Анализ инцидентов информационной безопасности в государственных органах Российской Федерации: возможные пути улучшения уровня защиты конфиденциальной информации

Романычев Никита Олегович
аспирант, Российский государственный университет правосудия имени В. М. Лебедева, n.romanychev@yandex.ru

В статье рассмотрены основные проблемы защиты информационных систем государственных органов с применением анализа конкретных случаев утечек информации, в том числе случаев утечек из судебной системы. Рассмотрены основные нормативно-правовые акты, регулирующие защиту конфиденциальной информации, основные уязвимости государственных органов.
Ключевые слова: Информационная безопасность, государственные органы, персональные данные, конфиденциальная информация, государственная информационная система, ФСТЭК, судебная система.

Введение

Утечка информации в государственных учреждениях – широко распространенная проблема, которая затрагивает широкий перечень организаций госсектора. Государственный сектор представляет собой совокупность предприятий и учреждений, которые находятся в государственной собственности.

В научном сообществе выделяют проблемы информационной безопасности, например Сосипатров Р. А., Бабаев Д. Б выделяют следующие [1]: •Недостаток квалифицированных специалистов:

•Недостаточное финансирование:

•Отсутствие единой стратегии: в разных государственных органах могут быть разные подходы к обеспечению безопасности, что ведет к несогласованности действий и снижению общего уровня защиты информации.

•Угрозы со стороны внешних источников: хакеры, фишерные ссылки и тому подобное.

Рассмотрим аналитический отчет Infowatch, согласно которому в 2024 году доля успешных кибератак в России составляет а 70,1% [2]. При этом почти каждое пятое нарушение связано с эксплуатацией внутренних рисков.

При этом интересны данные компании «Еса Про» от декабря 2025 года [3]. Согласно этим данным большинество утечек происходит в госсекторе (73% от всех). Специалисты компании, указывают, что «связано это с политической мотивацией хакеров.»

На уязвимость сегмента также влияют низкий уровень кибербезопасности многих организаций из-за «халатности сотрудников и недостатка финансирования».

Основная часть

Государственные учреждения обрабатывают и хранят большие объемы информации ограниченного доступа и требующие принятия защитных мер:

1. Данные, которые относятся к категории «государственная тайна»;
2. Служебные документы;
3. Коммерческая тайна, которая может содержаться в судебных документах.
4. Персональные данные граждан. Государственные органы собирают и хранят персональные сведения о гражданах в своих информационных системах.

Реальных примеров **утечек информации в госучреждениях** достаточно много, так как в последние годы государственные органы все чаще находятся под атакой не только внешних злоумышленников, но и внутренних нарушителей. В связи с этим государственные организации должны обеспечивать многоуровневую модель защиты таких данных.

Утечки информации опасны для государственных органов, так как они могут привести к серьёзным последствиям, включая ущерб безопасности, финансовые потери и репутационные риски. Опять же, это связано с большим объемом информации ограниченного доступа.

Одним из первых эшелонов защиты должны быть средства защиты от утечек со стороны внутренних нарушителей, на долю которых приходится немалая часть зафиксированных инцидентов.

Требования законодательства и регуляторов

Учреждения госсектора обязаны выполнять требования законодательства и регуляторов в сферах информационной и экономической безопасности. Они включают требования в части профилактики коррупционных правонарушений, соблюдения принципов, требований, ограничений и запретов, накладываемых на госслужащих. Ниже приведен список главных законодательных актов, устанавливающих правила и требования работы с информацией:

- Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных»
- Федеральный закон от 26.07.2017 №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»
- Закон Российской Федерации N 5485-1 «О государственной тайне»;
- Постановление Правительства Российской Федерации №1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных";
- Приказ N 21 ФСТЭК России;
- Указ Президента РФ N 188 от 6.03.1997 «Об утверждении перечня сведений конфиденциального характера».

Для того чтобы исполнить требования регуляторов и не нарушить действующее законодательство организации государственного сектора должны использовать всю доступную нормативно-правовую базу и создать условия для ее исполнения в рамках организации.

21-й приказ ФСТЭК содержит огромное количество защитных мер, при этом не все они обязательны, а их перечень открытый. Госорган - оператор персональных данных может подобрать наиболее подходящие под себя меры.

В научном сообществе выделяют, что одной из основных проблем государственных органов при обеспечении информационной безопасности является неопределенность системного нормативно- правового регулирования вопросов обеспечения достоверности в деятельности государственных органов. Такого мнения придерживается Дубень А. К. в своей работе [4].

Переходя от мер защиты к тому, от чего нужно защищаться, рассмотрим риски для привилегированной информации в судах.

Классификация рисков может быть проведена по разным параметрам, например банк данных угроз БИ ФСТЭК России использует нарушителя как критерий и определяет два вида рисков - от внешнего нарушителя и от внутреннего.

Внутренний нарушитель имеет доступ к информационной системе на момент начала атаки. К этому относятся риски похищения или изменения сведений, которые возникают из-за действий внутреннего пользователя, который получает доступ к информационным системам из-за служебного положения или из-за нахождения на территории с ограниченным доступом. В данном случае это могут как атаки с техническими средствами, так и без них. А также под эту категорию попадают судьи и работники суда, их умышленные (инсайдерские) и неумышленные действия, которые могут раскрыть привилегированную информацию.

И наоборот, внешний нарушитель атакует извне информационной системы, по сетям общего пользования. Также внешние угрозы возникают при использовании возможностей аппаратных закладок и программ, предназначенных для хищения электронных сведений. К этой группе относятся хакерские атаки, попытки внедрения стороннего ПО, попытки мошенничества или атак при помощи социальной инженерии и так далее.

Также следует рассмотреть, какие именно атаки могут быть направлены на информационную систему. Их можно также поделить на технические и социальные

К техническим рискам можно отнести: атаки с использованием вредоносного ПО, атаки типа «отказ в обслуживании» (DDoS), хакерские атаки **К социальным можно отнести:** фишинг, мошенничество, коррупционные схемы.

Фишинг – это атака с целью получить доступ к конфиденциальным данным пользователей, таким как логины, пароли, номера банковских карт. Обычно злоумышленники создают поддельные письма или сообщения, в которых маскируются под доверенные лица или организации.

Рассмотрев риски для привилегированной информации и уже имеющиеся меры защиты от них, мы можем перейти к конкретным ситуациям различным атак на суды.

Рассмотрим конкретные случаи утечек

В 2022 году была выложена в открытый доступ почтовая переписка Министерства культуры, администрации города Благовещенска и аппарата губернатора Тверской области.

Как сообщает «Коммерсант» [5], в утекших документах можно найти информация о зарплатах, увольнениях, дефектах объектов культурного наследия.

Журналисты также узнали у специалистов по инфомрационной безопасно причину данной утечки: эксплуатация уязвимости почтовых серверов. Также специалисты указывали на «пренебрежение госорганами политикой кибербезопасности».

Таким образом мы видим пример внешней, умышленной хакерской атаки.

В конце 2021 года произошла утечка исходного кода с сайта госуслуг г. Пензы. [6] В этой ситуации «Госуслуги» никто не взламывал — компания в сфере кибербезопасности «Cybersec» обнаружила хранилище данных, которое было полностью доступно из-за неверных настроек безопасности.

В данном случае можно говорить о **внутренней, неумышленной угрозе** информационной базе госоргана, которая появилась в ходе неверных действий сотрудников, настраивающих доступы.

До этого, в конце 2019 года тоже была утечка на «Госуслугах» [8].

В интернете была найдена база данных с персональной информацией о клиентах «Госуслуг», однако «Ростелеком», отрицает факт утечки, несмотря на то, что сервер находится на их площадке.

В свободном доступе в интернете оказалась информация десятков тысяч пользователей портала «Госуслуги». Персональные данные стали доступны всем желающим в результате утечки.

По информации компании DeviceLock, утечка произошла в результате ошибки в конфигурации Elasticsearch-сервера.

Как и в предыдущем случае, можно говорить о **внутренней, неумышленной угрозе** информационной базе ГИС, которая появилась в ходе неверных действий сотрудников, настраивающих систему поиска и аналитики Elasticsearch.

В июле 2017 года произошел еще один случай, Пенсионный фонд по Москве и Московской области [10], случайно отправил электронные письма с персональными данными своих работников внешним получателям. Тогда, предположительно, были раскрыты персональные данные 17 тысяч человек.

Такое письмо получил web-разработчик Сергей Дерябин, автор блога для IT-специалистов Geektimes.

Это тоже **внутренняя, неумышленная угроза** информационной базе Пенсионного фонда, которая появилась в ходе неверных действий сотрудников, отвечающих за отправку электронных писем.

Из рассмотренных случаев можно вывести общий признак для большинства утечек – они связаны с неисполнением правил информационной безопасности и защиты персональных данных.

Этот вывод подтверждается статистикой, собранной в 2019 г. экспертно-аналитическим центром группы компаний InfoWatch [11]. Согласно их отчету, «было зафиксировано 1348 утечек, случившихся по вине или по неосторожности внутренних нарушителей (далее — внутренние утечки). Отмечавшийся в 2017–2018 гг. рост числа внутренних утечек, в 2019 г. сменился небольшим снижением (на 3,3%). Однако, более показательно снижение доли внутренних утечек от общего числа утечек — если в 2018 г. этот показатель составлял 61,6%, то в 2019 г. — 53,7%. При этом уже четыре года подряд доля внутренних утечек от общего числа утечек колеблется в диапазоне 53–61%, т.е. более половины всех утечек, зафиксированных в мире ЭАЦ ГК InfoWatch, происходят из-за ошибок или умышленных действий сотрудников, включая руководство, владельцев и операторов информации.»

Попробуем рассмотреть другую сферу государственных органов и их информационных систем. В судебной системе используются автоматизиров анные информационные системы, по типу ГАС «Правосудие». Сбор и обработка информации о всех случаях утечек данных из судов поможет определить наиболее уязвимое звено в системе защиты привилегированных данных.

В 2024 году произошла крупная кибератака на ГАС «Правосудие» [12], в ее ходе могло быть безвозвратно удалено или скомпрометировано до 33% судебных актов.

Причиной угрозы стал вирус – шифровальщик, но важно понять, как он попал в систему. Согласно словам руководителя департамента расследований T.Hunter, эксперта рынка НТИ SafeNet («Сейфнет») Игоря Бедерова

«вирус-шифровальщик вряд ли попал в систему в результате взлома, т. е. это был либо инсайт, либо недогляд кого-то из сотрудников, который перешел не по той ссылке или скачал то ПО»

Таким образом это может быть примером **внутренней, умышленной угрозы**, реализованной через фишинг, если один из работников действительно по неосторожности скачал вредоносное ПО.

В 2022 году произошел случай в Новосибирском областном суде [13]. Судья Шатовкина истребовала в Советском райсуде Новосибирска копии процессуальных документов по уголовному делу и поручила своему помощнику факсом отправить их в правительство области.

Затем копии этих данных были найдены в кабинете замначальника судебного управления обладминистрации Сергея Соколова.

Пример Внутренней, умышленной угрозы, реализованной путем несанкционированного копирования защищенной информации.

В 2012 году был получен доступ к компьютеру администратора сайта суда через вирус-троян, который был выложен на стороннем сайте и скачан работником суда на игровом форме. Так, Хамовнический суд Москвы [14] отразил атаку группы Anonymous на свой сайт, но на главной странице были опубликованы антивластные лозунги и неприличные выражени и прочее.

Это пример **внутренней, неумышленной угрозы**, она была реализована из -за Невнимательности сотрудника суда при соблюдении безопасности.

20 апреля 2018 г. Московский городской суд [15] рассмотрел апелляционную жалобу и назначил очередное судебное заседание назначено на 24 апреля 2018 г. Однако после окончания судебного заседания в нескольких СМИ появились сообщения о результате рассмотрения дела в апелляционной инстанции по существу со ссылкой на пресс-службу Московского городского суда.

Причина этой утечки была в том, что сотрудник пресс-службы просто перепутал заседания и распространил информацию относительно другой жалобы.

Это пример **внутренней, неумышленной угрозы**, она была реализована из -за ошибки сотрудника пресс-службы.

Также можно привести примеры внешних, умышленных угроз, которые реализовывались через коррупцию. Например, в 2021 в Арбитражном суде города Москвы [16] судья Елена Кондрат передала своей коллеге пакет с взяткой за вынесение решения о привлечении к субсидиарной ответственности ряда лиц в рамках обособленного спора при банкротстве.

В 2019 году в Лазаревском районном суде г. Сочи [17] судья пообещал повлиять на отмену судебного акта в апелляции с принятием по делу нового решения в пользу ответчика.

В 2025 году в том же суде [18] делопроизводитель суда брала деньги за подстройку ГАС «Правосудие».

Таким образом мы рассмотрели случаи утечек и изменения данных в судебной системе, которые можно найти в открытом доступе. Исходя из данных, основной причиной нарушения тайны защищенных данных является ошибочное действие сотрудника суда.

Текущая ситуация с защитой информационных систем представляется следуюшим образом: меры по защите, установленные приказом ФСТЭК № 21 весьма разнообразные и покрывают различные уязвимости ГИС и АИС органов. Закрыты как технические, так и социальные способы атаки, также предусмотрена эшелонированная защита. Однако большинство нарушений безопасности связано с невнимательностью, либо неисполнением мер по защите информации. Это в свою очередь связано с низким уровнем компетенции в использовании цифровых технологий и отсутствии специализированных курсов обучения цифровой безопастности.

Ключевым способом распространения вредоносного программного обеспечения является рассылка писем по электронной почте с использованием почтовых доменов организаций госсектора (70 % случаев успешных кибератак в 2023 году). При использовании электронной почты в отношении объекта атаки в 93 % случаев подключаются технологии социальной инженерии, способствующие реакции получателя письма на его содержимое. Все это способствует утечке данных и неэффективности работы системы информационной безопасности [19].

В Закон РФ от 26.06.1992 N 3132-1 (ред. от 28.12.2025) "О статусе судей в Российской Федерации", в статье 20.1, части 2 установлено требование периодического повышения квалификации для судей. Предлагается ввести такое же требование для должностей помощника судьи, секретаря судебного заседания. В данном случае требуются регулярные курсы повышения квалификации в сфере цифровых технологий, на которых их могут обучить как простым и эффективным методам снижения нагрузки, по типу использования макросов программ для работы с текстом для автоматизированного заполнения данных в документов, так и использованию систем ИИ.

Соответствующие курсы могут быть реализованы через юридические ВУЗы, с привлечением экспертов в области ИТ-правоотношений, по аналогии с курсами повышения квалификации для судей.

Введение в единый акт о защите привилегированной информации правовых норм, устанавливающих периоди-

ческую оценку цифровых компетенций судей и сотрудников аппарата судов, позволит создать объективные критерии для оценки их готовности к работе в условиях цифровизации.

Особенно важно, как именно проводить повышение квалификации в области информационной безопасности. Если просто ввести множество политик и требований, то сотрудники их частично игнорировать или обходить. При этом сам процесс обучения тоже может стокнуться с такой проблемой.

Наиболее эффективные ркезультаты покажет обучение, которое четко обяснит сотрудникам госорганов зачем им защищать персональные и другие ограниченные к распространению данные; как это отражается на них самих, когда их персональные данные попадают на продажу в сеть Интернет.

Также, при разработке курса обучения, необходимо сосредоточится на предложении безопасных альтернатив рабочих инструментов. Например, вместо облачного хранилища одного из частных сервисов, создать собственное в рамках локальной сети.

Само обучение должно быть представлено в разных формат, с возможностью выбора одного из нескольких, так как даже такой небольшой выбор уменьшает давление на сотрудников и повышает эффективность обучения.

Также необходимо пересмотреть модуль обучения, имеющийся в ГАС Правосудие. Так как платформа идеально подходит для проведения онлайн-курсов прямо на месте работы, она должна обладать самой актуальной информацией и именно на нее должны быть подвязаны программы обучения и оценки компетенций. Подобные способы обучения часто используются в коммерческих организациях, разрабатывающих свои программные системы.

17 сентября 2024 г Министерство цифрового развития подготовило рекомендации по информационной безопасности для госслужащих в письме № П25-30502 [20].

Письмо разделено на три части: защита от мошенников, рекомендации по защите учётных записей, Меры по обеспечению безопасности информации

Рекомендации как раз направлены на предотвращение атак с использованием социальной инженерии и применяются программах по повышению цифровой грамотности.

Как отмечают Скалкина, И. Э. и П. В. Попова в своей работе еще одним важным аспектом является ожидаемая выгода, которую могут принести цифровые системы. Скалкина, И. Э. и П. В. Попова, указывают, что «в классических моделях принятия технологий, если цифровая система обеспечивает сотруднику преимущества в его рабочих процессах (например, экономию времени), это приводит к положительным результатам. оценка цифровой системы» [21].

Заключение

В заключение хочется отметить, что для развития сферы защиты информации необходим комплексный подход, включающий несколько основных направлений. Во-первых, требуется не сбавлять темпы в модернизацию технической инфраструктуры государственных органов. Во-вторых, требуется активно работать над повышением цифровой грамотности среди работников данных органов, так как пока что это самое незащищенное звено в системе безопасности.

Литература

1. Сосипатров Р. А., Бабаев Д. Б. «Обеспечение информационной безопасности в государственном и муниципальном управлении: общая оценка законодательства» // Экономика и социум. 2021. №3-2 (82). URL: https://cyberleninka.ru/article/n/obespechenie-informatsionnoy-bezopasnosti-v-gosudarstvennom-i-munitsipalnom-upravlenii-obschaya-otsenka-zakonodatelstva (дата обращения: 24.01.2026).
2. «Россия: утечки информации ограниченного доступа 2023-2024» // АО «Инфовотч» URL: https://www.infowatch.ru/sites/default/files/analytics/files/rossiya-utechki-informatsii-ogranichennogo-dostupa-2023-2024.pdf?ysclid=mkmuz4zr6r327787693
3. «Хакеры власть не признают» // Издание «Коммерсантъ» URL: https://www.kommersant.ru/doc/8313330
4. Дубень Андрей Кириллович «Административно-правовые основы деятельности государственных органов при обеспечении информационной безопасности» // Образование и право. 2024. №8. URL: https://cyberleninka.ru/article/n/administrativno-pravovye-osnovy-deyatelnosti-gosudarstvennyh-organov-pri-obespechenii-informatsionnoy-bezopasnosti
5. «Культурная переписка» // URL: https://www.kommersant.ru/doc/5306329?ysclid=mknqjz9cip19167699
6. «Привлечь внимание к проблеме»: кто слил исходный код «Госуслуг» и чем это грозит
7. // Сетевое издание «forbes.ru» URL: https://www.forbes.ru/tekhnologii/451375-privlec-vnimanie-k-probleme-kto-slil-ishodnyj-kod-gosuslug-i-cem-eto-grozit?ysclid=mknqkbzern484710087
8. На «Госуслугах» масштабная утечка. Скомпрометированы данные десятков тысяч россиян
9. // Сетевое издание «CNews» («СиНьюс») URL: https://www.cnews.ru/news/top/2019-12-30_v_gosuslugah_masshtabnaya?ysclid=mknql5aac511000546
10. Пенсионный фонд ответил на сообщения об утечке данных 17 тыс. человек // Сетевое издание rbc.ru URL: https://www.rbc.ru/rbcfreenews/5964e1059a7947032b1e6d7a?ysclid=mknqlf08my929347988
11. Исследование утечек информации ограниченного доступа в 2019 году // Экспертно-аналитический центр InfoWatch. 2020 г URL: https://www.infowatch.ru/sites/default/files/analytics/files/InfoWatch_МирУтечки_за2019.pdf
12. «Эксперт сообщил о возможной атаке вируса-шифровальщика на ГАС «Правосудие» // Сетевое издание «ВЗГЛЯД.РУ» URL: https://vz.ru/news/2024/10/8/1291381.html
13. «Судье не дали выбрать из двух зол меньшее» // Издание «Коммерсантъ» URL: https://www.kommersant.ru/doc/7364124
14. «Хакеры слили в сеть информацию из Хамовнического суда» // Сетевое издание «NTV.RU» URL: https://www.ntv.ru/novosti/323562/
15. «Защита просит Мосгорсуд объяснить появление информации о решении по делу до его вынесения» // Сетевое издание «Адвокатская газета» URL: https://www.advgazeta.ru/novosti/zashchita-prosit-mosgorsud-obyasnit-poyavlenie-informatsii-o-reshenii-po-delu-do-ego-vyneseniya/
16. «Взятка в $50 000 или «грязная провокация»: ВС подтвердил «уголовку» для судьи АСГМ» // сетевое издание «Право.ru» URL: https://pravo.ru/story/237858/
17. «Начинается процесс над судьей и адвокатом, которые не донесли взятку до апелляции» // Сетевое издание LEGAL.REPORT URL: https://legal.report/nachinaetsja-process-nad-sudej-i-advokatom-kotorye-ne-donesli-vzjatku-do-apelljacii
18. «Нужного судью не дождались» // Издание «Коммерсантъ» URL: https://www.kommersant.ru/doc/7971762
19. Попкова Алена Анатольевна, Парфенов Константин Владимирович, Алборов Арсен Робинзонович Угрозы

информационной безопасности в государственном секторе России // Известия вузов. Социология. Экономика. Политика. 2024. №4. URL: https://cyberleninka.ru/article/n/ugrozy-informatsionnoy-bezopasnosti-v-gosudarstvennom-sektore-rossii (дата обращения: 24.01.2026).

20. Письмо Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 17 сентября 2024 г. № П25-305029 О рекомендациях для государственных служащих, направленных на обеспечение информационной безопасности сотрудников на рабочих местах // СПС «Гарант» URL: https://www.garant.ru/products/ipo/prime/doc/410917788/

21. Скалкина, И. Э. П. В. Попова Обучение персонала цифровым компетенциям как инструмент развития организации // Молодой ученый. — 2023. — № 2 (449). — С. 167-170. — URL: https://moluch.ru/archive/449/98686.

Analysis of information security incidents in government agencies of the Russian Federation: possible ways to improve the level of protection of confidential information.

Romanychev N.O.
Lebedev Russian State University of Justice

The article discusses the main problems of protecting information systems of government agencies using the analysis of specific cases of information leaks, including cases of leaks from the judicial system. The main regulatory legal acts regulating the protection of confidential information, the main vulnerabilities of government agencies are considered.

Keywords**:** Information security, government agencies, personal data, confidential information, state information system, FSTEC, judicial system.

References

1. Sosipatrov R. A., Babaev D. B. "Ensuring information security in state and municipal management: a general assessment of legislation" // Economics and Society. 2021. №3-2 (82). URL: https://cyberleninka.ru/article/n/obespechenie-informatsionnoy-bezopasnosti-v-gosudarstvennom-i-munitsipalnom-upravlenii-obschaya-otsenka-zakonodatelstva (date of request: 24.01.2026).
2. "Russia: leaks of restricted access information 2023-2024" // JSC "Infowatch" URL: https://www.infowatch.ru/sites/default/files/analytics/files/rossiya-utechki-informatsii-ogranichennogo-dostupa-2023-2024.pdf?ysclid=mkmuz4zr6r327787693
3. "Hackers do not recognize the government" // Kommersant edition URL: https://www.kommersant.ru/doc/8313330
4. Duben Andrey Kirillovich "Administrative and legal bases of the activity of state bodies in ensuring information security" // Education and law. 2024. №8. URL: https://cyberleninka.ru/article/n/administrativno-pravovye-osnovy-deyatelnosti-gosudarstvennyh-organov-pri-obespechenii-informatsionnoy-bezopasnosti
5. "Cultural correspondence" // URL: https://www.kommersant.ru/doc/5306329 ?ysclid=mknqjz9cip19167699
6. "Draw attention to the problem": who leaked the source code of Gosuslug and what is the threat
7. // Online edition "forbes.ru " URL: https://www.forbes.ru/tekhnologii/451375-privlec-vnimanie-k-probleme-kto-slil-ishodnyj-kod-gosuslug-i-cem-eto-grozit?ysclid=mknqkbzern484710087
8. There is a large-scale leak at Gosuslugi. The data of tens of thousands of Russians has been compromised
. 9 // Online publication CNews URL: https://www.cnews.ru/news/top/2019-12-30_v_gosuslugah_masshtabnaya ?ysclid=mknql5aac511000546
10. The pension fund responded to reports about the data leak of 17 thousand people // Online publication rbc.ru URL: https://www.rbc.ru/rbcfreenews/5964e1059a7947032b1e6d7a ?ysclid=mknqlf08my929347988
11. Investigation of information leaks with limited access in 2019 // Expert and analytical center InfoWatch. 2020 URL: https://www.infowatch.ru/sites/default/files/analytics/files/InfoWatch_МирУтечки_за2019.pdf
12. "The expert reported on a possible attack of a cryptographic virus on GAS "Justice" // Online publication "VZGLYAD.<url>" URL: https://vz.ru/news/2024/10/8/1291381.html
13. "The judge was not allowed to choose the lesser of two evils" // Kommersant edition URL: https://www.kommersant.ru/doc/7364124
14. "Hackers leaked information from the Khamovnichesky court to the network" // Online edition "NTV.RU " URL: https://www.ntv.ru/novosti/323562 /
15. "The defense asks the Moscow City Court to explain the appearance of information about the decision on the case before it is made." // Online edition "Advocate Newspaper" URL: https://www.advgazeta.ru/novosti/zashchita-prosit-mosgorsud-obyasnit-poyavlenie-informatsii-o-reshenii-po-delu-do-ego-vyneseniya /
16. "A $50,000 bribe or a "dirty provocation": the Supreme Court confirmed the "criminal record" for the ASGM judge" // online edition "Право.ги " URL: https://pravo.ru/story/237858/
17. "The trial of the judge and lawyer who did not deliver the bribe before the appeal begins" // LEGAL.REPORT online publication URL: https://legal.report/nachinaetsja-process-nad-sudej-i-advokatom-kotorye-ne-donesli-vzjatku-do-apelljacii
18. "They didn't wait for the right judge" // Kommersant edition URL: https://www.kommersant.ru/doc/7971762
19. Popkova Alyona Anatolyevna, Parfenov Konstantin Vladimirovich, Alborov Arsen Robinsonovich Threats to information security in the public sector of Russia // Izvestiya vuzov. Sociology. Economy. Politics. 2024. No. 4. URL: https://cyberleninka.ru/article/n/ugrozy-informatsionnoy-bezopasnosti-v-gosudarstvennom-sektore-rossii (date of request: 24.01.2026).
20. Letter of the Ministry of Digital Development, Communications and Mass Media of the Russian Federation dated September 17, 2024 No. P25-305029 On Recommendations for Civil Servants Aimed at Ensuring Information Security of Employees in the Workplace // SPS "Garant" URL: https://www.garant.ru/products/ipo/prime/doc/410917788 /
21. Skalkina, I. E. P. V. Popova Training of personnel in digital competencies as a tool for the development of an organization // Young scientist. — 2023. — № 2 (449). — Pp. 167-170. — URL: https://moluch.ru/archive/449/98686.