ВОРОНЕЖСКИЙ ИНСТИТУТ МВД РОССИИ
КАЗАНСКИЙ ЮРИДИЧЕСКИЙ ИНСТИТУТ МВД РОССИИ

ИЗУЧЕНИЕ ЗАРУБЕЖНОГО ОПЫТА ФОРМИРОВАНИЯ МАССИВА СТАТИСТИЧЕСКОЙ ИНФОРМАЦИИ ИЗ МАТЕРИАЛОВ ЭЛЕКТРОННЫХ ОБРАЗОВ УГОЛОВНЫХ ДЕЛ

Аналитический обзор с предложениями

Воронеж
2021

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ И ОБОЗНАЧЕНИЙ

В настоящем НИР применяют следующие обозначения и сокращения

BJS − Бюро судебной статистики США;

CM/ECF − система организации движения электронных дел в судах;

EGVP − электронный судебный и административный почтовый ящик Германии;

OMB − Административно-бюджетное управление США;

UCR – Единая программа отчета о преступности США;

RCA SINGAPORE − Закон о регистрации преступников Сингапура;

АБД «Центр» − автоматизированный централизованный учет подозреваемых, обвиняемых и осужденных лиц;

АИС − автоматизированная информационная система;

АИПС – автоматизированная информационно-поисковая система;

ГИАЦ МВД РФ − «Главный информационно-аналитический центр Министерства внутренних дел Российской Федерации»;

ИБД-Ф − интегрированный банк данных федерального уровня;

ИБД-Р − интегрированный банк данных регионального уровня;

ИЦ – информационный центр;

ИС ЕРДР − информационная система «Единый реестр досудебных расследований»;

ИМТС − «Интегрированная мультисервисная телекоммуникационная система»;

УПК РК – Уголовно-процессуальный кодекс Республики Казахстан;

СТРАС ОПС − Специализированная территориально распределенная автоматизированная система органов предварительного следствия;

МСПД «Дионис» − магистральная система передачи данных «Дионис»;

НЦИП США − национальный центр информации о преступности США;

ЭП − электронная подпись.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Постановлением Правительства Российской Федерации от 27.12.2012 № 1406 (с изменениями на 29.12.2020)[1] утверждена федеральная целевая программа «Развитие судебной системы на 2013−2024 годы», основной идеей которой является модернизация системы посредством создания мобильного электронного правосудия, а также формирования электронных дел и электронного архива, что позволит, по мнению законодателя, обеспечить доступ граждан к правосудию, а также качественную и эффективную работу судов.

Минюстом России в соответствии с пунктом 28 дорожной карты реализации целевой модели суперсервиса «Правосудие онлайн» федерального проекта «Цифровое государственное управление» национальной программы «Цифровая экономика Российской Федерации», утвержденной протоколом Президиума Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности от 21.09.2020 № 20, разрабатывается законопроект, направленный на унификацию правил дистанционного обращения в суд в электронном виде, дистанционного получения информации о начавшемся судебном процессе, дистанционного доступа к материалам электронных дел, включая получение судебных актов или их копий в электронном виде, а также дистанционного участия в судебных заседаниях.

В рамках проводимой работы предполагается применение комплексного подхода в регулировании вопросов использования дистанционных технологий, включающего досудебную и судебную стадию уголовного судопроизводства.

Обозначая понятия «электронный документ», «электронная подпись» и «электронный образ уголовного дела», мы можем констатировать тот факт, что основной кодифицированный нормативный правовой акт, регулирующий порядок уголовного судопроизводства на территории России (УПК РФ), не дает нам разъяснений по данному вопросу, что, по нашему мнению, является неприемлемым.

Однако в некоторых нормативных правовых актах мы можем встретить различные варианты определений обозначенных выше понятий.

Так, под электронным документом согласно приказу Судебного департамента при Верховном Суде РФ от 27.12.2016 № 251[2] стоит понимать

---

[1] О федеральной целевой программе «Развитие судебной системы России на 2013−2024 годы : постановление Правительства РФ от 27.12.2012 № 1406 (ред. от 29.12.2020) [Электронный ресурс]. – URL: http://consultant.ru (дата обращения: 06.03.2021).

[2] Об утверждении Порядка подачи в федеральные суды общей юрисдикции документов в электронном виде, в том числе в форме электронного документа : приказ Судебного департамента при Верховном Суде РФ от 27.12.2016 № 251 (ред. от 05.11.2019) [Электронный ресурс]. – URL: http://consultant.ru (дата обращения: 06.03.2021).

документ, который был создан в электронном формате без его предварительного документирования на бумажный носитель и подписан электронной подписью. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», употребляя словосочетание «электронный документ», предлагает нам определять его как «документированную информацию, представленную нам в пригодном для восприятия электронном виде с использованием электронных вычислительных машин». В Регламенте удостоверяющего центра Евразийской экономической комиссии сказано, что электронным документом стоит считать документ, составленный в электронном виде (отвечающий требованиям общей инфраструктуры документирования информации) и заверенный электронной подписью[3]. В Федеральном законе от 06.04.2011 № 63-ФЗ (ред. от 08.06.2020) «Об электронной подписи» сказано, что «информация в электронной форме, подписанная квалифицированной электронной подписью, признается электронным документ»[4]. В ГОСТ Р 7.0.8-2013 термин «электронный документ» обозначен как «информация, представленная в электронной форме»[5]. Одни ученые, говоря об электронном документе, определяют его как «документ, созданный в цифровой форме»[6], другие − как «документ, созданный без предварительного документирования на бумажном носителе»[7].

Вопросы обеспечения безопасности служебной информации ограниченного распространения на сегодняшний день являются объектом большого количества исследований и отличаются высокой полемичностью среди специалистов. Вызвано данное положение дел прежде всего отсутствием должного закрепления указанной категории информации в законодательстве Российской Федерации[8].

Досудебное производство в электронном формате предусмотрено уголовно-процессуальным законодательством в США, Канаде, Эстонии,

---

[3] п. 1.6.1 Регламента удостоверяющего центра Евразийской экономической комиссии (приложение к Положению об удостоверяющем центре Евразийской экономической комиссии, утв. решением Коллегии Евразийской экономической комиссии от 09.07.2018 № 110) [Электронный ресурс]. – URL: http://consultant.ru (дата обращения: 10.03.2021).

[4] Об электронной подписи : федеральный закон от 06.04.2011 № 63-ФЗ (ред. от 08.06.2020) (с изм. и доп., вступ. в силу с 01.01.2021) [Электронный ресурс]. – URL: http://consultant.ru (дата обращения: 06.03.2021).

[5] ГОСТ Р 7.0.8-2013. Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Делопроизводство и архивное дело. Термины и определения : утв. приказом Росстандарта от 17.10.2013 № 1185-ст. // [Электронный ресурс] – URL: http://consultant.ru (дата обращения: 06.03.2021).

[6] Янковая В. Ф. Понятия «электронный документ» и «архивный электронный документ» // Делопроизводство. − 2019. − № 3. − С. 10−16.

[7] Ульянцева С. Э., Скрипко Е. А. Основы методологии управления документами // Делопроизводство. − 2020. − № 1. − С. 18−21; № 2. − С. 30 − 36.

[8] Нестеровский О. И., Филиппова Н. В. Правовое обеспечение информационной безопасности : учебное пособие [Электронный ресурс]. – Электр. дан. и прогр. – Воронеж : Воронежский институт МВД России, 2019.

Швеции, Дании, Нидерландах, Сингапуре, Южной Корее, Италии, Испании, ФРГ и других странах. Изучим зарубежный опыт формирования массива статистической информации из материалов электронных образов уголовных дел более подробно.

ГЛАВА 1. ИЗУЧЕНИЕ ЗАРУБЕЖНОГО ОПЫТА ПРАВОВОГО РЕГУЛИРОВАНИЯ СОЗДАНИЯ ЭЛЕКТРОННЫХ ОБРАЗОВ УГОЛОВНЫХ ДЕЛ В СФЕРЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ТЕХНИЧЕСКИХ СРЕДСТВ, ИСПОЛЬЗУЕМЫХ ДЛЯ СОЗДАНИЯ ЭЛЕКТРОННЫХ ОБРАЗОВ УГОЛОВНЫХ ДЕЛ, С ОДНОВРЕМЕННОЙ ОЦЕНКОЙ ДОПУСТИМОСТИ РАСПРОСТРАНЕНИЯ ТАКОГО ОПЫТА НА ТЕРРИТОРИИ РОССИЙСКОЙ ФЕДЕРАЦИИ С УЧЕТОМ ТРЕБОВАНИЙ ОТЕЧЕСТВЕННОГО ЗАКОНОДАТЕЛЬСТВА

№	*Государство*	*Программное обеспечение*
1	*Соединенные Штаты Америки (США)*	*Программное обеспечение включает две подсистемы «Управление делами или Электронный Архив дел» (Case Management/Electronic Case Files (CM/ECF)) и «Открытый доступ к судебным электронным отчетам» (Public Access to Court Electronic Records). Подсистема CM/ECF состоит из двух компонентов: Управление делами (CM) и Электронный Архив Дел (ECF). Подсистема CM/ECF написана с использованием языков программирования Perl и Java для работы под операционной системой Solaris или Red Hat Linux с возможностью развертывания веб-сервера Apache. Система »Открытый доступ к судебным электронным отчетам» является дополнением к CM/ECF. Она позволяет пользователям получать доступ к электронным файлам дел, созданным с использованием CM/ECF. Каждый суд имеет собственные ресурсы для электронного хранения, но открытый доступ к файлам дел обеспечивается централизованно через общую систему доступа.*
2	*Канада*	*В судебной системе Канады используется программное обеспечение e-court, включающее две системы, как и в США, а также активно применяются web-технологии, которые сочетают онлайн-платформы (The Civil Resolution Tribunal (CRT) − первый канадский онлайн-трибунал), с возможностью использования телефона, видеоконференций, почты и в некоторых случаях личных встреч для разрешения мелких претензий.*
3	*Сингапур*	*Электронная система правосудия (Electronic Filing System – EFS. Электронная система состоит из следующих компонентов:* *– Программа, установленная на компьютер юридической фирмы, которую можно скачать с официального веб-сайта системы, если адвокатская фирма зарегистрирована для участия в ней. Данная оболочка обеспечивает пользователя образцами и формами для заполнения документов, необходимых в судебном разбирательстве, позволяет прикрепить отсканированные (в формате PDF) документы к делу;* *– серверное программное обеспечение, позволяющее осуществлять коммуникации между судом и адвокатом, отслеживать поступление пошлины за рассмотрение дела;*

		– программное обеспечение, установленное на компьютер судьи, которое обеспечивает судебный процесс, направляет его ход через все стадии судопроизводства. *– Отдельная система электронных сертификатов, выдаваемых юридическим фирмам, которая позволяет отслеживать и идентифицировать отправителя документов.*
4	*Бельгия*	*Программное обеспечение Phenix, функционирующее на использовании web-технологий, основными компонентами которого являются:* *– система электронных ящиков (e-Box) для уведомлений и сообщений и подачи заявлений;* *– система электронного хранения (e-Deposit) для подачи заключений, представлений и доказательств по гражданским и уголовным делам;* *– система аутентификации пользователей (eID).*
5	*Италия*	*Система электронного гражданского процесса Processo Civile Telematico. Электронные документы, подписанные ЭП, пересылаются посредством сертифицированной системы электронной почты «Пек». Система PolisWeb позволяет получать информацию о гражданских исках, арбитражных делах и т.д. Судебные дела в Processo Civile Telematico ведутся в цифровой папке. Она содержит и направленные по почте электронные документы, и принятые судом акты. Доступ к Processo Civile Telematico пользователь получает через сертифицированный электронный адрес. Это дает возможность направлять электронные запросы и получать виртуальные консультации по исковым документам, судебным решениям.* *SICP (Sistema Informativo della Cognizione Penale) – цифровая платформа уголовного судопроизводства, включающая следующие элементы:* *– веб-сайт для подразделений полиции;* *– программное обеспечение для ведения реестра уголовных дел, мониторинга процессуальных сроков, формирования процессуальных документов;* *– серверное программное обеспечение для ведения базы данных досудебных мер процессуального принуждения.*
6	*Германия*	*Программное обеспечение «Электронный судебный и административный почтовый ящик» (EGVP), включающее в себя подсистему обеспечения безопасного и конфиденциального документооборота, а также систему информационных судебных ресурсов (платный личный кабинет, официальные сайты судов), реализованных на основе web-технологий. Программное обеспечение EGVP основано на клиентском ПО OSCI Governikus Communicator от Governikus и разработано с использованием языка программирования Java.*
7	*Чешская Республика*	*Программный комплекс электронных баз данных по уголовным делам «Электронное уголовное судопроизводство», к которому имеют доступ сотрудники полиции, прокуратуры и судов. Программный комплекс включает в себя:*

		− серверное программное обеспечение, обеспечивающее эффективное функционирование электронных баз данных; *− программное обеспечение, предназначенное для организации безопасного и конфиденциального документооборота;* *− клиентское программное обеспечение, установленное на компьютеры сотрудников полиции, прокуратуры и судов.*
8	*Испания*	*Программное обеспечение Justicia Digital, состоящее из приложений:* *LexNet − платформа для безопасного обмена информацией между судебными органами и органами предварительного расследования;* *Minerva Digital – программное обеспечение для управления электронным уголовным делом и мониторингом его движения между инстанциями судопроизводства;* *Horus − программное обеспечение для просмотра документов (файлов);* *Portafirmas − программное обеспечение для электронной подписи документов;* *Archivo − архивная система;* *Wasmin и Cargador − технологические шлюзы для организации взаимодействия внешних систем с Minerva Digital.*
9	*Китайская Народная Республика*	*Программное обеспечение, включающее в себя комбинацию web-технологий и программно-технических комплексов:* *− интернет-портал по приему сообщений о преступлениях в цифровом виде – «cyberpolice»;* *− программно-аппаратные комплексы по:* *а) формированию материалов уголовного дела в цифровом виде;* *б) обработке и обмену несекретной информациией;* *в) проведению видеоконференц-связи;* *− интеллектуальную систему судебного разбирательства, сотоящую из компонентов: регистрация дела, судебное разбирательство и решение. Функционирование данной системы основано на работе информационных платформ, которые позволяют :* *а) генерировать электронные досье с делом;* *б) добавить материалы к облачному кабинету;* *в) выполнить интеллектуальную транскрипцию судебных заседаний;* *г) составить флип-лист электронного перекрестного допроса, а также оформить судебные документы;* *− единую платформу народной судебной блокчейн-конвенции для распределенного хранения и борьбы с подделками доказательств (технология блокчейн);* *− Шанхайскую интеллектуальную вспомогательную систему по рассмотрению уголовных дел с использованием возможностей искусственного интеллекта.*

Опыт США

Первые шаги по введению электронного документооборота в уголовном судопроизводстве в США были предприняты довольно давно. Еще в 1997 г. сотрудниками Административного управления судов среди работников судебной системы, прокуроров, адвокатов и других причастных к ее функционированию лиц, была проведена разъяснительная работа и инициировано обсуждение проектов введения электронного документооборота, практики применения его отдельными судами, выработки общих подходов и общих стандартов его осуществления. В качестве целей указанных реформ назывались: обеспечение доступа граждан к материалам рассматриваемых дел, сокращение сроков их рассмотрения; облегчение работы персонала судов, экономия затрат и повышение производительности труда и эффективности использования персонала, помещений и других ресурсов, снижение затрат на обработку, хранение и копирование документов, упрощение планирования работы судов и составления статистической отчетности и др.[9]

Стоит сказать, в что в США отсутствует единая, общенациональная уголовноправовая система и обусловлено это особенностями федерализма[10].

Действующая в США система электронного документооборота в максимальной степени приспособлена к особенностям американского судопроизводства. Специфической чертой американского уголовного судопроизводства является отсутствие процессуально регламентированной стадии досудебного производства и уголовного дела в российском его понимании, границы между следствием и оперативно-розыскной деятельностью и, что еще более важно, обязательных требований к соблюдению письменной процессуальной формы доказательств как гарантии их допустимости.

Уголовно-процессуальное законодательство США не предполагает наличия единого уголовного дела, в котором сосредоточены все материалы в подшитом и пронумерованном виде. На бумажном носителе информации представлены лишь сведения о лице, совершившем преступление, данные о потерпевшем и движение уголовного дела. Собирание доказательств

[9] Electronic case files in the federal courts: A Preliminary Examination of Goals, Issues, and the Road Ahead Discussion Draft. Administrative Office of the United States Courts. March, 1997.

[10] К источникам регламентирующим порядок электронного правосудия в США относятся: Конституция США, акты Конгресса (касающиеся вопросов судопроизводства в федеральных судах и включенные в Свод законов США), акты Конгресса по делегированию Верховному Суду США права устанавливать нормы уголовного судопроизводства, федеральные правила уголовного судопроизводства, федеральные правила апелляционного производства, нормы судебного разбирательства федеральными магистратами дел о малозначительных преступлениях, федеральные правила о доказательствах и некоторые другие (принятые Верховным Судом США и вошедшие в Свод законов США), правила уголовного судопроизводства (устанавливаемые нижестоящими федеральными судами и действующие только в этих судах). К источникам уголовно-процессуального права штатов относятся конституции штатов, соответствующие разделы сводов законов.

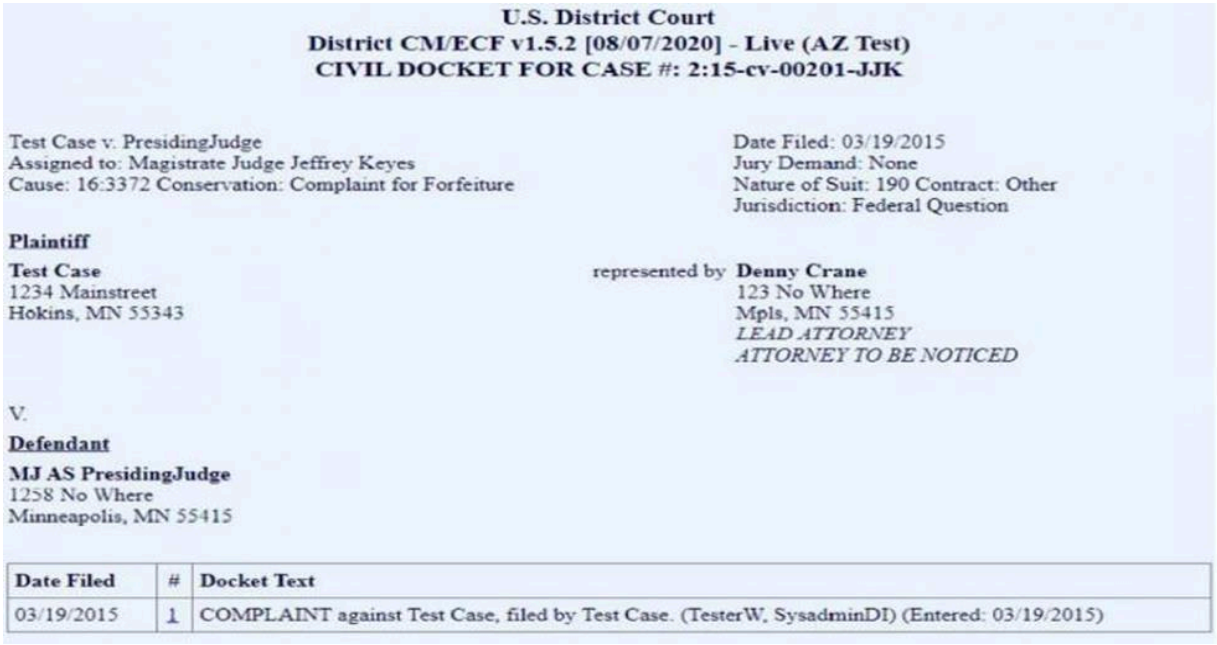
осуществляется как стороной обвинения, так и стороной защиты, на равных условиях[11].

Документирование мероприятий, осуществляемых в ходе расследования, выполняется традиционным для полиции способом − посредством записей (notes) и отчетов (reports). Согласно п. 14 разд. 725.15 Кодекса Департамента полиции Милуоки, офицеры, получившие сообщение о происшествии, должны полно и точно отмечать в записных книжках все, что ими обнаружено по прибытии на место (собрать досье). Эти записи в дальнейшем используются лицом, проводящим расследование, для составления итогового отчета. Все сотрудники, работавшие на месте происшествия, также составляют отчеты, отражающие выполненную ими работу и ее результаты (п. 4 разд. 725.20), в том числе обнаружение улик (п. 7 разд. 725.25)[12], после этого все собирается воедино.

Доказательства представляются сторонами в электронном виде по сети Интернет прямо в административный аппарат судов, где они регистрируются и приобщаются к материалам электронного уголовного дела, которое ведется с использованием специализированной системы электронного документооборота CM/ECF (Case Management and Electronic Case Files) − это система управления делами и электронной судебной регистрации для большинства федеральных судов США. Стоит отметить, что каждому делу, загруженному в эту систему, присваивается номер в формате *D: YY-TT-SSSSS*, где D = офис отдела (большинство районов делятся на подразделения), YY = год, TT = тип (например, bk = банкротство, cv = гражданское, cr = уголовное), SSSSS = порядковый номер. Номер дела не содержит идентификатора суда (рис.1). Основной список дела − это досье. Лист досье содержит хронологический список каждой регистрации и любых связанных документов (в формате PDF) по делу.

[11] Ищенко П. П. Современные подходы к цифровизации досудебного производства по уголовным делам // lex russica. − 2019. − № 12. − С. 68−79.

[12] Глушков М. Р. Документирование полицейского расследования в США // Право : журнал Высшей школы экономики. − 2016. − № 2. − С. 212–222.



U.S. District Court
District CM/ECF v1.5.2 [08/07/2020] - Live (AZ Test)
CIVIL DOCKET FOR CASE #: 2:15-cv-00201-JJK

Test Case v. PresidingJudge
Assigned to: Magistrate Judge Jeffrey Keyes
Cause: 16:3372 Conservation: Complaint for Forfeiture

Date Filed: 03/19/2015
Jury Demand: None
Nature of Suit: 190 Contract: Other
Jurisdiction: Federal Question

Plaintiff

Test Case
1234 Mainstreet
Hokins, MN 55343

represented by **Denny Crane**
123 No Where
Mpls, MN 55415
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

V.

Defendant

MJ AS PresidingJudge
1258 No Where
Minneapolis, MN 55415

Date Filed	#	Docket Text
03/19/2015	1	COMPLAINT against Test Case, filed by Test Case. (TesterW, SysadminDI) (Entered: 03/19/2015)

Рисунок 1 − Образец судебного дела

Чтобы представить суду доказательства, участник уголовного процесса просто размещает их в виде файла в соответствующее уголовное дело − папку на сайте суда. Все документы должны быть представлены в формате PDF, не допускающем внесения изменений в их содержание. Бумажные документы должны быть отсканированы и сохранены в указанном формате. Система обеспечивает доступ к материалам дела для ознакомления широкому кругу лиц, вовлеченных в судопроизводство, и сохранность содержащихся в них персональных данных свидетелей и потерпевших.

Непосредственно порядок представления оценки электронным доказательствам по делу, признания их достоверными и допустимыми, несмотря на существование законодательного акта, в США осуществляется очень детально на основании судебно-прецедентной практики. Как свидетельствуют научные источники, еще в 1970-х годах у судей США возник вопрос, касающийся допустимости доказательства: является ли оригиналом распечатанный электронный документ, созданный с помощью электронной вычислительной машины. В процессе правоприменения суды США отошли от формального подхода к этому вопросу и признали, что поскольку информация, выводимая с помощью ЭВМ, человеком воспринимается визуально или аудиально, то такая информация фактически является письменным доказательством и отвечает критерию допустимости как доказательство. То есть сегодня у судов США не возникает вопроса о том, является ли то или иное электронное доказательство оригиналом или копией, поскольку такая идентификация потеряла смысл. Такой подход судов США значительно упростил процесс признания электронных доказательств в деле допустимыми и способствовал достижению цели гражданского процесса − защиты нарушенных прав, свобод и интересов граждан.

Основная цель системы CM/ECF − выполнить юридические обязательства секретаря суда как хранителя судебных материалов.

Все документы, которые загружаются в эту систему, необходимо подавать в формате PDF. Другие типы файлов могут быть инкапсулированы внутри файлов PDF, например аудиофайлы в формате MP3 или видеофайлы. Загруженные файлы проверяются в соответствии с требованиями, каждый суд устанавливает свой срок подачи документов в данном формате.

Система CM/ECF работает как автоматизированный служащий суда для получения судебных документов и предоставления онлайн доступа к судебным заявлениям, ходатайствам, объяснениям сторон и иным документам по делу, подаваемым сторонами и юристами. CM/ECF предусматривает возможность поиска материалов судебного дела и документов в базе данных, исходя из номера и статуса дела, даты подачи, существа дела, наименования стороны и др.

Работающая как вэб-приложение, система CM/ECF является децентрализованной − каждый федеральный суд управляет своим приложением CM/ECF, используя свои собственные серверы.

Для получения доступа к этой системе сотрудники полиции, прокуроры и адвокаты должны зарегистрироваться на специальном сайте, предоставляющем публичный доступ к электронным документам дел, находящихся в производстве судов (Public Access to Court Electronic Records − PACER) или на сайтах конкретных судов, рассматривающих дело[13].

Приводимый в действие программой электронного открытого доступа Административного Офиса Судов США PACER является сервисом открытого электронного доступа, который позволяет пользователям получать сведения о судебных делах и материалы судебных дел из федеральных судов.

Система PACER предлагает:

1) 24-часовой доступ к документам дела через интернет;

2) возможность скачивать и распечатывать документы непосредственно из суда;

3) одновременный доступ к файлу дела несколькими лицами (сторонами).

PACER предлагает «экран запроса» (рис. 2, 3), через который пользователь может получить доступ к досье дела, содержащий:

1) перечень всех сторон и иных лиц, участвующих в деле (включая судей, юристов, поверенных);

2) сведения о деле (например, номер дела, суть иска, требуемая сумма);

3) хронологию событий по делу;

4) реестр исков (журнал регистрации поступивших требований);

5) ежедневное перечисление новых дел;

6) решения апелляционных судов;

7) решения и сведения о статусе дела;

8) формы документов, поданных по отдельным делам.

[13] Ищенко П.П. Современные подходы к цифровизации досудебного производства по уголовным делам // Lex russica. − 2019. − № 12. − С. 68−79.

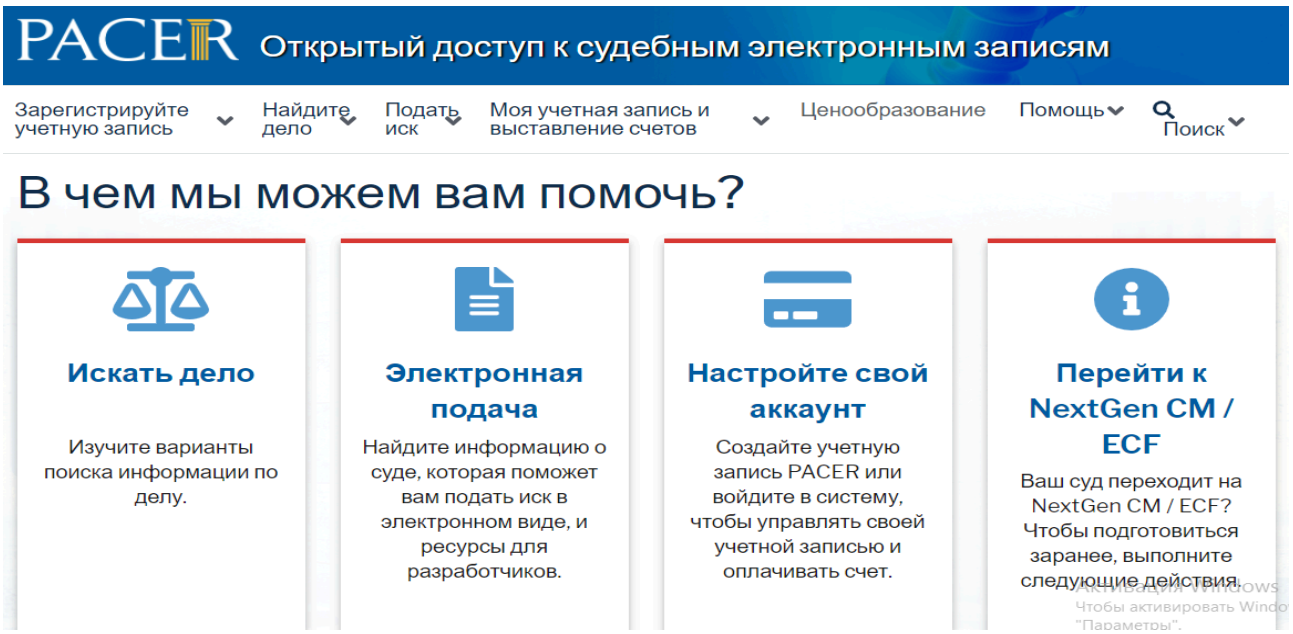


Рисунок 2 – Public Access to Court Electronic Records – PACER

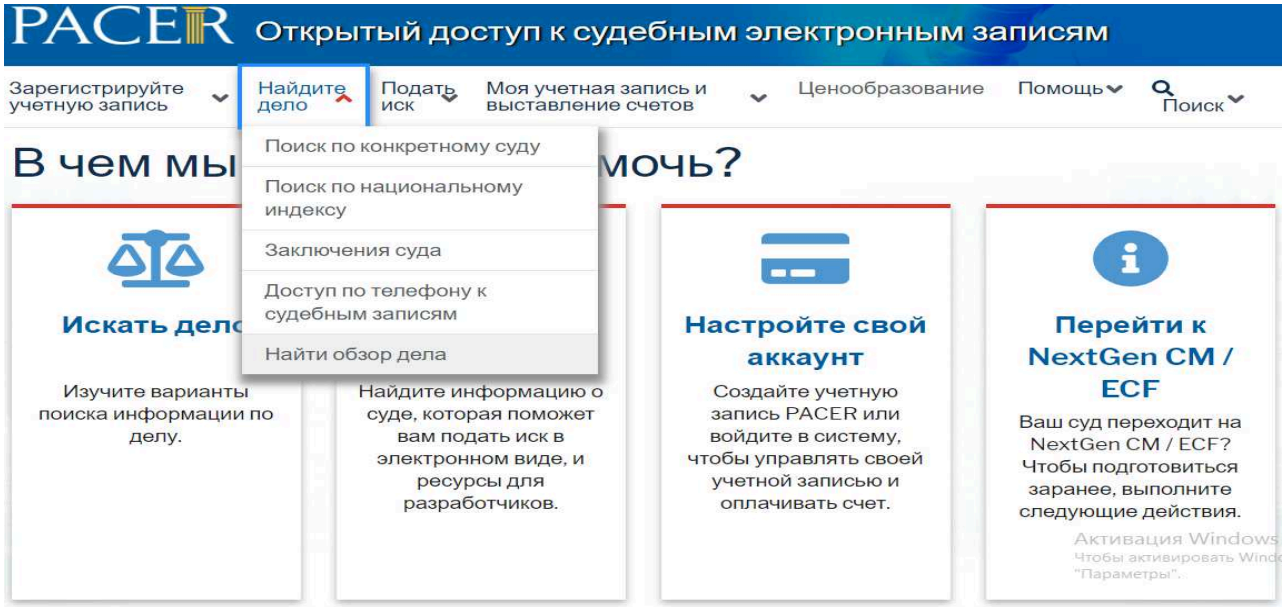


Рисунок 3 – Public Access to Court Electronic Records – PACER (поисковик)

Стоит отметить, что в системе PACER заложена возможность поиска информации по наименованию сторон, юристам либо судьям, номеру социального страхования (SSN) стороны, номеру дела или дате подачи документа.

Результат предоставляемой информации зависит от параметров поиска, либо от досье дела и судебных постановлений. Получаемая из PACER информация может быть просмотрена, скопирована (информация может сохраняться в формате HTML, plaint text либо ascii DOS file. В иных случаях информация может быть «вырезана и вставлена» в текстовое приложение), распечатана либо загружена на компьютер пользователя.

Каждый федеральный суд поддерживает базу PACER в отношении сведений по делам, находящимся в его юрисдикции. Каждый суд имеет собственный Унифицированный Локатор Ресурсов (URL). Множество параметров сведений, установленных в системе PACER по каждому суду, передается каждый вечер в U.S. Party/Case Index (указатель сторон/дел), находящийся в сервисном центре PACER в Сан Антонио, Техас.

Перед собой мы поставили вопрос: **«Какое оборудование и программное обеспечение необходимо для хранения документов в системах CM/ECF?»** Проанализировав данные, мы пришли к выводу, что для подачи документов в электронные системы подачи документов CM/ECF требуется следующее оборудование и программное обеспечение:

1) Персональный компьютер под управлением стандартной платформы, такой как Windows.

2) Текстовый процессор, совместимый с PDF, например Corel WordPerfect или Microsoft Word.

3) Интернет-служба.

4) Веб-браузер. Для CM/ECF рекомендуются последние версии Mozilla Firefox или Microsoft Internet Explorer. Некоторые пользователи имели положительный опыт работы с другими веб-браузерами, но перечисленные здесь были протестированы и сертифицированы на совместимость с CM/ECF.

5) Для апелляционного CM/ECF пользователям потребуется подключаемый модуль Java 1.6.

6) Программное обеспечение для преобразования документов из формата текстового процессора в формат переносимого документа (PDF). Corel WordPerfect и Microsoft Word могут конвертировать документы в PDF, или можно использовать дополнительный продукт, например Adobe Acrobat.

7) Сканер документов, если сторонам судебного процесса необходимо создать PDF-изображения документов, которые они хотят подать, используя CM/ECF.

Опыт Канады

Одними из первых электронное уголовное дело ввели в Канаде. Первые дискуссии относительно введения подобного способа судопроизводства стали возникать еще в самом начале XXI века. Основными аргументами стали достаточная развитость информационного обеспечения в государственных органах, позволяющая вести электронный документооборот, необходимость сбережения природных и временных ресурсов, а также возможность быстрой передачи документа, что весьма затруднительно для Канады с ее территориями.

Отличительная особенность применения электронного уголовного дела в Канаде заключается в том, что исполнительные и судебные органы каждой провинции выбирали, стоит ли осуществлять применение электронного уголовного дела. В настоящее время лишь провинции Квебек, Манитоба не используют электронную систему подачи документов. В остальных девяти

провинциях система электронного уголовного дела активно функционирует начиная с 2008 года.

Верховный суд Канады в своем руководстве Guidelines for Printed and Electronic Versions of Appeal Documents установил требования для уголовных дел, переданных в суд в формате электронного документа[14]. В частности, документ обязан иметь разрешение PDF (как и в США), при этом электронная версия не должна отличаться от бумажного варианта. При расхождении в содержимом печатная версия считается официальной и верной. При этом электронная версия не требует наличия подписей, в отличие от печатных оригиналов, для которых их наличие обязательно.

Электронное уголовное дело записывается на CD-ROM диск, который почтовым сообщением или курьерской службой направляется в судебное учреждение. Передача электронного уголовного дела через e-mail или через сеть Интернет запрещена в связи с соображениями безопасности и возможности хищения данных злоумышленниками. На диск наклеивается пояснительная надпись с указанием стороны, подающей документы, и номера дела. К направляемым документам прилагается специальная форма Electronic Filing Form, которая предусмотрена Верховным судом Канады.

Стоит отметить, что Федеральному суду Канады систему электронной подачи документов оформила Lexis-Nexis Canada. Согласно данному соглашению, в целях безопасности данная система предусматривает использование счета для просмотра электронного уголовного дела пользователя и пароля, предоставляемого провайдером. Подача документов в Федеральный суд Канады осуществляется согласно официальному уведомлению Notice to the Profession[15].

Для каждой провинции существует своя система принятия электронного уголовного дела. К примеру, в Британской Колумбии для подачи электронных документов сторонам процесса необходимо зарегистрироваться в «Судебном онлайн сервисе» или сервисе «Британская Колумбия онлайн», согласиться с условиями соглашения пользователя, а также иметь регистрационную карту, в которой указан счет пользователя.

В судебной системе провинции Альберта действует система электронной подачи документов, при этом ее использование не является обязательным, за исключением апелляционного производства. Документы в рамках электронной апелляции, именуемой e-appeals, подаются через сайт Апелляционного суда в формате WordPerfect или Word 97. Апелляционное производство в провинциях Новая Шотландия и Остров принца Эдуарда также требует электронного документооборота – апелляционное досье и материалы

[14] Supreme Court of Canada - Guidelines for Preparing Documents to be Filed with the Supreme Court of Canada (Print and Electronic) (scc-csc.ca) [Электронный ресурс]. – URL: https://scc-csc.ca/parties/gl-ld2021-01-27-eng.aspx.

[15] Notices to the Profession & Public (albertacourts.ca) [Электронный ресурс]. – URL: https://www.albertacourts.ca/qb/resources/notices-to-the-profession-public.

дела отсылаются в электронном виде наряду с бумажными копиями в формате WordPerfect.

В провинции Ньюфаундленд правило 5А Ньюфаундлендских судебных правил допускает электронную подачу некоторых документов. При этом в документах должна присутствовать электронная подпись. Однако в судах Ньюфаундленда система электронной подачи мало практикуется.

Примечательно, что самая крупная провинция Канады − Квебек − отказывается от электронного уголовного дела по весьма специфичной причине. В соответствии с законодательством провинции любые электронные страницы, документы, файлы должны быть составлены как на английском языке (официальным на всей территории Канады), так и на французском (который признается вторым официальным в Квебеке). В связи с этим материалы уголовного дела должны быть переведены на второй язык (на практике – на французский), на что требуется достаточно много времени.

Опыт Китайской Народной Республики

Внедрение современных информационных технологий в деятельность правоохранительных органов КНР относится к задачам общегосударственных масштабов.

Предпосылкой для внедрения информационных технологий в уголовно-процессуальную деятельность органов предварительного расследования КНР послужило разъяснение, данное Министерством общественной безопасности 29 декабря 2015 года, «Об изменении и совершенствовании процедуры возбуждения уголовного дела». В данном ведомственном акте особое внимание уделено необходимости широкого использования информационно-телекоммуникационной сети Интернет для приема и регистрации сообщений и заявлений о преступлениях правоохранительными органами КНР. Возможность приема сообщения о преступлении посредством сети Интернет была впоследствии закреплена и в иных нормативных актах, регламентирующих уголовно-процессуальную деятельность (ст.108 УПК КНР, ст.166 Приказа Министерства общественной безопасности КНР № 127 «О процессуальных требованиях расследования уголовного дела органами общественной безопасности», ст.ст. 157−160 Правил применения норм УПК КНР Народной прокуратурой).

Вышеперечисленные нормативные правовые акты регламентируют порядок обработки и регистрации принятого сообщения о преступлении в электронном виде. Кроме того, регламентируется порядок ведения информационных баз данных в режиме онлайн, а также определяются методы автоматического приема и контроля аудиовизуальных данных и электронных данных обратившихся граждан. В деятельности правоохранительных органов КНР также предусмотрен порядок присвоения уникального

идентификационного номера заявлению гражданина, по которому впоследствии заявитель может контролировать ход и результаты производимой проверки посредством использования специализированного ведомственного портала в сети Интернет.

Таким образом, китайский законодатель достаточно эффективно обеспечил реализацию прав граждан на доступ к информации о ходе и результатах рассмотрения заявления о преступления, предоставив тем самым заявителю возможность своевременно обращаться в контролирующие и надзирающие органы по поводу его нарушенных прав и законных интересов в результате незаконных решений или действий (бездействия) должностных лиц, осуществляющих соответствующую проверку поданного заявления.

Следует отметить, что аналогичные формы контроля заявителем хода проверки сообщения о преступлении посредством современных информационно-телекоммуникационных технологий предусмотрены также в таких странах, как Испания, Италия и Федеративная Республика Германия.

Процесс цифровизации в уголовно-процессуальной деятельности органов правопорядка КНР начал зарождаться еще в 2004 году, когда организацией «Общество Интернета Китая» при непосредственном участии Пресс-канцелярии Госсовета КНР была создана группа приема сообщений о нарушениях закона. В продолжение развития данной идеи органами правопорядка КНР в 2015 году создан интернет-портал по приему сообщений о преступлениях в цифровом виде – «cyberpolice» (http: // www.cyberpolice.cn /wfjb). Правовой основой функционирования портала выступили Решения Постоянного комитета Всекитайского собрания Народных представителей по обеспечению безопасности в сети Интернет, УК КНР, Закон КНР «О методах регулирования информационного обслуживания сети Интернет».

В марте 2016 года Верховный народный прокурор КНР Цао Цзяньминь поставил задачу активизировать разработку еще 6 программно-аппаратных комплексов, в том числе комплексов по формированию материалов уголовного дела в цифровом виде с возможностью совершения процессуальных действий, связанных с согласованием процессуальных действий и решений с надзирающим прокурором и контролирующими органами, посредством телекоммуникационных технологий.

В целях оптимизации порядка досудебного производства по уголовным делам с 1 января 2018 года Верховная прокуратура КНР начала внедрение в деятельность органов предварительного расследования мобильного программно-аппаратного комплекса для обработки и обмена несекретной информации. Данный комплекс представляет собой совокупность мобильных приложений для цифровой обработки процессуальных документов, проведения следственного действия – допроса, направления на имя руководителей организаций, учреждений запросов о предоставлении информации, а также проведения видеоконференцсвязи с сотрудниками, оказывающими содействие в ходе предварительного расследования.

На сегодняшний день система электронных образов уголовных дел в КНР интегрирована с электронными системами народных судов, в том числе в части отражения по уголовным делам статистической информации. Так, в связи с нарастающей тенденцией перехода к электронному правосудию в последнее время были приняты следующие нормативные акты:

− Регламент Верховного народного суда КНР «О некоторых вопросах аудио- и видеозаписи судебных заседаний народных судов КНР» (2017) № 5 от 22.02.2017 года;

− Уведомление Верховного народного суда КНР «О дальнейшем ускорении создания и углубленного исследования процессов автоматической генерации электронного архива» (2018) № 21;

− Регламент Верховного народного суда КНР «О некоторых вопросах рассмотрения дел интернет-судами» (2018) № 16 от 03.09.2018;

− Уведомление Верховного народного суда «Об усилении и стандартизации онлайн-судопроизводства в условиях профилактики и контроля распространения эпидемии COVID-19» (18.02.2020).

Опыт Сингапура

Развитие электронного уголовного судопроизводства в таком государстве, как Сингапур, было обусловлено необходимостью создания прозрачной, беспристрастной судебной системы. В этой связи основной акцент в цифровизации правосудия государством был сделан на деятельности судов, рассматривающих уголовные дела по существу. Вопрос формирования электронных макетов уголовных дел на досудебном производстве в Сингапуре носит вторичный характер, подчиняясь в основном интересам открытости судебной системы. Следует подчеркнуть, что система формирования электронного уголовного дела в Сингапуре строится на принципах анализа искусственным интеллектом данных по уголовному делу с формированием возможных в конкретной ситуации процессуальных решений.

Так, в целях внедрения современных информационных технологий в уголовно-процессуальную деятельность судов были разработаны и впоследствии успешно внедрены следующие системы:

– LawNetLegalWorkbench, которая представляет собой массив справочно-правовой информации, позволяющей обеспечить интеллектуальный поиск по юридическим базам данных, в том числе с целью формирования и анализа судебной практики по отдельным категориям уголовных дел;

– база данных сотрудников судебных органов (JODB), которая содержит судебные рабочие документы и сборники, систему правил вынесения приговоров (SINGS), которая обеспечивает критерии вынесения приговора;

– система управления приоритетами ресурсов (IMPRESS), которая фиксирует все прошлые решения по делам, рассмотренным как в Верховном суде, так и подчиненными судами.

Электронное правосудие в Сингапуре в части организационно-правового обеспечения реализуется посредством:

– предоставления услуг и приложений для виртуальных судов;

– компьютеризации процессов управления делами;

– совместной разработки межведомственных систем;

– компьютеризации судебной администрации и корпоративных услуг.

Сингапур является одним из первых государств, которое стало предоставлять развернутые виртуальные судебные услуги для населения через мультимедийные приложения. В судах Сингапура впервые была применена процедура видеоконференции, являющаяся в настоящее время наиболее универсальной и продуктивной технологией, используемой в уголовном судопроизводстве.

Сингапур, затрагивая вопросы осуществления расследования, исходит из позиции, что надлежащее производство по уголовным делам является основополагающим для эффективной и действенной судебной системы. Электронное управление делами нашло свое отражение в первой волне компьютеризации страны и представлено следующими системами:

– система регистрации и информации по уголовным делам (в данной системе формируется основная информация по уголовному делу, в том числе о принятых процессуальных решениях, сроках, изъятых вещественных доказательства, избранных мерах пресечения и т.д.);

– система уведомлений о процессуальных нарушениях в ходе производства по уголовному делу (например, в части соблюдения процессуальных сроков, а также о поступивших жалобах на действия и решения органов расследования);

– система электронного документооборота между судами, правоохранительными органами и прокуратурой, которая позволяет обеспечить моментальную коммуникацию между ведомствами в целях координации совместных действий при производстве по уголовному делу.

Для управления процессуальным порядком производства по уголовным делам в июне 1999 г. внедрена система TICKS 2000. Система TICKS 2000 предоставляет онлайн интерфейсы для правоохранительных органов и для электронного обмена данными. Для иных заинтересованных участников процесса, если уголовное дело находится на рассмотрении в суде и они не имеют своих собственных систем управления делами, суды предоставляют удаленный доступ к TICKS 2000, чтобы они могли регистрировать и получать информацию о своих делах в онлайн режиме.

Система TICKS 2000 позволяет отправлять судебные и иные процессуальные документы в электронном виде с использованием электронных документов вместо бумажных.

Кроме того, электронная судебная система eLitigation доступна только юридическим фирмам и государственным организациям. Для входа потребуется полученный от государства электронный идентификатор SingPass. Через систему можно подавать электронные документы в суды; хранить, извлекать и обновлять материалы по делу; направлять судебные документы юридическим фирмам с помощью eService; получать уведомления и предупреждения, связанные с делами; создавать отчеты, искать оформленные дела с использованием быстрого доступа.

Есть возможность выбрать один из трех способов направления уведомлений другой юридической фирме:

1. Оформить и вручить – документ вручается только после того, как суд одобрит и ответит на принятый документ. Документы, во вручении которых суд откажет, получателю не направляются;

2. Немедленно оформить и вручить – документ вручается сразу же после подачи независимо от решения суда;

3. Отсрочить оформление и вручение – документ вручается в указанное время независимо от одобрения суда.

Безусловно, положительный опыт Сингапура направляет мировое сообщество к мысли о создании по-настоящему безбумажного электронного правосудия.

Опыт Бельгии

Однако встречаются и неудачные попытки перехода уголовного судопроизводства на электронный формат. Так, в 2005 г. в Бельгии был предпринят шаг к оцифровке правосудия путем введения системы Phenix. Предполагалось, что система Phenix повысит эффективность и результативность, а также упростит и ускорит процедуру расследования. Целью проекта системы Phenix было преобразование различных компьютерных систем органов расследования преступлений и судебной системы в структурированное, согласованное единое целое. Это был один из самых масштабных проектов, потому что система Phenix намеревалась оцифровать всю правовую систему сразу, однако по объективным причинам (большие финансовые затраты) было ясно, что это невозможно. В рамках реализации настоящей системы был продуман также порядок аутентификации пользователей, который включал в себя применение электронного паспорта (eID). Проект Phenix можно рассматривать как крупномасштабную, но неудачную попытку перехода стадии расследования от бумажного носителя в электронный формат. Несмотря на эту дорогостоящую неудачу, Бельгия продолжает пытаться привести в действие проект Phenix.

Phenix берет свое начало с 2001 года как проект внедрения систем электронного правосудия, основанный на принципах электронного наполнения дела с использованием стандартов открытых ресурсов. К 2008 году система была полностью развернута и используется не только как

средство электронного общения внутри судов, но, что более важно, как средство, представляющее новые возможности гражданам с целью упрощения процедуры обращения в суд и уменьшения судебных издержек. Данный проект скоординирован с подобными, внедренными в других европейских странах.

Компьютеризация судебного делопроизводства осуществлялась в Бельгии и ранее, но была несистемной. К моменту принятия акта о системе Phenix в судебной системе страны было более 10 000 пользователей, носителей трех национальных языков, использовались 13 различных приложений с более чем 100 банками данных, что не позволяло обмениваться электронными данными между судами, использующими различные системы.

Акт о системе Phenix, определяющий комплексное решение указанных проблем, был принят 10.08.2005. Им регулируются как внутренние (между судебными органами и органами прокуратуры), так и внешние (общение со сторонами дела, обществом, иными публичными сервисами, в том числе «электронный нотариат», электронные базы данных адресов и телефонов и т.п.) судебные коммуникации.

Система Phenix основывается на концепции электронного дела, которое начинает формироваться в момент подачи искового заявления и пополняется документами, передаваемыми суду в электронном виде сторонами. Каждый переданный в систему файл получает уникальный национальный идентификатор (номер). Судебные решения доступны только для сторон дела, но некоторые из них, без указания сторон, доступны для ознакомления любому пользователю и выступают в качестве примера разрешения конфликтов для общества. Особо следует отметить положение, согласно которому все протоколы передачи данных и форматы файлов должны использовать открытые стандарты, которые определены в акте о системе как стандарты, свободно и бесплатно доступные в сети Интернет и не имеющие легальных ограничений по их применению и использованию[16].

Бельгия, как и другие европейские страны, приняла концепцию электронного государства. Бельгийская стратегия электронного правительства имеет целью создание единой виртуальной публичной администрации, учитывающей особенности и компетенцию всех государственных органов. Данная концепция нацелена на внедрение информационно-коммуникационных технологий в публичное управление для улучшения координации между гражданами и органами государственной власти с целью демократизации технологий управления страной. Внедрение и использование информационных технологий достаточно трудоемкий процесс в таком комплексном публичном секторе как судопроизводство. Система электронного правосудия в Бельгии направлена на улучшение сотрудничества и интерактивного общения между судами, полицией, представителями и сторонами дела с целью упрощения передачи данных между ними, ускорения

[16] Гулемин А. Н. На пути к электронному государству : зарубежный и международный опыт электронного правосудия // DOI: 10.7256/1811-9018.2015.12.17059.

судебных процедур для обеспечения большей прозрачности в деятельности судебных органов, что является элементом, гарантирующим свободу доступа к правосудию всех граждан.

Внедрение системы позволило сторонам экономить время, единая централизованная система управления файлами позволила сократить издержки и пошлины, оплата которых также возможна посредством электронных переводов, любому гражданину, разместившему файлы в системе, обеспечен свободный доступ к ней.

В целом система обеспечивает 4 главных элемента:

– упрощенный обмен данными между судами;

– упрощенный обмен данными между сторонами, участвующими в процессе, вне зависимости от того, являются ли они профессиональными юристами или нет;

– обеспечение статистической информацией, использование системы в качестве архива документов;

– электронную регистрацию и передачу в нужную инстанцию документов, размещаемых в системе, с использованием электронной подписи, возможность осуществления электронных платежей[17].

Опыт Чешской Республики

В Чехии с 2005 г. также достаточно успешно развивается система электронных уголовных дел. На сегодня она представляет собой огромную и сложную систему электронных баз данных «Электронное уголовное судопроизводство». Эта система позволяет отслеживать движение всех уголовных дел, находящихся в производстве следователя, видеть все задачи, сроки рассмотрения и их статус. Кроме того, системой предусмотрена возможность онлайн согласования всех следственных действий и получения всех необходимых процессуальных решений. Лица, имеющие доступ к системе, могут видеть, как продвигаются конкретные уголовные дела, система может даже анализировать эффективность расследования дела. Также возможно экстраполировать статистические данные по уголовным делам из системы.

Опыт Федеративной Республики Германии

Страной, чей опыт использования электронного правосудия заслуживает особого интереса в рамках проводимого анализа, является Германия. Важнейшим инструментом, обеспечивающим функционирование электронного правосудия в Германии, является Электронный судебный и административный почтовый ящик (EGVP). Для использования этой системы

[17] Гулемин А.Н. На пути к электронному государству: зарубежный и международный опыт электронного правосудия // DOI: 10.7256/1811-9018.2015.12.17059.

пользователю необходимо установить на свой персональный компьютер специальную программу «Электронный судебный и административный почтовый ящик». Программа является абсолютно бесплатной и доступна для установки на официальных сайтах. Программа стала результатом успешной административной реформы и содействует осуществлению новых положений законодательства страны об электронном правосудии.

В соответствии с германским законодательством научно-технические средства связи должны обеспечивать эффективный документооборот правовой информации между населением и государственным аппаратом. Система EGVP предоставляет пользователям такие возможности, как круглосуточный доступ к информационным судебным ресурсам, надежная передача данных, защищенная связь с использованием криптографических механизмов, возможность электронной обработки файлов, получение автоматических уведомлений по электронной почте, поддержка всех аккредитованных карточек подписи. В целом такая электронная форма организации документооборота выступает в качестве дополнительной к обычной письменной форме.

Правила судопроизводства включают в себя квалификационные требования, направленные на обеспечение безопасности и прозрачности судебного процесса. Повышенная безопасность и конфиденциальность представления электронных сообщений требуют соответствующих технических и организационных мер в судах. Все документы, представленные в суд, должны быть заверены с использованием электронной цифровой подписи, она гарантирует подлинность ответственного лица и заменяет собственноручную подпись. Сайты германских судов наполнены необходимой информацией, которая помогает пользователю ознакомиться с правилами судопроизводства в каждом из них. Решения судов также публикуются на официальных сайтах и доступны для широкого круга.

Важно отметить, что Германия, практикуя электронные правовые ресурсы, имеет целью в первую очередь сделать правосудие доступным для всего населения и для каждого человека. Например, на сайтах судов и прочих правовых сайтах предоставленная информация изложена не на сложном «юридическом» языке, полном правовых и зачастую непонятных населению терминов, а на простом, доступном населению языке. Данный подход, несомненно, позволяет гражданам в полной мере осуществлять защиту собственных прав без привлечения правовой помощи извне. Помимо этого сайты содержат специальную информацию для людей с ограниченными возможностями, для них информация предоставляется в видеоматериалах, где коммуникация осуществляется посредством жестов.

Анализ услуг электронного правосудия в Германии позволяет сделать вывод, что его главным достижением является электронное управление документами. Отличительной чертой германского опыта является то, что эта страна очень аккуратно относится к процессу информатизации судопроизводства. Также Германия особое внимание уделяет вопросу

обеспечения безопасного и конфиденциального документооборота. Реформы в сфере электронного правосудия в Германии имеют приоритетной целью внедрение в него дополнительных протоколов безопасности и не подразумевают насыщения новыми электронными службами правосудия, широко используемыми в ряде других стран.

Правовая основа использования электронных документов в уголовном процессе Германии была заложена Законом от 1 апреля 2005 г. «Об использовании электронных форм коммуникации в судопроизводств» (Justizmodernisierungsgesetz). В качестве основной цели его принятия было названо введение полностью электронной коммуникации и системы документооборота между участниками судопроизводства. Упомянутый закон обеспечил необходимое правовое регулирование в сфере электронного правового документооборота для подачи электронных документов органами предварительного расследования в суд, их обработки внутри суда (включая возможность ведения дела в электронной форме), а также для вынесения решения в электронной форме и его последующего вручения всем заинтересованным лицам. Особенностью системы электронного оборота процессуальных документов в судопроизводстве Германии является требование об использовании электронной подписи на таких документах.

Кроме того, стоит сказать о том, что процесс электронного делопроизводства в ФРГ не стоит на месте и в 2017 г. Федеральным законом «О внедрении электронного документооборота в уголовное судопроизводство и дальнейшем развитии электронных правовых отношений»[18], был дан путь к дальнейшему совершенствованию электронных носителей информации. Указанный закон предписывает оформлять результаты предварительного расследования в электронном формате. Уголовное дело в виде электронного досье формируется из оформленных в виде цифровых файлов процессуальных решений и таких же оцифрованных доказательств. Все «аналоговые» доказательства подлежат обязательной оцифровке путем сканирования, цифрового фотографирования или видеозаписи, после чего приобщаются к уголовному делу в виде файла, заверенного цифровой подписью. В цифровом виде оформляются обвинительное заключение, судебные решения, принятые на досудебной стадии производства, заключения прокурора. Жалобы, ходатайства, исковые заявления стороны защиты также подаются в виде электронного документа и приобщаются к делу. Подача документов в бумажном виде допускается только при отсутствии технической возможности изготовления электронного документа. За систематическое нарушение этих требований участники уголовного судопроизводства могут быть привлечены к административной ответственности[19].

[18] Gesetz zur der elektronischen Akte in der Justiz und zur weiteren des elektronischen Rechtsverkehrs. Vom 5. Juli 2017. − URL: https://www.bgbl.de/xaver/bgbl/start.xav (дата обращения: 12.10.2021).

[19] Зазулин А. И. Нормативное обеспечение электронного документооборота в уголовном судопроизводстве: опыт ФРГ // Правопорядок: история, теория, практика. − 2018. − № 4 (19). − С. 76−80.

С материалами цифрового досье могут ознакомиться любые участники процесса, которым такое право предоставлено законом, в том числе путем получения цифровых копий на носитель информации или в виде распечатанных документов. Адвокат имеет право получать документы по электронной почте на специальный почтовый ящик, доступ к которому осуществляется при помощи смарт-карты. Документы, отправленные адвокатом с этого электронного адреса, принимаются без заверения их квалифицированной электронной подписью. Наличие цифровых возможностей не лишает адвоката права лично знакомиться с материалами уголовного дела. Он вправе потребовать от следственных органов предоставления полной описи файлов, приобщенных к материалам электронного досье, а также может лично проверить соответствие находящихся в нем цифровых документов их материальным оригиналам.

Технологически электронный документооборот обеспечивается специализированной защищенной системой передачи данных DE-MAIL, связывающей органы следствия, прокуратуры, суд, адвокатов и прочих участников уголовного судопроизводства, которые могут направлять и получать процессуальные документы по электронной почте.

Опыт Италии

SICP (Sistema Informativo della Cognizione Penale) – это цифровая платформа уголовного судопроизводства, используемая всеми итальянскими судами и государственными обвинителями, включая органы предварительного расследования. Однако становление данной системы сопровождалось проблемами, связанными с обеспечением взаимодействия судов и органов государственного обвинения.

Управление итальянской судебной системой разделено между Министерством юстиции (МЮ), отвечающим за организацию и функционирование всех служб, связанных с правосудием (статья 110 Конституции), и Судебным советом (или Высшим советом магистратуры), ответственным за широкий круг полномочий, связанных со статусом судей, прокуроров и общей организацией правосудия. Соответственно, ответственность за разработку и внедрение информационно-телекоммуникационных технологий лежит главным образом на Министерстве юстиции.

REGE (Registro Generale) – это программно-аппаратный комплекс, обеспечивающий производство по уголовному делу в цифровом виде, используемый итальянскими судами и обвинителями с начала 1990-х годов по 2015 год. Эта система обеспечивала возможность регистрации уголовных дел и предоставляла доступ к информационным базам данных различным подразделениям органов уголовной юстиции, а также ограниченные функциональные возможности управления делопроизводством в электронном формате. С конца 1990-х годов Министерство юстиции Италии

предпринимало различные попытки разработать централизованную электронную платформу, чтобы обеспечить основу для цифрового уголовного судопроизводства. Первые две попытки разработать такую платформу (REGE Relazionale и REGE Web) потерпели неудачу главным образом из-за нехватки ресурсов.

Полностью функциональный сервер должен был быть построен и установлен в каждом органе предварительного расследования и прокуратуры. Все серверы должны были быть совместимыми и подключенными, чтобы обеспечить синхронный обмен данными. Системы требовали новых аппаратных конфигураций, которые не были доступны в организациях и были слишком дорогими для приобретения. Точно так же необходимая пропускная способность для обеспечения всех необходимых функций была слишком дорогой для развертывания. Таким образом, были не в полной мере учтены характеристики существующей инфраструктуры и те барьеры, которые препятствовали изменениям, необходимым для полноценного функционирования новой системы.

Чтобы справиться с этими неудачами, Министерство юстиции Италии предприняло третью попытку разработать полностью функциональную интегрированную систему электронного уголовного судопроизводства в 2005 году. Система, названная SICP, была разработана и опробована в нескольких судах и органах предварительного расследования. Данная система была разработана для преодоления проблем REGE Relazionale и REGE Web путем передачи данных на несколько крупных централизованных серверов. Эта новая архитектура сделала возможным устойчивое развитие полностью функциональной и интегрированной сети данных в виде образа электронного уголовного дела для поддержки обмена данными и процедурной совместимости между судами и органами. Однако, хотя это решение было эффективным с технической точки зрения, оно контрастировало с существующим законодательством, согласно которому любая информация об уголовном деле должна храниться на сервере, физически расположенном по месту нахождения органа предварительного расследования или прокуратуры. Необходимые изменения, позволяющие развернуть новую электронную платформу, не были одобрены. Фактически политический климат того времени и постоянная напряженность в отношениях между исполнительной и судебной властью не позволяли одобрить изменения в законодательстве, необходимые для перемещения баз данных в региональные подразделения органов уголовной юстиции. Таким образом, в период с начала 1990-х годов до 2015 года продолжала действовать старая система REGE, которая не удовлетворяла современным требованиям в сфере информационно-технологического обеспечения уголовного судопроизводства.

Чтобы преодолеть проблемы, связанные с плохой функциональностью REGE, суды и органы предварительного расследования внедрили несколько локальных систем для обеспечения надлежащего и эффективного производства по уголовному делу с применением электронного образа

уголовного дела. Такой шаг был вызван необходимостью снизить нагрузку на суды и органы расследования, занимающиеся рассмотрением тяжких преступлений (например, по уголовным делам об организованной преступности, терроризме и коррупции), поскольку функции системы REGE не удовлетворяли потребности названных органов. Однако разработанные местными органами системы электронного уголовного судопроизводства были технически несовместимы, что препятствовало эффективному взаимодействию правоохранительных органов при производстве по уголовному делу. По некоторым оценкам, в 2014 году итальянские суды и органы предварительного расследования использовали около 20 различных программно-аппаратных комплексов для производства по уголовному делу в электронном виде. В том же году стало очевидно, что для эффективного развития электронного судопроизводство необходима разработка и внедрение совместимой централизованной системы производства по уголовному делу в электронной форме.

Министерство юстиции Италии решило повторно развернуть SICP, в том числе пролоббировав соответствующие законодательные изменения, чтобы обеспечить бесперебойную работу системы. Это стало возможным благодаря новому политическому климату и улучшению качества сотрудничества между министерством юстиции и судебной системой.

После углубленного анализа Министерство юстиции Италии приняло решение сделать SICP общей централизованной системой, которая внедряется во всех итальянских судах и органах уголовной юстиции. Все барьеры, которые привели к провалу SICP в 2008 году, были наконец преодолены, и в 2015−2016 годах во всех итальянских судах и органах расследования была внедрена полностью интегрированная и совместимая система производства по уголовным дела в электронном виде.

Однако судьи и прокуроры работают с SICP параллельно с уже существующими системами поддержки электронного судопроизводства и другими приложениями, поддерживающими аналогичные процедуры, которые еще не были интегрированы в SICP. В результате SICP работает вместе со множеством старых систем, которые эта система должна была заменить.

SICP предлагает два набора функций: один для органов предварительного расследования и прокуратуры и один для судебной системы. Поскольку они используют одни и те же системы, это обеспечивает полную совместимость между органами правосудия. SICP также содержит в себе интегрированную электронную базу данных для полицейских сил.

SICP предусматривает следующую совокупность функций:

– портал электронной подачи процессуальных документов: веб-сайт, используемый полицией для регистрации возбужденных уголовных дел (не совместимый с полицейскими базами данных);

− реестр уголовных дел, по которым осуществляется производство предварительного расследования;

− модуль формирования основных итоговых процессуальных документов предварительного расследования;

− база данных досудебных мер процессуального принуждения (например, о лицах, содержащихся под стражей или задержанных по подозрению в совершении преступления);

− возможность формирования судебных актов и актов прокурорского реагирования в досудебном производстве;

− мониторинг процессуальных сроков;

− формирование расписания судебных заседаний по уголовным делам, назначенным к рассмотрению;

− система случайного распределения уголовных дел между судьями;

− возможность автоматического формирования статистической информации подразделения уголовной юстиции или конкретного суда.

В течение всего срока становления в уголовном судопроизводстве Италии централизованной системы производства по уголовному делу в электронном формате возникали сложности, обусловленные плохо спланированными технологическими решениями, организационными и политическими факторами.

По сей день органы предварительного расследования и суды Италии продолжают одновременно использовать иные системы электронного правосудия даже при внедрении полностью интегрированной и совместимой системы SICP. Такое положение объясняется техническим несовершенством данной системы и отсутствием эффективной защиты от неправомерного искажения материалов электронного уголовного дела.

Опыт Испании

В Испании Министерство юстиции, Судебный совет и 12 автономных округов разделяют ответственность за отправление правосудия. Эта фрагментированная структура управления препятствует развитию электронного правосудия. Хотя Испания и преуспела в разработке функциональных платформ, фрагментация повлияла на характер и результаты инвестиций в электронное правосудие. Анализ инвестиций в электронное правосудие в Испании дает ценную информацию для понимания характера его развития, а также некоторых последствий фрагментированной системы правосудия, обусловленной технологической инфраструктурой судебного управления.

Министерство юстиции Испании обладает большинством управленческих функций в сфере отправления правосудия, включая развитие электронного уголовного судопроизводства.

Судебный совет управляет статусом судей, определяет бюджет (находящийся в ведении Министерства юстиции) и управляет судебной системой.

С середины 1990-х годов судебные технологии были интегрированы в повседневную деятельность судов и органов предварительного расследования и прокуратуры. В настоящее время испанская судебная система работает с девятью системами производства по уголовному делу в электронном виде: восемь были разработаны и используются судами автономных сообществ, а еще одна, Minerva, была разработана Министерством юстиции и используется в судах, непосредственно подчиненных Министерству юстиции. Четыре системы электронной подачи документов интегрированы с различными платформами: Justicia.cat, Avantius и JustiziaSip, созданными различными автономными сообществами, а также LexNet, разработанной Министерством юстиции. Учитывая децентрализованный характер испанской судебной системы, потребовалось юридическое вмешательство для поддержки внедрения интегрированных архитектур электронного правосудия в целях установления общих функциональных, процедурных и технических стандартов и содействия совместимости и перекрестной стандартизации во всех приложениях электронного правосудия.

Первые законодательные положения, которые заложили основу для более интегрированной электронной судебной системы, были приняты в 2007 году. Они регулируют использование и функциональные возможности LexNet, приложения, принятого Министерством юстиции для доставки повесток и обмена процессуальными документами. После этого парламент утвердил общие рамки использования современных информационных технологий в отправлении правосудия, включая электронную подачу документов, в 2011 году. Тем же постановлением парламента Испании был учрежден Национальный технический комитет (Comité Técnico Estatal de Administración Judicial Electrónica, или CTEAJE) для содействия развитию электронного правосудия и координации иных проектов в данной сфере. Определение правовой базы и создание CTEAJE заложили необходимую основу для развития электронного правосудия в такой сложной институциональной судебной системе.

В 2015 году парламент Испании одобрил закон, который требует использования электронной подачи документов во всех судебных разбирательствах[20]. Статья 230 Закона о судебной системе 2013 года устанавливает, что суды должны использовать все имеющиеся в их распоряжении технологические системы (например, электронные, компьютерные или телематические) для осуществления своей деятельности и выполнения своих функций. Электронные документы имеют юридическую силу, если технические средства обеспечивают их подлинность, целостность и соответствие установленным требованиям. Подзаконные акты

[20] Закон 39/2015 об общем регламенте работы государственных органов (Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas // https://boe.es/boe/dias/2015/10/02/pdfs/BOE−A−2015−10565.pdf) и Закон 40/2015 о нормативно-правовой базе государственного сектора (Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, http://boe.es/boe/dias/2015/10/02/pdfs/BOE-A-2015-10566.pdf/

устанавливают случаи и технологии, гарантирующие выполнение этих требований, а также когда судьи и прокуроры обязаны использовать имеющиеся в их распоряжении системы. В результате в 2018 году Судебный совет издал приказ, устанавливающий организационно-технические требования по созданию предпосылок для обязательного использования судьями и адвокатами системы электронного уголовного судопроизводства, систем судебного обеспечения и электронных картотек. Приказ также определяет требования к подготовке кадров и порядок проверки соответствия системы электронного уголовного судопроизводства и систем судебного обеспечения техническим и функциональным требованиям.

В то время как правовая база производства по уголовному делу в электронном формате является общей для всей страны, технологические реализации отличаются от региона к региону. Justicia Digital − это набор систем, разработанных Министерством юстиции. Он состоит из семи приложений: LexNet, Minerva Digital, Horus, Portafirmas, архивная система (Archivo) и два шлюза (Wasmin и Cargador) для обеспечения взаимодействия между Minerva Digital и внешними системами. LexNet − это платформа для безопасного обмена информацией между судебными органами и органами предварительного расследования. Она используется для обмена разнообразными процессуальными документами, в том числе направления всего образа электронного уголовного дела. Это похоже на систему электронной почты, но она гарантирует дополнительную безопасность (т. е. подлинность отправителя, конфиденциальность и целостность содержания направляемых документов) и удостоверяет дату доставки документа. По данным Министерства юстиции, LexNet удовлетворяет коммуникационные потребности системы отправления правосудия, включая стандарты уведомлений и обмена документами. Она доступна (в ограниченном виде) и для иных участников уголовного судопроизводства и совместима с различными аналогичными платформами по всей стране. Как только дело было направлено через LexNet, Минерва Digital управляет им в электронном виде: проверяет поданные данные, поручает дело судье, определяет задачи, которые должны быть выполнены, и выполняет множество задач, необходимых для управления делом, таких как регистрация и составление процессуальных документов. Minerva также позволяет отслеживать дела, находящиеся в производстве на досудебном этапе, и принимаемые по ним промежуточные процессуальные решения.

Как правило, после того как дело было назначено к рассмотрению, судья инструктирует своего секретаря о том, как осуществить подготовку к судебному заседанию, при необходимости дает указания о том, как составлять документы (например, судебные приказы и определения).

Должностные лица органов расследования используют «Минерву» для составления процессуальных документов. С содержанием документа можно ознакомиться с помощью средства просмотра файлов (Horus) и подписать его с помощью Portafirma (аналог электронной цифровой подписи). Как только

документ подписан, он сохраняется в массиве электронного уголовного дела и передается через LexNet заинтересованным участникам уголовного процесса.

Однако различные компоненты системы электронного уголовного судопроизводства не интегрированы. Например, чтобы ознакомиться с документом в файле электронного уголовного дела, должностное лица органа расследования или прокурор должен проверить номер дела в системе Minerva, а затем войти в программу просмотра файлов и ввести номер дела.

Хотя большинство испанских судов работают с LexNet, эта система не является общенациональной. Автономные сообщества Кантабрия, Каталония и Наварра создали свои собственные системы электронного документооборота (Avantius, JustiziaSip и Justicia.cat), которые отвечают требованиям, установленным различными нормативными актами. LexNet предоставляет функции электронной подачи документов Министерству юстиции и другим автономным сообществам: Андалусии, Арагону, Астурии, Канарским островам, Каталонии (только для отправки уведомлений), Галисии, Ла-Риохе, Мадриду и Валенсии.

Испанская система электронного правосудия включает в себя девять автономных систем. Учитывая эти условия, невозможно интегрировать или стандартизировать указанные системы, используемые в различных регионах и судах.

Внедрение электронной системы подачи документов также усложнило испанскую систему электронного правосудия. Несмотря на общую правовую базу, которая была определена законодательством, позволившим использовать электронный документооборот (2007 год), и законодательством, сделавшим электронный документооборот обязательным с 2015 года, ряд различных систем продолжают действовать самостоятельно. Большинство судов используют LexNet, но в некоторых судах все еще используются три другие системы электронного документооборота. Следовательно, необходимые системы для электронного возбуждения дела и обмена процессуальными документами в электронном виде отличаются от региона к региону. Адвокатам может понадобиться более одной электронной системы электронного судопроизводства, если они работают по всей стране.

Отсутствие стандартизации между различными компонентами электронного правосудия также препятствует единообразному применению уголовно-процессуального законодательства. То же самое происходит и с четырьмя электронными системами документооборота. Существование различных систем электронного судопроизводства и документооборота ставит под угрозу равный доступ граждан к правосудию.

Для решения этих проблем Судебный совет установил минимальные требования к совместимости программных платформ и провел тесты для проверки выполнения системой минимально необходимых стандартизированных функций. Это вмешательство обеспечило единообразие

в применении уголовно-процессуального закона и, следовательно, справедливость судебной системы.

CTEAJE также играет важную роль в продвижении к более интегрированной и однородной системе электронного правосудия. Она обеспечивает институциональную основу для сотрудничества между органами, участвующими в развитии электронного правосудия, а также технологические достижения, которые помогают повысить согласованность между компонентами системы электронного уголовного дела, способствующими сохранению гарантий безопасности информации и неразглашения данных предварительного расследования.

Оценка допустимости распространения опыта цифровизации уголовного судопроизводства

Представляется целесообразным рассмотреть положительные и отрицательные стороны возможного внедрения электронного уголовного дела в уголовное судопроизводство. При этом надо иметь в виду, что результаты оценки развития информационных технологий могут иметь разное значение. То, что для одних может стать позитивным, для других может быть негативным, и наоборот. Это касается участников уголовного процесса, а также прав и свобод граждан, интересов общества и государства.

Прежде всего, существует проблема, которая видится пока в отрицательном значении для граждан, вовлеченных в уголовное судопроизводство, − это сложность в обеспечении информационной безопасности. Проблемы использования современных технологий связаны с идентификацией личности, возможностью внесения извне изменений в сохраненные электронные документы, используемые в уголовном деле. Для решения этого вопроса потребуется качественное техническое решение. При этом технологии, поддерживающие, к примеру, блокчейн и криптовалюты, вряд ли могут удовлетворить национальные потребности в этом вопросе. Подобные технологии не в полной мере отвечают интересам государства, его безопасности.

Отрицательный момент просматривается и в возможности фальсификации информации. Возможность иметь доступ к цифровой информации всегда будет вызывать сомнения в достоверности и быть лишним поводом к ее дополнительной проверке. Несмотря на существующие различные методы защиты целостности цифровых данных, проблема связана с возможностью раскрытия персональных данных, кражи коммерческой, профессиональной, служебной и государственной тайны. Возникают вопросы, требующие дополнительной защищенности. Это относится к носителям электронной информации, а также к сведениям об участнике уголовного судопроизводства, в отношении которого были приняты меры безопасности.

Положительно для органов расследования и суда в электронном уголовном деле то, что оно удобно, компактно, мобильно, легко управляемо.

Так, электронная форма уголовного дела позволит сэкономить время на пересылку материалов (от одного отдела полиции в другой по подследственности; от следователя прокурору или руководителю следственного органа для проверки; от прокурора в суд на рассмотрение и т.д.); обеспечивать сокращение бумажных расходов, удобство при ознакомлении участников уголовного судопроизводства с материалами уголовного дела, компактность хранения, легкость копирования.

В перспективе технические средства копирования, хранения, передачи электронной информации сделают ненужными бумажные уголовно-процессуальные документы, то есть возможен переход исключительно на электронный документооборот. Это также экономит расходы на канцелярские товары. Вместе с тем увеличатся затраты на приобретение более качественной компьютерной техники, сканеров, видеокамер и т. д.

Электронные документы могут рассматриваться в качестве конечного продукта проведения следственных действий. В данном случае возможна угроза разрушения стереотипного восприятия «классических» следственных действий. Это можно рассматривать и как отрицательный момент, и как необходимость развития законодательства. Дело в том, что оперирование электронной (цифровой) информацией не вполне вписывается в традиционную систему следственных действий. Так, например, в ходе осмотра носителя цифровой информации задействованы не только органы чувств, приходится, по сути, искать, сортировать информацию, выполнять технические и программные действия. Поэтому вряд ли это соответствует обычному осмотру.

В этой связи необходимо регулирование в первую очередь основных начал проведения следственных действий и иной деятельности с использованием информационных технологий и электронных документов путем формулирования норм о гарантиях подлинности электронных доказательств, например, о неизменности информации, защите от возможных посягательств и доступности для последующего изучения, депонировании электронных копий, обязательном участии специалиста при проведении следственных или судебных действий, связанных с копированием, депонированием, осмотром, изъятием электронной информации. Однако следует отметить, что в последние годы в отечественном уголовно-процессуальном законодательстве возникли предпосылки для постепенной цифровизации уголовного судопроизводства и возможного внедрения в процесс системы электронного уголовного дела. Так, например, Федеральным законом от 06.07.2016 № 375-ФЗ в УПК РФ была введена ч. 7 ст. 185, которая предусматривает осмотр и выемку электронных сообщений и иных передаваемых по сетям электросвязи сообщений. Федеральный закон от 23.06.2016 № 220-ФЗ ввел в УПК РФ новую статью 474.1 «Порядок использования электронных документов в уголовном судопроизводстве». Федеральный закон от 27.12.2018 № 533-ФЗ внес изменения в УПК РФ в части регламентации производства следственных действий в отношении

электронных носителей информации, дополнив его ст. 164.1 «Особенности изъятия электронных носителей информации и копирования с них информации при производстве следственных действий».

Таким образом, можно сделать вывод о том, что производство по уголовному делу в электронном виде будет иметь следующие преимущества:

1. Сокращение сроков уголовного судопроизводства путём сокращения сроков направления ходатайств, передачи материалов дела в суд для применения меры пресечения, дачи разрешения на проведение следственных действий, которые производятся только по решению суда, передачи материалов руководителю следственного органа, прокурору, в суд для рассмотрения жалоб, осуществления проверок и т.д. Также сокращаются сроки ознакомления участников процесса с материалами уголовного дела, поскольку это можно делать в любое время (а не только рабочее), в любом месте и одновременно всеми участниками процесса.

2. Улучшение доступа к процессуальной информации всех участников уголовного судопроизводства, создание дополнительных возможностей для их взаимодействия. Так, в электронном виде могут заявляться и разрешаться ходатайства и отводы, эксперт и специалист могут дистанционно направлять свои заключения, в ряде случаев постановление о назначении экспертизы также может направляться эксперту в электронном виде.

3. Создание дополнительных возможностей обеспечения права на защиту соответствующих участников уголовного судопроизводства. Так, например, защитник дистанционно может направлять дознавателю, следователю, суду документы для приобщения их к делу в качестве доказательств, знакомиться с материалами уголовного дела, приносить жалобы в электронном виде и т.д. Это сократит время работы защитника, его расходы и в конечном итоге позитивно скажется на доступности квалифицированной юридической помощи для подозреваемого и обвиняемого. Это же касается и представителей потерпевшего, гражданского истца, гражданского ответчика и частного обвинителя.

4. Создание дополнительной гарантии права участников уголовного судопроизводства на доступ к процессуальной информации, что в конечном итоге влияет на степень реальной обеспеченности прав и свобод каждого из участников уголовного процесса.

5. Повышение требований к качеству работы дознавателя, следователя, суда, качеству составления процессуальных документов, производства следственных и иных процессуальных действий, повышение ответственности должностных лиц, ответственных за производство по делу, и качества уголовного судопроизводства в целом.

6. Облегчение проверки материалов уголовного дела руководителем следственного органа, прокурором, судом и контроля за производством по делу в целом (материалы для проверки помещаются в специальный раздел, куда получают доступ соответствующие участники процесса). Упрощение и сокращение процесса дачи судом разрешения на проведение соответствующих

процессуальных действий (обыска, выемки, контроля и записи переговоров и т.д.), процесса продления сроков предварительного расследования руководителем соответствующего следственного органа.

7. Сокращение расходов в ходе производства по уголовному делу (почтовые расходы, расходы на изготовление копий материалов уголовного дела, расходы на юридическую помощь, некоторые процессуальные издержки и т.д.).

8. Организационное упрощение процесса пересмотра судебных решений вышестоящими судебными инстанциями (в части доступа к процессуальным документам и материалам, подлежащим проверке).

9. Систематизация и структурирование материалов уголовного дела, необходимые в работе дознавателя, следователя, прокурора и суда.

10. Возможность автоматизировать ведение статистики по уголовным делам.

11. Существенное снижение риска фальсификаций и исправлений в материалах уголовного дела (в первую очередь в отношении следственных и процессуальных действий, материалы которых уже помещены на электронный портал).

12. Повышение транспарентности правосудия по уголовным делам.

Внедрение в уголовно-процессуальную материю технологии удостоверения процессуального документа любым участником уголовного процесса электронной подписью вместо обычной позволит в режиме онлайн осуществлять процессуальные действия и подтверждать их. Это дает широкие возможности по дистанционному обеспечению прав и законных интересов участников. Однако на видеозаписи наглядно будут видны все ошибки и промахи лица, производящего расследование, что потребует более высокого профессионализма. Все это может стать предметом обжалования и прокурорского надзора.

Электронное уголовное дело позволит более широко использовать математические методы алгоритмизации в поддержке принятия процессуальных решений. Сама идея не нова и имеет как положительные, так и отрицательные стороны. Применение такой тщательно разработанной программы посягает на внутреннее убеждение правоприменителя (следователя, дознавателя, судьи). Оценка доказательств (электронных, цифровых или иных) была и будет оставаться в сфере усмотрения субъекта оценки, основываясь на внутреннем убеждении. Последнее связано с логической мыслительной деятельностью, выступающей неким принципом оценки, позволяющим отойти от формальной теории доказательств.

Анализ рассмотренных систем электронного документооборота в уголовном судопроизводстве стран с различными системами уголовного судопроизводства позволяет сделать некоторые выводы, имеющие значение для внедрения аналогичных цифровых технологий в российское уголовное судопроизводство.

Во-первых, следует обратить внимание, на то, что все необходимые для цифровизации уголовного судопроизводства технологии у нас уже давно разработаны, доступны, широко распространены. Так, нельзя не заметить, что отдельными ведомствами в данном направлении уже предпринимались весьма значительные шаги. Так, МВД России, реализуя ведомственную программу «Основные направления комплексной информатизации органов предварительного следствия в системе МВД России на 2002−2006 годы», создало Специализированную территориально распределенную автоматизированную систему органов предварительного следствия (СТРАС ОПС)[21]. Хотя реализация данной программы не предполагала полномасштабной цифровизации досудебного производства и была направлена лишь на создание централизованного федерального банка данных электронных копий уголовных дел, который предполагалось использовать преимущественно в организационных, криминалистических и методических целях, при ее создании и использовании было практически отработано применение основных технологических решений, необходимых для введения электронного документооборота в досудебном производстве по уголовным делам.

В качестве эффективного средства информационного обеспечения работы ОВД рассматривалась единая информационно-телекоммуникационная система органов внутренних дел, которая еще до 2010 г. должна была охватить все органы внутренних дел. Задачами создания данной системы являлись авторизация сбора, хранения и обработки информации, организация удаленного доступа сотрудников всех правоохранительных служб к информационным ресурсам системы МВД, организация взаимодействия с информационными системами всех правоохранительных и государственных органов РФ, а также с Интерполом. Таким образом, СТРАС ОПС была технически реализована в составе единой информационно-телекоммуникационной системы органов внутренних дел, являлась ее составной частью и использовала ее в качестве защищенной «транспортной среды» для передачи данных. Система была реализована на широко распространенных и апробированных клиент-серверных технологиях, использовании интернет-приложений и протоколов.

Создаваемые следователями в ходе расследования на автоматизированных рабочих местах электронные документы формировали в локальной базе данных следственного подразделения копию уголовного дела. В процессе расследования материалы электронного уголовного дела были доступны руководителю следственного подразделения для осуществления ведомственного контроля. По окончании расследования сформированные

[21] Положение о порядке функционирования автоматизированной системы органов предварительного следствия в системе МВД России : приказ МВД России от 27.01.2006 № 45. − М. : МВД России, 2006; Основные направления комплексной информатизации органов предварительного следствия в системе МВД России на 2002−2006 годы : методические рекомендации. М. : МВД России; СК при МВД России, 2002.

электронные копии уголовных дел отправлялись при помощи единой информационно-телекоммуникационной системы в Централизованную базу данных для хранения и использования. Обращение пользователей к системе было обеспечено в режимах прямого доступа либо, при отсутствии такового, по электронной почте посредством ведомственной сети передачи данных (МСПД) «Дионис».

Масштабы работ, проведенных при создании СТРАС ОПС, изначально не соответствовали довольно узко поставленной цели, однако реализованные технические и организационные решения, наработанный опыт использования этой системы должны быть учтены и использованы в ходе дальнейших работ по цифровизации досудебного производства по уголовным делам.

С 2011 года стали применяться облачные технологии и на базе единой информационно-телекоммуникационной системы органов внутренних дел была создана новая интегрированная мультисервисная телекоммуникационная система (ИМТС)., которая стала включать более широкие возможности цифровизации

Кроме того, стоит сказать о том, что формирование и ведение автоматизированных централизованных учетов осуществляется посредством ГИАЦ и ИЦ на базе интегрированного банка данных федерального уровня (ИБД-Ф) и интегрированного банка данных регионального уровня (ИБД-Р), а также автоматизированных информационных систем (АИС) и автоматизированных информационно-поисковых систем (АИПС).

На сегодняшний день в служебной деятельности успешно используются ИБД регионального уровня (ИБД-Р), причем практические работники отмечают удобство обмена общедоступной информацией. В банки данных включаются сведения о лицах, состоящих на учетах органов внутренних дел; способах совершения нераскрытых преступлений и приметах лиц, скрывшихся с места совершения преступления; вещах, разыскиваемых и выявленных, а также имеющих заводские номера или характерные особенности. По запросу из ИБД можно получить информацию о наличии в нем сведений о проверяемом объекте, сведения биографического характера, сведения о признаках внешности, сведения о кличках и прозвищах разыскиваемого лица, фотоизображение разыскиваемого лица, сведения о вещах, поставленных на учет превентивно или в связи с розыском.

Ведется централизованный учет преступлений и лиц, подозреваемых, обвиняемых в их совершении, путем формирования и ведения банков данных ИБД-Ф и ИБД-Р (подсистема «АБД-Центр»), централизованный учет похищенных и изъятых номерных вещей и документов (подсистема «Номерные вещи»), централизованный учет лиц, пропавших без вести, неопознанных трупов и лиц, неспособных по состоянию здоровья или возрасту сообщить данные о своей личности (базы данных АИПС «Опознание»), централизованный учет лиц, объявленных в федеральный или международный розыск (подсистема «ФР-Оповещение»), централизованный учет утраченного или выявленного огнестрельного оружия или иного

вооружения (подсистема «Оружие»), централизованный учет разыскиваемых транспортных средств (подсистема «Автопоиск»), централизованный учет похищенных предметов, имеющих культурную (историческую, научную, художественную) ценность (подсистема «Антиквариат»), централизованный учет правонарушений и преступлений, совершенных на территории РФ иностранными гражданами, а также в отношении них (АИС «Криминал-И»).

ГИАЦ МВД России формирует оперативно-справочные учеты, автоматизированные информационно-поисковые системы и банки данных: АИС «Картотека уголовных дел», Дактилоскопическая картотека, «АБД-Центр», АИС «ФР-Оповещение», АИПС «Опознание», АИПС «Оружие», АИПС «Антиквариат», АИС «Криминал-И», АИПС «Досье-мошенник», АБД «Наемники», АИПС «Наркобизнес», АИПС «Сейф», АИПС «Насилие», АИПС «Вещь» и т.д.

Во-вторых, рассматриваемые технологии могут быть применены для цифровизации уголовного судопроизводства независимо от его типа, принадлежности к правовой семье, правовых традиций конкретного государства и иных особенностей. Рассмотренные примеры также демонстрируют единообразие используемых технических решений, таких как замена бумажных документов электронными файлами в PDF-формате, а самого уголовного дела − папкой на сервере, обеспечение электронного документооборота на основе интернет-технологий, а за счет этого и упрощенного доступа участников уголовного судопроизводства к материалам расследования обеспечение стороне защиты возможности собирать и представлять доказательства в электронной форме и др. Это указывает на универсальный характер используемых технологий и их способность модернизировать любую систему уголовного судопроизводства, вне зависимости от национальных особенностей.

В-третьих, введение электронного делопроизводства требует определенных изменений в самом уголовном процессе. Так, никакая цифровизация невозможна, если законодатель не признает доказательства информацией, а не формально определенным документом и не приравняет файл к протоколу. Современные технологии способны куда лучше обеспечить аутентичность и неизменность информации, нежели многочисленные подписи под архаичными протоколами. Применение новых технологий фиксации доказательственной информации потребует выработки и новых технических и процессуальных средств по обеспечению допустимости таких доказательств.

Рассмотренные примеры показывают, что данная задача вполне может быть решена при существующем уровне развития технологий, при сохранении общей структуры и порядка осуществления досудебного производства по уголовным делам.

Таким образом, внедрение в практику уголовного судопроизводства электронного уголовного дела решит многие существующие проблемы.

ГЛАВА 2. ИЗУЧЕНИЕ ЗАРУБЕЖНОГО ОПЫТА В СФЕРЕ СОЗДАНИЯ ЭЛЕКТРОННЫХ ОБРАЗОВ УГОЛОВНЫХ ДЕЛ И ФОРМИРОВАНИЯ ИХ МАССИВА

Федеральная статистическая система США

Статистическая служба США – одна из наиболее совершенных и мощных среди зарубежных стран с децентрализованной статистикой. Её центральным статистическим органом с 1913 г. является Министерство торговли. Оно собирает всю статистическую информацию и исчисляет большинство обобщающих социально-экономических показателей совместно с Министерством труда. Выделяются статистические службы Министерства внутренних дел, Министерства здравоохранения, образования и благосостояния, Министерства финансов и т. д.

Всего в США сбором и обработкой первичной информации занимается примерно 70 министерств и ведомств наряду с 400 частными организациями. Все эти организации имеют свои статистические службы, весьма различные по задачам, количеству занятых сотрудников и издают свои специальные публикации. Причем эта обширная информация с разной степенью детализации помещается в Статистическом ежегоднике США и во многих случаях является основным источником данных для большинства зарубежных экономистов и иных пользователей такой информации в других странах.

Основным методом статистических наблюдений в США являются переписи, которые содержат важнейшие сведения обо всех объектах совокупности. Экономические переписи проводятся раз в пять лет. Они дополняются еще детальными характеристиками, данные о которых получаются от 10-20% объектов выборочного наблюдения (например, социально-экономические характеристики граждан). Большая часть таких централизованных обследований проводится с помощью рассылки по почте разработанных вопросников-анкет, и через нее собираются ответы на эти анкеты (метод самоисчисления).

При некоторых обследованиях проводятся прямые личные опросы по более сложным программам. Этот метод является одним из традиционных, но он все меньше применяется для больших совокупностей объектов наблюдения. За последние десятилетия наибольшее распространение получил выборочный метод. Он позволяет не только существенно сокращать время, но и стоимость обследований, получать более точную информацию. В основном применяется случайная районированная выборка, которая основывается на положениях теории вероятности и определении величины погрешности в зависимости от объема выборочной совокупности.

Определенное распространение получил также метод «критических пунктов». Он основан на обследовании части объектов, имеющих

специальные характеристики, присущие относительно небольшому их числу, например крупных фирм.

В США нашло широкое применение также стандартных, то есть унифицированных классификаций для увеличения сравнимости статистических данных не только внутри страны, но и на международной арене.

Федеральная статистическая система Соединенных Штатов является децентрализованной сетью федеральных агентств, которые производят данные о людях, экономиках, природных ресурсах и инфраструктурах в США.

В отличие от многих других стран в США нет первичного статистического агентства. Вместо этого статистическая система децентрализована, с 13 статистическими агентствами, два из которых являются независимыми агентствами, а остальные 11, как правило, расположены в различных государственных ведомствах. Эта структура поддерживает статистическую работу в непосредственной близости от различных отделов на уровне кабинетов, которые используют эту информацию.

Федеральная статистическая система координируется Управлением управления и бюджета (OMB). OMB устанавливает и обеспечивает соблюдение статистической политики и стандартов, обеспечивает выделение ресурсов для приоритетных статистических программ и утверждает статистические обследования, проводимые федеральным правительством в соответствии с Законом о сокращении бумажного документооборота. К основным статистическим агентствам, функционирующим в США, можно отнести:

- Бюро статистики юстиции;
- Бюро судебной статистики;
- Бюро переписи населения;
- Бюро статистики труда;
- Национальный центр статистики образования;
- Национальная служба сельскохозяйственной статистики;
- Национальный центр статистики здравоохранения;
- Бюро экономического анализа;
- Службу экономических исследований;
- Управление энергетической информации;
- Национальный центр науки и инженерной статистики;
- Статистику отдела доходов;
- Бюро статистики транспорта;
- Управление исследований, оценки и статистики.

Бюро судебной статистики (BJS) из Департамента юстиции США является главным федеральным агентством, ответственным за измерение преступности, уголовной виктимизации, уголовных преступников, жертв преступлений, а также за изучение функционирования уголовных и

гражданских систем правосудия на федеральном уровне, уровне штата и местном уровне. BJS собирает, анализирует и публикует данные о преступности в США. Агентство публикует данные о статистике, собранной примерно из пятидесяти тысяч агентств, офисов, судов и учреждений, которые вместе составляют систему правосудия США. Данное бюро собирает, анализирует, публикует и распространяет информацию о преступности, преступниках, жертвах преступлений и работе систем правосудия на всех уровнях государственного управления. Эти данные имеют решающее значение для политиков на федеральном уровне, уровне штата и на местном уровне в борьбе с преступностью и обеспечении эффективного и беспристрастного правосудия.

В США сбор уголовно-статистических отчетов в отдельных штатах стал развиваться с начала 20-го столетия. Сбор данных о преступности в США всегда сопровождался серьезными затруднениями. Главное препятствие в этом порождает сама система управления страной, в которой существуют три уровня: федеральный, штатов и местный.

В США существуют три основные формы сбора данных о преступности:

– единый отчет о преступности ФБР (Uniform Crime Report);

– результаты национального виктимологического опроса (National Crime Victimization Survey), проводимого бюро статистики при департаменте юстиции США;

– самоотчеты правонарушителей (self-report survey).

Следует также отметить, что отчеты, составляемые ФБР, содержат сведения только о восьми видах так называемых «индексных» преступлений:

– убийство;
– изнасилование;
– грабеж;
– разбойное нападение;
– похищение имущества (кроме автотранспорта);
– кража автотранспорта;
– поджог.

Национальный виктимологический опрос также содержит сведения не обо всех видах преступлений, однако в его процессе собираются данные о ситуационных факторах совершения преступлений, а также демографическая информация о жертвах. Отмечается некоторое несоответствие данных в этих трех формах учета, однако они не являются значительными.

ФБР публикует криминальную информацию в различном виде. Основной ежегодник – «Единый отчет преступности. Преступность в США», в котором в федеральном масштабе и в разрезе штатов публикуются:

1) подробные данные о восьми видах индексных (серьезных) преступлений (убийство, изнасилование, грабеж, нападение, проникновение в помещение, кража-воровство, кража автомашины, поджог);

2) показатели о раскрытых преступлениях;

3) сведения об арестах по 21 виду преступного поведения, в том числе индексным преступлениям;

4) сведения о сотрудниках правоохранительных органов

Важным мероприятием, способствующим объединению разрозненных полицейских сил США, была разработка национальной системы информации о преступлениях и преступниках.

В 1930 г. была разработана и внедрена национальная добровольная программа сбора данных по единой форме отчетности о преступлениях.

Необходимость создания информационной системы уголовной юстиции неоднократно подчеркивалась специалистами и учеными США. Министерство юстиции решило обратиться к электронной обработке данных, которая стала главной надеждой преодоления трудностей по сбору сведений о преступлениях и преступниках. Первым шагом в этой области было создание национального центра информации о преступности (НЦИП) в составе ФБР для обслуживания учреждений, наблюдающих за соблюдением законов на всех трех уровнях. Как правило, по крайней мере, одно из учреждений штата имеет один терминал в системе НЦИП.

К началу 1975 года терминалы сети НЦИП имелись во всех федеральных учреждениях принудительного соблюдения законов (37), во всех агентствах ФБР в стране (59), в полицейских департаментах штатов, а также в округе Колумбия и Канаде.

Одновременно ФБР проводило работу по унификации различных сообщений о преступлениях органами охраны правопорядка в стране и с этой целью разработало форму и требования к «единой программе отчета о преступности» (UCR) в качестве одного из элементов будущей комплексной системы данных. Для внедрения в практику комплексной системы данных управление помощи органам принудительного исполнения закона департамента юстиции в 1972 году предложило штатам субсидии и специальную программу, по которой штаты — участники были обязаны организовать центры статистического анализа преступности; сообщать о преступлениях по единой форме; разработать программу статистического управления и администрации; ввести в ЭВМ досье преступников и проводить статистический учет уголовных дел преступников согласно требованиям ввода в ЭВМ; развивать средства статистического учета местных органов и органов штатов.

В масштабах штата или всей страны подсчитываются не все преступления. Вместо этого используются два метода для определения размера преступности и ее колебаний.

1. Исследование по потерпевшим проводится регулярно федеральным правительством с 1972 года. Этот метод похож на опрос общественного мнения, когда жителей и работающих в определенном районе опрашивают для установления, какие преступления были совершены против них или их собственности. Объем преступности определяется по результатам опроса, выраженного в процентах ко всему населению.

2. Единая программа отчета о преступности (UCR) дает уголовную статистику для использования в административной деятельности, операций и управлении правоохранительных органов. Например, в Калифорнии эта программа функционирует в Бюро криминальной статистики (BCS). Выполняя эту программу, правоохранительные органы штата предоставляют информацию в Бюро статистики по «отобранным» правонарушениям. Правонарушения затем классифицируются по определениям программы UCR для устранения различий между различными штатами в определении преступлений по их кодексам. Эта информация объединена не только в этом отчете о преступности и правонарушениях, она обрабатывается и направляется в ФБР для использования в ежегодной публикации – «Преступность в США». Правонарушения, отобранные из-за их тяжести, частоты и вероятности быть сообщенным в полицию: умышленное убийство, изнасилование, грабеж, нанесение телесных повреждений, проникновение в помещение, кража, угон и поджог. За исключением кражи, программа UCR не подсчитывает менее тяжкие преступления и проступки.

В 1982 году Федеральное бюро статистики юстиции (BJS) и ФБР начали совместное исследование национальной программы UCR, которая была в действии с 1930 года. Это исследование было завершено в 1985 году и опубликовано как «документ о будущем программы единой отчетности о преступности». Этот документ рекомендовал переделать общую систему UCR в «систему отчетности, основанную на происшествии» (IBR). Эта рекомендация была утверждена министерством юстиции США в конце 1985 года.

По системе IBR, правоохранительные органы должны подавать отдельную запись по каждому уголовному проявлению, включая данные о преступлениях, совершенных в его рамках, а также информацию о потерпевших, подозреваемых и задержанных, имеющих к нему отношение. Эта система должна предоставить законодателям, администраторам и планирующим, данные, которые позволят более точно измерить число преступлений, совершенных в обществе, тяжесть этих преступлений и характеристики потерпевших в этих преступлениях.

Статистическая система Сингапура

Статистической отчетностью в Сингапуре занимается два государственных органа власти. Общая статистика систематизирована в Министерстве торговли и промышленности, внутри которого существует Департамент статистики Сингапура[22]. Статистика по преступности[23], которая также публикуется на официальном сайте Департамента статистики Сингапура, ведется и в Министерстве внутренних дел, где за это направление отвечает отдел исследований и статистики. В то же время в отличие от России

[22] https://www.singstat.gov.sg/

[23] https://data.gov.sg/dataset/overall-crime-cases-crime-rate

официальный сайт МВД Сингапура[24] систематезированных данных о статистике не представляет. Следует обратить внимание, что Сингапур, как и некоторые другие страны, такие как Великобритания, США, Франция, Япония и другие, представлен на крупном немецком статистическом портале Statista[25]. Statista – немецкая компания, специализирующаяся на рыночных и потребительских данных. По данным компании, на ее платформе зарегистрировано более 2 млн пользователей и она содержит более 1 млн статистических данных по более чем 80 000 тем из более чем 22 500 постоянно обновляемых источников и 170 различных отраслей.

Организация ведения статистики в Сингапуре происходит следующим образом.

Когда преступление совершено, зарегистрировано или информация о нем получена иным образом, преступник подлежит наказанию, а также может быть привлечен к уголовной ответственности. Судебные записи изначально создавались во времена колониального правления, когда властям приходилось отслеживать известных преступников. Сегодня они чаще всего используются при проверке биографических данных для целей приема на работу и проверки безопасности. В соответствии с Первым и вторым списками Закона о регистрации преступников Сингапура (RCA SINGAPORE), регистрируемые преступления охватывают широкий спектр преступлений. Он нередко выходят за рамки Уголовного кодекса. Некоторые из них также включены в иные законодательные акты:

– Закон о преступлениях, связанных с оружием [гл. 14] (разделы с 3 по 8);
– Закон о банкротстве 1995 г. (часть X);
– Закон о радиовещании и телевидении [гл. 28] (Раздел 5);
– Закон о внутренней безопасности [гл. 143];
– Закон о злоупотреблении наркотиками [гл. 185];
– Закон о государственной тайне [гл. 213];
– Закон об организованной преступности 2015 года [Закон 26 2015 года];
– Женская хартия [гл. 353].

Если лицо поймают за совершением правонарушения, не подлежащего регистрации, оно не можете подлежать регистрации в соответствии с RCA. Правонарушения, не подлежащие регистрации, включают мелкие правонарушения, такие как разбрасывание мусора или пешеходная прогулка по автодороге.

Лицо может получить судимость и быть внесено в базу, если оно:

– осуждено в Сингапуре за преступление, подлежащее регистрации;

– осуждено за совершенные правонарушения, а также зарегистрировано в Малайзии;

– приказано быть изгнанным или депортированным из Сингапура или Малайзии;

[24] https://www.mha.gov.sg/
[25] https://www.statista.com/statistics/628339/crime-rates-in-singapore/

– все вышеперечисленное из любого места за пределами Сингапура и Малайзии, с подробностями, предоставленными соответствующими властями места совершения деяния.

Если лицо признано виновным в правонарушении, подлежащем регистрации во втором приложении RCA SINGAPORE, включая такие преступления, как нанесение вреда здоровью, комиссар полиции имеет право по своему усмотрению не включать его имя в реестр при условии, что лицо подпадает под следующие требования:

– за преступление назначен штраф до 1000 сингапурских долларов вместо тюремного заключения;

– нет судимости.

Если комиссар полиции решит не регистрировать лицо, видеорегистратор полицейского все равно сохранит данные о нем в течение 6 месяцев с даты их получения, и если комиссар полиции не решит зарегистрировать лицо в течение этого периода, регистратор уничтожит данные.

В полицейском реестре хранятся следующие данные: имя человека, отпечатки пальцев, фотография, совершенное преступление и вынесенный приговор. Там также имеются образцы организма человека, такие как волосы, мазки, взятые изо рта человека, и образцы крови, которые образуют базу данных ДНК, хранящуюся у регистратора.

Судимость в Сингапуре является постоянной. После того как запись будет зарегистрирована в Реестре преступников, она никогда не будет полностью стерта или удалена до тех пор, пока человек не умрет или не достигнет возраста 100 лет, в зависимости от того, что произойдет раньше.

Однако некоторые сведения о судимости за мелкие преступления могут быть сняты по истечении 5 лет подряд без совершения преступлений с даты вынесения приговора, если тюремного заключения не было, или со дня освобождения правонарушителя из тюрьмы.

Все судимости, связанные с правонарушениями, перечисленными в третьем приложении RCA SINGAPORE, которые, как правило, являются серьезными преступлениями, такими как изнасилование, убийство или групповое ограбление, останутся постоянными.

Правонарушитель также может быть лишен права на снятие судимости, если:

– приговор включал тюремный срок более 3 месяцев или штраф в размере более 2000 сингапурских долларов;

– на лицо уже зарегистрировано более одной судимости;

– у лица уже есть предыдущая запись в реестре.

Если лицо было лишено права на снятие судимости, оно может обратиться к комиссару полиции с просьбой о возобновлении данной возможности, после чего комиссар примет окончательное решение на основе фактов каждого дела.

Не смотря на то, что отсутствие судимости в реестре означает, что у лица ее больше нет, в заявлении о приеме на работу оно можете указать, что судимости более нет, однако все равно нужно будет заявить, что лицо было осуждено ранее. Даже если запись в отношении лица была удалена или утеряна, данные, включая записи ДНК, все равно останутся в Реестре[26].

МВД Сингапура представляет через свой интернет-ресурс достаточно большой объем различных государственных услуг[27]. В том числе они представляют выписку из статистического реестра о наличии у лица судимости[28].

Статистическая система Китая

Статистические данные в Китае собираются Национальным бюро статистики. Они строятся на основе огромного количества классификаторов, которые называют статистическими стандартами. Все они представлены на официальном сайте бюро[29].

Законодательно ведение статистики урегулировано законом Китайской Народной Республики о статистике, принятым на 168-м заседании Исполнительного совета Государственного совета КНР 12 апреля 2017 г. Проблема исследования статистики КНР заключается в наличии слишком большого количества подразделений различных органов власти, ведущих статистику в соответствии с утвержденными классификаторами. При этом сами классификаторы слишком сильно конкретизированы. Так, к примеру, каталог ведения статистики насчитывает 97 пунктов сфер деятельности для подсчета данных[30]. Основную информацию об уголовной статистике, представленную в форме таблиц, можно найти на официальном сайте Верховного суда КНР[31].

Статистическая система Федеративной Республики Германии

Сбором и представлением данных о статистике преступности в Германии занимается Bundeskriminalamt – Федеральное ведомство уголовной полиции Германии[32]. В целом данная организация занимается достаточно большим объемом направлений, в том числе научными разработками в области борьбы с преступностью. В то же время объемы представляемых

[26] https://asl-law.com.sg/2020/01/15/heres-what-you-need-to-know-about-criminal-records-in-singapore/
[27] https://eservices.police.gov.sg/content/policehubhome/homepage.html
[28]https://eservices.police.gov.sg/content/policehubhome/homepage/criminal-record-case-disclosure-conference-singpass.html
[29] http://www.stats.gov.cn/tjsj/tjbz/
[30] http://www.stats.gov.cn/tjsj/tjbz/tjypflml/index_4.html
[31] http://gongbao.court.gov.cn/Details/c70030ba6761ec165c3c2f0bd2a12b.html
[32]https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/PolizeilicheKriminalstatistik/pks_node.html

полицией данных достаточно большие. К примеру, отчет о преступности за 2011 год составил 754 листа[33]. При этом следует обратить внимание, что полиция Германии представляет в свободном доступе таблицы с показателями по конкретным видам преступлений, что говорит об открытой системе статистической отчетности.

Статистика преступности полиции (PCS) охватывает только случаи, которые были достаточно подробно описаны в полицейских отчетах.

При внесении сведений в статистические данные должны быть проверены следующие индикаторы:

− деяние составляет уголовное преступление (т.е. все элементы, составляющие преступление, как определено в положении уголовного закона, должны быть указаны);

− место преступления (место выявления преступления);

− время / период выявления преступления (не менее года).

Расплывчатые детали, которые невозможно подтвердить, особенно в отношении количества уголовных правонарушений недостаточны для внесения дела в PCS.

В крупномасштабных расследованиях (например, о мошенничестве) правила регистрации гласят, что только тщательно расследованные дела подлежат рассмотрению. При этом все противоправные (уголовные) действия, перечисленные в перечне правонарушений, на которые подается жалоба, обрабатываются (уголовной) полицией. Наказываемые покушения также подпадают под это определение.

В целом руководство по ведению статистики преступности в Германии имеется в открытом доступе даже на англоязычном сайте ведомства[34], как и ряд других, связанных с этим документов[35].

Общие статистические данные представлены на отдельном портале[36], где они систематизируются после получения от органов государственной власти, занимающихся ведением статистики. Данный портал достаточно большой и представляет не только систематизированную информацию, но и нормативно-правовое регулирование связанных направлений и иные имеющие значение для ресурса и его деятельности документы[37].

Статистическая система Бельгии

В Бельгии федеральная полиция представляет статистику преступности, дорожного движения и несчастных случаев, а также устройства самой

[33] file:///C:/Users/ugpro6/Downloads/pks2011.pdf

[34]https://www.bka.de/SharedDocs/Downloads/EN/Publications/PoliceCrimeStatistics/2020/pks2020Guidelines.pdf?__blob=publicationFile&v=3

[35] https://www.bka.de/EN/CurrentInformation/PoliceCrimeStatistics/2020/pcs2020_node.html

[36] https://www.govdata.de/

[37] https://www.govdata.de/web/guest/open-government

полиции. Данные представляются в четких и понятных для населения графиках и таблицах[38].

Министром внутренних дел Бельгии выбрана прозрачная коммуникация с обществом в представлении информации о преступлениях, установленных полицией Бельгии.

Статистика преступности полиции (PCS) публикуется ежеквартально.

С такой периодичностью публикация не наносит ущерба полноте функционирования правоохранительной системы.

Опубликованные цифры отражают показатель зарегистрированных в Бельгии преступлений.

В то же время государство не отрицает, что в рамках обеспечения безопасности оно может представлять несколько отличающиеся цифры для разных уровней правительства (муниципалитет, милицейская зона, районная, областная, региональная и федеральная). Кроме того, возможен при необходимости долгосрочный анализ, поскольку учитываются разные годы. Полиция полагается на собственные ежемесячные средства для подготовки и оценки своей операционной деятельности.

Основные данные статистики зарегистрированных преступлений предоставляет первичный официальный отчет, подготавливаемый полицией.

Преступление включается в отчет независимо от того, является оно оконченным или рассматривается как покушение. При составлении официального отчета для каждого преступления, совершенного в Бельгии, 1 из 581 муниципалитета должен быть выбран в качестве основы систематизации данных. Таким образом, статистика плотно привязана к географии. Именно эти муниципалитеты затем объединяются в более высокие географические уровни (полицейская зона, судебный округ и т.д.) в отчетах.

Согласно инструкциям, официальный отчет должен быть заполнен в течение 3 недель и передан в Общую национальную базу данных ANG. Общая национальная база данных (ANG) – это полицейская база данных, в которой факты регистрируются на основе официальных отчетов, вытекающих из работы судебной и административной полиции. Это позволяет делать подсчеты, работать с различными статистическими переменными, такими как количество зафиксированных фактов, методы работы, объекты, использованное в преступлении транспортное средство, место назначения. Для некоторых официальных отчетов процесс обработки происходит с некоторой задержкой. На ежегодной основе полнота цифр не меняется, поскольку на момент закрытия отчетов указанное проверяется при подготовке ежегодной полицейской статистики преступности. За счет этого Бельгия гарантирует всему миру надежность своих цифр.

Данные статистики представляются в следующем объеме:

− сами уголовные преступления: преступления против Уголовного кодекса (преступления, проступки и нарушения) и нарушения специальных законов (например, Закон о наркотиках 1921 г.);

[38] http://www.stat.policefederale.be/criminaliteitsstatistieken/rapporten/

− явления, похожие на преступления: факты, которых нет в Уголовном кодексе как таковых, но с которыми регулярно встречается полиция в повседневной практике;

− совокупность преступлений;

− объект или транспортное средство, к которому относится это преступление (например, угон автомобиля);

− место совершения преступления (например, кража со взломом в доме) или способ совершения преступления;

− предметы, с помощью которых преступление было совершено (например, кража с применением оружия);

− описание преступника;

− данные, полученные в результате работы рабочей группы по статистике полиции (WPS);

− направленность деяния: (соотносится с местом преступления) – совершено (например, дорога общего пользования, учебное заведение);

− предметы: предметы, похищенные при различных типах краж;

− транспортные средства: угнанные автомобили представлены по маркам;

− факты, не связанные с преступлениями напрямую: ряд правонарушений, которые сами по себе не наказуемы, но о которых сделано официальное сообщение (например, самоубийство, семейные трудности, потеря вещей) [39].

Следует обратить внимание, что Бельгия представляет достаточно большой объем методической информации о том, что включается в статистику преступности. Так, на официальном сайте полиции можно найти раздел «Методология: примечания и номенклатура»[40], где имеются следующие данные:

– общая методическая записка[41];

– методическая записка «Подозреваемые»[42];

– список сокращений[43];

– регистр PV[44];

– определения преступных форм[45];

– описание номенклатуры[46];

– изменения номенклатуры[47].

[39]http://www.stat.policefederale.be/assets/pdf/methodologie/methodologische_nota_PCS_algemeen.pdf

[40] http://www.stat.policefederale.be/criminaliteitsstatistieken/rapporten/

[41]http://www.stat.policefederale.be/assets/pdf/methodologie/methodologische_nota_PCS_algemeen.pdf

[42] http://www.stat.policefederale.be/assets/pdf/methodologie/methodologie_verdachten.pdf

[43] http://www.stat.policefederale.be/assets/pdf/notas/lijst_afkort_sept_2018.pdf

[44] http://www.stat.policefederale.be/assets/pdf/notas/pv_register_okt_2019.pdf

[45] http://www.stat.policefederale.be/assets/pdf/notas/definities_crim_fig_april_2018.pdf

[46] http://www.stat.policefederale.be/assets/pdf/notas/beschrijving_nomenclatuur_okt_2019.pdf

[47] http://www.stat.policefederale.be/assets/pdf/notas/wijzig_qlf_okt_2019.pdf

Указанные данные помогают гражданским лицам в полной мере разобраться, как организована бельгийская отчетность по преступности.

Статистическая система Испании

Испанская полиция самостоятельно на собственном ресурсе не представляет сведений о преступности. Указанные данные в очень ограниченном объеме можно найти в различных разделах Национального института статистики Испании. При этом следует отметить, что система поиска на электронном ресурсе института работает за счет ключевых слов. В то же время найти подробную статистику преступности в табличной форме и методику ее построения крайне трудно. В основном на ресурсе представлены краткие обзоры в данной области.

Статистическая система Италии

В Италии существует три направления ведения статистики по преступности. В целом статистической отчетностью занимается Национальный институт статистики[48]. В то же время найти на нем статистику преступности достаточно проблемно, так как его деятельность в большей мере направлена на сферы, с ней не связанные. Вместе с тем отдельные исследования в этой области институтом ведутся[49]. Следует учитывать, что институт статистики использует на своем интернет-ресурсе систему поиска через ключевые слова (теги), что облегчает получение нужной информации. Но объемной базы со статистикой по всем преступлениям на ресурсе института нет.

Второй ресурс, представляющий статистические сведения, – это полиция Италии[50]. Необходимо учитывать тот факт, что деятельность полиции направлена на противодействие преступности с привлечением гражданских лиц, поэтому на официальном сайте полиции имеются следующие разделы[51]:

– беглецы (список беглецов максимальной опасности);

– проверьте онлайн, если автомобиль угнан (введя номерной знак или номер шасси, можно проверить, не угнан ли автомобиль);

– утерянные документы (позволяет проверить, был ли документ украден или утерян);

– поддельные банкноты (сервис, позволяющий проверить банкноту на подделку);

– украденные вещи (перечень украденных и возвращенных государственной полицией вещей).

[48] https://www.istat.it/en/
[49] https://www.istat.it/en/archivio/254589
[50] https://www.poliziadistato.it/
[51] https://www.poliziadistato.it/articolo/10582

Представленные разделы синхронизированы с соответствующими полицейскими базами данных и позволяют получить оттуда необходимую информацию. Полиция также представляет статистическую информацию[52], однако она достаточно краткая и касается в основном наркоторговли[53]. При этом полиция готовит весьма крупные годовые обзоры в этой сфере[54].

Наиболее полную статистическую информацию в области преступности готовит Департамент расследований по борьбе с мафией[55]. Данная организация готовит отдельно сведения по противодействию организованной преступности[56] и обзоры о состоянии преступности в целом[57]. В то же время данные отчеты не имеют высокой частоты периодичности и издаются раз в полгода, хотя и состоят из порядка 600 листов. Однако отчеты представлены в текстовой форме и сильно ориентированы на преступления, совершенные итальянской мафией и её членами. Табличная форма в отчетах не используется, что говорит о том, что Италия не применяет современные автоматизированные системы по сбору статистических сведений в области преступности.

Статистическая система Чешской Республики

В Чешской Республике статистика о преступности ведется по принципу «от общего к частному». Так, Чешское статистическое управление собирает и представляет общие данные о преступности и несчастных случаях[58]. Более подробная информация сконцентрирована в МВД Чешской Республики[59]. В то же время следует понимать, что данное ведомство отвечает за достаточно широкий спектр направлений. Так, оно представляет статистическую отчетность по административной деятельности министерства[60], организации работы с иностранцами по представлению временного либо постоянного места жительства на территории Чехии[61], данные по запретам занимать государственные должности[62], сведения о международной защите запросивших указанную услугу лиц[63], сведения о численности жителей муниципальных образований[64], сведения о выданных разрешениях на

[52] https://www.poliziadistato.it/articolo/10273
[53] https://www.poliziadistato.it/articolo/4075e217562bb35a883494644
[54] https://www.poliziadistato.it/statics/22/2020.pdf
[55] https://direzioneinvestigativaantimafia.interno.gov.it/
[56] https://direzioneinvestigativaantimafia.interno.gov.it/page/rilevazioni_statistiche.html
[57] https://direzioneinvestigativaantimafia.interno.gov.it/page/relazioni_semestrali.html
[58] https://www.czso.cz/csu/czso/kriminalita_nehody
[59] https://www.mvcr.cz/statistiky.aspx
[60] https://www.mvcr.cz/clanek/statistiky-spravni-cinnosti.aspx
[61] https://www.mvcr.cz/clanek/cizinci-s-povolenym-pobytem.aspx
[62] https://www.mvcr.cz/clanek/lustrace-29644.aspx?q=Y2hudW09Mg%3d%3d
[63] https://www.mvcr.cz/clanek/mezinarodni-ochrana-253352.aspx
[64] https://www.mvcr.cz/clanek/informativni-pocty-obyvatel-v-obcich.aspx

хранение оружия и боеприпасов[65] и сведения о преступности[66]. Необходимо отметить, что на сайте МВД Чешской Республики представлены достаточно подробные ежегодные отчеты о преступности с детализованной информацией. Сами отчеты занимают порядка 150 страниц текста и цифр и представляются в виде готового сборника. В то же время более обширную информацию о преступности представляет чешская полиция[67] отдельно от МВД. Чешская полиция публикует данные в следующих разделах: статистика преступности, карты преступности, статистика дорожно-транспортных происшествий, дорожно-транспортные происшествия на карте, ежедневная статистика дорожно-транспортных происшествий. Сами данные о преступности публикуются в таблицах Microsoft Excel. Они разбиты по населенным пунктам. Представляются данные практически по всем видам преступлений, что делает работу полиции полностью прозрачной. Также следует обратить внимание на то, что чешская полиция использует в свой работе информационные базы данных, доступ к которым частично представляется гражданским лицам в целях получения наиболее важной информации, например о розыске пропавшего человека, транспортного средства и т.д. Подготавливаемые статистические отчеты в Чехии заполняются автоматически за счет выгрузки данных из указанных баз данных в соответствующие таблицы.

Отдельно следует отметить, что кроме указанного свою статистику ведет пожарно-спасательная служба Чешской Республики, готовя на постоянной основе статистические ежегодники, которые публикует на своем сайте[68].

Статистическая система Республики Казахстан

В соответствии с подпунктом 5 статьи 12 Закона Республики Казахстан от 19 марта 2010 года «О государственной статистике», а также с подпунктом 258) пункта 17 Положения о Министерстве национальной экономики Республики Казахстан, утвержденного постановлением Правительства Республики Казахстан от 24 сентября 2014 года № 1011, председателем комитета по статистике Министерства национальной экономики Республики Казахстан 30 ноября 2016 года был издан приказ № 292 об утверждении Методики по формированию и распространению официальной статистической информации в электронном виде[69].

В соответствии с указанным приказом и методикой статистические данные оформляются и готовятся следующим образом.

---

[65] https://www.mvcr.cz/clanek/zbrane-a-strelivo-92.aspx
[66] https://www.mvcr.cz/clanek/statistiky-kriminality-dokumenty.aspx
[67]https://www.policie.cz/clanek/policie-cr-web-informacni-servis-statistiky-statisticke-prehledy.aspx
[68] https://www.hzscr.cz/clanek/statisticke-rocenky-hasicskeho-zachranneho-sboru-cr.aspx
[69] https://www.gov.kz/memleket/entities/stat/documents/details/42585?lang=ru

При формировании информационного материала в электронном виде соблюдаются следующие параметры:

1) соответствие названия информационного материала по содержанию;

2) форматы информационного материала:

текстовой – *.doc, *.rtf, *.pdf;

графической – *.jpg, *.jpeg, *.gif, *.png;

табличной – *.xls, *.pdf.

3) для формата информационных материалов *.xls листы, не содержащие данных, удаляются;

4) стиль оформления документа.

Информационный материал размещается в сроки и объемах, согласно Плану статистических работ на текущий год. Процесс предоставления информационного материала модератору осуществляется посредством электронной почты или других внутренних информационных ресурсов. При отправке информационного материала по электронной почте пошагово расписывается место для размещения предоставленного информационного материала согласно структуре интернет-портала (раздел, подраздел).

После получения модератором информационных материалов время размещения – 30 минут (в зависимости от объема информационных материалов). Ответственный исполнитель на постоянной основе проводит мониторинг размещенных на интернет-портале информационных материалов и своевременно подает заявку координатору на удаление неактуальной информации и размещение (актуализацию) нового информационного материала. Он также проводит мониторинг на наличие и достоверность отображаемой статистической информации в ИАС «Талдау»[70].

ИАС «Талдау» – это новый подход Агентства РК по статистике к представлению статистической информации в электронном виде, пилотная версия системы доступна пользователям сети Интернет с мая текущего года. На главной странице ИАС «Талдау» пользователь имеет возможность просмотреть интерактивную карту Казахстана, посредством которой может перейти на страницу любого интересующего его региона и ознакомиться с данными по его развитию. Она позволяет пользователю быстро анализировать большие объемы данных в удобном для него формате[71].

ИАС «Талдау» является интерактивной системой предоставления всей актуальной статистической и аналитической информации по статистическим показателям Комитета по статистике и разработана для следующих задач:

1. Предоставление большому кругу заинтересованных пользователей статистической информации в удобном режиме.

2. Стандартизация доступа к статистической информации.

3. Поддержка принятия управленческих решений посредством анализа представленной статистической информации.

[70] https://www.stat.gov.kz/api/getFile/?docId=ESTAT232383

[71] https://www.inform.kz/ru/ias-taldau-predlagaet-proanalizirovat-razvitie-kazahstana-po-bolee-chem-600-tatpokazatelyam_a2415005

4. Оптимизация процесса подготовки отчетности.

Кроме того, в модернизированной «Талдау» расширены функции поиска информации и экспорта не только таблиц, но и графических изображений, актуализированы карты регионов, обеспечена возможность построения своих графиков и диаграмм с возможностью дальнейшего редактирования.

Среди аналитических функций ИАС можно выделить модуль «Сводная таблица», который представляет собой аналитический инструмент для сравнения показателей в разрезе классификаторов (справочников) и дат. ИАС также реализует возможность анализа динамики показателей.

В ИАС «Талдау» Комитета по статистике Республики Казахстан предусмотрены следующие виды анализа статистических данных: анализ динамических рядов; анализ регионального разреза показателей; корреляционный анализ; математический анализ; рейтинг регионов в совокупности показателей[72].

Все методики формирования статотчетности на данный момент доступны в свободном доступе и выложены на интернет−ресурсе Бюро национальной статистики по всем направлениям. Статистические отчеты по преступности можно сформировать и изучить в зависимости от запроса через электронную форму, имеющуюся на сайте Комитета по правовой статистике и специальным учетам Генеральной прокуратуры Республики Казахстан[73]. Таким образом, можно считать, что Казахстан перешел на автоматизированную систему сбора статистики.

[72] Увалиева И.М., Тлебалдинова А.С., Солтан Г.Ж. Анализ казахстанских и российских информационных систем образовательной статистики // Вестник НГИЭИ. − 2016. − №6 (61). − URL: https://cyberleninka.ru/article/n/analiz-kazahstanskih-i-rossiyskih-informatsionnyh-sistem-obrazovatelnoy-statistiki (дата обращения: 04.06.2021).

[73] https://qamqor.gov.kz/portal/page/portal/POPageGroup/Services/Pravstat

ГЛАВА 3. ИЗУЧЕНИЕ ЗАРУБЕЖНОГО ОПЫТА ПО ВОПРОСАМ ОБЪЕМА И ВИДОВ ПРОЦЕССУАЛЬНЫХ И ИНЫХ ДОКУМЕНТОВ, ВКЛЮЧАЕМЫХ В ЭЛЕКТРОННЫЙ ОБРАЗ, ОЦЕНКА ТРУДОЗАТРАТ НА ЕГО ФОРМИРОВАНИЕ, ПЕРЕДАЧА ЭЛЕКТРОННОГО ДЕЛА ПРОКУРОРУ И В СУД, А ТАКЖЕ ОСОБЕННОСТИ ОЗНАКОМЛЕНИЯ УЧАСТНИКОВ СУДОПРОИЗВОДСТВА С ЕГО МАТЕРИАЛАМИ (ОПЫТ РЕСПУБЛИКИ КАЗАХСТАН)

№	*Государство*	*Программное обеспечение*
1	*Казахстан*	*Информационная система «Единый реестр досудебных расследований», включающая в свой состав следующие программные модули:* *- «Электронное уголовное дело»;* *- «SMS-оповещение»;* *- «Публичный сектор»*

Информатизация судопроизводства в целом и уголовного в частности осуществляется по всему миру, в связи с чем опыт зарубежных государств, в особенности стран, имеющих схожий с российским порядок производства по уголовным делам, представляет теоретический и практический интерес. В частности, в Республике Казахстан в декабре 2017 г. в Уголовно-процессуальный кодекс (далее – УПК РК) были внесены изменения, позволяющие расследовать уголовные дела в электронном формате.

Согласно материалам сайта Верховного Суда Республики Казахстан, первое электронное уголовное дело было рассмотрено уже в январе 2018 г.

Законом Республики Казахстан от 21.12.2017 № 118-VI в УПК Республики Казахстан[74] был введен новый термин: «формат уголовного судопроизводства» (ст. 42-1 УПК РК) и предусмотрено два формата: бумажный и электронный. Помимо данной нормы УПК РК содержит понятие электронного документа, определяя его как документ, в котором информация предоставлена в электронно-цифровой форме и удостоверена посредством электронной цифровой подписи (п. 15 ст. 7 УПК РК). Форму электронного документа могут иметь: заявление об уголовном правонарушении (ч. 1 ст. 181 УПК РК); гражданский иск (ч. 5 ст. 167 УПК РК); замечания на полный или краткий протокол судебного заседания (ст. 348, 348-1 УПК РК); протокол главного судебного разбирательства (ч. 8 ст. 347 УПК РК); ходатайство прокурора о восстановлении срока на подачу апелляционной жалобы (ч.1 ст. 419 УПК РК); запрос на истребование уголовного дела для подачи ходатайства, лицами, имеющими право на внесение представления, принесение протеста на вступившие в законную силу судебные акты (ст. 486

[74] Уголовно-процессуальный кодекс Республики Казахстан (с изм. и доп. по сост. на 21.01.2019). − URL: https://online.zakon.kz/Dokument/?doc_id=31575852#pos=3;-227 (дата обращения: 02.10.2021).

УПК РК); ходатайство, протест или представление о пересмотре вступивших в законную силу судебных актов (ч. 1 ст. 488 УПК РК).

При осуществлении электронного документооборота базовым понятием является понятие электронного документа. В пункте 15 ст. 7 УПК РК под таковым понимается документ, в котором информация предоставлена в электронно-цифровой форме и удостоверена посредством электронной цифровой подписи. С нашей точки зрения, данное определение представляется не вполне удачным, поскольку не охватывает электронные документы, удостоверенные или защищенные от внесения изменений иным криптографическим способом.

В виде электронных документов могут быть оформлены следующие доказательства: заключение эксперта (ч. 1 ст. 283 УПК РК); заключение специалиста (ст. 117 УПК РК). Защитник и представитель потерпевшего вправе опрашивать лиц, предположительно владеющих информацией, относящейся к уголовному делу, с помощью технических средств. Ход и результаты такого опроса могут быть отражены на электронном носителе, который приобщается к уголовному делу (п. 5 ч. 3 ст. 122 УПК РК). Сведения в форме электронного документа для приобщения их к уголовному делу в качестве доказательств вправе предоставить подозреваемый, обвиняемый, защитник, частный обвинитель, потерпевший, гражданский истец, гражданский ответчик и их представители, а также любые граждане и организации (ч. 4 ст. 122 УПК РК).

Таким образом, процедура электронного производства по уголовному делу в УПК РК подробно не регламентирована, обозначены лишь возможность ее ведения и определенный перечень процессуальных документов и видов доказательств, которые могут иметь электронный формат.

Вместе с этим законодатель предоставил Генеральному прокурору Республики Казахстан полномочия принимать нормативные акты, обязательные для исполнения всеми органами уголовного преследования, по вопросам ведения уголовного судопроизводства в электронном формате (ч. 6 ст. 58 УПК РК). Такой нормативный акт был принят 3 января 2018 г. и содержит Инструкцию о ведении уголовного судопроизводства в электронном формате (далее − Инструкция).

Исходя из положений данной Инструкции, для осуществления электронного судопроизводства в Республике Казахстан существует информационная система «Единый реестр досудебных расследований» (ИС ЕРДР). Данная информационная система имеет дополнительный функционал − модуль «Электронное уголовное дело» (модуль е-УД), предназначенный для организации подготовки, ведения, отправления, получения и хранения электронного уголовного дела (рис. 4). Также ИС ЕРДР имеет функционал «SMS-оповещение», позволяющий через мобильную связь и (или) электронную почту направлять текстовые сообщения участникам уголовного процесса для их уведомления либо явки к лицу, ведущему уголовный процесс; а также функционал «Публичный сектор», позволяющий

участникам уголовного процесса получать удаленный доступ к материалам электронного уголовного дела, подавать жалобы и ходатайства. В отсутствие возможности удаленного доступа участники уголовного процесса знакомятся с материалами уголовного дела путем воспроизведения лицом, ведущим уголовный процесс, соответствующих материалов, с возможностью получения их электронной копии (п. 26 Инструкции).

Должностное лицо органа уголовного преследования получает доступ к ведению электронного уголовного дела в ИС ЕРДР при прохождении процессов авторизации и аутентификации посредством: электронной цифровой подписи (ЭЦП), выданной Национальным удостоверяющим центром Республики Казахстан; персонального идентификационного номера-кода, присваиваемого государственным органом, осуществляющим в пределах своей компетенции статистическую деятельность в области правовой статистики и специальных учетов; идентификации с использованием биометрического считывателя (п. 9 Инструкции) (рис. 5). При производстве досудебного расследования следственной, следственно-оперативной группой, доступ в модуле е-УД к находящемуся в производстве группы электронному уголовному делу получают члены группы, осуществляющие данное досудебное расследование (п. 31 Инструкции).

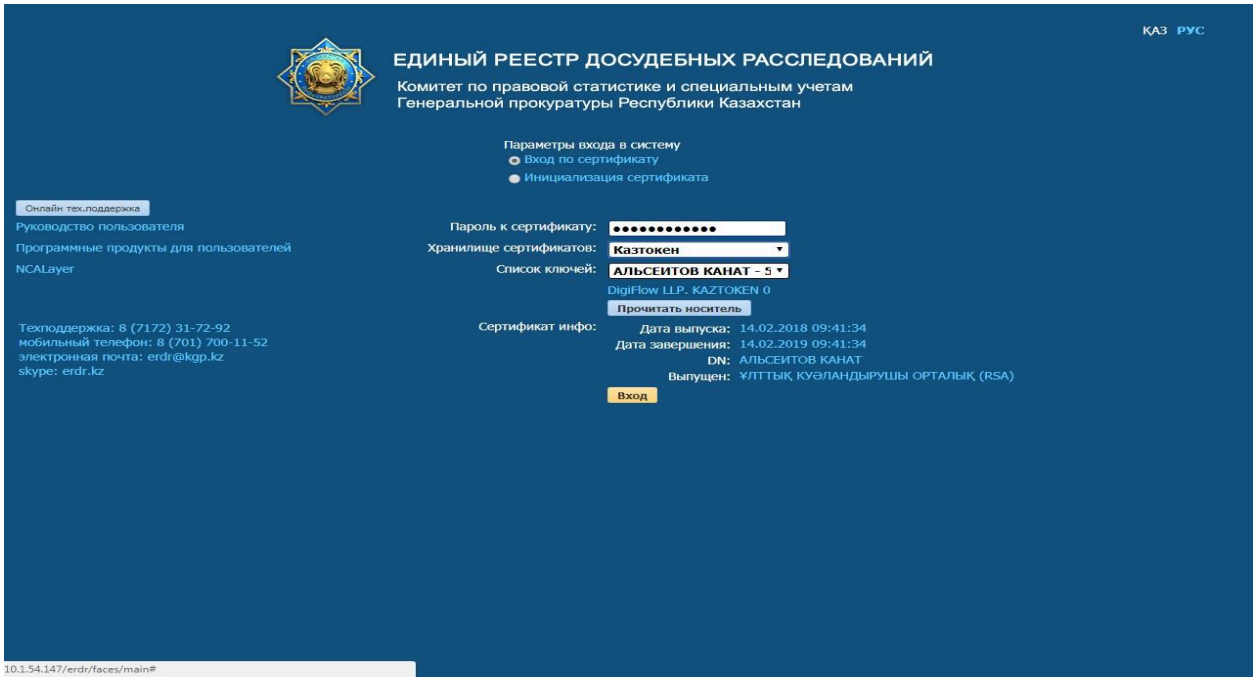


Рисунок 4 − Интерфейс идентификации пользователя е-УД

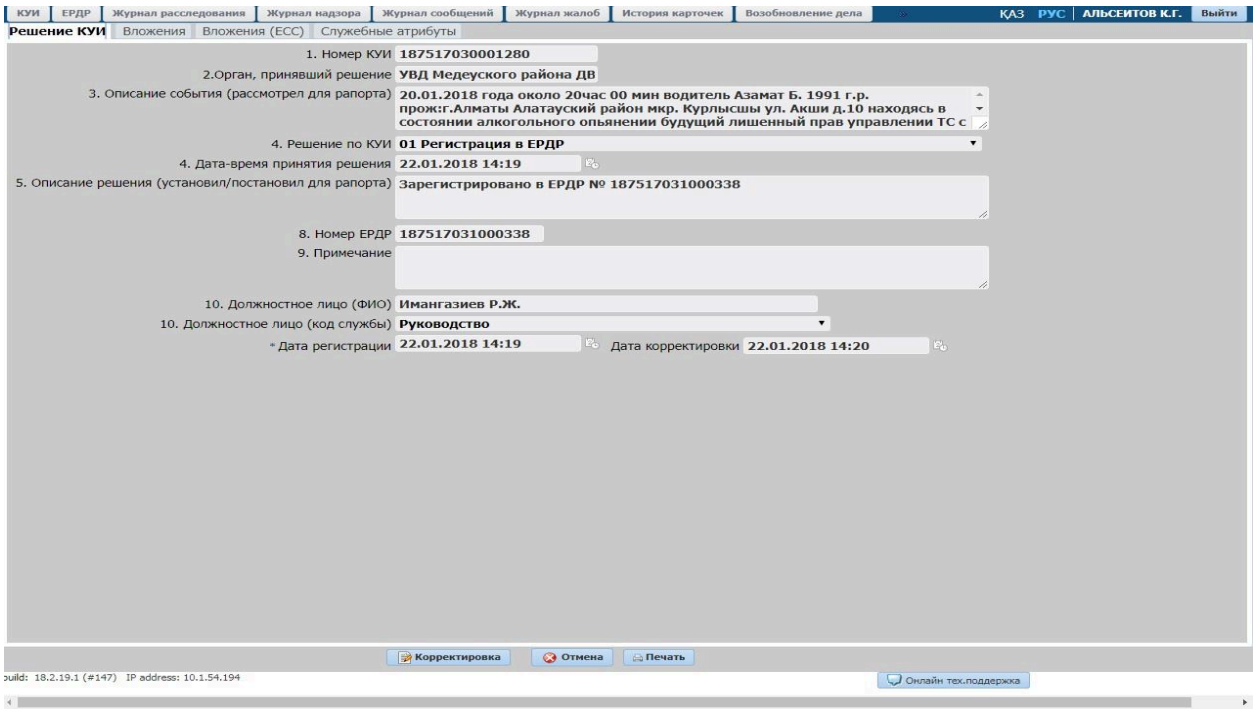


Рисунок 5 − Интерфейс регистрации е-УД в ЕРДР

Еще до начала производства по уголовному делу в ИС ЕРДР автоматически формируются первые электронные документы: «Рапорт о регистрации КУИ», «Рапорт об обнаружении сведений об уголовном правонарушении», «Уведомление прокурора о начале досудебного расследования». В случае принятия решения о ведении электронного уголовного дела вышеуказанные рапорты автоматически вкладываются системой в материалы электронного уголовного дела, а также отражаются в описи электронного уголовного дела (п. 11 Инструкции). В ИС ЕРДР возможно автоматическое формирование сопроводительных писем прокурору и в суд.

Решение о выборе электронного формата уголовного дела принимает лицо, которому поручено досудебное расследование, при принятии его в свое производство (п. 10 Инструкции), о чем выносится мотивированное постановление (ч. 2 ст. 42-1 УПК РК). После вынесения постановления в модуле е-УД в течение 24 часов формируется автоматическое уведомление надзирающему прокурору. В тот же срок о принятом решении уведомляются подозреваемый, обвиняемый, их законные представители, защитник, частный обвинитель, гражданский ответчик, потерпевший, гражданский истец, их представители. Дальнейшее изменение формата ведения уголовного судопроизводства с бумажного на электронный не допускается, кроме случаев соединения уголовных дел (п. 10 Инструкции).

При создании электронных документов лицо, ведущее уголовный процесс, использует имеющиеся в ИС ЕРДР шаблоны. Подписание процессуальных и иных документов, составленных в электронном виде, осуществляется участниками уголовного процесса путем заверения электронной цифровой подписи или посредством планшета подписи (п. 12

Инструкции).

Документы материалов уголовного дела, созданные ранее на бумажном носителе, после принятия решения о ведении уголовного дела в электронном формате сканируются и вкладываются в электронное уголовное дело в виде PDF-документов незамедлительно, но не позднее двадцати четырех часов после вынесения постановления о ведении электронного судопроизводства (п. 11, 14, 16 Инструкции) (рис. 7). Бумажные документы, переведенные в электронный формат, сохраняются органами уголовного преследования, и подлежат направлению в прокуратуру или в суд вместе с электронным уголовным делом (п. 6 Инструкции) (рис. 6). Медиа-файлы, которые по решению лица, ведущего уголовный процесс, приобщены к электронному уголовному делу, подлежат вложению в модуль е-УД (п. 13 Инструкции). В ИС ЕРДР заполняются необходимые информационные учетные документы, осуществляется электронное взаимодействие с экспертами, специалистами, а также с судом (п. 5 Инструкции).

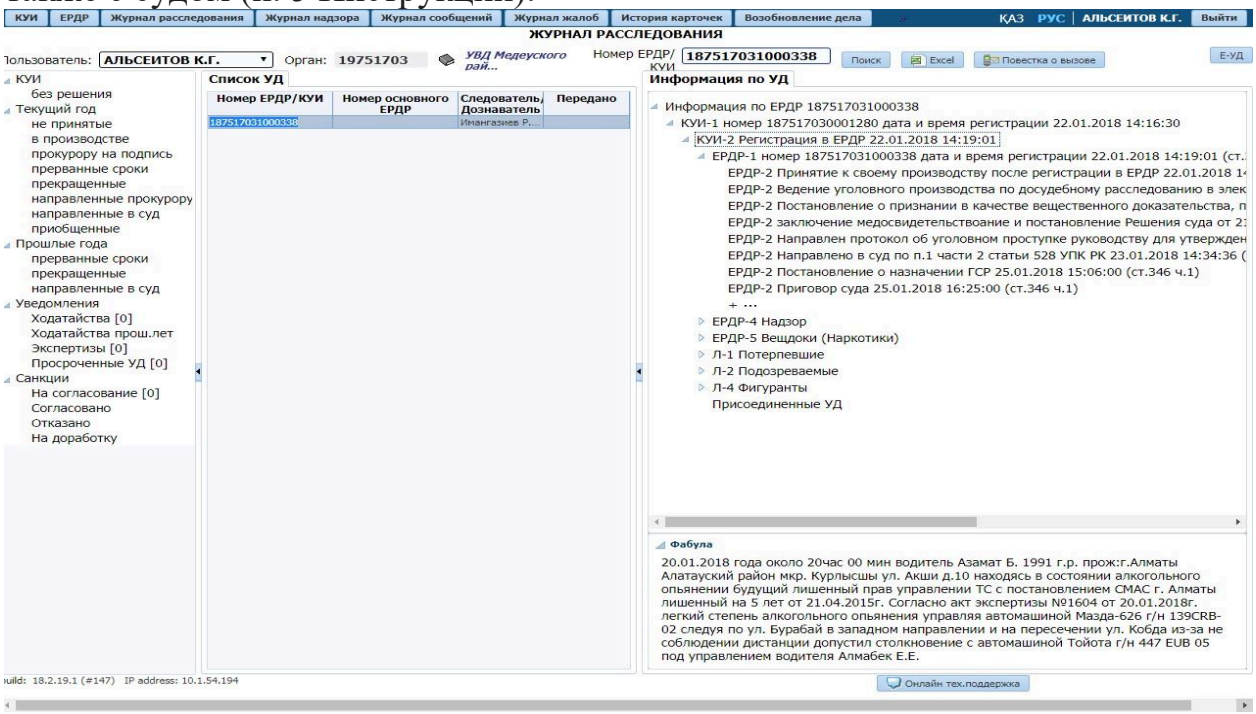


Рисунок 6 − Интерфейс журнала расследования е-УД

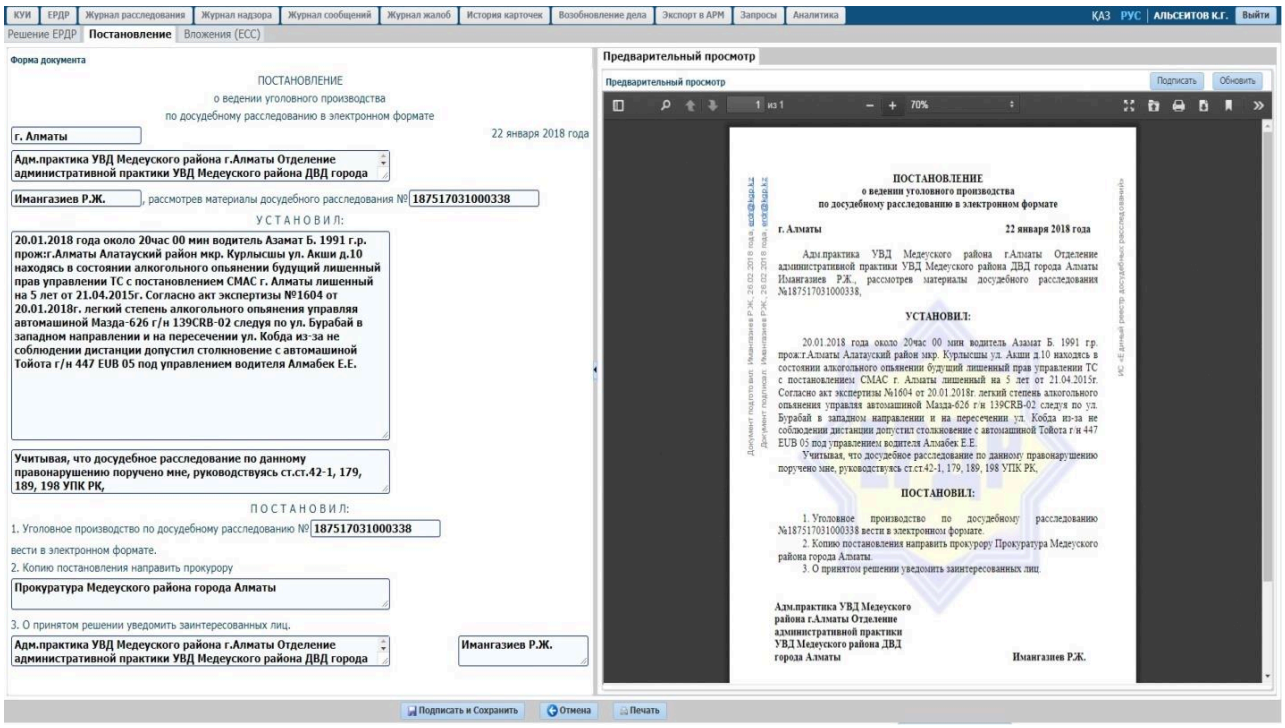


Рисунок 7 − Интерфейс шаблона постановления по е-УД

Изменение формата с электронного на бумажный УПК РК разрешает лишь при невозможности дальнейшего ведения уголовного судопроизводства в электронном формате (ч. 2 ст. 42-1 УПК РК). Инструкция о ведении судопроизводства в электронном формате конкретизирует данную норму. Так, согласно п. 22 Инструкции, переход с электронного на бумажный формат допускается в случае возникновения нештатных (к примеру, отсутствие электроэнергии, связи, доступа к модулю е-УД) или чрезвычайных ситуаций, но не ранее чем по истечении 24 часов с момента возникновения такой ситуации. Если по уголовному делу требуется проведение неотложных следственных или процессуальных действий, допускается переход до истечения 24 часов с момента возникновения нештатной или чрезвычайной ситуации.

Помимо этого переход с электронного формата уголовного судопроизводства на бумажный осуществляется в случаях: направления материалов уголовного дела в иностранное государство для продолжения уголовного преследования; приобщения к материалам уголовного дела сведений, составляющих государственные секреты и иную охраняемую законом тайну (п. 22 Инструкции); соединения уголовных дел по усмотрению лица, ведущего расследование (п. 17 Инструкции).

При переходе из электронного в бумажный формат в ИС ЕРДР в электронном виде заполняется мотивированное постановление и форма об изменении формата уголовного судопроизводства. Далее незамедлительно, но не позднее 24 часов осуществляется распечатывание материалов электронного уголовного дела. Ранее вложенные в модуль е-УД PDF-документы заменяются на оригиналы бумажных документов путем их истребования из мест хранения (п. 23 Инструкции).

При необходимости соединения уголовных дел, каждое из которых ведется в электронном формате, после вынесения лицом, ведущим уголовный процесс, постановления о соединении дел незамедлительно, но не позднее 24 часов обеспечивается соединение дел в модуле е-УД. Если производство по одному или нескольким из соединяемых дел велось в бумажном формате, то лицо, ведущее уголовный процесс, при вынесении постановления о соединении уголовных дел одновременно решает вопрос об определении формата соединенного уголовного дела, который, согласно п. 17 Инструкции, может быть и бумажным, и электронным.

В случае выбора дальнейшего ведения уголовного дела в электронном формате документы материалов соединяемых уголовных дел, которые велись в бумажном формате, незамедлительно, но не позднее 24 часов после принятия соответствующего решения вкладываются в электронное уголовное дело в виде PDF-документа с внесением в модуль е-УД сведений об изменении формата уголовного судопроизводства. В случае выбора дальнейшего ведения уголовного дела в бумажном формате незамедлительно, но не позднее 24 часов осуществляется переход с электронного на бумажный формат (п. 17 Инструкции).

Выделение уголовного дела в отдельное производство осуществляется в модуле е-УД путем выделения материалов дела с присвоением отдельного номера ЕРДР (п. 18 Инструкции). В случае прерывания сроков досудебного расследования в порядке ст. 45 УПК РК в модуле е-УД лицу, ведущему уголовный процесс, ограничивается доступ на совершение процессуальных и иных действий в рамках электронного уголовного дела, кроме тех, которые предусмотрены УПК РК (п. 19 Инструкции).

После принятия органом, ведущим уголовный процесс, решения о прекращении производства по электронному уголовному делу и после изучения прокурором законности принятого процессуального решения, электронное уголовное дело подлежит архивированию. Архивирование осуществляется автоматически, путем сохранения в модуле е-УД с определением соответствующего статуса (п. 20 Инструкции). Решение о передаче электронного уголовного дела по подследственности делает недоступным (неактивным) данное уголовное дело для передающего органа (п. 23 Инструкции).

Доступ к материалам электронных уголовных дел имеет надзирающий прокурор, получающий посредством ИС ЕРДР информирование о принимаемых по делу решениях и имеющий возможность проверки законности, согласования и утверждения процессуальных решений органов, ведущих уголовный процесс, а также передачи электронного уголовного дела в суд (п. 27-29 Инструкции).

Перечисленными вопросами нормативное регулирование производства по электронному уголовному делу по законодательству Республики Казахстан исчерпывается, тем не менее электронные уголовные дела расследуются и рассматриваются в судах. Что же касается возможности перенять опыт

соседнего государства, то анализ законодательства Республики Казахстан, регулирующего вопросы производства по электронному уголовному делу, показывает, что процессуальные вопросы охвачены в нем не в полном объеме. Так, например, законодатель предусматривает переход с электронного формата ведения уголовного дела на бумажный в случае возникновения нештатной или чрезвычайной ситуации, устанавливая срок 24 часа для такого перехода, чтобы предотвратить поспешный отказ от электронного формата уголовного дела, кроме случаев, не терпящих отлагательств (п. 22 Инструкции). Данная норма означает, что в случае любого технического сбоя при необходимости проведения следственных или процессуальных действий производство по уголовному делу окончательно переводится в бумажный формат, возможности изменения которого закон не предусматривает.

Переход из электронного формата уголовного судопроизводства на бумажный формат осуществляется в случаях:

− необходимости направления материалов уголовного дела в иностранное государство для продолжения уголовного преследования;

− необходимости приобщения к материалам уголовного дела сведений, составляющих государственные секреты и иную охраняемую законом тайну.

В УПК РК и Инструкции прямо не указано, каким образом после принятия решения об избрании электронного формата уголовного дела к нему приобщаются материалы и документы, предоставленные защитником либо иными участниками производства по уголовному делу, и оформленные в бумажном формате, каковы требования к электронным документам, представляемым участниками производства по делу следователю, в частности требования к объему документа, качеству сканирования, обязательным реквизитам. Не регламентировано, вправе ли лицо, ведущее производство по электронному уголовному делу, производить следственные действия не в электронном формате в случае производства их в условиях, исключающих ведение электронной документации (повторный осмотр места происшествия, допрос свидетеля по месту его нахождения и т. п.); возможно ли проводить следственные или иные процессуальные действия по электронному уголовному делу с составлением процессуальных документов в бумажном формате, когда возможность составления электронных документов отсутствует, но без перехода на бумажный формат в целом.

Остается открытым вопрос соблюдения сроков предварительного расследования, содержания лиц под стражей и производства следственных и процессуальных действий в случае возникновения долговременных (более 24 часов) сбоев работы ИС ЕРДР или иных нештатных ситуаций при условии нахождения всех материалов уголовного дела в электронном формате и невозможности их распечатывания.

Ведение уголовного судопроизводства на стадии досудебного расследования в электронном формате осуществляется в модуле е-УД посредством:

− заполнения необходимых учетных сведений и реквизитов электронных форм в ЕРДР;

− создания электронных документов на имеющихся шаблонах и PDF-документов в модуле е-УД;

− подписания электронных документов участниками уголовного процесса при помощи ЭЦП или планшета подписи;

− отправки SMS-оповещения для уведомления либо вызова участников уголовного процесса;

− электронного взаимодействия с судом в целях обеспечения процессов по рассмотрению уголовных дел и материалов в электронном формате;

− электронного взаимодействия с экспертами, специалистами для осуществления процедур назначения исследования и получения заключений в электронном формате либо перевода бумажных материалов в электронный формат.

Решение о выборе формата (электронный или бумажный) ведения уголовного дела принимается по своему усмотрению лицом, ведущим уголовный процесс, которому поручено осуществление досудебного расследования, при принятии его в свое производство.

После вынесения постановления в модуле е-УД в течение двадцати четырех часов формируется автоматическое уведомление надзирающему прокурору.

При этом в случае выбора электронного формата в ЕРДР незамедлительно заполняются соответствующая электронная форма, а также шаблон электронного документа.

Дальнейшее изменение формата ведения уголовного судопроизводства с бумажного на электронный формат не допускается, кроме случаев соединения уголовных дел.

Лицо, ведущее уголовный процесс, в течение двадцати четырех часов уведомляет о принятом решении участников уголовного процесса – подозреваемого, обвиняемого, их законных представителей, защитника, частного обвинителя, гражданского ответчика, потерпевшего, гражданского истца, их представителей.

Документы материалов уголовного дела, созданные ранее на бумажном носителе, после принятия решения о ведении уголовного дела в электронном формате вкладываются в электронное уголовное дело в виде PDF-документов незамедлительно, но не позднее двадцати четырех часов после вынесения постановления о ведении электронного судопроизводства.

При этом до принятия решения о ведении уголовного судопроизводства в электронном формате в ЕРДР автоматически формируются первые электронные документы: «Рапорт о регистрации КУИ», «Рапорт об обнаружении сведений об уголовном правонарушении» и «Уведомление прокурора о начале досудебного расследования».

В случае принятия решения о ведении электронного уголовного дела вышеуказанные рапорты автоматически вкладываются системой в материалы

электронного уголовного дела, а также отражаются в описи электронного уголовного дела.

Возможность автоматического формирования предусматривается также для сопроводительных писем прокурору и в суд.

Ведение электронного уголовного дела осуществляется с использованием электронных шаблонов уголовных документов, содержащихся в ЕРДР.

При создании электронных документов лицо, ведущее уголовный процесс, использует имеющиеся в ЕРДР шаблоны, но при этом формирует текст документа самостоятельно (рис. 8).

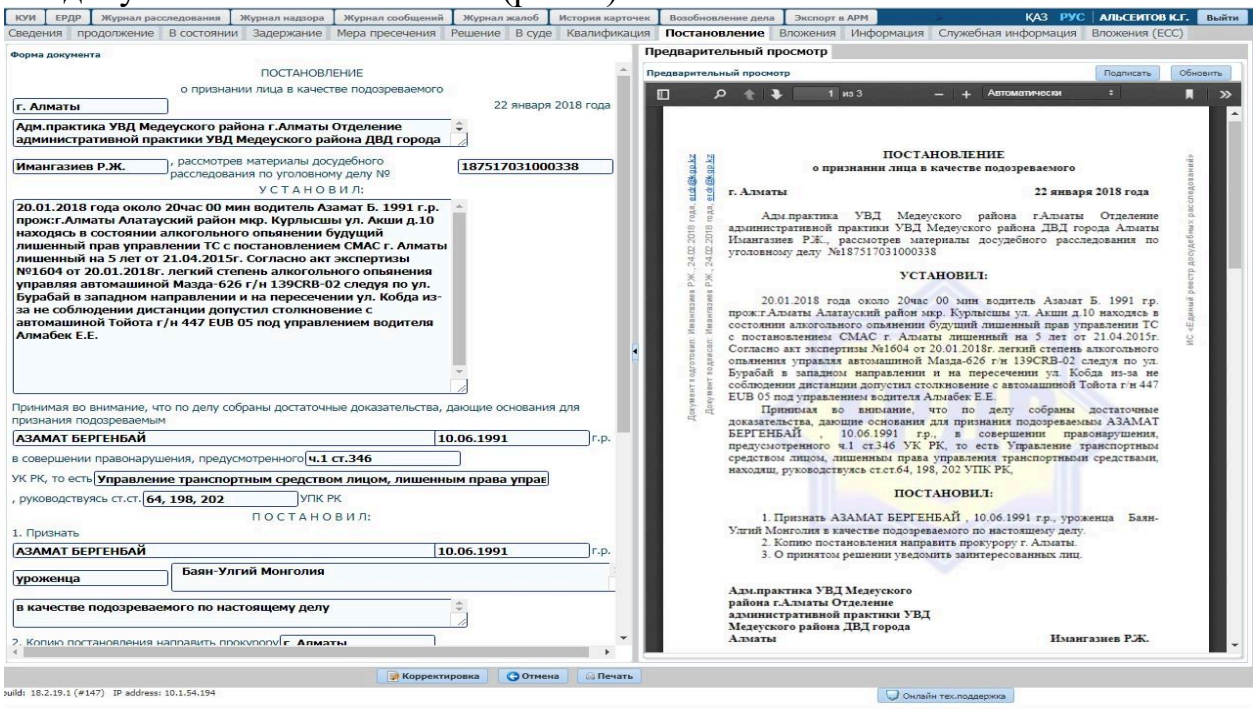


Рисунок 8 − Интерфейс шаблона для заполнения процессуального документа в е-УД

Подписание процессуальных и иных документов, составленных в электронном виде, осуществляется участниками уголовного процесса путем заверения ЭЦП или посредством планшета подписи.

Медиа-файлы, которые по решению лица, ведущего уголовный процесс, приобщены к электронному уголовному делу, подлежат вложению в модуль е-УД.

По процессуальным документам (например, протоколу осмотра места происшествия, протоколу эксгумации и т.д.), составленным в бумажном виде в ходе совершения выездных следственных действий, или по иным материалам уголовного дела, документы которых составлены на бумажном носителе по причине невозможности их ввода в электронном формате, формируется PDF-документ с вложением в модуль е-УД.

Документы, поступающие в бумажном формате и подлежащие приобщению к материалам электронного уголовного дела, при поступлении

лицу, ведущему уголовный процесс, также переводятся в PDF-документ и вкладываются в модуль е-УД.

Перевод указанных документов в PDF-документ и вложение в модуль е-УД производится незамедлительно, но не позднее двадцати четырех часов, после составления или поступления документа (материала).

Материалы проведенных негласных следственных действий вводятся в электронное дело после их исследования в виде PDF-документа или медиа-файла.

В случае необходимости направления в рамках ведения электронного уголовного дела сопроводительных писем, уведомлений, запросов и т.д. в бумажном виде после совершения действия все бумажные материалы незамедлительно, но не позднее двадцати четырех часов переводятся в PDF-документ и вкладываются в модуль е-УД.

При этом по запросу органа, ведущего уголовный процесс, наряду с бумажным экземпляром заключение эксперта и специалиста одновременно может быть составлено в форме электронного документа, который подлежит вложению в электронное уголовное дело.

При невозможности составления заключения в форме электронного документа бумажный вариант заключения лицом, ведущим уголовный процесс, переводится в PDF-документ, который также подлежит вложению в электронное уголовное дело.

При расследовании уголовных дел в электронном формате необходимо уделять внимание следующим проблемным вопросам:

− электронная информация подвержена воздействию извне, т. е. необходимо тщательно проработать механизм защиты базы данных от различных посягательств, которые могут влиять как на объективность досудебного расследования, так и на информацию статистического характера (сведения о судимости, отчеты и т. д.);

− повсеместное ведение досудебного расследования в электронном формате предполагает большие финансовые затраты, которые связаны с приобретением соответствующего оборудования − программно-аппаратных комплексов CERTEX VPN B стоимостью 1 696 428,57 тенге (около 285 480 руб.) и CERTEX VPN MB стоимостью 142 857,14 тенге (около 24 000 руб.), графического планшета для создания цифрового аналога подписи стоимостью 77 678,57 тенге (около 13 000 руб.), биометрического смарт-картридера стоимостью 51 785,71 тенге (около 8 700 руб.). Приведенный перечень оборудования имеет сопоставимые аналоги и не является исчерпывающим. В среднем для оснащения одного автоматизированного рабочего места следователя (дознавателя) необходимо приобрести оборудование на общую сумму около 3 500 000 тенге (589 000 руб.);

− практика производства досудебного расследования уголовных дел в электронном формате показывает, что скорость работы модуля «е-УД» напрямую зависит от его загруженности, что говорит о необходимости

наличия существенных серверных мощностей для регистрации и обработки поступающей в систему информации по уголовному делу.

На реализацию рассматриваемого процесса в Республике Казахстан с декабря 2017 по 2021 г. было выделено из республиканского бюджета 1 161 887 тенге. В настоящий момент примерное соотношение курса тенге составляет 16,8283 RUB за 100 KZT. Ответственным органом за исполнение пункта данной программы была назначена Генеральная прокуратура РК. В то же время, по различным данным, на реализацию всей системы денег потребовалось на много больше.

Так, исходя из имеющейся информации, каждое ведомство получало финансовое обеспечение из разных бюджетов. МВД РК – из местного бюджета было выделено 9 млрд. тенге (по ранее указанному курсу примерно 1 514 546 999 руб.), НБПК РК – 750 млн тенге из республиканского бюджета (126 212 249 руб.), ГП РК – из республиканского бюджета − 100 млн. тенге (16 828 299руб.), КГД РК – приобретено техники на 75 млн. тенге (12 621 224 руб.), из республиканского бюджета дополнительно выделено 200 млн тенге (33 656 599 руб.).

Таким образом, на реализацию проекта было затрачено порядка 10 126 161 887 тенге (примерно 1 704 060 руб.), из них на 86 000 сотрудников МВД Республики Казахстан было потрачено порядка 9 001 161 887 тенге (1 514 742 руб.), что составляет в среднем 104 664 тенге на 1 сотрудника полиции (17 613 руб).

По различным данным, в МВД России в настоящий момент числится порядка 828 650 сотрудников. Таким образом, затраты на реализацию такого проекта в России (по самым минимальным показателям с учетом текущего курса валют и уровня инфляции в 19.22% с декабря 2017 г.) могут составить порядка 17 400 033 391 руб. только на МВД России, не включая другие ведомства [75].

Сложности переходного периода при передаче уголовного дела прокурору

Опыт Федеративной Республики Германии показывает, что при передаче материалов уголовного дела прокурору органы предварительного расследования достаточно широко используют различные телекоммуникационные средства, предназначенные для передачи данных в электронном формате. Примером подобной телекоммуникационной системы служит единый портал документооборота «Elektronischer Dokumenterdurchlauf»[76]. Однако зачастую немецкий правоприменитель сталкивается с проблемами передачи некоторых материалов уголовных дел, в отношении которых действует режим ограниченного обращения, то есть

[75] Данные предоставлены Комитетом по правовой статистике и специальным учетам Генеральной прокуратуры Республики Казахстан.

[76] https://www.diadoc.ru.

содержащих охраняемую законом тайну и не подлежащих свободной передаче в виде электронного документа. Принимая во внимание данное обстоятельство, часть материалов уголовного дела при электронном типе производства передается прокурору на бумажном носителе.

В некоторых азиатских странах, например Сингапуре, все материалы уголовного дела передаются в прокуратуру в электронном виде посредством зашифрованных каналов связи[77].

Вещественные доказательства подлежат фактический передаче прокурору в упаковке, на которую нанесен специальный QR−код, определяющий принадлежность вещественного доказательства к конкретному уголовному делу. Однако системы, которые используются сингапурскими правоохранительными органами, бывают уязвимы для хакерских атак, что ставит под угрозу сохранность сведений, содержащихся в материалах уголовного дела. В этой связи проблемы, связанные с передачей уголовного дела надзирающему прокурору, в Сингапуре до сих пор не разрешены.

В Китайской Народной Республике при переходе на электронную форму производства по уголовным делам (об этом писали ранее см. стр. 7 к настоящей работе) возникли проблемы передачи его материалов надзорному ведомству для ознакомления и принятия процессуальных решений. В связи с отсутствием в КНР единой телекоммуникационной системы взаимодействия между правоохранительными органами, передача материалов уголовного дела в электронном виде невозможна, что приводит к фактическому предоставлению материалов прокурору на физическом носителе.

Таким образом, необходимость создания единой системы обмена процессуальными документами обуславливает значительные вложения государства в финансирование создания закрытых информационно-телекоммуникационных систем и поддержания их стабильности.

[77] Электронная служба подачи документов (Electronic Filing System) и электронная служба извлечения документов (Electronic Extract Service) // Rusakova E.P., Dudin M.N., Shakhov O.F., Shakhova M.S., Sizova Yu.S. Digital technologies as a driver of intellectual stratification of human resources: socioeconomic inequality. International Journal of Recent Technology and Engineering. 2019. Vol. 8. № 2. p. 4436-4440

ГЛАВА 4. ИЗУЧЕНИЕ ЗАРУБЕЖНОГО ОПЫТА В СФЕРЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (ПРОТИВОДЕЙСТВИЕ УГРОЗЕ УТЕЧКИ ПРЕДСТАВЛЯЮЩИХ ТАЙНУ СЛЕДСТВИЯ ДАННЫХ, ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ ОТ ВРЕДОНОСНЫХ ПРОГРАММ, НЕСАНКЦИОНИРОВАННОГО ДОСТУПА И КОМПЬЮТЕРНЫХ АТАК, А ТАКЖЕ ПРЕДОТВРАЩЕНИЕ УГРОЗ ВНЕСЕНИЯ ИЗМЕНЕНИЙ В ЭЛЕКТРОННЫЕ ДОКУМЕНТЫ КАК ИЗВНЕ, ТАК И ВНУТРИ СИСТЕМЫ)

№	Государство	Обеспечение информационной безопасности
1	Соединенные Штаты Америки (США)	CM/ECF (Case Management and Electronic Case Files) − система организации движения электронных дел в судах. Идентификация, аутентификация и авторизация пользователя по логину и паролю. Генерация отметки безопасности в виде хеш-суммы для каждого поданного документа PDF для обеспечения целостности и достоверности данных. Разграничение доступа с помощью редактирования конфиденциальной информации для различных уровней доступа (один документ хранится в различных видах: версия документа, доступная для всеобщего просмотра, и неотредактированная версия с соответствующими ограничениями доступа). Использование децентрализованных баз данных для повышения отказоустойчивости. Использование нескольких систем безопасности с комбинацией аппаратных, программных и процедурных барьеров (многоуровневая защита).
2	Федеративная Республика Германия	Электронный судебный и административный почтовый ящик (EGVP). Аутентификация и авторизация пользователя с помощью электронной цифровой подписи (далее − ЭЦП). Сквозное шифрование передаваемых сообщений и информации, основанное на стандартах протокола OSCI. Обеспечение подлинности документов с помощью ЭЦП. Использование различных типов шифрования для информации различных степеней конфиденциальности (информация в документах разделяется на части в соответствии с требованиями по безопасности и шифруется с помощью различных типов шифрования, таким образом, уполномоченные лица имеют доступ только к необходимой части данных документа).
3	Чешская Республика	Электронное уголовное судопроизводство. Отправка документов в электронной форме и приложений к ним осуществляется с использованием ЭЦП. Шифрование передаваемых сообщений.
4	Республика Казахстан	Единый реестр досудебных расследований. Аутентификация и авторизация пользователя с помощью ЭЦП.

№	Государство	Обеспечение информационной безопасности
		Шифрование трафика на алгоритме ГОСТ 28147–89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования». Обеспечение подлинности передаваемых документов с помощью ЭЦП.

Обеспечение информационной безопасности является одной из важнейших задач при создании любой распределенной системы обработки электронных документов.

Правовую основу защиты служебной информации ограниченного распространения составляют следующие нормативные правовые документы:

− Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[78];

− Указ Президента РФ от 6 марта 1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера»[79];

− Постановление Правительства РФ от 3 ноября 1994 г. № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти и уполномоченном органе управления использованием атомной энергии»[80];

− ведомственные акты (Приказ МВД России от 09.11.2018 № 755 «О некоторых вопросах обращения со служебной информацией ограниченного распространения в системе МВД России»[81]).

В соответствии с «Положением о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти» к служебной информации ограниченного распространения относится несекретная информация, касающаяся деятельности организаций, ограничения на распространение которой диктуются служебной необходимостью, а также поступившая в организации несекретная информация, доступ к которой ограничен в соответствии с федеральными законами. Руководители федеральных органов

[78] Об информации, информационных технологиях и о защите информации : Федеральный закон от 27.07.2006 № 149-ФЗ [Электронный ресурс]. – URL: http://consultant.ru (дата обращения: 08.03.2021).

[79] Об утверждении Перечня сведений конфиденциального характера : указ Президента РФ от 06.03.1997 № 188 (ред. от 13.07.2015) [Электронный ресурс]. – URL: http://consultant.ru (дата обращения: 08.03.2021).

[80] Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти и уполномоченном органе управления использованием атомной энергии : постановление Правительства РФ от 20.02.2016 № 123 (ред. от 06.08.2020) [Электронный ресурс]. – URL : http://consultant.ru (дата обращения: 08.03.2021).

[81] О некоторых вопросах обращения со служебной информацией ограниченного распространения в системе МВД России : приказ МВД России от 09.11.2018 № 755 [Электронный ресурс]. – URL: http:// mvd.consultant.ru (дата обращения: 08.03.2021).

исполнительной власти в пределах своей компетенции определяют категорию должностных лиц, уполномоченных относить служебную информацию к разряду ограниченного распространения и обеспечивать ее защиту. Данное определение не раскрывает сущности рассматриваемой категории информации даже по той причине, что непонятно, что такое служебная необходимость и кто ее определяет. При анализе данного определения становится очевидным, что законодатель к служебной информации относит, во-первых, ту информацию, которая образуется в деятельности государственного органа, и связывает ее со служебной необходимостью и, во-вторых, ту информацию, которая поступает в официальном информационном обмене в орган государственной власти и содержит, налоговую тайну, аудиторскую тайну, тайну следствия, тайну судопроизводства, рассматриваемую в данном исследовании, тайну совещания судей и др.

Далее будет рассмотрен опыт иностранных государств в сфере обеспечения информационной безопасности.

Опыт США

Ранний прототип описанной выше системы CM/ECF был создан осенью 1995 года небольшой группой автоматизации Административного управления судов США (AOUSC) для изучения возможности создания полностью интегрированной службы управления делами и электронными файлами. Прототип был создан для обработки документов одного из больших судебных процессов в окружном суде США. Эта служба начала работать в январе 1996 года, а затем была пересмотрена и внедрена осенью 1996 года для одного из крупнейших судов США по делам о банкротстве. В 1997 году AOUSC опубликовал печатный труд «Электронные дела в федеральных судах: предварительное рассмотрение целей, проблем и предстоящего пути» («Electronic Case Filesin the federal courts: A Preliminary Examinationof Goals, Issues, and the Road Ahead»), в котором описывается возможность уменьшения зависимости федеральных судов от бумажных документов, используя новые технологии для хранения, ведения и поиска информации из файлов дела в оцифрованной форме[82]. К 2005 году 80% судов полностью внедрили CM/ECF, и теперь все суды используют эту систему. Тем не менее мало что было опубликовано с описанием системы и объяснением основных причин этого успеха.

Успех можно измерить разными способами: степень принятия судами, юридическим сообществом и общественностью; объем и степень использования как передачи документов в суды, так и из них; надежность, достоверность и безотказность услуги; эффективность и результативность

[82] Electronic Case Filesin The Federal Courts: A Preliminary Examination of Goals, Issues, and the Road Ahead [Электронный ресурс]. – URL: https://silo.tips/download/electronic-case-files (дата обращения: 10.03.2021).

обслуживания и продуктивность персонала; улучшение общего качества правосудия.

Все федеральные судебные исполнители, а также юридический и административный персонал приняли CM/ECF в качестве системы официального учета и управления делами. Более 625 000 юристов подали документы в CM/ECF в электронном виде. Ежегодно открывается более 2 100 000 новых дел, представляется более 60 000 000 новых записей в досье и электронных документов, а также 525 000 000 электронных уведомлений передаются из судов сторонам. Системы CM/ECF хранят значительный объем судебной информации: 41 000 000 дел, более 500 000 000 документов и 850 000 000 записей в досье, которые включают активные и закрытые дела.

Спрос на услуги CM/ECF является значительным: более 325 000 частных лиц и организаций ежегодно делают полмиллиарда запросов в открытом доступе (PACER) и загружают несколько миллиардов страниц судебной информации и документов[83].

Серверы и системы CM/ECF всегда в сети, круглые сутки, 365 дней в году. Вновь представленные документы, записи в досье и обновления доступны всем пользователям в течение нескольких секунд, а автоматические электронные уведомления суда передаются в течение нескольких секунд или минут.

Службы CM/ECF доказали свою устойчивость к нескольким крупным стихийным бедствиям и антропогенным катастрофам, а также к резким изменениям в отчетности и государственной политике. Террористическая атака 11 сентября 2001 года на Всемирный торговый центр, ураган «Катрина», обрушившийся на Новый Орлеан и другие населенные пункты Персидского залива в 2005 году, и наводнения в нескольких штатах Среднего Запада вызвали лишь незначительные перебои в работе служб CM/ECF. Все это говорит о высокой степени защищенности информации, хранящейся в данной системе, особенно в рамках обеспечения доступности и целостности информации.

В 2005 году Конгресс США внес в закон США о банкротстве кардинальные изменения, которые привели к огромному увеличению числа новых дел, поданных в течение многих месяцев, но не повлекли за собой увеличения кадровых ресурсов суда и каких-либо задержек в рассмотрении дел.

Различные организации и судебные органы описали, что желательно или необходимо для судебной власти для предоставления услуг электронного управления делами и электронной подачи документов. CM/ECF достигла или превзошла все стандарты или принципы, опубликованные различными органами. Эти принципы включают такие вопросы, как: равный и своевременный доступ (письменный, аудио и видео) к судебным записям; непрерывность и устойчивость обслуживания; качество, безопасность и

[83] Electronic Filing (CM/ECF) [Электронный ресурс]. – URL: https://www.uscourts.gov/court-records/electronic-filing-cmecf (дата обращения: 10.03.2021).

проверка информации, прозрачность судебного процесса; эффективный обмен информацией между государственными структурами и публикация мнений в режиме онлайн.

Обеспечение информационной безопасности в CM/ECF

При создании в 1995 году рабочего прототипа системы было неясно, как обеспечить защиту информации, хранящейся в ней, а в частности, какой международный стандарт для цифровых подписей может быть выбран. Было решено, что CM/ECF будет временно использовать традиционные логин и пароль для идентификации пользователя. Успешная парольная аутентификация пользователя рассматривалась как «подпись» для любых документов, поданных пользователем. Кроме того, система генерировала отметку безопасности «хеш-таблицы» для каждого поданного документа PDF, чтобы обнаруживать любую последующую ошибку или вмешательство, которые могут изменить поданный документ. Каждый принятый документ имеет электронную отметку времени, и при необходимости доступна программа проверки документов, чтобы убедиться, что документ в CM/ECF соответствует исходному представлению. Документы CM/ECF с ограниченным доступом или закрытым статусом имеют дополнительные ограничения. Этот «временный» подход сработал настолько хорошо, что используется по сей день. При сотнях тысяч пользователей и миллионах документов, поданных каждый месяц, не было случаев, когда податели документов отрицали, что они действительно составляли приписываемую им регистрацию, и не было случаев подделки документов.

Судьи, сотрудники судов, адвокаты и общественность − все имеют доступ к одним и тем же данным CM/ECF. Большая часть информации в системе является общедоступной, но некоторая часть − нет, например, дела несовершеннолетних, запечатанные обвинительные заключения и документы, содержащие коммерческую тайну. Таким образом, система включает функции для ограничения доступа к информации, которая должна быть доступна только определенным лицам. Некоторые документы, доступные для общественности, содержат определенные элементы информации, которые должны быть ограничены для защиты интересов конфиденциальности, например, номера банковских счетов, номера социального страхования, некоторые медицинские факты и имена несовершеннолетних лиц. Когда такие документы подаются, по решению суда, ответственность за редактирование такой конфиденциальной информации лежит на лице, подающем данную информацию. Таким образом, заявитель отправляет отредактированную версию документа, доступную для всеобщего просмотра, и неотредактированную версию с соответствующими ограничениями доступа.

Система CM/ECF должна быть доступна семь дней в неделю, чтобы быстро реагировать на запросы, обеспечивать эффективный ввод информации без перебоев в течение нескольких секунд и обеспечивать точную и

своевременную информацию, которая не может быть незаконно изменена или недостоверна. Чтобы достичь таких стандартов, судебные компьютерные установки требуют избыточности, включая резервные источники питания, компьютерные диски RAID, память с коррекцией ошибок, репликацию базы данных в реальном времени, переключение при отказе и надежные внутренние сети связи. Система CM/ECF избежала зависимости от какого-либо отдельного местоположения или компьютерного комплекса и запретила любое отдельное критическое местоположение (оборудование или сеть), чтобы не вызвать серьезный сбой для всей судебной системы. CM/ECF разрешила каждому крупному суду или региональному офису вести и поддерживать свои базы данных. Скорость отклика системы постоянно отслеживается, и для большинства отчетов и запросов ответы и обновления экрана ожидаются в течение нескольких секунд или долей секунд. Так как не существует стопроцентно защищенной компьютерной системы и базы данных, была реализована концепция «многоуровневой защиты» с комбинацией аппаратных, программных и процедурных барьеров, чтобы избежать угроз, уязвимостей и защитить конфиденциальные данные и информацию от манипуляций, ненадлежащего доступа или кражи личных данных пользователя[84].

Однако стоит отметить, что данная система, как и многие другие, неидеальна. Так, в январе 2021 года появились сообщения о том, что электронная система подачи документов CM/ECF могла быть скомпрометирована серьезным нарушением безопасности − настолько серьезным, что пользователям посоветовали избегать подачи «строго конфиденциальных» документов через цифровую службу. Административное управление судов США объявило 6 января, что оно работает с Министерством внутренней безопасности (DHS) над проведением аудита безопасности для выявления потенциального взлома его системы управления делами (CM/ECF). Отмечается, что причиной данных событий является резкий переход к удаленной работе в 2020 году вследствие пандемии COVID-19 и отсутствие времени для адаптации и усиления протоколов безопасности данных. Из-за цифровой кибератаки был произведен пересмотр подхода к тому, как стороны должны обрабатывать и представлять «строго конфиденциальные судебные документы». Каждому федеральному суду поручено издать общие постановления, в которых излагаются его конкретные процедуры подачи и определения документов, которые он считает «строго конфиденциальными»[85].

[84] Insights to Building a Succesful E-filing Case Management Service: U.S. Federal Court Experience [Электронный ресурс]. – URL : https://www.iacajournal.org/articles/abstract/10.18352/ijca.74/ (дата обращения: 10.03.2021).

[85] Vulnerabilities In Federal Court's E-Filing System Serves As Stark Data Security Warning For Employers [Электронный ресурс]. – URL: https://www.fisherphillips.com/news-insights/federal-courts-efiling-system-start-data-security.html (дата обращения: 10.03.2021).

Опыт Федеративной Республики Германии

Инфраструктура EGVP, обеспечивающая функционирование электронного правосудия в Германии, которая была описана в главе 1, использует для передачи информации входящий в ее состав специальный почтовый ящик электронного правительства (beBPo)[86]. Система EGVP выглядит как программа электронной почты, однако она дополнена важными техническими функциями, обеспечивающими безопасность информации, а именно протоколом передачи и проверки электронной цифровой подписи и сквозным шифрованием, основанным на стандартах протокола OSCI. EGVP гарантирует целостность, подлинность, конфиденциальность и отслеживаемость передачи сообщений, а также обеспечивает защиту в небезопасных сетях, таких как Интернет. OSCI − это стандарты протокола для безопасного обмена электронными сообщениями через интернет и другие сети Германии. OSCI − это обязательный стандарт передачи для электронного правительства. Благодаря данному протоколу шифрования власти могут автоматически обмениваться файлами и информацией друг с другом, с компаниями и с гражданами[87].

Поскольку электронная подпись по закону приравнивается к рукописной, документы также могут быть авторизованы в цифровом виде. Особенно высокий уровень безопасности требуется для передачи конфиденциальных документов с электронными подписями. Используемый стандарт должен гарантировать, что данные являются подлинными, не могут быть изменены и что доступ к ним имеют только уполномоченные лица и процессы. Кроме того, отправляемые и получаемые данные должны поддаваться проверке. Стандартный транспортный протокол OSCI отвечает этим высоким требованиям благодаря своей концепции многоуровневого шифрования. Это позволяет властям предлагать конфиденциальные операции через интернет.

Разделив содержимое, структуру и макет, части документа, которые важны для всех участников, могут быть легко записаны, разделены на различные области безопасности и при этом постоянно сохранены как полный документ в «необработанной форме». OSCI поддерживает безопасную и юридически обязательную связь как единый процесс[88].

Обмен сообщениями с помощью OSCI основан на определенных формах. В сообщениях OSCI данные об использовании и содержании строго разделены − доступ посторонних лиц исключен из-за различных типов

---

[86] Elektronisches Gerichts - Und Verwaltungspostfach [Электронный ресурс]. – URL: https://egvp.justiz.de (дата обращения: 10.03.2021).

[87] IT-Sicherheit der EGVP-Infrastruktur [Электронный ресурс]. – URL: https://egvp.justiz.de/Informatio№_IT_Sicherheit_EGVP_2018_08_28.pdf (дата обращения: 10.03.2021).

[88] OSCI – der technische Protokollstandard für die öffentliche Verwaltung [Электронный ресурс].– URL: https://www.itzbund.de/DE/itloesungen/standardloesungen/osci/osci_node.html (дата обращения: 10.03.2021).

шифрования, уполномоченные лица имеют доступ только к необходимой части данных. Расширенные данные об использовании позволяют отправлять сообщения на основе правил. Централизованные услуги передаются посредникам без потери конфиденциальности и при сохранении защиты данных, что означает, что дорогостоящие технологии и сложная организация / администрирование могут быть централизованы.

Низкие технические требования для конечного пользователя: помимо персонализированной чип-карты для подписи пользователю необходим только доступ в интернет со стандартным браузером и устройством для чтения карт для подписи (терминал для чип-карт класса 3).

Пример применения протокола OSCI.

На своем компьютере пользователь выбирает желаемую форму с помощью гиперссылок, например, запрос свидетельства о рождении из ответственного органа регистрации актов гражданского состояния (или ЗАГСа) через городскую информационную систему. Подпись гарантирует, что пользователь действительно работает с формой из нужного места, которое также отвечает только за выполнение обещанных и ожидаемых действий. Кроме того, передача происходит через защищенное SSL-соединение. Структура данных, необходимая для этой бизнес-операции, четко указана в спецификации OSCI, например: «для заявки на свидетельство о рождении», также указано, какие данные гражданин должен ввести, какие являются необязательными и могут ли определенные поля принимать только определенные значения, например только числовые записи в поле «Год рождения». Прежде чем гражданин подпишет заявление после его заполнения, ему повторно представляются данные заявления. Только после этой юридически необходимой визуализации он подписывает свои записи. Теперь создано сообщение OSCI, которое может быть передано получателю. Поскольку их содержимое обычно является важными и в некоторых случаях очень конфиденциальными личными данными, содержимое защищено от несанкционированного просмотра или манипуляции на пути передачи с использованием криптографических методов.

Помимо данных содержимого сообщения, которое защищено открытым ключом получателя, есть данные пользователя, адресованные посреднику. Сюда входит, например, информация об отправителе и получателе сообщения: например, сертификат гражданина, который подает заявку на получение свидетельства о рождении, становится идентификатором отправителя в пользовательских данных.

Другим компонентом пользовательских данных являются условия привязки доставки в орган регистрации к процессу оплаты, поскольку за выдачу свидетельств о рождении взимается плата. Если сообщение OSCI отправляется в направлении органа регистрации, одновременно запускается дебетовая позиция с соответствующим номером кассы, которая также является частью пользовательских данных.

Все пользовательские данные хранятся отдельно от данных контента в так называемой маршрутной квитанции. Посредник OSCI действует как посредник между отправителем и получателем в инфраструктуре OSCI. Он интерпретирует пользовательские данные и обеспечивает правильную доставку, управляемую событиями. С другой стороны, у него нет доступа к данным контента. Когда гражданин отправляет свое заявление, система также шифрует данные пользователя на переводном листе − не для органа регистрации, а для посредника. Никакие посторонние лица не могут перехватить или манипулировать даже частями сообщения на пути передачи.

После получения посредник расшифровывает маршрутную квитанцию, добавляет (цифровую) метку времени ввода и интерпретирует пользовательские данные приложения. В качестве дополнительной функции он проверяет, действительны ли сертификаты коммуникационного партнера, и документирует результат в маршрутной накладной. В упомянутом примере посредник признает, что требуется оплата сбора, указав кассовый аппарат в качестве условия доставки сообщения в соответствующий орган. В качестве дополнительной функции приложение «приостанавливается» до получения платежа[89].

Опыт Чешской Республики

При внедрении электронного правосудия (eJustice) в Чехии учитывалось, что значительное количество сторон судебного разбирательства обращаются в судебные органы из-за неблагоприятного жизненного события или ситуации и ищут у них правовой защиты. Следовательно, общение должно быть как можно более простым и должно использовать общедоступные средства связи (интернет, мобильные телефоны). Только так электронное правосудие может помочь выполнить условия права на справедливое судебное разбирательство. Важно, чтобы технологические средства, используемые для связи с судебными органами, всегда были простыми в использовании, чтобы инструменты eJustice были удобными для пользователя, сохраняя при этом высокий уровень безопасности и защиты всей информации.

В среде правосудия невозможно использовать решения инфокоммуникационных технологий, которые не могут гарантировать достаточную скорость и реакцию информационных систем. При внедрении таких информационных систем всегда необходимо учитывать достаточный запас при оценке количества сотрудников или пользователей, работающих с определенным приложением. Количество пользователей может значительно увеличиться внезапно и в долгосрочной перспективе (например, произойдут законодательные изменения, которые приведут к значительному увеличению количества дел и количества сотрудников). Информационные системы должны быть стабильными. В связи с необходимостью соблюдения ряда

[89] Systeme und ihr Umfeld. E-Government/E-Business. Rechtsverbindliche Kommunikation mit OSCI [Электронный ресурс]. – URL: http://2014.kes.i№fo/archiv/heft/abonnent/0102/43.htm (дата обращения: 10.03.2021).

процедурных сроков нельзя мириться с простоями длительного характера или нестабильностью отдельных приложений. Отдельные решения должны быть полностью совместимы и в совокупности должны составлять единое целое. Из-за большого объема личной и секретной информации, обрабатываемой судебными органами, необходимо обеспечить защиту сети и баз данных от атак.

Все инфокоммуникационные решения в судебной системе должны основываться на центральной коммуникационной и интеграционной платформе, которая позволит легко развертывать и управлять отдельными технологиями и информационными системами при их использовании. Информационные и коммуникационные технологии в судебной системе влияют не только на технические разработки и прогресс, но и на ряд законодательных изменений, которые оказывают значительное влияние на решения в области информационных технологий (например, введение новых государственных реестров, централизованного учета правонарушений и т.д.).

Пользовательский интерфейс информационных систем, используемых как судебным персоналом, так и участниками судебного процесса или общественностью, должен быть простым и удобным для пользователя, что обеспечит необходимый уровень доступности информации. Работа с приложениями должна быть простой для понимания даже тех людей, которые обычно не используют коммуникационные технологии.

Быстрое развитие информационных технологий открывает новые возможности как для ускорения работы в судебной системе, так и для улучшения взаимного общения с общественностью. Новые, более мощные технологии также несут риски для безопасности судебной системы. Используемые системы должны быть способны реагировать на новые вызовы в разумные сроки и иметь возможность внедрять их в свою структуру. Необходимо постоянно отслеживать и оценивать новые технологические тенденции и при необходимости внедрять и использовать их.

В настоящее время министерство реализует все меры, изложенные в Законе о кибербезопасности[90], включая все соответствующие законы. В частности, речь идет о выдаче единых документов по безопасности, за которыми будут следить все организации Министерства юстиции. Кроме того, была создана группа безопасности CERT MSp, которая активно занимается инцидентами безопасности, обнаруженными в Министерстве юстиции, и реализует упреждающие и ответные меры таким образом, чтобы устранить риски безопасности. Деятельность CERT MSp также заключается в обработке инцидентов безопасности и передаче их результатов в Управление национальной безопасности.

Основная цель повышения уровня безопасности eJustice − внедрение стратегического управления информационной безопасностью, которое

[90] Zákon č. 181/2014 Sb. Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) [Электронный ресурс]. – URL: http://2014.kes.info/archiv/heft/abonnent/0102/43.htm (дата обращения: 10.03.2021).

необходимо для обеспечения безопасной и надежной работы судебной системы. Это стратегическое управление направлено на уменьшение возможных сбоев в деятельности организаций и последствий инцидентов безопасности, соблюдение законодательных и других требований внешней безопасности и обеспечение максимальной защиты.

Конкретные инструменты управления информационной безопасностью eJustice:

– Обеспечение защиты судебной информации (информации во всех форматах данных, хранящейся на компьютерах и/или на информационных носителях, передаваемой по инфраструктуре связи и передаваемой между информационными системами) от внешних или внутренних, преднамеренных или непреднамеренных угроз.

– Обеспечение конфиденциальности информации − информация должна быть доступна только тем, кто уполномочен и должен знать ее для своей работы. Должен быть обеспечен адекватный уровень защиты от несанкционированного доступа и раскрытия информации.

– Обеспечение целостности информации − информация может быть изменена только уполномоченными лицами или по указанию уполномоченных лиц и контролируемым образом. Точность и полнота информации не должны быть нарушены несанкционированными или непреднамеренными изменениями.

– Обеспечение доступности информации − информация должна быть доступна уполномоченным лицам, когда они в ней нуждаются.

– Соблюдение требований правовых норм и других нормативных актов, в частности Закона о кибербезопасности, Закона о защите личных данных, Закона об информационных системах государственного управления, Закона об электронной подписи и постановлений ЕС.

– Сообщение и расследование любых утечек информации, предполагаемых нарушений или выявленных уязвимостей. Последующее информирование соответствующих сотрудников подразделения (даже если они обнаружены сотрудниками другого судебного подразделения), ответственного персонала министерства и заинтересованных сторон.

– Эффективность и адекватность мер защиты информации по отношению к рискам ― меры (включая механизмы системы менеджмента информационной безопасности) должны быть соразмерны важности защищаемой информации, угрозам, которым она подвержена, и выявленным потребностям информационной безопасности.

– Повышение осведомленности о безопасности информации − предоставление информации о требованиях и процедурах обеспечения безопасности информации всем лицам, имеющим доступ к информации и информационным системам судебных органов.

– Управление и обеспечение безопасности информации, когда третьи стороны имеют доступ к информации и информационным системам. Доступ к закрытой информации регулируется договорными отношениями.

– Внедрение услуг в области информационных технологий на основе договорных отношений, что обеспечит соблюдение требований по обеспечению безопасности и исправлению любых недостатков[91].

Другая цель обеспечения безопасности eJustice – создание и разработка полной документации по безопасности, которую министерство предоставит для всего сектора юстиции. Это набор документов и стандартов, которые определят уровень безопасности отдельных областей, а не только в информационных системах. Структура политик безопасности будет соответствовать Закону о кибербезопасности. Также планируется расширить центральный периметр, чтобы сформировать полнофункциональный слой для двух географически разделенных центров обработки данных, которые смогут работать независимо и обеспечивать высокий уровень доступности обслуживаемых сервисов. Предлагаемая разработка направлена на создание достаточно надежного и расширяемого периметра центральной сети, резервных высокоскоростных соединений инфраструктуры и, наконец, что не менее важно, установление правил безопасности для управления передачей данных. Построенная таким образом инфраструктура сможет удовлетворить потребности в развертывании новейших стандартов и технологий безопасности. Будущее состояние центрального периметра безопасности создает полностью избыточную систему, подавляя угрозу так называемой единой точки отказа (SPOF), и обеспечивает бесперебойную работу информационных систем в случае сбоев или планового обслуживания.

В рамках технических мер будет реализован ряд инструментов безопасности, таких как инструмент для защиты целостности сетей связи, проверки личности пользователя, управления правами доступа, защиты от вредоносного кода, сбора и оценки событий безопасности и других технологий в соответствии с Законом о кибербезопасности.

Основным результатом реализации этой цели является обеспечение доступности, конфиденциальности и целостности важных информационных активов, которые имеют ключевое значение для безопасного и бесперебойного функционирования системы правосудия. Построенный в 2015 году центральный периметр безопасности вместе с осуществлением организационных мер должен в конечном итоге повысить доверие к информационным технологиям в судебной системе и обеспечить дальнейшую модернизацию системы электронного правосудия.

[91] Resortní strategie pro rozvoj eJustice [Электронный ресурс]. – URL: https://www.mvcr.cz/mvcren/ (дата обращения: 10.03.2021).

ГЛАВА 5. ФОРМИРОВАНИЕ ПРЕДЛОЖЕНИЙ О ВОЗМОЖНОСТИ СОЗДАНИЯ В МВД РОССИИ СИСТЕМЫ ФОРМИРОВАНИЯ СТАТИСТИЧЕСКОЙ ИНФОРМАЦИИ О ПРЕСТУПЛЕНИЯХ ИЗ МАТЕРИАЛОВ ЭЛЕКТРОННЫХ ОБРАЗОВ УГОЛОВНЫХ ДЕЛ

В связи с необходимостью ведения уголовных дел в электронном формате представляется целесообразным рассмотреть возможность создания в МВД России системы формирования статистической информации о преступлениях из материалов электронных образов уголовных дел.

На основе проведенного анализа зарубежного опыта создания электронных уголовных дел, используемого программного обеспечения и технических средств следует выделить наиболее перспективные направления, в качестве возможных вариантов реализации, создания системы формирования статистической информации о преступлениях из материалов электронных образов уголовных дел:

1. Создание модуля «Электронное уголовное дело» в рамках реализации федеральной государственной автоматизированной информационной системы, функционирующей на цифровой платформе (например, по образу реализации цифровой платформы «Госуслуги»).
2. Создание региональной информационной системы на уровне субъекта Российской Федерации, включающей в свой состав модуль «Электронное уголовное дело».

Рассмотрим указанные выше предложения более подробно.

При реализации первого предложения будут задействованы современные цифровые технологии, позволяющие осуществить переход к цифровой трансформации.

С точки зрения защиты информации, способы обеспечения безопасности данных в рассматриваемой системе должны учитывать степень конфиденциальности информации, содержащейся в уголовном деле.

Должностные категории (следователи и дознаватели) всех субъектов России будут формировать массивы электронных уголовных дел. В процессе формирования материалов электронных уголовных дел, целесообразно реализовать взаимодействие модулей «Электронное уголовное дело» и «Формирования статистической отчетности». Особенности и технические аспекты взаимодействия данных модулей следует определять на этапе технического проектирования. Достаточно важно заметить, что функционал рассматриваемого модуля статистической отчетности должен предусматривать возможность автоматического формирования актуальной статистической информации из материалов электронных уголовных дел. При этом возможно формирование различных стандартных статистических отчетов, в том числе с возможностью их визуализации.

Модуль «Электронное уголовное дело» в рамках реализации федеральной государственной автоматизированной информационной системы

должен обеспечивать одновременную круглосуточную работу пользователей с информацией в интерактивном режиме и может состоять из:

- пользовательской компоненты;
- серверной компоненты.

Пользовательская компонента предполагает установку приложения, как правило, на языке Java. Приложение включает в себя встроенную Java-машину и предполагает автоматическое обновление клиента в случае изменений. Программа-клиент содержит графический интерфейс пользователя и интерфейс для взаимодействия с сервером приложений.

Серверная компонента может включает в себя:

- сервер базы данных;
- сервер приложений;
- почтовый сервер;
- сервер логики;
- сервер приема XML отчетов;
- модуль входной и выходной обработки данных;
- сервер приема подтверждающих файлов.

Сервер базы данных PostgreSQL содержит структуру базы данных в виде таблиц и логику работы базы данных в виде хранимых процедур и триггеров. Также может быть использован сервер, работающий не с реляционными базами данных (NoSQL), позволяющий хранить файлы, прикрепленные к материалам уголовного дела (сканы документов, аудио и видео файлы).

Сервер приложений реализуется на языке Java (версии не ниже 1.8) и используется для подготовки запросов клиента и обращения к серверу базы данных. Сервер приложений одновременно является HTTP-сервером и используется для загрузки обновлений на клиентские машины.

Почтовый сервер предназначен для извлечения сообщений и файлов из почты, их первичного анализа и размещения в базе данных, а также для отправки квитанций и сообщений, формируемых в системе обработки статистики, в подразделения. Реализуется почтовый сервер на языке Java (версии не ниже 1.8).

Сервер логики реализуется на языке Java (версии не ниже 1.8) и предназначен для логического контроля как вновь поступающих разделов отчетов, так и для уже хранимых в базе данных.

Сервер приема XML отчетов предназначен для разбора поступающих на ввод документов, их форматного контроля и записи в базу данных. Реализуется сервер приема XML отчетов на языке Java (версии не ниже 1.8).

Модуль входной и выходной обработки данных предназначен для информационного обмена с другими системами.

Сервер приема подтверждающих файлов также реализуется на языке Java (версии не ниже 1.8). Он предназначен для первичного контроля реквизитов подтверждающих файлов и их записи в базу данных.

Серверные компоненты должны быть разработаны для работы в круглосуточном режиме, кроме периодов проведения регламентных, ремонтных и восстановительных работ.

Другими словам модуль «Электронное уголовное дело» будет представлять из себя комплекс программ, состоящий из совокупности отдельных программных компонент, обеспечивающих пользователю выполнение технологических операций при сборе, обработке и хранении информации из электронных образов материалов уголовных дел (Рис.9).

Рисунок 9 – Предлагаемая схема взаимодействия модуля формирования статистической отчетности в рамках федеральной государственной автоматизированной информационной системы

Федеральная государственная автоматизированная информационная система может включать в себя закрытый контур (взаимодействие правоохранительных органов и органов правосудия) и открытый контур, предназначенный для взаимодействия с другими участниками уголовного

процесса (адвокаты, свидетели и т.д.) и позволяющий использовать информацию открытого характера.

Следует заметить, что доступ к модулю «Электронное уголовное дело» в рамках федеральной государственной автоматизированной информационной системы могут получить сотрудники прокуратуры и судов, имеющих соответствующие права в рамках конкретного уголовного дела. В качестве важной особенности следует отметить, что взаимодействие следователя, прокурора и судьи в рамках уголовного дела должно осуществляться в закрытом контуре. Вопросы организации доступа, разграничения прав, возможностей пользователей модуля «Электронное уголовное дело» определяются разработчиком или оператором федеральной государственной автоматизированной информационной системы на этапе технического проектирования.

Следователь (дознаватель), используя свои учетные данные проходит аутентификацию и идентификацию и получает доступ к модулю «Электронное уголовное дело». При том на данной стадии автоматически могут формироваться определенные данные (например, ФИО следователя, должность, звание, наименование подразделения и т.д.), необходимые для работы с электронным уголовным делом или его элементами (электронными бланками и т.д.).

Для получения дополнительных сведений и формирования материалов уголовного дела следователь может формировать запросы к государственным автоматизированным, в том числе и ведомственным системам, используя систему межведомственного взаимодействия (СМЭВ).

Модуль формирования статистической отчетности, получив все необходимые сведения из электронного образа уголовного дела, помещает их в базу данных, представляющую собой массив статистической информации.

Заметим, что на этапе технического проектирования федеральной государственной автоматизированной информационной системы совместно с разработчиком необходимо определить формы, содержание статистических отчетов и формат передачи их внешним информационным системам.

В соответствии с определенным порядком модуль формирования статистической отчетности осуществляет выгрузку информации во внешние информационные системы. В качестве внешних могут выступать информационные системы органов прокуратуры, подразделений МВД, осуществляющих ведение статистической отчетности и т.д. Форма и содержание конкретного вида статистического отчета для соответствующего ведомства определяются также на этапе технического проектирования.

Взаимодействие между модулем «Электронное уголовное дело» и федеральной государственной автоматизированной информационной системой в процессе прохождения пользователем процедуры идентификации и аутентификации может быть реализовано с использованием протокола SAML 2.0. При попытке доступа неавторизованного пользователя к модулю «Электронное уголовное дело», система должна перенаправлять пользователя

на страницу авторизации для прохождения процедуры идентификации и аутентификации в соответствии с протоколом SAML 2.0.

В случае успеха рассматриваемая система должна вернуть модулю «Электронное уголовное дело» следующие атрибуты: ФИО, e-mail, ID пользователя, признак доступа к модулю «Электронное уголовное дело».

В случае отказа в идентификации и аутентификации автоматизированная система должна сообщить пользователю об ошибке и предоставить повторную попытку прохождения данных процедур. Модуль «Электронное уголовное дело» должен обеспечить разграничение доступа пользователя к функциям на основе собственных механизмов.

При выходе пользователя из модуля «Электронное уголовное дело» необходимо использовать функцию завершения пользовательской сессии протокола SAML 2.0. Механизмы взаимодействия на основе протокола SAML 2.0 уточняются на этапе разработки конструкторской документации.

В рамках личного кабинета следователь (дознаватель) в модуле «Электронное уголовное дело» выполняет работу с материалами уголовного дела, представленными в электронном виде.

Формирование массива информации в модуле «Электронное уголовное дело» может быть реализовано следующими способами:

– в виде входных почтовых сообщений, поступивших на адрес электронной почты;

– в виде файлов, поступивших непосредственно из внешних информационных систем;

– в виде файлов, загруженных пользователем через интерфейс ввода;

– в виде файлов, сформированных на основе значений показателей, введенных непосредственно через интерфейс ввода.

Ввод информации показателей и информации в формы и бланки электронного уголовного дела может быть реализован через интерфейс системы. При этом должны быть предусмотрены следующие возможности:

– ввод информации и показателей посредством графического образа формы (бланки документов: статистические карточки на выявленное преступление, о результатах расследования, на лицо совершившее преступление, о движении уголовного дела, о потерпевшем, о результатах рассмотрения дела судом первой инстанции и т.д.) в соответствии с выбранными реквизитами;

– загрузка файла установленного формата, содержащего сведения по форме отчетности;

– копирование значений показателей (информации);

– редактирование ранее введенной информации по материалам уголовного дела;

– выполнение форматного контроля;

– выполнение логического контроля;

– выполнение контроля сигнальных значений;

– формирование протокола обработки;

– утверждение электронной формы (бланка документа) электронной подписью (ЭП);

– прикрепление к электронным материалам уголовного дела файлов разных форматов (сканы документов, аудио и видео файлов и т.д.).

– сохранение формы (бланка документа) в файл, в том числе с пометкой ЭП (с возможностью прикрепления протокола обработки, а также результатов выполнения контроля сигнальных значений).

Для полноценного формирования электронного образа уголовного дела потребуется перевод различных документов (рапорта сотрудников полиции, протокол осмотра места происшествия, копии документов, схема места совершения правонарушения и т.д.) с бумажного носителя в электронный вид.

Для работы с большим количеством бумажных носителей, которые должны храниться в электронном виде, необходимо использовать технологию сканирования и распознавания. Данная работа должна проводиться последовательно в несколько этапов:

1) Первичная подготовка:
   - подготовка документов для осуществления сканирования;
   - проверка наличия поисковых атрибутов;
   - сверка с внутренней описью заголовков документов;
   - проверка нумерации листов.

При подготовке документов должно проверяться их физическое состояние на предмет выявления:

а) документов с малоконтрастными и угасающими текстами;

б) документов, требующих реставрации и укрепления основы и т.д.

2) Сканирование документов (оцифровка):
   - документы, направляют на сканирование, результатом которого является файл - электронная версия документа;

При сканировании пользователю должно быть предложено указать на бумажном носителе следующие сведения:
   - имя файла, в котором будет находиться электронный образ документа;
   - дата и время сканирования.

3) Оптическое распознавание
   - файл - электронный образ документа, полученный при сканировании, передается на распознавание, которое осуществляется с помощью специального программного обеспечения (ПО), функциональные возможности которого позволяют преобразовывать изображение в текстовые данные - последовательность кодов, используемую для представления символов в компьютере.

4) Верификация
   - при распознавании часть информации может быть переведена в текстовые данные не корректно. После распознавания необходимо обеспечить контроль качества распознавания с возможностью ручной корректировки

результатов распознавания и, возможно, отправкой на повторное сканирование.

5) Индексирование

– выделение и сопоставление текстовых данных электронного образа документа, полученных при распознавании, с атрибутами конкретного документа.

6) Выгрузка в единый банк данных

В результате выполнения предыдущих этапов к началу данного этапа подготовлены:

– сканированный образ бумажного документа;

– распознанный образ электронной версии документа, полученной после сканирования, содержащий текстовые данные;

– соответствие между текстовыми данными распознанного образа и атрибутами конкретного документа.

Указанная информация передается на хранение и дальнейшее использование в единый банк данных.

Необходимо разработать положения и требования, регламентирующие процедуру сканирования и оцифровки документов, а также описывающие все процессы обработки информации и действия оператора.

Достаточно важно заметить, что материалы электронного уголовного дела могут формироваться из информации и файлов, полученных посредством электронной почты. Выборка входных почтовых файлов и сообщений, должна выполняться автоматически посредством почтового модуля взаимодействия. Почтовый модуль взаимодействия должен осуществлять автоматическую проверку на наличие во входящем каталоге входных файлов и сообщений. При наличии новых сообщений они должны быть выбраны из входящего каталога и переданы на дальнейшую обработку. Выбранные сообщения из входящего каталога должны удаляться.

Поступающие файлы для повышения уровня сохранности автоматически должны архивироваться. Затем должен быть выполнен разбор сообщения и выделена «полезная информация» - статистический отчет в установленном формате. Далее из него выделяется документ.

Выделенный документ должен пройти этапы форматного и логического контроля. Документы, в которых не выявлено ошибок на этапе форматного контроля, должны быть записаны в базу сбора независимо от результатов этапа логического контроля.

По результатам контроля документа должно быть автоматически сформировано сообщение, содержащее протокол контроля, и осуществлена отправка его на адрес электронной почты, с которой поступило входное сообщение.

Затем должны быть выполнены следующие действия:

- проверка на наличие в базе дубля документа (совпадение значений всех показателей), при отсутствии в базе дубля поступивший документ записывается в массив ввода для дальнейшего контроля;

- многоуровневый логический контроль (проверка выполнения контрольных соотношений между взаимоувязанными показателями внутри раздела, внутри формы, между относящимися к разным формам за текущий отчетный период, за различные отчетные периоды);

- формирование протокола обработки – итоговый результат контроля документа.

При проведении логического контроля должны быть предусмотрены два типа контрольных соотношений: «ошибка» и «предупреждение». Для показателей с текстовой информацией этап логического контроля не выполняется. Эти показатели должны считаться логически правильными.

Кроме автоматического ввода входной информации должен быть предусмотрен ручной ввод документов, который предназначается для ввода и обработки информации, которая не вводится в систему в автоматическом режиме. Для ручного ввода документов должны быть предусмотрены возможности ввода (коррекции) значений показателей в графическом образе формы. Также должна быть предусмотрена возможность для пользователя загрузки значений показателей из файла информации в графический образ формы.

Для документов с форматными ошибками должна быть предусмотрена возможность их коррекции посредством текстового редактора. Для коррекции значений показателей документов должна быть предусмотрена возможность изменения значений показателей и осуществления повторного выполнения операции логического контроля.

Допускается коррекция алгоритма проверки показателей в ходе сбора форм отчетности, после которой требуется проведение контроля поступивших сведений по обновленному алгоритму, с уведомлением адресатов о результатах такой проверки.

Для контроля результатов ввода и обработки документов пользователь должен иметь возможность получения в режиме реального времени справочных сведений о результатах «прохождения» документа через различные этапы приема и обработки, а также просмотреть или распечатать протокол контроля для каждого документа. Также должна быть предусмотрена возможность формирования справочной информации об отклонении показателей от сигнальных значений.

Функция должна позволять ответственным сотрудникам проставлять отметки на показателях, требующих подтверждения. На основе данных отметок должны информироваться пользователи, ответственные за представление данных показателей.

Ответственным за ввод информации сотрудникам должна быть предоставлена возможность ввода сведений об источниках формирования данных. Должно быть предусмотрено выполнение операции логического контроля по инициативе пользователя для документов, хранящихся в базе сбора на данный момент времени, а также автоматическая отправка квитанций в адрес отправителя документа.

Пользователям или группе пользователей должна быть предоставлена возможность утверждения отчетности, хранящейся в базе сбора электронной подписью, после чего коррекция значений показателей в отчете становиться недоступной.

Для каждого документа, хранимого в базе сбора, должно быть предусмотрено хранение информации о способе (введена пользователем, загружена из внешней информационной системы, поступила по электронной почте) и времени поступления.

В модуле «Электронное уголовное дело», могут быть реализованные следующие функции и операции:

– сбор и обработка поступающих массивов электронных образов уголовных дел (в том числе сканы документов, аудио и видео файлы);

– хранение и ведение массивов электронных образов уголовных дел;

– ведение нормативно-справочной информации;

– подготовка, ведение и распространение информационно-аналитических материалов;

– формирование массива статистической информации из материалов электронных образов уголовных дел;

– мониторинг процессов сбора и обработки статистической отчетности из массивов электронных образов уголовных дел;

– администрирование системы.

После формирования в рассматриваемом модуле массива электронных образов уголовных дел, можно будет реализовать в качестве одной из функции – получение статистических данных из электронных образов уголовных дел. Данная функция может работать как в автоматическом, так и в автоматизированном режиме. Данное обстоятельство должно быть уточнено на этапе технического проектирования.

Формирование статистических данных из массива электронных образов уголовных дел должно обеспечивать:

– ввод, копирование, редактирование значений показателей форм статистической отчетности;

– загрузку документов форм статистической отчетности в базу данных из файла (в том числе поступающего через почту);

– загрузку документов форм статистической отчетности, поступающих из внешних информационных систем;

– выполнение форматного контроля статистической отчетности;

– выполнение логического контроля статистической отчетности в соответствии с алгоритмом проверки показателей;

– формирование протокола обработки статистической отчетности;

– интерактивное отображение сообщений об ошибках и предупреждениях при вводе документов, в соответствии с правилами форматно-логического контроля;

– корректировку значений показателей форм статистической отчетности;

– просмотр описания метаданных информационных объектов, участвующих в формировании документов;

– агрегирование статистической отчетности;

– преобразование статистических показателей в соответствии с актуальной версией формы статистической отчетности.

В рамках рассматриваемого модуля должно быть реализовано:

– сбор статистической отчетности;

– агрегирование статистической отчетности;

– конвертирование статистической отчетности.

Статистические данные из массива электронных уголовных дел могут быть сформированы и переданы через модуль формирования статистической отчетности. Внутренние механизмы формирования массивов статистической информации из электронных образов уголовных дел определяются разработчиком модуля «Электронное уголовное дело» на этапе технического проектирования.

Для выгрузки метаданных, сформированных в модуле, во внешние информационные системы должны быть предусмотрены следующие возможности:

– выбор объектов метаданных для выгрузки;

– выгрузка объектов метаданных;

– просмотр протокола выгрузки файлов.

Перечень информационных систем, в которые будет реализовываться выгрузка метаданных, определяется на этапе технического проектирования.

Следует заметить, что программное обеспечение модуля «Электронное уголовное дело» должно позволять осуществлять подготовку файлов установленного формата, содержащих статистическую информацию, для передачи не только во внутренние, но и во внешние информационные системы.

Технологическое взаимодействие с открытыми сетями передачи данных не осуществляется. При этом должна быть возможность задания источников данных (координаты показателей), приемников данных (файл в формате офисных приложений, с указанием координат показателей) и цепочки преобразований (простое копирование либо преобразование данных с использованием стандартных функций и математических операций в файл-приемник определенной структуры).

Технология реализации должна позволять корректировку шаблонов выходных данных путем изменения состава и структуры показателей, предназначенных для выгрузки во внешние информационные системы, а также с учетом изменяющихся требований к формату данных.

Формирование сведений для внешних информационных систем должно выполняться на основе заранее подготовленных макетов. В качестве примера,

взаимодействие может быть реализовано со следующими внешними системами:

– Государственная автоматизированная система правовой статистики (ГАС ПС);

– Статистика ГИАЦ;

– Интернет сайт МВД России;

– Другие системы (ЕМИСС, ГАС «Управление», ГАС «Правосудие», и т.д.).

Состав и формат выгружаемых метаданных, содержимое протокола выгрузки определяются на этапе технического проектирования для каждой внешней системы.

При взаимодействии с внешними системами (например, с ГАС ПС) в рассматриваемом модуле должны быть реализованы следующие возможности:

– форматный контроль загружаемых метаданных;

– просмотр протокола загрузки;

– просмотр загруженных метаданных.

Форматный контроль загружаемых метаданных должен обеспечивать проверку на соответствие согласованному формату обмена данными. Для каждой внешней информационной системы, из которой будет реализовываться выгрузка отчетов, порядок, формат, состав и периодичность сбора статистической отчетности определяются отдельно, на этапе технического проектирования.

При этом, на этапе технического проектирования требуется разработать формат представления отчетов, который будет использоваться для сбора отчетности.

Перечень информационных систем, метаданные из которых будут загружаться в модуль «Электронное уголовное дело», определяется также на этапе технического проектирования.

Модуль «Электронное уголовное дело» должен позволять пользователю в автоматическом или автоматизированном режиме выполнять технологические операции для решения задач по администрированию пользователей, управлению параметрами функционирования. При этом целесообразно реализовать следующие возможности:

– предоставление пользователям (группам пользователей) определенного уровня доступа (роли доступа в рамках исполнения ролевой политики);

– предоставление пользователям доступа к объектам и функциям модуля в соответствии с присвоенной ролью;

– управление параметрами функционирования (например, параметры обмена почтовыми сообщениями, формирования выходной информации, взаимодействия с внешними информационными системами, сбора и обработки документов, работы фоновых процессов и др.);

– экспорт/импорт объектов.

Предоставление доступа роли к объектам и функциям модуля должно быть реализовано через ролевую модель с необходимым уровнем детализации объектов и функций. Перечни ролей доступа, функций (групп функций) и объектов (групп объектов), на основе которых будет формироваться ролевая модель, разрабатываются на этапе технического проектирования.

Дополнительно для каждой формы статистической отчетности должен быть разработан механизм предоставления пользователям функций по формированию и представлению документов формы, а также ведению полного жизненного цикла формы отчетности (описание и актуализация метаданных, ввод и корректировка показателей, агрегирование и преобразование, формирование выходной информации).

В модуле «Электронное уголовное дело» должна быть предусмотрена возможность корректировки параметров функционирования:

– обмена почтовыми сообщениями (списки допустимых и недопустимых расширений файлов, идентификаторы в файлах обмена, настройки почтового ящика, максимально допустимый размер файла);

– пути хранения поступивших в модуль файлов;

– взаимодействия с внешними информационными системами (перечень информационных систем, форматы файлов и параметры обмена данными);

– работы фоновых процессов (интервалы между запусками процессов сбора и обработки документов, интервалы обновлений окна мониторинг подсистемы аудита).

Программное обеспечение модуля «Электронное уголовное дело» должно обеспечивать взаимодействие с внешними и внутренними системами, а также соответствовать архитектуре современных цифровых платформ, в части:

– организации резервного копирования данных;

– восстановления данных из резервных копий, в том числе после аварий;

– использования принципов работы облачных технологий и отказоустойчивых схем организации сети для обеспечения непрерывности работы;

– совокупного набора механизмов защиты информации в части противодействия актуальным угрозам.

Федеральная государственная автоматизированная информационная система при функционировании, в качестве рекомендаций, должна обеспечивать достижение следующих показателей надежности:

- время восстановления работоспособности системы после отказа в работе программного обеспечения должно составлять не более 1 ч;

- время восстановления работоспособности системы после устранения сбоев в работе технической инфраструктуры должно составлять не более 3 ч.

Функционирование программного обеспечения федеральной государственной автоматизированной информационной системы должно

обеспечивать непрерывный круглосуточный режим работы. При этом режиме надежность работы системы должна выполнять следующие цели:

– минимизация числа сбоев и отказов;

– способность продолжать работу несмотря на отказы;

– минимизация времени восстановления работоспособности после отказов.

Должен быть реализован механизм первичного контроля вводимых данных на основе проверки типов, размерности, допустимости значений, вводимых данных. Взаимодействие пользователей с модулем «Электронное уголовное дело» должно осуществляться посредством визуального графического интерфейса. Интерфейс не должен быть перегружен графическими элементами и должен обеспечивать отображение экранных форм.

Средства редактирования должны использовать функциональные клавиши, режимы работы, поиска, использования оконной системы. Ввод-вывод данных, прием управляющих команд и отображение результатов их исполнения должны выполняться в интерактивном режиме. Интерфейс должен соответствовать современным эргономическим требованиям и обеспечивать доступ к основным функциям и операциям.

Эксплуатация модуля «Электронное уголовное дело» может быть реализовано в следующих режимах:

– штатный режим:

– режим технического обслуживания;

– аварийный режим.

Контроль доступа к ресурсам рассматриваемого модуля должен быть применим к каждому объекту и каждому субъекту в соответствии с установленными ролями пользователей.

Для обеспечения юридически значимых действий (в частности, в случае взаимодействия со СМЭВ) с электронной подписью в модуле «Электронное уголовное дело» необходимо обеспечить поддержку национальных стандартов в области криптографической защиты информации ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хэширования» и ГОСТ Р 34.10-2012 «Информационная технология.

К основным достоинствам рассматриваемого варианта можно отнести:

– возможность интеграции с множеством баз данных государственных органов исполнительной власти в целях повышения уровня автоматизации получения информации;

– концентрация массива электронных уголовных дел в одном хорошо защищенном месте;

– возможность использования современной цифровой инфраструктуры, организации каналов связи;

– возможность организации высокой степени защиты информации, содержащейся в электронных уголовных делах, в том числе с использованием биометрических технологий (3-х уровневая идентификация).

К наиболее возможным недостаткам рассматриваемого можно отнести:

– необходимость увеличения серверных мощностей центров обработки данных, необходимых для масштабирования информационной системы;

– увеличение до необходимого уровня пропускной способности каналов связи;

– необходимость интеграции с информационными системами органов прокуратуры или обеспечение доступа сотрудников прокуратуры к материалам электронных уголовных дел;

– необходимость интеграции с информационными системами органов судебной власти.

Второй вариант предполагает создание региональной информационной системы на уровне субъекта Российской Федерации, включающей в свой состав модуль «Электронное уголовное дело». При этом территориально данная система должна располагаться в субъекте Федерации, например, в специально организованном дата-центре. Дата-центр представляет собой специализированное здание для размещения (хостинга) серверного и сетевого оборудования и подключения абонентов к каналам сети Интернет. Дата-центр исполняет функции обработки, хранения и распространения информации, ориентирован на решение различных задач путём предоставления информационных услуг.

Данное обстоятельство обусловлено тем, что возникает потребность в организации эффективной защиты информации на всех уровнях и этапах функционирования системы.

В данном случае будет необходимо построение системы защиты информации, которая будет основываться на нескольких этапах:

– анализ возможных угроз безопасности инфокоммуникационной системы (из множества вероятных воздействий выбирают воздействия, которые могут реально произойти);

– планирование системы защиты (описание единой совокупности мер противодействия угрозам различной природы);

– реализация данной системы защиты (установка и настройка средств защиты);

– сопровождение системы защиты (контроль работы, регистрация событий, анализ и коррекция системы защиты).

На этапе планирования необходимо определить средства защиты, реализующие следующие мероприятия по защиты информации:

– идентификация и аутентификация субъектов (пользователей, процессов) инфокоммуникационной системы;

– разграничение доступа к ресурсам;

– контроль целостности данных;

– обеспечение конфиденциальности информации;

– регистрация и анализ событий;

– резервирование ресурсов и компонентов и др.

В отличие от защиты автономных автоматизированных рабочих мест защита данных в инфокоммуникационных системах реализуется с помощью двух основных способов: с использованием межсетевых экранов и путем реализации виртуальных частных сетей.

При использовании межсетевых экранов целостность периметра сети обеспечивается использованием технологий межсетевого экранирования в точке подключения защищаемой сети к внешней неконтролируемой сети (сети Интернет). Межсетевой экран повышает безопасность объектов внутренней сети за счет игнорирования несанкционированных запросов из внешней среды.

При организации VPN-сетей происходит максимально возможное обособление потоков данных. Для объединения удаленных компьютерных сетей в VPN используются виртуальные выделенные каналы.

Таким образом, технология VPN обеспечивает гарантированное качество облуживания потоков пользовательских данных, а также их защиту от возможного несанкционированного доступа или разрушения в публичной сети.

В качестве примера отечественного комплексного средства защиты, включающего в себя функцию VPN, можно привести средство сетевой защиты ViPNet, заработанное компанией «ИнфоТеКС».

Кроме того, в целях повышения уровня автоматизации процесса целесообразно интегрировать модуль «Электронное уголовное дело» с базами данных различных государственных органов. Учитывая практический опыт правоохранительных органов, необходима интеграция с базами данных следующих государственных структур:

- МФЦ;
- администрация субъекта РФ;
- структуры министерства образования в субъекте РФ;
- наркологический диспансер;
- психоневрологический диспансер;
- пенсионный фонд;
- медицинские учреждения (поликлиники по месту жительства);
- финансовые учреждения (банки).

Обобщенная схема взаимодействия следователя (дознавателя) с государственными органами для формирования актуальной и разно форматной статистической информации о преступлениях из материалов электронных образов уголовных дел представлен на следующем рисунке (рис. 10).

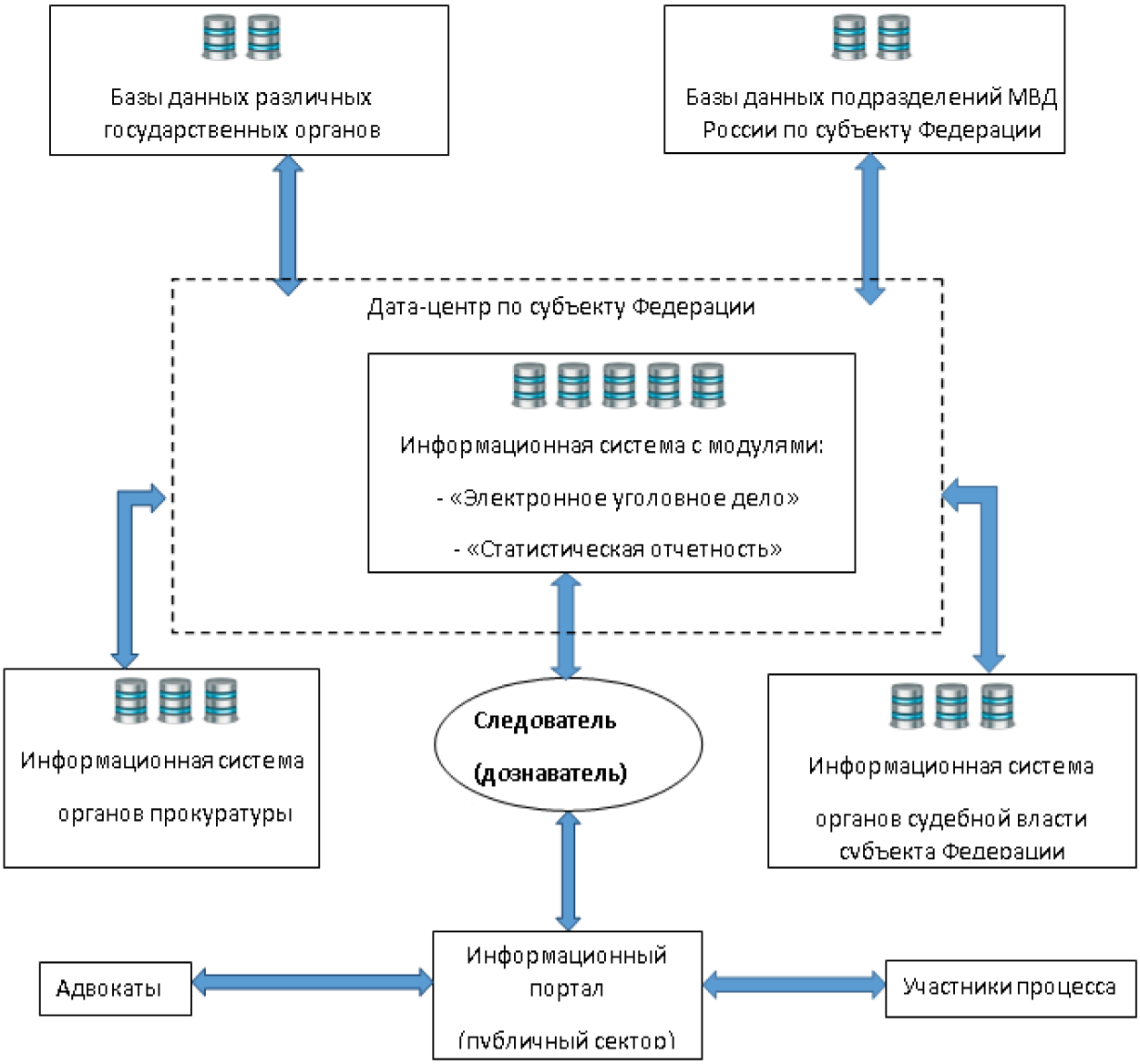


Рисунок 10 – Обобщенная схема взаимодействия следователя (дознавателя) с государственными органами

На представленном выше рисунке видно, что автоматизируются процессы досудебного расследования и прокурорского надзора. Следователь при выполнении своих функциональных обязанностей получает за достаточно короткое время необходимую информацию (в том числе и персональные сведения) из различных источников (базы данных госорганов и подразделений МВД), используя функционал модуля «Электронное уголовное дело». Кроме того, фактически в режиме реального времени возможно взаимодействие следователя (дознавателя), прокурора и судьи.

Для организации взаимодействия следователя (дознавателя) с адвокатами и участниками процесса целесообразно использовать информационный портал, который может быть реализован с использованием веб-технологий.

Данный информационный портал будет представлять открытый публичный сектор, в котором участники процесса могут получать процессуальные документы в режиме online, подавать ходатайства, жалобы на действия (бездействия) следователя (дознавателя) и прокурора, а также знакомиться с материалами уголовного дела дистанционно при его окончании.

Достаточно важно заметить, что информационная система, расположенная в дата-центре, может содержать модуль, позволяющий в автоматическом режиме формировать статистическую информацию о преступлениях из материалов электронных образов уголовных дел.

Из анализа представленной выше схемы, можно констатировать, что организация взаимодействия информационных систем органов прокуратуры, судебной системы, МВД (модуля «Электронное уголовное дело»), органов исполнительной власти позволит повысить уровень цифровизации на региональном уровне и перейти на новый уровень цифровой трансформации.

Формирование предложений о возможности создания в МВД России системы формирования статистической информации о преступлениях из материалов электронных образов уголовных дел

Для создания в МВД России автоматизированной системы формирования статистической информации о преступлениях из материалов электронных образов уголовных дел необходимо разработать следующие алгоритмы, например, на языке Python:

1. Осуществления нормализации и масштабирования всех электронных документов единого образца для унификации параметров детекции с помощью методов библиотеки OpenCV. Для работы данного алгоритма необходимо определить какие формы статистических карточек и другие документы из электронного образа уголовного дела будут использованы для формирования статистической информации о преступлениях.

2. Детектирования на изображениях по заданным статичным координатам ключевых информационных полей документа для дальнейшего извлечения сущностей.

Рассматриваемый алгоритм предполагает формирование областей детекции шаблонного исследуемого документа (формы статистической карточки), из которых в последствии будут извлечены сущности (признаки), необходимые для формирования массива статистической информации о преступлениях.

3. Извлечения текста и цифровой информации из распознанных ключевых полей, используя технологию оптического распознавания символов pyTesseract.

Данный алгоритм направлен на получение статистической информации из исследуемых документов.

4. Сохранения извлеченной информации по каждой обрабатываемой форме в структурированный формат данных.

После извлечения необходимой информации из электронного образа документа реализуется алгоритм, позволяющий сохранить статистическую информацию в структурном виде, например, формат Excel или другой структурированный формат данных. Таким образом, осуществляется накопление массива статистической информации о преступлениях из материалов электронных образов уголовных дел в структурированном виде.

5. Анализа и визуализации накопленной статистической информации с помощью инструментов Pandas, numPy, matplotlib языка программирования Python.

На последнем этапе функционирования автоматизированной системы реализуются алгоритмы анализа и визуализации данных, позволяющие обрабатывать большие массивы накопленной структурированной статистической информации о преступлениях из материалов электронных образов уголовных дел и визуализировать их в виде различных графиков.

Указанные подходы потребуют разработки отдельных модулей для обработки и распознавания соответствующих типовых форм электронных документов.

Таким образом можно констатировать, что в настоящее время существуют различные технологии, позволяющие реализовать механизмы формирования статистических показателей из электронных образов уголовных дел. Важно заметить, что данные механизмы формирования статистических показателей из электронных образов уголовных дел должны определяться разработчиком модуля «Электронное уголовное дело» на этапе технического проектирования.

ЗАКЛЮЧЕНИЕ

Анализируя степень восприятия российским уголовно-процессуальным законом информационных и цифровых технологий, следует заметить, что в нем получили закрепление лишь некоторые из них, преимущественно те, которые сложно игнорировать по причине распространенности в повседневном обиходе и, соответственно, частоты встречаемости в современной судебно-следственной практике. В первую очередь это относится::

− к признанию законодателем электронных носителей информации вещественными доказательствами, к определению порядка их изъятия и хранения (ч. 4 ст. 81, ст. 81.1, ч. 2.1 ст. 82, ст. 164.1 УПК РФ);

− признанию документами материалов, содержащих сведения как в письменном, так и в ином виде (фото- и киносъемки, аудио- и видеозаписи и иных носителей информации − ч. 2 ст. 84 УПК РФ);

− признанию доказательственного значения материалов контроля и записи переговоров, а также информации о соединениях между абонентами и (или) абонентскими устройствами и получаемых в результате этого документов и фонограмм (ст. ст. 186, 186.1 УПК РФ);

− признанию возможности производства по решению суда осмотра и выемки электронных сообщений или иных сообщений, передаваемых по сетям электросвязи (ч. 7 ст. 185 УПК РФ);

− признанию процессуальной значимости результатов применения технических средств в процессе производства следственных действий (ч. ч. 5, 8 ст. 166, ч. 3 ст. 180, ч. 4 ст. 189 УПК РФ), среди которых упоминаются и электронные носители информации.

На стадии досудебного производства УПК РФ предусматривает возможность изготовления процессуальных документов электронным способом (ч. 2 ст. 474, ст. 474.1), что, однако, не отменяет необходимости изготовления их и в бумажном виде. Использование отдельных коммуникационных технологий, таких как производство допроса при помощи видео- конференц- связи, безосновательно ограничено лишь судами.

Таким образом, можно сделать следующие выводы.

1. Переход на электронную форму ведения уголовного дела возможен в ближайшей перспективе при развертывании соответствующих информационных технологий, обеспечивающих информационные процессы в сфере уголовного судопроизводства, и введении единого электронного удостоверения личности гражданина на территории Российской Федерации.

2.Электронный паспорт[92]должен обеспечивать подписание процессуальных документов в электронной форме и содержать персональную электронную подпись. Мы полагаем, что определение «электронная подпись»

[92] Проект Федерального закона "Об основном документе, удостоверяющем личность гражданина Российской Федерации" // Интернет-портал Российской газеты // URL: http://www.rg.ru/2013/01/29/elektr-pasport-site-dok.html.

зафиксированное в Федеральном законе[93], отражает все признаки данного правового понятия, таким образом, электронная подпись − это информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

Кроме того, субъекты доказывания, кроме названного вида информационной технологии, должны иметь возможность применять усиленную квалифицированную подпись, содержащуюся в служебном удостоверении личности названных субъектов, с целью обеспечения информационной безопасности материалов уголовного дела в электронной форме и дополнительной идентификации должностных лиц.

3. «Электронное уголовное дело» − основной источник уголовно-процессуальной информации в электронном виде. Названная форма должна удовлетворять следующим требованиям:

− обеспечивать накопление, хранение и воспроизведение данной информации, а также ее защиту от модификации;

− удовлетворять требованиям относимости, допустимости, достоверности, а в совокупности и достаточности требований, предъявляемых уголовно-процессуальным законом к содержащейся в нем уголовно-процессуальной информации;

− позволять исследовать и оценивать данную информацию в ходе судебного разбирательства.

4. «Электронное уголовное дело» будет представлять собой информационный продукт, созданный в ходе движения уголовного дела в рамках уголовного судопроизводства в соответствии с требованиями уголовно-процессуального закона.

Представленные аналитические материалы «Изучение зарубежного опыта формирования массива статистической информации из материалов электронных образов уголовных дел» позволяют нам выделить предложения по совершенствованию уголовно-процессуального законодательства, затрагивающего вопросы досудебного производства в электронном формате.

На основании сказанного предлагаем внести изменения:

1. В ст. 5 УПК РФ, дополнив ее пунктом 28.1, изложив его в следующей редакции: «28.1) электронный документ – зафиксированная на материальном носителе в электронно-цифровой форме информация, предназначенная для передачи во времени и пространстве с использованием средств вычислительной техники, отвечающая требованиям аутентичности, достоверности, целостности и пригодности для использования с реквизитами, позволяющими её идентифицировать».

2. В ст. 74 ч. 2 УПК РФ дополнив ее пунктом 4.1, изложив его в следующей редакции: «4.1) электронное доказательство – это любые сведения,

[93] Об электронной подписи : федеральный закон от 06.04.2011 № 63-ФЗ (ред. от 11.06.2021) [Электронный ресурс]. – URL : http://consultant.ru (дата обращения: 06.10.2021).

имеющие юридическую силу, зафиксированные на электронном и/или материальном носителе, заверенные электронной цифровой подписью и пригодные для передачи по информационно-коммуникационным сетям, положенные в основу обвинения, а также используемые судом, прокурором, следователем, дознавателем, в порядке, определенном настоящим Кодексом, имеющие значение для раскрытия и расследования преступления».