ВОРОНЕЖСКИЙ ИНСТИТУТ МВД РОССИИ

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

Учебно-практическое пособие

Воронеж
2022

ББК 67

Коллектив авторов: Н.А. Моругина, В.В. Бутов, О.И. Нестеровский, Ю.М. Баркалов

Рецензенты: М. М. Буслов – начальник отделения НЦБ Интерпола ГУ МВД России по Воронежской области, канд. юрид. наук; Н.А. Лещева – старший следователь по ОВД КМО ГСУ ГУМВД России по Воронежской области.

Изучение зарубежного опыта формирования массива статистической информации из материалов электронных образов уголовных дел [Электронный ресурс] / Н.А. Моругина [и др.]. – Электр. дан. и прогр. – Воронеж : Воронежский институт МВД России, 2022. – 1 электр. опт. диск (CD-ROM) : 12 см. – Систем. требования: процессор Intel с частотой не менее 1,3 ГГц ; ОЗУ 512 Мб ; операц. система семейства Windows ; CD-ROM дисковод.

В пособии представлен анализ зарубежного опыта формирования массива статистической информации из материалов электронных образов уголовных дел, выделены предложения по совершенствованию уголовно-процессуального и уголовного законодательства, затрагивающего вопросы досудебного производства в электронном формате. Издание предназначено для курсантов и слушателей образовательных организаций МВД России, сотрудников ГИАЦ МВД России.

ISBN 978-5-88591-933-3

СОДЕРЖАНИЕ

ВВЕДЕНИЕ……..4

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, формирования их массива, с одновременной оценкой допустимости распространения такого опыта на территории Российской Федерации с учетом требований отечественного законодательства……..6

ГЛАВА 2. 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)……16

ГЛАВА 3. Формирование предложений о возможности создания в МВД России системы формирования статистической информации о преступлениях из материалов электронных образов уголовных дел……28

ЗАКЛЮЧЕНИЕ……..…34

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.

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 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 цифровой 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

---

[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).

[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).

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, Швеции, Дании, Нидерландах, Сингапуре, Южной Кореи, Италии, Испании, ФРГ и других странах.

[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.

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, ФОРМИРОВАНИЯ ИХ МАССИВА, 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. Состав электронной системы правосудия состоит из 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	*Чехия*	*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 информацией;* *в) проведению видеоконференцсвязи;* *− интеллектуальную систему судебного разбирательства, состоящую 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.*

Создание электронных образов уголовных дел с учетом требований уголовно-процессуального законодательства США

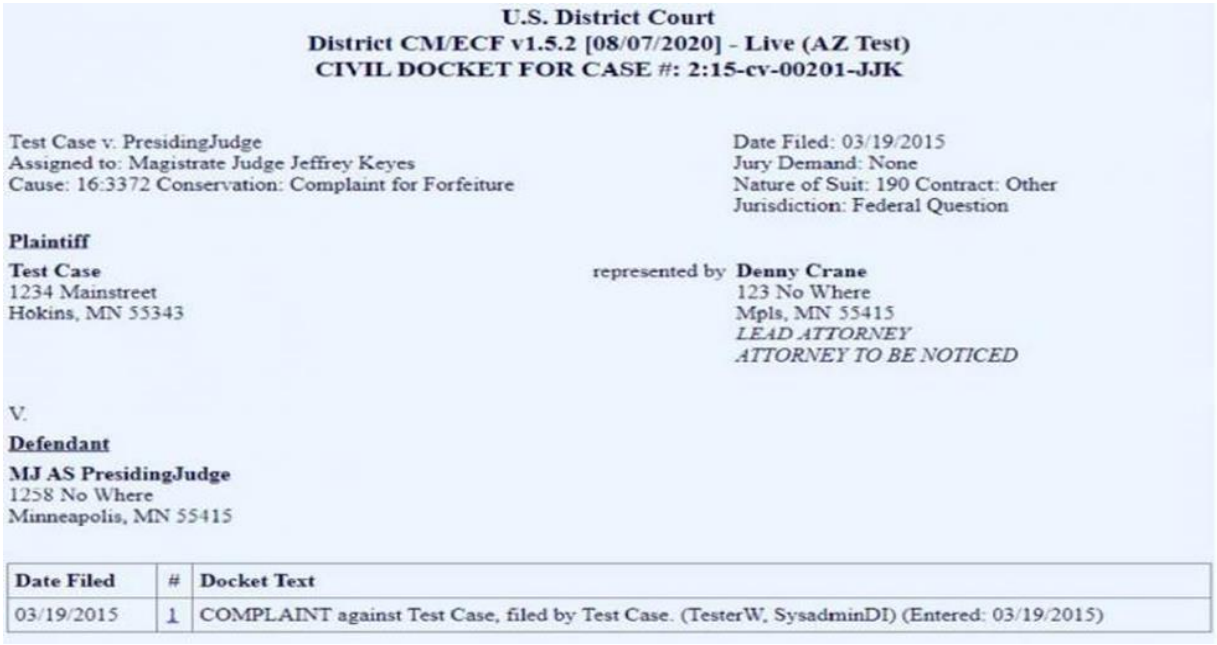
Уголовно-процессуальное законодательство США не предполагает наличия единого уголовного дела, в котором сосредоточены все материалы в подшитом и пронумерованном виде. На бумажном носителе информации представлены лишь сведения о лице, совершившем преступление, данные о потерпевшем и движение уголовного дела. Собирание доказательств осуществляется как стороной обвинения, так и стороной защиты, на равных условиях[9].

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)[10], 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.

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

[10] 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[11].

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.

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

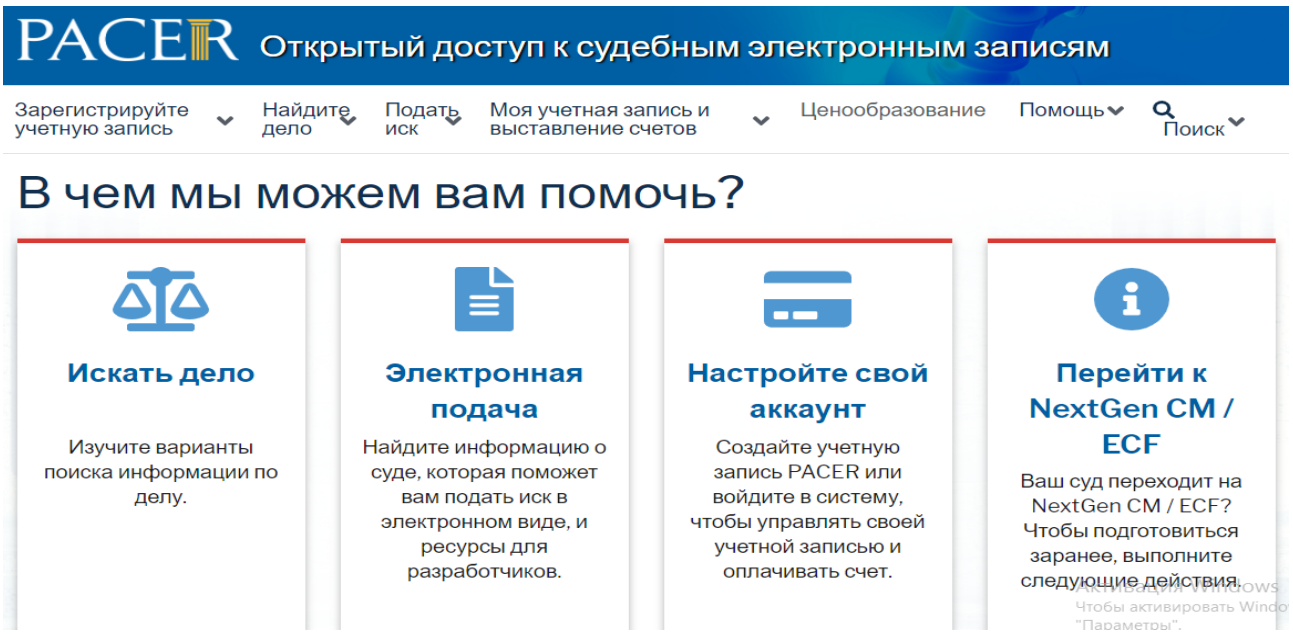


Рисунок 2 – Public Access to Court Electronic Records − PACER

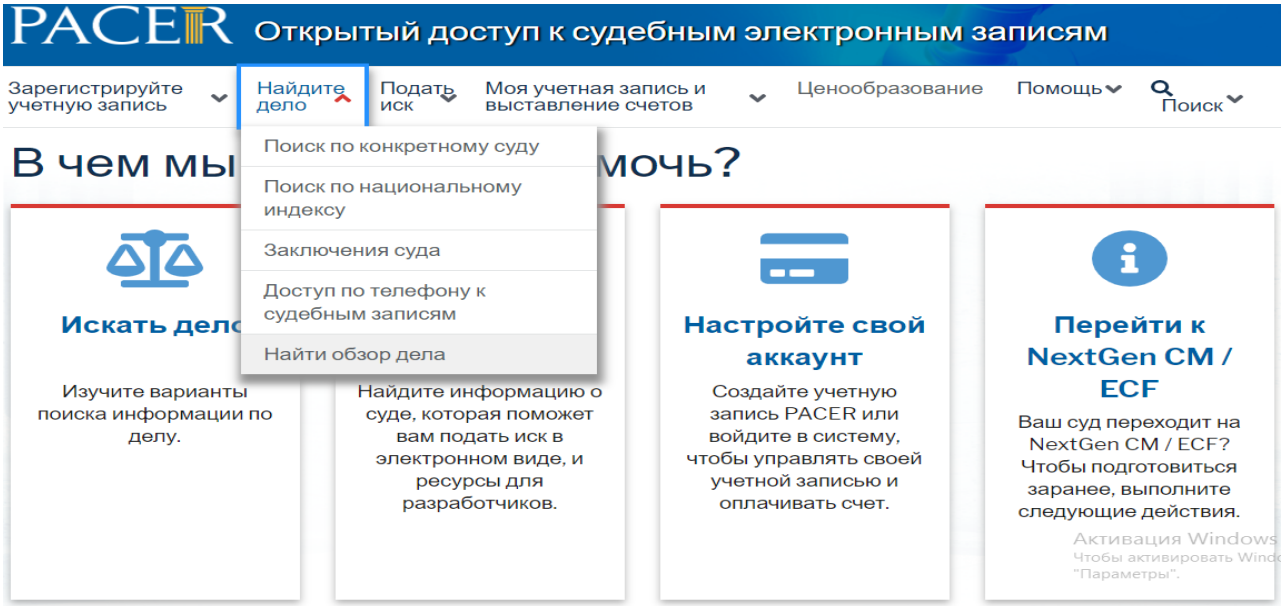


Рисунок 3 – Public Access to Court Electronic Records – PACER (поисковик)

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[12]. 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[13].

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

[12] 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.

[13] 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 5A 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.

ГЛАВА 2. 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) − это 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.

		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»[14];

− Указ Президента РФ от 6 марта 1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера»[15];

− 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»[16];

− ведомственные акты (Приказ МВД России от 09.11.2018 № 755 «О некоторых вопросах обращения со служебной информацией ограниченного распространения в системе МВД России»[17]).

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 исполнительной власти в пределах своей компетенции определяют категорию

[14] 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).

[15] 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).

[16] 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).

[17] 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).

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[18]. 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 обслуживания и продуктивность персонала; улучшение общего качества правосудия.

[18] 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).

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[19].

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 проверка информации, прозрачность судебного процесса; эффективный обмен

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

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[20].

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»[21].

[20] 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).

[21] 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)[22]. 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[23].

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[24].

Обмен сообщениями с помощью OSCI основан на определенных формах. В сообщениях OSCI данные об использовании и содержании строго

---

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

[23] 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).

[24] 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).

разделены − доступ посторонних лиц исключен из-за различных типов 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 привязка 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[25].

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

[25] 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 постоянно внедрять и использовать их.

В настоящее время министерство реализует все меры, изложенные в Законе о кибербезопасности[26], 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

[26] 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[27].

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.

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

ГЛАВА 3. ФОРМИРОВАНИЕ ПРЕДЛОЖЕНИЙ О ВОЗМОЖНОСТИ СОЗДАНИЯ В МВД РОССИИ СИСТЕМЫ ФОРМИРОВАНИЯ СТАТИСТИЧЕСКОЙ ИНФОРМАЦИИ О ПРЕСТУПЛЕНИЯХ ИЗ МАТЕРИАЛОВ ЭЛЕКТРОННЫХ ОБРАЗОВ УГОЛОВНЫХ ДЕЛ

В связи с постоянно возрастающей в мире тенденцией перехода на электронный формат расследования электронных уголовных дел представляется целесообразным рассмотреть возможности 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 создания системы формирования статистической информации о преступлениях из материалов электронных образов уголовных дел:

1. Создание модуля «Электронное уголовное дело» в рамках реализации сервиса единой информационно-аналитической системы обеспечения деятельности подразделений МВД России (ИСОД МВД России).
2. Создание региональной информационной системы на уровне субъекта Российской Федерации, включающей в свой состав модуль «Электронное уголовное дело».

Представляется целесообразным рассмотреть указанные выше предложения более подробно.

При реализации первого предложения будут задействованы современные облачные технологии и фактически реализован еще один сервис ИСОД МВД России, в рамках функционирования последнего соответствующие должностные категории (следователи и дознаватели) со всех субъектов России будут формировать массивы электронных уголовных дел.

С точки зрения защиты информации в данном случае, т.к. построение модуля «Электронное уголовное дело» будет осуществляться на уже действующей системе, то способы реализации защиты информации, обрабатываемой в данном модуле, необходимо просто распространить на новый созданный сервис, без необходимости построения всей системы защиты, или предусмотреть введение новых мер защиты информации под степень конфиденциальности информации, содержащейся в уголовном деле.

Достаточно важно заметить, что функционал рассматриваемого сервиса 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. Для формирования нестандартной статистической информации могут быть использованы технологии SQL-запросов. К основным достоинствам рассматриваемого варианта можно отнести:

– возможность интеграции с множеством баз данных МВД России в целях повышения уровня автоматизации получения информации;

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

– создана инфраструктура организации каналов связи и функционирующая интегрированная мультисервисная телекоммуникационная сеть;

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

– интеграция с модулями сервиса СОДЧ «Уголовное дело. Дознаватель-следователь».

К наиболее возможным недостаткам рассматриваемого можно отнести:

– не возможность учета объемов обрабатываемой информации и нагрузки на информационно-телекоммуникационную сеть передачи данных;

– 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, включающий в свой состав модуль «Электронное уголовное дело». При этом территориально данная система должна располагаться в информационном центре ГУ МВД по субъекту Федерации. Данное обстоятельство обусловлено тем, что возникает потребность в организации эффективной защиты информации на всех уровнях и этапах функционирования системы, а также удобством интеграции с базами данных правоохранительных органов.

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.

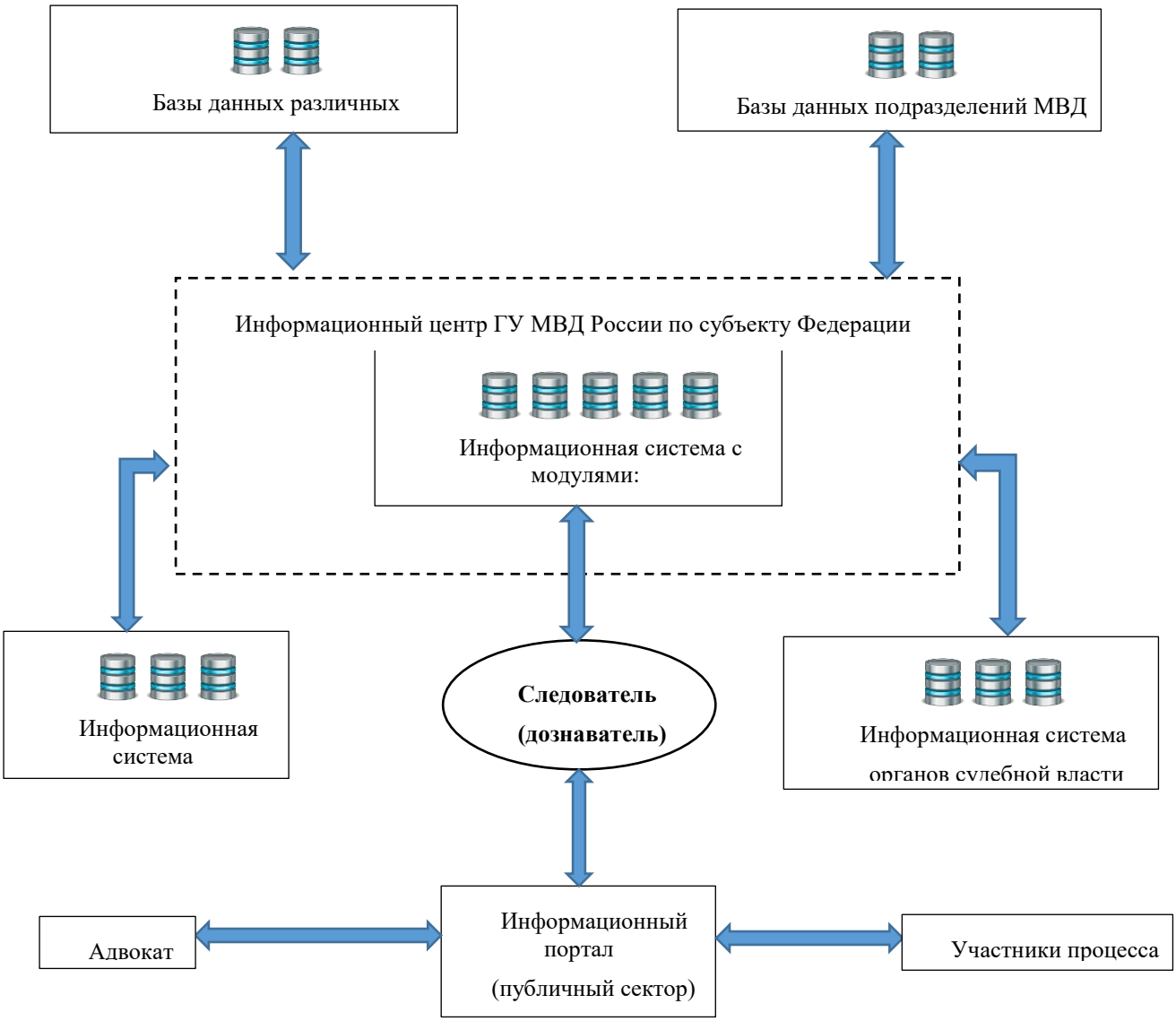


Рисунок 4 – Обобщенная схема взаимодействия следователя (дознавателя) с государственными органами

Из представленной выше схемы, очевидно, 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 ознакамливаться с материалами уголовного дела дистанционно при его окончании.

Достаточно важно заметить, что информационная система, расположенная в информационном центре ГУ МВД по субъекту Федерации, должна 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. Осуществление 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. Детектирование 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. Извлечение 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. Сохранение 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. Анализ и визуализация 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.

ЗАКЛЮЧЕНИЕ

Представленные аналитические материалы «Изучение зарубежного опыта формирования массива статистической информации из материалов электронных образов уголовных дел» позволяют нам выделить предложения по совершенствованию уголовно-процессуального и уголовного 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, имеющие юридическую силу, зафиксированные на электронном и/или материальном носителе, заверенные электронной цифровой подписью и пригодные для передачи по информационным 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».

Учебное издание

Моругина Надежда Анатольевна
Бутов Владислав Вячеславович
Нестеровский Олег Игоревич
Баркалов Юрий Михайлович

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

Учебно-практическое пособие

Редактор В.Ю. Калинская
Компьютерная верстка В.Ю. Калинской

Объем 1,25 МБ. Тираж 10 экз.

Воронежский институт МВД России
394065, Воронеж, просп. Патриотов, 53