопасность, защита данных. E-mail: danilenko@isa.ru (ответственный за переписку).

Ensuring security in the formation of R&D plans for the holding

A.Yu. Danilenko, G.P. Akimova
Federal Research Center "Computer Science and Control" of Russian Academy of Sciences, Moscow, Russia

Abstract. This article examines the specifics of working with documents used for decision-making on research and development projects, including the joint processing of paper and electronic documents. Potential threats and methods of attack by potential violators are presented, and methods for building an information security system are formulated.

Keywords: *research and development, information security, technology investments, threats to paper and electronic documents*.
DOI: 10.14357/20790279250407 **EDN:** KLAUFH

References

1. Pasport Programmy innovatsionnogo razvitiya. [Passport of the Innovative Development Program]. https://www.aeroflot.com/media/aflfiles/media/strategy/pasport_programmy_innovatsionnogo_razvitiia.pdf.
2. Publichnoye aktsionernoye obshchestvo «Aeroflot – rossiyskiye avialinii». Konsolidirovannaya finansovaya otchetnost' v sootvetstvii s mezhdunarodnymi standartami finansovoy otchetnosti za 2023 god. [Public joint-stock company Aeroflot – russian airlines. Consolidated financial statements in accordance with International Financial Reporting Standards for the year ended 31 December 2023.]. https://cdn.financemarker.ru/reports/2023/MOEX-/A/AFLT_2023_12_Y_%D0%9C%D0%A1%D0%A4%D0%9E.pdf.
3. Sber v 2024-2026 godakh uvelichit investitsii v tekhnologii v 1,5 raza. [Sber will increase investment in technology by 1.5 times in 2024-2026.]. https://www.interfax.ru/business/934900.
4. Pasport. Programmy innovatsionnogo razvitiya PAO «NK «Rosneft'». Moskva 2021. [Passport. Innovative Development Programs of Rosneft Oil Company. Moscow 2021.]. https://www.rosneft.ru/upload/site1/document_file/passport-proginfr.pdf?ysclid=mfdxu2doq9155565532.
5. Nauchnoye vnedreniye. [Scientific implementation.]. https://rapsinews.ru/incident_publication/20211220/307611054.html.
6. Innovatsionnoye razvitiye. [Innovative development]. https://sustainability.gazpromreport.ru/2023/about-gazprom/innovative-development/?ysclid=mfdy6jwz4b720052440.
7. Intellektual'naya sobstvennost'. Patentnye issledovaniya. Soderzhaniye i poryadok provedeniya. GOST R 15.011—2024. [Intellectual Property. Patent Research. Contents and Procedure. GOST R 15.011-2024].
8. *Ivakhnenko A.* Tak ustroyen poisk zaimstvovaniy v Antiplagiate. [Andrey Ivakhnenko. This is how the Antiplagiat search works.]. https://habr.com/ru/companies/antiplagiat/articles/429634/.
9. Izvlecheniye priznakov iz tekstovykh dannykh s ispol'zovaniyem TF-IDF. [Feature Extraction from Text Data Using TF-IDF]. https://habr.com/ru/companies/otus/articles/755772/.
10. Bazovaya model' ugroz bezopasnosti personal'nykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personal'nykh dannykh. Utverzhdena Zamestitelem direktora FSTEK Rossii 15 fevralya 2008 g. [Basic model of personal data security threats when processed in personal data information systems. Approved by the Deputy Director of the Federal Service for Technical and Export Control of Russia on February 15, 2008].
11. Polozheniye o poryadke obrashcheniya so sluzhebnoy informatsiyey ogranichennogo rasprostraneniya v federal'nykh organakh ispolnitel'noy vlasti… (utv. postanovleniyem Pravitel'stva RF ot 3 noyabrya 1994 g. N 1233). S izmeneniyami i dopolneniyami ot: 20 iyulya 2012 g., 20 fevralya, 18 marta 2016 g., 6 avgusta 2020

g. [Regulations on the Procedure for Handling Restricted Official Information in Federal Executive Bodies (approved by RF Government Resolution No. 1233 of November 3, 1994). As amended on July 20, 2012, February 20, March 18, 2016, and August 6, 2020].
12. Ob utverzhdenii trebovaniy o zashchite informatsii, ne sostavlyayushchey gosudarstvennuyu taynu, soderzhashcheysya v gosudarstvennykh informatsionnykh sistemakh. Prikaz FSTEK Rossii ot 11 fevralya 2013 g. № 17. [On approval of requirements for the protection of information that does not constitute a state secret, contained in state information systems. Order of the FSTEC of Russia dated February 11, 2013, No. 17].
13. Sredstva vychislitel'noy tekhniki. Zashchita ot nesanktsionirovannogo dostupa k informatsii. Pokazateli zashchishchennosti ot nesanktsionirovannogo dostupa k informatsii. Rukovodyashchiy dokument FSTEK Rossii. Utverzhdeno resheniyem predsedatelya Gosudarstvennoy tekhnicheskoy komissii pri Prezidente Rossiyskoy Federatsii ot 30 marta 1992 g. [Computer equipment. Protection against unauthorized access to information. Indicators of security against unauthorized access to information. Guidance document of the Federal Service for Technical and Export Control of Russia. Approved by the decision of the Chairman of the State Technical Commission under the President of the Russian Federation on March 30, 1992].
14. Avtomatizirovannyye sistemy. Zashchita ot nesanktsionirovannogo dostupa k informatsii. Klassifikatsiya avtomatizirovannykh sistem i trebovaniya po zashchite informatsii. Rukovodyashchiy dokument FSTEK Rossii. Utverzhdeno resheniyem predsedatelya Gosudarstvennoy tekhnicheskoy komissii pri Prezidente Rossiyskoy Federatsii ot 30 marta 1992 g. [Automated Systems. Protection from Unauthorized Access to Information. Classification of Automated Systems and Information Security Requirements. Guidance Document of the Federal Service for Technical and Export Control of Russia. Approved by the decision of the Chairman of the State Technical Commission under the President of the Russian Federation on March 30, 1992].

Galina P. Akimova. Ph.D.(Eng.), Senior Research Scientist, Federal Research Center "Computer Science and Control" of Russian Academy of Sciences, 44/2 Vavilova str., Moscow, 119333, Russia, author of more than 50 printed works, research interests: system programming, system analysis, information technology, the influence of the human factor, information and analytical systems, electronic document management, electronic archive. E-mail: akimova@isa.ru

Andrey Yu. Danilenko. Ph.D.(Phys.-Math.), Senior Research Scientist, Federal Research Center "Computer Science and Control" of Russian Academy of Sciences, 44/2 Vavilova str., Moscow, 119333, Russia, author more than 40 publications (1 monograph), research interests: system programming, system analysis, information technology, electronic document management, information security, data protection. E-mail: danilenko@isa.ru