



ГЕНЕРАЛЬНАЯ
ПРОКУРАТУРА РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ

Н.О. 2025

№ 621

Москва

**Об утверждении Концепции цифровой трансформации органов
и организаций прокуратуры Российской Федерации до 2030 года,
а также о внесении изменений в отдельные организационно-
распорядительные документы Генерального прокурора
Российской Федерации**

В целях совершенствования информационного обеспечения органов и организаций прокуратуры Российской Федерации, определения основных приоритетов и принципов цифрового развития, руководствуясь статьей 17 Федерального закона «О прокуратуре Российской Федерации»,

П Р И К А З Ы В А Ю:

1. Утвердить прилагаемую Концепцию цифровой трансформации органов и организаций прокуратуры Российской Федерации до 2030 года (далее – Концепция).

2. Назначить ответственным руководителем за планирование и реализацию мероприятий в сфере цифровой трансформации заместителя Генерального прокурора Российской Федерации, курирующего вопросы деятельности Главного управления правовой статистики и информационных технологий Генеральной прокуратуры Российской Федерации, ответственным подразделением – Главное управление правовой статистики и информационных технологий Генеральной прокуратуры Российской Федерации.

3. Главному управлению правовой статистики и информационных технологий Генеральной прокуратуры Российской Федерации обеспечить координацию работ в сфере цифровой трансформации и внедрения информационных технологий, а также интеграцию их в единое информационное пространство системы Генеральной прокуратуры Российской Федерации.

4. Главному управлению обеспечения деятельности органов и организаций прокуратуры Генеральной прокуратуры Российской Федерации в установленном порядке организовать формирование, утверждение и размещение плана-графика закупок товаров, работ, услуг на очередной финансовый год и плановый период с учетом реализации мероприятий

Концепции в пределах лимитов бюджетных обязательств, доведенных до Генеральной прокуратуры Российской Федерации.

5. Начальникам главных управлений, управлений и отделов Генеральной прокуратуры Российской Федерации, прокурорам субъектов Российской Федерации, военным и иным приравненным к ним специализированным прокурорам, ректору Университета прокуратуры Российской Федерации обеспечить реализацию Концепции, взять под личный контроль вопросы эффективного использования информационных систем и комплексов в деятельности подчиненных подразделений, органов и организаций прокуратуры.

6. Прокурорам субъектов Российской Федерации и приравненным к ним специализированным прокурорам, прокурору комплекса «Байконур»:

6.1. Определить из числа своих заместителей ответственного за реализацию мероприятий по цифровой трансформации, обеспечить реализацию мероприятий в соответствии с Концепцией.

6.2. Ежегодно, до 25 января представлять в Главное управление правовой статистики и информационных технологий Генеральной прокуратуры Российской Федерации докладные записки об итогах работы за год в сфере цифровой трансформации и внедрения информационных технологий, содержащие информацию:

1) о деятельности ответственных за реализацию мероприятий по цифровой трансформации органов прокуратуры Российской Федерации, рабочих групп по распространению цифровых компетенций;

2) о внедрении и использовании цифровых технологий, в том числе в рамках межведомственного взаимодействия;

3) о проведении мероприятий по контролю за качеством и своевременностью исполнения поручений в информационно-коммуникационной сфере;

4) об организации консультативной и методической поддержки работников по вопросам внедрения цифровых решений и сопровождения процессов цифровой трансформации;

5) об используемых информационных системах (включая эксплуатируемые локально), о практике их применения, положительном опыте и выявленных недостатках, об оснащенности программно-техническими средствами;

6) о предложениях по совершенствованию надзорной деятельности на основе применения цифровых технологий, функционала информационных систем, актуализации организационно-распорядительных документов, регламентирующих обозначенную сферу;

7) о реализации исполнителями обязательств по централизованным государственным контрактам, о состоянии исполнения иных государственных контрактов, заключенных в пределах доведенных лимитов бюджетных обязательств по соответствующему виду расходов бюджетных средств в сфере информационно-телекоммуникационных технологий, с разбивкой по кодам

классификации операций сектора государственного управления;

8) о потребностях в сфере информационно-коммуникационных технологий;

9) об организации защиты информации;

10) о соблюдении требований приказа Генерального прокурора Российской Федерации от 24.11.2021 № 701 «Об утверждении Инструкции по эксплуатации средств вычислительной техники, информационных систем и информационных ресурсов органов прокуратуры Российской Федерации», о выявленных нарушениях, принятых мерах и проблемных вопросах;

11) о ходе опытной эксплуатации АИК «Надзор-WEB», о проблемах, возникающих при его использовании, возможных предложениях по совершенствованию функционала в соответствии с приказом Генерального прокурора Российской Федерации от 30.09.2024 № 712 «Об использовании автоматизированного информационного комплекса «Надзор-WEB» в органах и организациях прокуратуры Российской Федерации»;

12) о результатах организации работы по осуществлению информационного взаимодействия в электронном виде с Федеральной службой судебных приставов для администрирования доходов федерального бюджета в соответствии с указанием Генерального прокурора Российской Федерации от 07.11.2022 № 658/11 «Об организации работы по направлению в федеральную службу судебных приставов сведений для администрирования доходов федерального бюджета».

7. Военным прокурорам сведения, указанные в пункте 6.2 настоящего приказа, представлять в Главную военную прокуратуру.

Главной военной прокуратуре обобщенные сведения направлять в Главное управление правовой статистики и информационных технологий Генеральной прокуратуры Российской Федерации в сроки, указанные в пункте 6.2 настоящего приказа.

8. Ректору Университета прокуратуры Российской Федерации сведения, указанные в пункте 6.2 настоящего приказа, направлять в установленные сроки в Главное управление правовой статистики и информационных технологий Генеральной прокуратуры Российской Федерации.

9. Внести изменения в следующие организационно-распорядительные документы Генерального прокурора Российской Федерации:

9.1. В приказе Генерального прокурора Российской Федерации от 24.11.2021 № 701 «Об утверждении Инструкции по эксплуатации средств вычислительной техники, информационных систем и информационных ресурсов органов прокуратуры Российской Федерации»:

1) абзац четвертый пункта 8 изложить в следующей редакции:

«ежегодно анализировать состояние работы по соблюдению требований приказа;»;

2) дополнить пунктами 8.1 и 8.2 следующего содержания:

«8.1. Заместителю Генерального прокурора Российской Федерации – Главному военному прокурору, начальникам структурных подразделений

Генеральной прокуратуры Российской Федерации, ректору Университета прокуратуры Российской Федерации результаты анализа состояния работы по соблюдению требований настоящего приказа с информацией о выявленных нарушениях, принятых мерах и проблемных вопросах направлять в Главное управление правовой статистики и информационных технологий Генеральной прокуратуры Российской Федерации в срок до 25 января.

8.2. Прокурорам субъектов Российской Федерации, приравненным к ним специализированным прокурорам, прокурору комплекса «Байконур» отражать состояние работы по соблюдению требований настоящего приказа с информацией о выявленных нарушениях, принятых мерах и проблемных вопросах в докладных записках об итогах работы за год в сфере цифровой трансформации и внедрения информационных технологий, представляемых в соответствии с приказом Генерального прокурора Российской Федерации «Об утверждении Концепции цифровой трансформации органов и организаций прокуратуры Российской Федерации до 2030 года, а также о внесении изменений в отдельные организационно-распорядительные документы Генерального прокурора Российской Федерации».

9.2. В приказе Генерального прокурора Российской Федерации от 30.09.2024 № 712 «Об использовании автоматизированного информационного комплекса «Надзор-WEB» в органах и организациях прокуратуры Российской Федерации» изложить пункт 4 в следующей редакции:

«4. Начальникам главных управлений, управлений и отделов Генеральной прокуратуры Российской Федерации, ректору Университета прокуратуры Российской Федерации направлять в Главное управление правовой статистики и информационных технологий Генеральной прокуратуры Российской Федерации ежегодно, к 25 января сведения о ходе опытной эксплуатации АИК «Надзор-WEB», о проблемах, возникающих при его использовании, возможные предложения по совершенствованию функционала.

Прокурорам субъектов Российской Федерации, приравненным к ним специализированным прокурорам, прокурору комплекса «Байконур» информацию о ходе опытной эксплуатации АИК «Надзор-WEB», о проблемах, возникающих при его использовании, возможные предложения по совершенствованию функционала отражать в докладных записках об итогах работы за год в сфере цифровой трансформации и внедрения информационных технологий, представляемых в соответствии с приказом Генерального прокурора Российской Федерации «Об утверждении Концепции цифровой трансформации органов и организаций прокуратуры Российской Федерации до 2030 года, а также о внесении изменений в отдельные организационно-распорядительные документы Генерального прокурора Российской Федерации».

Военным прокурорам окружного звена сведения о ходе опытной эксплуатации АИК «Надзор-WEB» представлять в Главную военную прокуратуру.

Главной военной прокуратуре обобщенные сведения о ходе опытной эксплуатации АИК «Надзор-WEB» в органах военной прокуратуры представлять в Главное управление правовой статистики и информационных технологий Генеральной прокуратуры Российской Федерации в сроки, указанные в абзаце первом настоящего пункта.».

9.3. В указании Генерального прокурора Российской Федерации от 07.11.2022 № 658/11 «Об организации работы по направлению в Федеральную службу судебных приставов сведений об администрировании доходов федерального бюджета»:

- 1) абзац восьмой пункта 1 признать утратившим силу;
- 2) дополнить пунктами 1.1 и 1.2 следующего содержания:

«1.1. Начальников главных управлений и управлений Генеральной прокуратуры Российской Федерации ежегодно, до 25 января информировать Главное управление правовой статистики и информационных технологий Генеральной прокуратуры Российской Федерации о результатах организации работы по осуществлению информационного взаимодействия в электронном виде с Федеральной службой судебных приставов для администрирования доходов федерального бюджета.

1.2. Прокуроров субъектов Российской Федерации, приравненных к ним специализированных прокуроров, прокурора комплекса «Байконур» информацию по пункту 1.1 настоящего указания отражать в докладных записках об итогах работы за год в сфере цифровой трансформации и внедрения информационных технологий, представляемых в соответствии с приказом Генерального прокурора Российской Федерации «Об утверждении Концепции цифровой трансформации органов и организаций прокуратуры Российской Федерации до 2030 года, а также о внесении изменений в отдельные организационно-распорядительные документы Генерального прокурора Российской Федерации».»;

3) в пункте 2 слова «абзаце восьмом пункта 1» заменить словами «пункте 1.1»;

4) в абзаце третьем пункта 3 слова «абзацем восьмым пункта 1» заменить словами «пунктами 1.1 и 1.2».

10. Признать утратившим силу с 01.01.2026 приказ Генерального прокурора Российской Федерации от 14.09.2017 № 627 «Об утверждении Концепции цифровой трансформации органов и организаций прокуратуры до 2025 года».

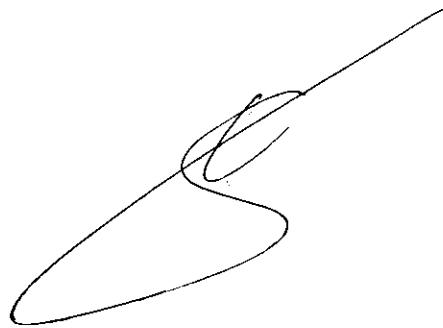
11. Настоящий приказ опубликовать в журнале «Законность» и разместить на официальном сайте Генеральной прокуратуры Российской Федерации в информационно-телекоммуникационной сети «Интернет».

12. Контроль за исполнением настоящего приказа оставляю за собой.

Приказ направить заместителям Генерального прокурора Российской Федерации, советникам Генерального прокурора Российской Федерации, старшим помощникам Генерального прокурора Российской Федерации по особым поручениям, помощникам заместителей Генерального прокурора Российской Федерации по особым поручениям, начальникам главных управлений, управлений и отделов Генеральной прокуратуры Российской Федерации, ректору Университета прокуратуры Российской Федерации, прокурорам субъектов Российской Федерации, приравненным к ним военным и иным специализированным прокурорам, прокурору комплекса «Байконур», которым довести его содержание до сведения подчиненных работников.

Генеральный прокурор
Российской Федерации

действительный государственный
советник юстиции

A large, stylized handwritten signature in black ink, consisting of several loops and a long horizontal stroke extending to the right.

И.В. Краснов

УТВЕРЖДЕНА

приказом
Генерального прокурора
Российской Федерации

от 11.09.2025 № 621

КОНЦЕПЦИЯ
цифровой трансформации органов и организаций
прокуратуры Российской Федерации до 2030 года

1. Введение

Цифровая трансформация органов и организаций прокуратуры Российской Федерации (далее – органы прокуратуры) осуществляется в рамках государственной политики по созданию необходимых условий для развития экономики данных и цифровой трансформации государства.

Реализация Концепции цифровой трансформации органов и организаций прокуратуры Российской Федерации до 2030 года (далее – Концепция) направлена на комплексную оптимизацию и совершенствование деятельности органов прокуратуры на основе современных цифровых решений в целях:

преимущественного использования данных в цифровой форме, формирования баз данных для внедрения в деятельность органов прокуратуры технологий искусственного интеллекта;

расширения среды электронного взаимодействия с учетом потребностей граждан, общества и государственных органов в получении качественных и достоверных сведений;

развития цифровой инфраструктуры на основе применения российских информационно-телекоммуникационных технологий, обеспечения стабильного функционирования технологической основы для реализации полномочий органами прокуратуры в условиях достижения технологической независимости (суверенитета);

автоматизации процессов деятельности органов прокуратуры с использованием компонентов единых отраслевых цифровых платформ и модели управления на основе данных с учетом внедрения технологий обработки больших объемов данных, машинного обучения и искусственного интеллекта;

повышения уровня информационной безопасности органов прокуратуры;

развития цифровых компетенций работников органов прокуратуры путем совершенствования системы подготовки для реализации полномочий в условиях цифровой экономики, формирования компетенций управления

данными для искусственного интеллекта, применения больших фундаментальных моделей, внедрения и применения инструментов искусственного интеллекта для решения рабочих задач.

Концепция определяет цели, задачи, принципы и основные направления в области цифровой трансформации органов прокуратуры, механизм ее реализации, учитывает тенденции и перспективы развития экономики данных и цифровой трансформации государства.

Концепция разработана в соответствии с положениями следующих документов:

Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы, утвержденная Указом Президента Российской Федерации от 09.05.2017 № 203;

Стратегия научно-технологического развития Российской Федерации, утвержденная Указом Президента Российской Федерации от 28.02.2024 № 145;

Стратегия национальной безопасности Российской Федерации, утвержденная Указом Президента Российской Федерации от 02.07.2021 № 400;

Национальная стратегия развития искусственного интеллекта на период до 2030 года, утвержденная Указом Президента Российской Федерации от 10.10.2019 № 490;

Доктрина информационной безопасности Российской Федерации, утвержденная Указом Президента Российской Федерации от 05.12.2016 № 646;

Указ Президента Российской Федерации от 07.05.2024 № 309 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года»;

Указ Президента Российской Федерации от 31.03.2023 № 231 «О создании, развитии и эксплуатации государственных информационных систем с использованием единой цифровой платформы Российской Федерации «ГосТех»;

Стратегическое направление в области цифровой трансформации государственного управления, утвержденное распоряжением Правительства Российской Федерации от 16.03.2024 № 637-р.

Указанные документы определяют актуальные задачи, связанные с устойчивым развитием российской экономики на новой технологической основе и форсированной цифровизацией государственного управления, социальной сферы. Решение этих задач органами прокуратуры в современных условиях возможно на основе поступательного и взаимосвязанного развития, гармонизации нормативной правовой базы, комплексной автоматизации процессов внутренней деятельности, модернизации информационно-технологической платформы, совершенствования системы кадрового обеспечения.

Кроме перечисленных документов, приняты во внимание нормативные акты, определяющие задачи цифровой трансформации органов публичной власти, государственных корпораций, а также акты, устанавливающие условия использования информационных технологий для целей цифровой трансформации государственного управления, экономики и социальной сферы.

Реализация мероприятий Концепции в части обеспечения информационной безопасности осуществляется с учетом положений Концепции обеспечения информационной безопасности в органах и организациях прокуратуры Российской Федерации, утвержденной приказом Генерального прокурора Российской Федерации от 30.06.2023 № 425.

В соответствии с указанными документами реализация Концепции направлена на формирование устойчивых тенденций цифровой трансформации органов прокуратуры, включая:

комплексную оптимизацию процессов деятельности, формирование обновленной регуляторной базы, обеспечивающей благоприятный правовой режим для осуществления цифровой трансформации органов прокуратуры;

формирование и развитие цифровой среды органов прокуратуры с учетом потребностей граждан, общества и государства в своевременном получении качественных и достоверных сведений на основе применения российских информационно-телекоммуникационных технологий и средств защиты информации;

обеспечение согласованного развития цифровой экосистемы органов прокуратуры (включающей цифровую среду, а также правила и механизмы взаимодействия между собой органов прокуратуры, граждан, общества, органов власти, международного сообщества) и других субъектов контрольно-надзорной деятельности системы государственного управления.

Положения Концепции являются обязательными при разработке программ, реализации мероприятий и инициатив, связанных с деятельностью органов прокуратуры, до 2030 года включительно.

2. Цели и задачи цифровой трансформации органов и организаций прокуратуры Российской Федерации

Целями цифровой трансформации являются:

совершенствование деятельности органов прокуратуры по обеспечению верховенства закона, единства и укрепления законности, защиты прав и свобод человека и гражданина, а также охраняемых законом интересов общества и государства;

обеспечение возможности использования цифровых инструментов для оперативной реализации надзорных функций, в том числе с применением технологий искусственного интеллекта для выявления признаков нарушений на основе анализа оцифрованных данных объектов надзора;

обеспечение устойчивого и бесперебойного функционирования собственной цифровой инфраструктуры, повышение ее информационной безопасности;

создание условий готовности к изменениям в общественно-политической и экономической ситуации, связанным с переходом к экономике данных;

обеспечение возможности гибкой и точной фокусировки органов прокуратуры на социально актуальных сферах правоотношений, в том числе профилактике правонарушений, возмещении ущерба, реализации технологий искусственного интеллекта для работы с обращениями граждан, прогнозировании перспективных направлений прокурорской деятельности;

развитие свободного, устойчивого и безопасного взаимодействия органов прокуратуры с гражданами, организациями, институтами гражданского общества, органами государственной власти и местного самоуправления;

обеспечение функционирования и развития системы информационной безопасности на основе комплекса организационных и технических мер защиты с применением современных методов прогнозирования, анализа и моделирования возможных угроз безопасности информации и снижения (ликвидации) ущерба от их воздействия.

Для достижения указанных целей необходимо обеспечить решение задач по следующим приоритетным направлениям.

Направление 1. Высокотехнологичный надзор – формирование на основе комплексной оптимизации выполнения надзорных функций единой безопасной цифровой платформы для обеспечения электронного взаимодействия органов прокуратуры всех уровней между собой и с другими государственными органами, внедрение современных механизмов и технологий противодействия киберпреступности и правонарушениям в цифровой среде.

Основные задачи:

участие в совершенствовании правового, научно-методического и организационно-технологического обеспечения автоматизированной оценки качества деятельности правоохранительных органов;

повышение эффективности надзора путем внедрения современных и перспективных информационных технологий обработки информации во всех сферах надзорной деятельности;

повышение оперативности прокурорского реагирования на нарушения закона, устранение причин и условий, им способствующих;

сокращение времени рассмотрения обращений граждан, государственных органов и организаций;

обеспечение своевременного, в том числе дистанционного, получения объективной, полной и достоверной информации о состоянии законности и работы по профилактике правонарушений и преступлений;

повышение обоснованности принимаемых решений в рамках исполнения надзорных функций на основе автоматизированного выявления и учета характерных закономерностей, соответствующих нарушениям в установленной сфере надзора, подготовки рекомендаций по выполнению проверки с учетом выявленных закономерностей.

Направление 2. Цифровая инфраструктура – обеспечение реализации нового качества электронного взаимодействия органов прокуратуры всех уровней с гражданами, организациями, государственными органами на основе создания безопасной высокотехнологичной универсальной цифровой среды.

Основные задачи:

комплексная оптимизация и взаимосвязанная цифровизация процессов внутренней и межведомственной деятельности органов прокуратуры;

совершенствование правовых, нормативно-технических, организационно-методических и иных основ разработки, внедрения, эксплуатации и развития существующих и вновь создаваемых компонентов цифровой среды органов прокуратуры, включая государственные и информационные системы;

создание и развитие устойчивой, надежной и безопасной информационно-телекоммуникационной инфраструктуры, реализующей в том числе «сквозные» технологии экономики данных и использующей существующие и вновь создаваемые российские центры обработки данных, защищенные сети связи и передачи данных, отечественные цифровые платформы работы с данными, в том числе единую цифровую платформу Российской Федерации «ГосТех»;

разработка и внедрение в деятельность органов прокуратуры всех уровней эффективных механизмов обеспечения дистанционного взаимодействия между собой, с гражданами, организациями и учреждениями, государственными органами, в том числе с использованием информационной системы межведомственного электронного взаимодействия системы Генеральной прокуратуры Российской Федерации, системы межведомственного электронного документооборота (МЭДО);

разработка системы управления нормативно-справочной информацией (далее – НСИ) и мастер-данными (единые справочники, содержащие информацию о структуре органа, перечни, рубрикаторы и классификаторы, позволяющие упорядочить и систематизировать информацию и документы, минимизировать сроки ввода данных в систему, снизить риски ошибок, связанных с человеческим фактором) органов прокуратуры на всем их жизненном цикле с учетом обеспечения возможности их содержательной обработки в других отраслях экономики данных Российской Федерации, включая интеграцию с федеральными государственными информационными системами «Единая система нормативной справочной информации» (ФГИС ЕСНСИ), «Единая информационная платформа Национальной системы управления данными» (ФГИС ЕИП НСУД) и другими федеральными государственными информационными системами, предназначенными

для обмена данными;

формирование требований и модели непрерывного повышения квалификации работников органов прокуратуры, в том числе с использованием дистанционных образовательных технологий, по вопросам реализации своих полномочий, оптимизации процессов подготовки и принятия управленческих решений в условиях формирования экономики данных и цифровой трансформации государства.

Направление 3. Среда доверия – обеспечение технической, организационной и правовой защиты интересов граждан, общества и государственных интересов при осуществлении взаимодействия в обновленной цифровой экосистеме органов прокуратуры.

Основные задачи:

совершенствование правового регулирования с целью формирования единой цифровой среды (электронный обмен информацией) доверия экосистемы органов прокуратуры;

создание системы взаимодействия с гражданами, обществом, организациями и учреждениями, которая позволяет использовать современные и перспективные каналы коммуникаций;

разработка и внедрение механизмов мониторинга и повышения удовлетворенности граждан, организаций и учреждений степенью защищенности своих конституционных прав и свобод, личных и имущественных интересов, в том числе от преступных посягательств;

обеспечение открытости, доступности и достоверности статистических данных для граждан и юридических лиц на основе внедрения органами прокуратуры и предоставления пользователям современных цифровых сервисов;

обеспечение участников взаимодействия средствами доверенных цифровых дистанционных коммуникаций;

повышение прозрачности информационного сопровождения процессов надзорной деятельности с соблюдением принципа обеспечения законности и разумной достаточности при сборе, накоплении и распространении информации;

обеспечение доступа граждан и организаций к открытой информации о деятельности органов прокуратуры, а также к информации, непосредственно затрагивающей их права и свободы;

повышение уровня общего доверия граждан к деятельности органов прокуратуры.

Направление 4. Обеспечение информационной безопасности – осуществление комплекса взаимосвязанных правовых, организационных, технических и иных мер по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления.

Основные задачи:

совершенствование форм и методов организации информационной

безопасности при создании, модернизации и внедрении информационных систем;

автоматизация процессов выявления, анализа и оценки актуальных угроз информационной безопасности и их источников;

совершенствование мониторинга и аудита защищенности информационной инфраструктуры и информационных ресурсов органов прокуратуры;

совершенствование контроля за действиями пользователей и предоставлением им прав доступа в целях предотвращения несанкционированного доступа к информационным ресурсам, техническим и программным средствам, средствам защиты информации и деструктивных воздействий на информационные ресурсы;

совершенствование системы обнаружения вторжений (компьютерных атак), форм и методов предотвращения и нейтрализации угроз информационной безопасности, ликвидации последствий их воздействия;

мониторинг и регистрация событий, влияющих на безопасность информации, оперативный анализ информации о таких событиях, своевременное выявление инцидентов информационной безопасности в информационных системах органов прокуратуры и реагирование на них;

контроль целостности и достоверности информации, обрабатываемой в информационных системах органов прокуратуры, а также целостности программно-аппаратных компонентов информационных систем;

координация деятельности органов прокуратуры по защите информации.

Ключевым результатом цифровой трансформации деятельности органов прокуратуры станет реализация «сквозного» служебного процесса обеспечения законности с использованием технологий искусственного интеллекта, интегрированных в существующие и вновь создаваемые информационные системы органов прокуратуры, реализованные на отечественных программных продуктах и функционирующие на оборудовании российского производства.

3. Текущее состояние информационных систем и комплексов, инфраструктуры органов и организаций прокуратуры Российской Федерации

3.1. Ведомственные информационные системы

В состав ведомственных информационных систем органов прокуратуры входят следующие автоматизированные информационные комплексы (далее – АИК) и автоматизированные информационные системы (далее – АИС):

АИК «Надзор-WEB», предназначенный для ведения ведомственного делопроизводства и документооборота в электронном виде;

АИС «Архивное дело ОП», предназначенная для автоматизации процессов делопроизводства по ведению номенклатуры дел, формированию,

оформлению дел, систематизации и приему дел на архивное хранение;

АИК «Кадры-ОП», предназначенный для автоматизированного управления кадрами органов и организаций прокуратуры и обеспечения кадрового учета;

АИС «Пенсия», предназначенная для учета и сопровождения пенсионного обеспечения бывших работников органов и организаций прокуратуры и членов их семей, в том числе постоянно проживающих за пределами Российской Федерации;

ведомственный программно-технический комплекс автоматизации финансово-хозяйственной деятельности органов и организаций прокуратуры Российской Федерации (ВПТК), предназначенный для автоматизации задач в области бухгалтерского учета и обеспечения финансово-хозяйственной деятельности органов прокуратуры;

специальное программное обеспечение – Единый портал прокуратуры Российской Федерации (СПО ЕПП, открытый и закрытый сегменты), предназначенное для доступа граждан, юридических лиц, индивидуальных предпринимателей и органов государственной власти к информации о деятельности прокуратуры Российской Федерации;

специальное программное обеспечение «Автоматизированное рабочее место «Статистика Генеральной прокуратуры Российской Федерации» (АРМ «Статистика»), предназначенное для сбора, обработки и формирования статистической отчетности в электронном виде в органах прокуратуры;

информационная система межведомственного электронного взаимодействия Генеральной прокуратуры Российской Федерации (ИС МЭВ ГП РФ), предназначенная для обеспечения информационного межведомственного электронного взаимодействия Генеральной прокуратуры Российской Федерации в целях обмена данными (получение и передача сведений) с участниками межведомственного электронного взаимодействия;

информационная система по организации и контролю коммуникационного взаимодействия с гражданами (мобильное приложение), предназначенная для своевременного и актуального информирования о деятельности органов прокуратуры, оптимизации процесса подачи обращений и доступа к документам;

платформа для внедрения интерактивного помощника по взаимодействию с органами прокуратуры Российской Федерации (чат-бот), предназначенная для навигационной помощи и поддержки пользователей в работе со специальным программным обеспечением – Единым порталом прокуратуры Российской Федерации, автоматизации обработки обращений пользователей, сокращения срока их рассмотрения и оперативного получения информации;

база данных «Документы Генеральной прокуратуры Российской Федерации» с использованием системы ведения баз данных (СВБД) «КонсультантПлюс», предназначенная для размещения актуальных архивных и текущих организационно-распорядительных и информационно-

методических документов Генеральной прокуратуры Российской Федерации с возможностью интегрированного поиска на базе системы ведения баз данных (СВБД) «КонсультантПлюс».

В целях надлежащей эксплуатации программного обеспечения, информационных систем и информационных ресурсов в органах прокуратуры распоряжением Генеральной прокуратуры Российской Федерации от 01.07.2022 № 364/11р утвержден единый реестр программного обеспечения, используемого в органах и организациях прокуратуры Российской Федерации.

3.2. Государственные информационные системы

Федеральная государственная информационная система «Единый реестр контрольных (надзорных) мероприятий» (далее – ФГИС ЕРКНМ) и ее подсистема «Единый реестр проверок» предоставляют пользователю доступ к личному кабинету со стороны органов прокуратуры и контрольных (надзорных) органов, предназначены для автоматизации функций формирования и ведения реестра плановых и внеплановых контрольных (надзорных) и профилактических мероприятий в отношении юридических лиц и индивидуальных предпринимателей, учета результата таких мероприятий, а также обеспечивают возможность формирования ежегодного плана контрольных (надзорных) мероприятий и их согласования с органами прокуратуры. Дополнительно система обеспечивает предоставление общедоступной информации, содержащейся в ФГИС ЕРКНМ, неограниченному кругу лиц посредством ее размещения оператором единого реестра контрольных (надзорных) мероприятий на специализированном сайте в информационно-телекоммуникационной сети «Интернет» на открытой части портала. Функции оператора системы закреплены за Генеральной прокуратурой Российской Федерации, методическое сопровождение – за Минэкономразвития России.

В целях реализации функции по ведению государственного единого статистического учета заявлений и сообщений о преступлениях, состояния преступности, раскрываемости преступлений, состояния и результатов следственной работы и прокурорского надзора осуществляется комплекс мероприятий, направленных на создание, развитие и ввод в эксплуатацию государственной автоматизированной системы правовой статистики (далее – ГАС ПС).

С 01.01.2025 возобновлена опытная эксплуатация модуля «Учет работы прокуроров» специального программного обеспечения ГАС ПС в подразделениях Генеральной прокуратуры Российской Федерации, Главной военной прокуратуре, прокуратурах субъектов Российской Федерации и приравненных к ним военных и иных специализированных прокуратурах. Обеспечен доступ к модулю работникам органов прокуратуры, организована техническая поддержка его работы.

3.3. Внешние информационные системы и сервисы

К внешним информационным системам и сервисам относятся: информационный ресурс «Маркер» (доступ в сети «Интернет»);

информационный ресурс «Спарк» (доступ в сети «Интернет»);
 специализированное сетевое издание X-Compliance (доступ в сети «Интернет»);
 справочно-правовая система «КонсультантПлюс»;
 программный комплекс «Стенографист»;
 система мониторинга и анализа неструктурированной информации из открытых источников данных (доступ в сети «Интернет»);
 специализированный программный продукт для обеспечения мониторинга, анализа и трансляции прямого эфира новостных и информационно-аналитических программ в режиме реального времени (доступ в сети «Интернет»).

Работникам органов прокуратуры в соответствии с возложенными обязанностями предоставлен доступ к иным информационным системам и сервисам для получения информации, необходимой для осуществления полномочий.

3.4. Текущее состояние инфраструктуры органов прокуратуры

Выполнено внедрение компонентов цифровой инфраструктуры в части:
 единой защищенной сети передачи данных органов прокуратуры;
 локальных вычислительных сетей органов прокуратуры;
 защищенной облачной вычислительной платформы (внешний центр обработки данных Генеральной прокуратуры Российской Федерации);
 автоматизированных рабочих мест работников прокуратуры;
 единой системы ведомственной телефонной связи и систем мультимедийного оснащения;
 обеспечения технической поддержки;
 мониторинга и анализа инцидентов информационной безопасности, обнаружения и предупреждения компьютерных атак в информационных системах органов прокуратуры.

3.4.1. Единая защищенная сеть передачи данных органов прокуратуры

В 2018 году в прокуратуре Российской Федерации создана единая защищенная сеть передачи данных органов прокуратуры Российской Федерации (далее – ЕЗСПД).

ЕЗСПД предназначена для обеспечения при передаче по каналам связи защиты информации, обрабатываемой в информационных системах органов прокуратуры, в которых производится обработка информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения и иных неправомерных действий.

ЕЗСПД подлежит применению в качестве общей инфраструктуры передачи данных, обеспечивающей защищенный доступ к российскому государственному сегменту информационно-телекоммуникационной сети RSNет (открытый сегмент ЕЗСПД) и доступ к информационным системам органов прокуратуры (сегментам информационных систем), в которых

производится обработка информации ограниченного доступа путем организации защищенного (закрытого) сегмента ЕЗСПД.

ЕЗСПД представляет собой совокупность компонентов, территориально распределенных по органам прокуратуры, и обеспечивает:

криптографическую защиту информации при ее передаче по каналам связи, выходящим за пределы контролируемых зон объектов информатизации; децентрализованное иерархическое управление средствами криптографической защиты информации в составе ЕЗСПД с размещением центров управления в Генеральной прокуратуре Российской Федерации, Главной военной прокуратуре и на региональных уровнях;

управление информационными потоками между информационными системами органов прокуратуры;

обнаружение вторжений (компьютерных атак), направленных на информационные системы органов прокуратуры и централизованное управление подсистемой обнаружения вторжений ЕЗСПД;

автоматическое выявление инцидентов на основе анализа событий средств подсистемы обнаружения вторжений ЕЗСПД;

интеграцию с ведомственным сегментом государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, находящиеся в зоне ответственности органов и организаций прокуратуры (далее – ведомственный сегмент ГосСОПКА);

возможность использования в качестве общей инфраструктуры передачи данных для информационных систем органов прокуратуры, в которых производится обработка информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну;

резервируемый защищенный доступ к российскому государственному сегменту информационно-телекоммуникационной сети «Интернет» (сеть RSNет) из ЕЗСПД и сегментов информационных систем органов прокуратуры на федеральном и региональном уровнях;

возможность подключения пользователей федеральных государственных органов и федеральных органов исполнительной власти (децентрализованный доступ пользователей ГАС ПС федеральных государственных органов и федеральных органов исполнительной власти) к ГАС ПС в рамках заключенных соглашений об информационном взаимодействии;

возможность подключения представителей субподрядчиков, обеспечивающих администрирование, создание или развитие информационных систем органов прокуратуры, в рамках заключенных государственных контрактов;

возможность подключения центров обработки данных федеральных государственных органов и федеральных органов исполнительной власти, осуществляющих централизованное взаимодействие автоматизированных информационных систем и пользователей указанных органов с ГАС ПС,

в рамках заключенных соглашений об информационном взаимодействии;
 возможность подключения объектов органов прокуратуры, расположенных в зданиях судов различной юрисдикции;
 требуемый уровень защищенности информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, при ее передаче по каналам связи между объектами информатизации органов прокуратуры.

В 2021 году на ЕЗСПД получен аттестат соответствия требованиям по защите информации № 0087.00016.2021. Документ удостоверяет соответствие ЕЗСПД требованиям безопасности информации, предъявляемым к государственным информационным системам первого класса защищенности (К1) приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах (далее – приказ ФСТЭК России № 17), и к информационным системам персональных данных, для которых согласно постановлению Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» (далее – постановление № 1119) установлена необходимость обеспечения первого уровня защищенности персональных данных (УЗ 1).

3.4.2. Локальные вычислительные сети органов прокуратуры

В органах прокуратуры построены структурированные кабельные системы, на базе которых с использованием современного оборудования российских производителей созданы изолированные двухконтурные локальные вычислительные сети.

Аналогично модернизированы сегменты ядра локальных вычислительных сетей аппарата Генеральной прокуратуры Российской Федерации, 102 прокуратур субъектов Российской Федерации и приравненных к ним специализированных прокуратур.

3.4.3. Защищенная облачная вычислительная платформа

Защищенная облачная вычислительная платформа предназначена для размещения информационных систем Генеральной прокуратуры Российской Федерации и предоставляет размещаемым информационным системам:

вычислительную инфраструктуру до уровня системы виртуализации, соответствующей требованиям о защите информации и позволяющей размещать государственные информационные системы по классу защищенности информации до первого включительно (в соответствии с требованиями приказа ФСТЭК России № 17) и (или) информационных систем персональных данных по уровню защищенности персональных данных до первого включительно (в соответствии с требованиями постановления № 1119, приказа ФСТЭК России от 18.02.2013 № 21);

сертифицированные средства защиты информации с целью обеспечения реализации мер в соответствии с требованиями законодательства в области

защиты информации, предполагаемых к реализации, возможности проведения аттестации на соответствие требованиям о защите информации информационных систем, развернутые на вычислительной инфраструктуре внешнего центра обработки данных;

услуги администрирования вычислительной инфраструктуры, виртуальной инфраструктуры и средств защиты информации.

Все информационные системы органов прокуратуры размещены на защищенной облачной вычислительной платформе – во внешнем центре обработки данных Генеральной прокуратуры Российской Федерации (далее – ВЦОД).

Инфраструктура облачной вычислительной платформы создана на высокопроизводительном оборудовании с использованием передовых практик обеспечения отказоустойчивости и надежности.

Облачная вычислительная платформа размещается в дата-центре и обеспечивает поддержание оптимального климата, а также гарантирует непрерывность электропитания. ВЦОД аттестован по требованиям информационной безопасности (уровень К1, УЗ 1).

3.4.4. Автоматизированные рабочие места работников прокуратуры

Работники органов прокуратуры для выполнения должностных обязанностей обеспечены типовыми автоматизированными рабочими местами (далее – АРМ), которые подключены к ЕЗСПД.

С использованием АРМ работники получают доступ к информационным системам и могут взаимодействовать с другими органами прокуратуры через электронную почту и видео-конференц-связь (далее – ВКС).

АРМ различаются характеристиками в зависимости от функционала, необходимого для работника.

Реализованная инфраструктура позволяет поддерживать установленное на АРМ программное обеспечение в актуальном состоянии и устанавливать обновления в автоматическом режиме.

Периодическая модернизация АРМ обеспечивает необходимый уровень вычислительной мощности для работы с большими объемами данных.

АРМ защищенного сегмента аттестовано по требованиям информационной безопасности (уровень К3, УЗ 3).

Внедрение и использование единого каталога пользователей в органах прокуратуры обеспечивает прозрачную авторизацию и аутентификацию при взаимодействии с информационными ресурсами. Его использование в качестве единого источника достоверной информации сокращает время обработки данных.

Взаимодействие работников органов прокуратуры через единую систему электронной почты или сервиса файлового хранения уменьшает время реагирования и позволяет получать информацию удаленно.

Использование сервиса сканирования и печати позволяет сократить объем хранимой информации за счет оцифровки и сжатия, а также обеспечивает мониторинг ресурсов используемой техники.

3.4.5. Единая система ведомственной телефонной связи и мультимедийное оснащение

На всех объектах органов прокуратуры установлены IP-телефоны и голосовые шлюзы для обеспечения взаимодействия работников и отказоустойчивого подключения к телефонным сетям общего пользования (далее – ТфОП).

Единая система ведомственной телефонной связи (далее – ЕСВТС) интегрирована с существующим комплексом телефонной связи аппарата Генеральной прокуратуры Российской Федерации.

Залы совещаний в 105 прокуратурах субъектов Российской Федерации и приравненных к ним специализированных прокуратурах оборудованы комплексами ВКС защищенного сегмента.

На всех АРМ закрытого сегмента работников прокуратуры установлены программные клиенты ВКС. В аппарате Генеральной прокуратуры Российской Федерации создана система ВКС открытого сегмента.

ЕСВТС интегрирована с единым каталогом пользователей органов прокуратуры.

Залы и переговорные помещения аппарата Генеральной прокуратуры Российской Федерации оснащены современным мультимедийным оборудованием, подключенным к системам ВКС закрытого и открытого сегментов с обеспечением необходимых требований информационной безопасности.

3.4.6. Единая техническая поддержка

Создана служба технической поддержки, обеспечивающая регистрацию и обработку запросов работников органов прокуратуры. Для регистрации обращений (заявок пользователей) организована единая «точка входа» по телефону и электронной почте, функционирующая в круглосуточном режиме.

Выполняются прием обращений, их регистрация, классификация и маршрутизация на следующие уровни поддержки. Осуществляются контроль хода выполнения работ по обращению, эскалация в случае возникновения проблем с исполнением обращения, информирование пользователей о ходе выполнения работ, закрытие запроса.

Проводится информирование пользователей по инцидентам, проблемам, работам массового характера, проводимым изменениям и технологическим работам. По запросам осуществляется изменение конфигураций сопровождаемого оборудования и программного обеспечения. Выполняется непрерывный мониторинг состояния инфраструктуры органов прокуратуры.

3.4.7. Мониторинг и анализ инцидентов информационной безопасности, обнаружение и предупреждение компьютерных атак, защита информации при ее передаче по каналам связи

В системе защиты информации органов прокуратуры мониторинг безопасности обеспечивается с помощью специальных программных и программно-технических средств мониторинга, выявления и реагирования

на инциденты безопасности.

Введенный в эксплуатацию ведомственный сегмент ГосСОПКА предназначен для выявления компьютерных инцидентов и атак на информационные ресурсы органов прокуратуры, реагирования на них, устранения их последствий и реализует следующие задачи:

- сбор и обработка инвентаризационных данных информационных ресурсов органов прокуратуры;

- сбор, обработка и анализ данных о событиях безопасности в информационных ресурсах органов прокуратуры;

- управление инцидентами информационной безопасности в информационных ресурсах органов прокуратуры;

- визуализация и построение сводных отчетов;

- хранение информации об инцидентах информационной безопасности в информационных ресурсах органов прокуратуры;

- сбор и анализ данных о состоянии информационных ресурсов органов прокуратуры для оценки текущего уровня их защищенности;

- взаимодействие с национальным координационным центром по компьютерным инцидентам (НКЦКИ).

Введена в эксплуатацию система мониторинга информационных пакетов в среде информационных систем и сетей органов и организаций прокуратуры Российской Федерации (СМИП ИСС), предназначенная для обеспечения защиты информации от ее утечки и разглашения. С этой целью СМИП ИСС позволяет контролировать все каналы сетевой коммуникации органов прокуратуры (электронная почта, системы мгновенных сообщений, накопители информации, принтеры и т. д.), а также проводить анализ содержания документа (контекстный анализ).

В информационную инфраструктуру внедрена система контроля действий привилегированных пользователей (администраторы, специалисты технической поддержки, разработчики), которая предназначена для предотвращения несанкционированного доступа к информационным ресурсам, минимизации человеческого фактора в действиях, защиты от внутренних угроз и от утечки конфиденциальных данных.

Система контроля действий привилегированных пользователей позволяет оперативно выявлять подозрительные действия и предотвращать угрозы, отслеживать соблюдение правил информационной безопасности, контролировать полномочия привилегированных пользователей, фиксацию и аудит всех действий пользователей с расширенными правами, что в свою очередь способствует снижению вероятности нанесения ущерба информационным ресурсам и инфраструктуре органов прокуратуры.

4. Актуальность цифровой трансформации органов и организаций прокуратуры Российской Федерации

Актуальность задачи цифровой трансформации органов прокуратуры обусловлена, с одной стороны, современными тенденциями развития экономики данных в Российской Федерации, повышением требований к защищенности государственных информационных ресурсов и систем, усилением государственной координации и расширением направлений межведомственного взаимодействия органов прокуратуры в установленной сфере деятельности, а с другой – нерешенностью следующих основных проблем:

исключение дублирования функционала и данных в информационных ресурсах и системах, в том числе дублирования операций по многократному вводу и обработке идентичных данных, снижающее достоверность и оперативность получения необходимой информации;

используемые технические решения в ряде случаев базируются на импортных технических и программных средствах, не позволяющих обеспечить надежное и безопасное функционирование информационных ресурсов и систем;

отсутствие удобных открытых интерфейсов и высокие издержки на установку, сопровождение и модернизацию клиентского программного обеспечения;

недостаточность использования современных инструментальных средств и методов комплексной обработки разнородных данных, не позволяющая обеспечить требуемый уровень аналитической поддержки деятельности руководителей органов прокуратуры;

сложность и масштабность проводимых в процессе цифровой трансформации преобразований, динамика развития информационных технологий, требующие тщательного подбора квалифицированных работников, владеющих цифровыми компетенциями и заинтересованных в применении новых подходов, постоянного повышения работниками уровня знаний и актуализации образовательных программ с учетом внедрения передовых технологий, в том числе технологий искусственного интеллекта.

Актуальность цифровой трансформации в части компонентов цифровой инфраструктуры:

ЕЗСПД:

модернизированная ЕЗСПД соответствует современным требованиям в части защищенности передаваемых данных, производительности, использования современных протоколов и интерфейсов, сетевого обеспечения межведомственного взаимодействия, единых подходов и стандартизации решений по структуре и функциям, мониторингу и управляемости компонентов ЕЗСПД;

в текущих условиях существует необходимость в подключении новых территориальных площадок органов прокуратуры с использованием

телекоммуникационного оборудования российского производства и их интеграции в существующую структуру ЕЗСПД;

локальные вычислительные сети органов прокуратуры:

созданные локальные вычислительные сети используют современное оборудование российского происхождения, имеют необходимую производительность и соответствуют требованиям по информационной безопасности;

существует необходимость организации структурированных кабельных систем и локальных вычислительных сетей на новых территориальных площадках органов прокуратуры и подключения их к ЕЗСПД;

защищенная облачная вычислительная платформа:

защищенная облачная вычислительная платформа, созданная в рамках цифровой трансформации органов прокуратуры, соответствует современным требованиям к производительности, использует современные информационно-телекоммуникационные компоненты, средства защиты информации, поддерживает эффективный мониторинг и управление;

операционные системы и программное обеспечение, используемые в информационных системах, имеют зарубежное происхождение, что увеличивает санкционные риски их применения;

расширение вычислительных ресурсов защищенной облачной платформы осуществляется в соответствии с развитием информационных систем органов прокуратуры и их потребностями в новых вычислительных ресурсах;

для поддержания производительности, отказоустойчивости и актуального состояния защищенной облачной вычислительной платформы требуется постоянное сервисное обслуживание и периодическая модернизация;

единая система ведомственной телефонной связи и мультимедийное оснащение:

созданные в ходе цифровой трансформации системы ВКС и телефонии единой системы ведомственной телефонной связи соответствуют образцам, используемым отечественными и зарубежными организациями. В целях сохранения достигнутых результатов необходимо постоянное сервисное обслуживание и периодическая модернизация для поддержания инфраструктуры телефонии и ВКС в актуальном состоянии в соответствии с меняющимися требованиями;

система мультимедийного оснащения, созданная в ходе цифровой трансформации, полностью соответствует современным тенденциям построения аналогичных систем, а также требованиям Генеральной прокуратуры Российской Федерации;

единая техническая поддержка:

необходимо проводить непрерывный контроль качества функционирования инфраструктуры органов прокуратуры за счет использования средств оперативного мониторинга, анализа, моделирования;

основными целями технической поддержки являются проактивный подход к сопровождению инфраструктуры, минимизация времени решения инцидентов, снижение времени простоя сопровождаемых систем;

информационная безопасность:

необходима полная реализация единой («сквозной») авторизации в информационных системах закрытого сегмента ЕЗСПД;

средства криптографической защиты информации части объектов ЕЗСПД территориального уровня требуют модернизации;

отсутствие решения или комплекса решений, обеспечивающих контроль доступа пользователей к информационным ресурсам и подключения устройств к информационной инфраструктуре, в том числе позволяющих осуществлять профилирование и проверку устройств по ряду требований безопасности (обновление антивирусных сигнатур, критичных обновлений безопасности операционной системы и т. д.). Реализация такого решения позволит дать дополнительный виток развития телекоммуникационной инфраструктуры в части организации мобильного доступа: внедрение беспроводных технологий, использование корпоративных планшетов и т. д.

5. Принципы цифровой трансформации органов и организаций прокуратуры Российской Федерации

Для достижения поставленных задач и индикаторов цифровая трансформация органов прокуратуры должна базироваться на следующих основных принципах:

оптимизация – сокращение ресурсных и временных затрат на внедрение и эксплуатацию информационных систем на основе цифровизации процессов органов прокуратуры;

консолидация – дифференцированное объединение (укрупнение) вычислительных и информационных ресурсов, отказ от разрозненных точек установки и эксплуатации технических средств и функций информационных систем с целью упрощения эксплуатации информационных систем, более эффективного использования ресурсов за счет возможности их перераспределения между системами;

надежность – обеспечение возможности сохранять во времени в установленных пределах значения всех параметров, характеризующих способность вычислительных и информационных ресурсов выполнять требуемые функции в заданных режимах и условиях эксплуатации и технического обслуживания;

стандартизация – установление типовых норм и требований к отдельным элементам, функциям, процессам и интерфейсам информационных систем для достижения оптимальной степени упорядоченности, а также технической и информационной совместимости компонентов информационных систем и, как следствие, снижения затрат на внедрение и эксплуатацию систем;

единая модель данных – стандартизация модели мастер-данных, позволяющая обеспечить централизованное хранение и обработку

нормативно-справочной информации, стандартизацию данных в информационных системах, разграничение зон ответственности за качество данных и задел для обеспечения гибкости настройки информационных систем при изменении наборов обрабатываемых данных без существенного изменения информационных систем;

унификация – установление оптимального перечня используемого оборудования и программного обеспечения, сокращение номенклатуры технических средств и интерфейсов информационных систем в целях упрощения процессов, связанных с внедрением, модернизацией и эксплуатацией информационных систем;

виртуализация – использование логического представления набора вычислительных ресурсов, абстрагированного от аппаратной реализации технических средств, с целью повышения эффективности использования и адаптивности (гибкости) цифровой инфраструктуры, сокращения капитальных и эксплуатационных расходов, обеспечения непрерывности функционирования информационных систем;

модульность – группировка функционально связанных частей вычислительных и информационных ресурсов в законченные узлы – модули, возможность внесения частичных изменений в функции информационной системы без ее полной переработки с целью ускорения внедрения и модернизации информационных систем, повышения их устойчивости к внешним и внутренним воздействиям;

импортозамещение – преимущественное использование отечественных аппаратных решений, а также российского и свободно распространяемого программного обеспечения, включенного в единый реестр российских программ для ЭВМ и баз данных, при модернизации существующих и создании новых компонентов цифровой инфраструктуры, обеспечении информационной безопасности с целью снижения санкционных и валютных рисков, развития национальной промышленной базы;

внедрение технологий искусственного интеллекта – комплекса технологических решений, позволяющего имитировать когнитивные функции человека (включая поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые с результатами интеллектуальной деятельности человека или превосходящие их. Комплекс технологических решений включает в себя информационно-коммуникационную инфраструктуру, программное обеспечение (в том числе в котором используются методы машинного обучения), процессы и сервисы по обработке данных и поиску решений;

информационная безопасность – состояние защищенности интересов органов и организаций прокуратуры в условиях угроз в информационной сфере, которое достигается обеспечением совокупности свойств информационной безопасности – целостностью, конфиденциальностью, доступностью информационных ресурсов и инфраструктуры органов и организаций прокуратуры.

6. Направления и мероприятия цифровой трансформации органов и организаций прокуратуры Российской Федерации

Эффективность достижения целей цифровой трансформации органов прокуратуры определяется качеством реализации системы ключевых мероприятий в рамках соответствующих основных направлений.

Направление 1. Высокотехнологичный надзор

В целях создания единой безопасной цифровой платформы для обеспечения электронного взаимодействия органов прокуратуры всех уровней между собой и с другими государственными органами при осуществлении надзорной деятельности необходима реализация следующих мероприятий:

- осуществление комплексной оптимизации ведомственных и межведомственных процессов надзорной деятельности с целью их цифровой трансформации;

- подготовка научно-методического, нормативного обеспечения и программно-технологической инфраструктуры для реализации возможности дистанционных прокурорских проверок;

- обеспечение органам прокуратуры доступа к данным, необходимым для осуществления высокотехнологичного надзора;

- разработка и внедрение технологий и механизмов для реализации возможности дистанционного получения статистической информации, исключающих возможность ее дублирования и направленных на обеспечение потребностей общества и государства в необходимых данных в режиме реального времени;

- интеграция ведомственных систем в том числе с внешними государственными информационными системами, содержащими данные оперативно-справочных, розыскных и иных учетов, реестры физических и юридических лиц;

- внедрение современных и перспективных технологий и инструментальных средств, включая сертифицированный отечественный аппаратно-программный комплекс обработки массивов больших данных, для работы с документами первичного учета;

- внедрение технологий искусственного интеллекта и цифровых решений для оптимизации управленческой, организационной и надзорной деятельности органов прокуратуры.

Направление 2. Цифровая инфраструктура

В целях создания универсальной безопасной и высокотехнологичной цифровой среды ведомственного и межведомственного взаимодействия, обеспечения требуемого качества электронных коммуникаций органов прокуратуры всех уровней с гражданами и обществом необходима реализация комплекса мероприятий в рамках информационной, вычислительной платформы, а также в рамках подсистем передачи данных, обеспечения информационной безопасности, обучения и кадрового обеспечения.

В части информационной подсистемы выполняются следующие мероприятия:

реализация государственной автоматизированной системы правовой статистики с использованием единой цифровой платформы Российской Федерации «ГосТех»;

разработка на базе ГАС ПС цифровых сервисов с использованием технологий искусственного интеллекта и больших данных, позволяющих выполнять поиск статистических карточек, аналогичных заданной карточке или их совокупности, выявлять тенденции роста нарушений, строить объяснительные модели причинно-следственных связей, проводить массовое выявление признаков нарушений законности по данным из государственных и ведомственных информационных систем на основе применения цифровых моделей объектов надзора и наборов признаков нарушения законности в заданной отрасли прокурорского надзора, осуществлять автоматизированную подготовку проектов мер прокурорского реагирования с выявлением и учетом аналогов из цифрового архива прокурорской и судебной практики, с построением дерева ссылок использованных норм права;

переход ФГИС ЕРКНМ на единую цифровую платформу Российской Федерации «ГосТех»;

создание на основе АИК «Надзор-WEB» подсистемы интеллектуальной обработки входящих обращений граждан, запросов организаций и органов государственной власти по поднадзорности, автоматизированного уведомления заявителей о ключевых этапах и результатах рассмотрения обращений;

выполнение импортозамещения компонентов информационной подсистемы по мере их морального устаревания и физического износа;

реализация унифицированного взаимодействия существующих и разрабатываемых информационных систем органов прокуратуры с единым хранилищем данных, обеспечение возможности «сквозной» комплексной аналитической обработки накопленных данных;

интеграция информационно-телекоммуникационной инфраструктуры органов прокуратуры с отечественными цифровыми платформами, в том числе при осуществлении надзорной деятельности, обеспечивающая формирование единой доверенной среды для работы с данными;

создание и организация сопровождения единой системы нормативно-справочной информации органов прокуратуры, включая интеграцию с федеральными государственными информационными системами ФГИС ЕСНСИ, ФГИС ЕИП НСУД и другими федеральными государственными информационными системами, предназначенными для обмена данными.

В части защищенной облачной вычислительной платформы:

развитие центра обработки данных, предоставляющего доступные, устойчивые и безопасные услуги по хранению и обработке данных

для экосистемы органов прокуратуры, с использованием отечественного оборудования и программного обеспечения;

адаптация существующих информационных систем к отечественным операционным системам и программному обеспечению;

внедрение современных и перспективных технологий и инструментов для работы с размещенными информационными системами.

В части ЕЗСПД:

адаптация существующих решений по построению узлов сети ЕЗСПД к использованию оборудования российского производства в объеме всей ЕЗСПД;

подключение новых объектов органов прокуратуры к сети ЕЗСПД с учетом принятых решений по адаптации и использованию оборудования российского производства;

обеспечение мониторинга качества предоставляемых сервисов при переходе на использование оборудования и программного обеспечения российского производства.

В части АРМ:

обеспечение всех работников органов прокуратуры единым защищенным автоматизированным рабочим местом;

создание мобильной компоненты, обеспечивающей определенным категориям пользователей органов прокуратуры возможность синхронной реализации надзорных функций как со стационарного, так и с мобильного автоматизированного рабочего места;

обеспечение технической поддержки инфраструктурных сервисов в рамках модели собственного владения;

дальнейшая интеграция базовых инфраструктурных сервисов с существующими и создаваемыми информационными системами;

мониторинг качества сервисов в системах электронной почты, сервиса файлового хранения, сервиса печати и сканирования;

апробация современных и перспективных отечественных технологий и программного обеспечения, направленных на повышение качества и надежности услуг по предоставлению инфраструктурных сервисов.

В части ЕСВТС:

максимально возможный перевод подключений прокуратур субъектов Российской Федерации и приравненных к ним специализированных прокуратур к ТфОП на цифровые потоки Е1;

сокращение канальной и номерной емкости подключений объектов прокуратуры к ТфОП в целях ее оптимизации;

обеспечение технической поддержки инфраструктуры ЕСВТС в рамках модели владения собственной инфраструктурой;

расширение комплектов мультимедийного оснащения за счет дополнительных средств, повышающих автоматизацию проведения мероприятий (рабочих встреч и совещаний);

внедрение современных средств коммуникаций – российского защищенного производственного мессенджера, который обеспечит для работников внутри контура безопасности Генеральной прокуратуры Российской Федерации возможности мгновенной доставки сообщений, создания групповых чатов, видеоконференций и аудиозвонков, использования в том числе на мобильных устройствах.

В части единой технической поддержки:

совершенствование процессов контроля качества сервисов, оценки удовлетворенности пользователей, осведомленности пользователей по процедурам технической поддержки;

развитие сервисов комплексного мониторинга инфраструктуры, в том числе мониторинга производительности информационных систем.

В части подсистемы обучения и кадрового обеспечения:

организация переподготовки работников органов прокуратуры, в том числе с использованием дистанционных образовательных технологий и электронного обучения, по вопросам рациональной организации исполнения своих полномочий в условиях современных реалий цифровой экономики;

внедрение образовательными организациями органов прокуратуры дистанционных образовательных технологий и электронного обучения, в том числе в сетевом взаимодействии с другими организациями общего и дополнительного образования, во все виды и формы деятельности обучающихся в соответствии с требованиями экономики данных;

разработка и реализация образовательными организациями органов прокуратуры с учетом требований цифровой экономики программ повышения квалификации, переподготовки и непрерывного профессионального развития педагогов, обеспечивающих их готовность к реализации современных моделей образовательного процесса.

Направление 3. Среда доверия

В целях формирования и развития единой цифровой среды доверия, позволяющей обеспечить техническую, организационную и правовую защиту интересов граждан, общества и государственных интересов при взаимодействии участников обновленной экосистемы органов прокуратуры, необходима реализация следующих мероприятий:

разработка и внедрение механизмов и технологий реализации доверенных цифровых дистанционных коммуникаций участников взаимодействия экосистемы органов прокуратуры, обеспечивающих удаленное подтверждение личности для совершения юридически значимых действий; обеспечение равного статуса различных способов идентификации и аутентификации физических и юридических лиц;

обеспечение доступа граждан и организаций к открытой информации о деятельности органов прокуратуры, а также информации, непосредственно затрагивающей их права и свободы.

Направление 4. Обеспечение информационной безопасности

Основными векторами для реализации в рамках системы обеспечения

информационной безопасности органов прокуратуры являются:

контроль действий пользователей и предоставленных им прав доступа в целях предотвращения несанкционированного доступа к информационным ресурсам, техническим и программным средствам, средствам защиты информации исключения деструктивных воздействий на информационные ресурсы, в том числе при проведении работ по созданию, модернизации и внедрению информационных систем;

мониторинг и аудит защищенности информационной инфраструктуры и информационных ресурсов органов прокуратуры в процессе обработки информации в информационных системах органов прокуратуры;

обнаружение вторжений (компьютерных атак), предотвращение и нейтрализация угроз информационной безопасности, ликвидация последствий их реализации в процессе взаимодействия информационных систем органов прокуратуры с внешними информационными системами;

контроль целостности и достоверности информации, обрабатываемой в информационных системах органов прокуратуры, а также целостности программно-аппаратных компонентов информационных систем;

безопасность информации при ее передаче по каналам связи;

осведомленность работников органов прокуратуры об угрозах, правила безопасности данных, обнаружение инцидентов и реагирование на них, безопасное обращение с электронной почтой и т. п.

Разработка и реализация мероприятий в части обеспечения информационной безопасности предусматривает:

модернизацию систем мониторинга и регистрации событий, влияющих на безопасность информации, автоматизацию анализа информации о таких событиях, что позволит своевременно выявлять инциденты информационной безопасности в информационных системах органов прокуратуры и реагировать на них;

использование российских технологий, программного обеспечения и оборудования для обеспечения защиты информации и процессов ее обработки;

расширение внедренной системы мониторинга утечек конфиденциальной информации;

непрерывное обучение работников с целью совершенствования навыков обеспечения работоспособности информационных систем, безопасной обработки информации в информационных системах органов прокуратуры и сети «Интернет».

7. Механизмы реализации Концепции

Механизмы реализации Концепции включают в себя научно-методическое, организационно-правовое и ресурсное обеспечение.

Научно-методическое обеспечение включает:

формирование единой научно-технической политики и научно-

методической базы цифровой трансформации органов прокуратуры на основе взаимодействия с ведущими научными, образовательными организациями и профессиональными сообществами, в том числе на международном уровне, проведения современных исследований и разработок с учетом потребностей органов прокуратуры в формировании продуктов цифровой среды;

формирование совместно с профессиональными сообществами экспертно-аналитических материалов и моделей будущего экосистемы органов прокуратуры;

формирование методологии планирования, координации, мониторинга и отчетности при реализации Концепции, а также соответствующей системы методической поддержки ее выполнения;

участие в формировании коммуникационных платформ, создаваемых для взаимодействия участников цифровых платформ и центров компетенций при проведении исследований и разработок по направлениям «сквозных» технологий.

Организационно-правовое обеспечение включает:

совершенствование мер правового регулирования с целью реализации мероприятий цифровой трансформации органов прокуратуры;

обеспечение реализации мероприятий Концепции и подготовку ежегодного доклада Генеральному прокурору Российской Федерации;

взаимодействие в установленной сфере деятельности с федеральными государственными органами, органами исполнительной власти субъектов Российской Федерации, органами местного самоуправления, с представителями предпринимательства, гражданского общества и научно-образовательного сообщества по вопросам цифровой трансформации органов прокуратуры;

обеспечение взаимодействия с центрами компетенций существующих и перспективных «сквозных» технологий по внедрению данных технологий в цифровую экосистему органов прокуратуры;

формирование нормативной базы компонентов образовательных программ образовательных организаций органов прокуратуры, важных для цифровой экономики, включая стандарты и государственные требования;

повышение уровня компетенций и развитие навыков в области искусственного интеллекта, внедрение комплексной системы подготовки квалифицированных кадров в сфере использования технологий искусственного интеллекта в деятельности органов прокуратуры.

Ресурсное обеспечение включает:

оценку возможностей использования находящихся на балансе аппаратно-программных ресурсов при проектировании и внедрении информационных систем;

консолидацию бюджетных средств, выделенных на создание информационных систем, имеющих ключевое значение в деятельности органов прокуратуры;

обеспечение ресурсами выполнения Концепции, координацию

финансирования предусмотренных мероприятий за счет средств бюджета Российской Федерации;

формирование кадрового потенциала в целях обеспечения развития цифровизации деятельности органов прокуратуры в сфере информационных технологий и защиты информации.

8. Этапы реализации Концепции

Состав и содержание этапов реализации Концепции¹ обусловлены необходимостью последовательного решения следующих задач:

завершение ранее начатых работ по созданию и (или) модернизации отдельных компонентов существующей цифровой инфраструктуры, информационных ресурсов и систем;

организация на принципах непрерывности обучения работников органов прокуратуры цифровым компетенциям и навыкам, в том числе с использованием ВКС, проведение комплексной оценки уровня «цифровой зрелости» органов прокуратуры;

реализация пилотных проектов ключевых компонентов цифровой инфраструктуры органов прокуратуры;

совершенствование типовых решений по результатам их пилотной реализации и дальнейшее тиражирование с учетом специфики деятельности конкретных органов прокуратуры и лучших практик.

Реализацию Концепции предполагается осуществить в три взаимосвязанных этапа.

Этап 1 (2026 год) включает:

- 1) обеспечение правовых оснований для получения доступа к данным, необходимым для осуществления высокотехнологичного надзора;
- 2) развитие ФГИС ЕРКНМ и ее подсистемы «Единый реестр проверок» с использованием компонентов единой цифровой платформы Российской Федерации «ГосТех»;
- 3) обеспечение создания и развития ГАС ПС;
- 4) разработку технологических решений, направленных на автоматизацию отдельных видов деятельности органов прокуратуры с применением технологий искусственного интеллекта при работе с массивами данных, включая интеллектуальную обработку служебных документов, обращений, прогнозирование преступности и правонарушений;
- 5) внедрение технологий искусственного интеллекта при осуществлении мероприятий в сфере информационной безопасности;
- 6) разработку технических заданий на подключение новых объектов к ЕЗСПД органов прокуратуры с использованием оборудования российского производства, отечественных решений в области операционных систем и программного обеспечения на автоматизированных рабочих местах органов

¹ Могут быть скорректированы с учетом финансирования.

прокуратуры;

7) импортозамещение инфраструктуры: автоматизированных рабочих мест, оборудования печати и сканирования, ВКС и IP-телефонии;

8) внедрение системы мониторинга внешних цифровых угроз с использованием информации из открытых и закрытых источников («теневых ресурсов»);

9) обеспечение ввода в эксплуатацию комплекса автоматизированных систем финансово-хозяйственной деятельности органов и организаций прокуратуры Российской Федерации (КАИС ФХД) и модернизированного автоматизированного информационного комплекса учета кадров и кадрового делопроизводства органов прокуратуры Российской Федерации (АИК «Кадры-ОП»).

Этап 2 (2027–2028 годы) включает:

1) обеспечение ввода в эксплуатацию и функционирования ГАС ПС;

2) модернизацию ГАС ПС с использованием сервисов единой цифровой платформы Российской Федерации «ГосТех»;

3) модернизацию АИК «Надзор-WEB» с целью обеспечения импортозамещения компонентов и внедрения системы защиты информации;

4) выполнение импортозамещения критичных компонентов информационных систем органов прокуратуры для обеспечения технологической независимости;

5) разработку и внедрение системы управления НСИ и мастер-данными, включая интеграцию с федеральными государственными информационными системами ФГИС ЕСНСИ, ФГИС ЕИП НСУД и другими федеральными государственными информационными системами, предназначенными для обмена данными;

6) обеспечение функционирования информационных систем органов прокуратуры на отечественных операционных системах;

7) адаптацию существующих решений по построению узлов сети ЕЗСПД органов прокуратуры к использованию оборудования российского производства, обеспечение мониторинга качества предоставляемых сервисов;

8) обеспечение работников органов прокуратуры единым защищенным стационарным и мобильным автоматизированным рабочим местом, использование отечественных решений в области операционных систем и программного обеспечения;

9) перевод подключений прокуратур субъектов Российской Федерации и приравненных к ним специализированных прокуратур к ТфОП на цифровые потоки Е1;

10) внедрение системы контроля действий поставщиков информационно-телекоммуникационных услуг (СКДПУ);

11) внедрение систем мониторинга утечек конфиденциальной информации, систем безопасного использования веб-ресурсов на прикладном уровне, организацию регламентированного обмена сведениями о компьютерных инцидентах и об угрозах безопасности информации

с Национальным координационным центром по компьютерным инцидентам;

12) организацию переподготовки работников органов прокуратуры, в том числе с использованием дистанционных образовательных технологий и электронного обучения, во взаимодействии с организациями общего и дополнительного образования.

Этап 3 (2029–2030 годы) включает:

1) завершение импортозамещения компонентов информационных систем органов прокуратуры;

2) разработку и опытную эксплуатацию цифровых сервисов ГАС ПС, АИК «Надзор-WEB» с использованием технологий искусственного интеллекта;

3) завершение мероприятий по переходу ФГИС ЕРКНМ на сервисы единой цифровой платформы Российской Федерации «ГосТех».