

**ФЕДЕРАЛЬНАЯ СЛУЖБА ИСПОЛНЕНИЯ НАКАЗАНИЙ**  
Федеральное казенное образовательное учреждение высшего образования  
«Самарский юридический институт Федеральной службы исполнения наказаний»  
Юридический факультет  
Кафедра управления и информационно-технического обеспечения  
деятельности УИС

## **ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА**

Тема: **Организационно-правовые аспекты использования информационных технологий в деятельности уголовно-исполнительной системы**

Выполнил:  
слушатель 662 группы 6 курса  
прапорщик внутренней службы  
**Ласточкин Владимир Валерьевич**

Научный руководитель:  
доцент кафедры управления  
и информационно-технического  
обеспечения деятельности УИС,  
кандидат педагогических наук,  
доцент  
**Улендеева Наталия Ивановна**

Рецензент:  
начальник филиала по  
Зеленодольскому району ФКУ УИИ  
УФСИН России по Республике  
Татарстан  
подполковник внутренней службы  
**Сабиров Зульфат Фазылович**

Решение начальника кафедры о допуске к защите допущена Верашу

Дата защиты: 02.07.2021

Оценка 4 (хорошо)

Самара  
2021

**Оглавление**

<b>Введение</b> .....	3
<b>ГЛАВА 1. ПРАВОВЫЕ АСПЕКТЫ РАЗВИТИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ДЕЯТЕЛЬНОСТИ УИС</b> .....	8
1.1. Понятие «информационные технологии» и их роль в деятельности УИС.	8
1.2. Нормативно–правовое регулирование использования информационных технологий в деятельности пенитенциарной системы.....	21
<b>ГЛАВА 2. ОРГАНИЗАЦИОННЫЕ АСПЕКТЫ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ДЕЯТЕЛЬНОСТИ УИС (НА ПРИМЕРЕ ЗЕЛЕНОДОЛЬСКОГО ФИЛИАЛА ФКУ УИИ УФСИН РОССИИ ПО РЕСПУБЛИКЕ ТАТАРСТАН)</b> .....	29
2.1. Классификация информационных технологий, используемых в различных сферах деятельности УИС.....	29
2.2. Особенности использования электронных средств надзора и контроля в деятельности УИС (на примере Зеленодольского филиала ФКУ УИИ УФСИН России по Республике Татарстан).....	36
<b>Заключение</b> .....	51
<b>Библиографический список</b> .....	55

## Введение

**Актуальность темы.** Развитие и распространение научно-технического прогресса в различных сферах и отраслях жизнедеятельности российского общества не обошли стороной органы и учреждения уголовно-исполнительной системы (УИС) страны.

В современных условиях развитие и совершенствование УИС прямо и непосредственно связано с использованием и применением информационных технологий, базирующихся на факторах, оказывающих влияние на все сферы функционирования органов и учреждений системы исполнения наказаний. А именно: информатизация государственной и социальной жизнедеятельности; использование баз данных для эффективного и качественного управления во всех областях социальной структуры, включая уголовно-исполнительную систему; реализацию функции исполнения уголовных наказаний, вопросы социальной и нравственной реабилитации лиц, отбывших наказания.

В этой связи имеет смысл более детально осветить вопросы использования в Федеральной службе исполнения наказания (ФСИН) различного вида прогрессивных информационных технологий, технологических систем и технических средств охраны, контроля и надзора за осужденными, отбывающими наказания в пенитенциарных учреждениях и без изоляции от общества. Рассматривая данное направление совершенствования УИС России, целесообразно расставить акценты на следующих обстоятельствах:

- во-первых, особым образом необходимо назвать нормативно-правовые акты, создающие объективные предпосылки для совершенствования имеющихся и развития новых технических средств и методов охраны, контроля и надзора за лицами, отбывающими наказания в местах лишения их свободы и без изоляции от общества;

- во-вторых, рост качества и эффективности охраны, контроля и надзора за осужденными с использованием информационно-технических средств и технологий – одно из наиболее приоритетных направлений в области реформирования пенитенциарной системы. Он обусловлен внедрением передовых технических средств и технологий надзора, повышения уровня квалификации и профессионального мастерства сотрудников пенитенциарных учреждений, совершенствования условий их службы;

- в-третьих, рассматриваемые достижения в области применения современных информационных технологий не должны ограничиваться исключительно контролем и надзором за осужденными. Описанные в настоящей работе информационные технологии, технико-технические мероприятия должны распространяться на реализацию и организацию деятельности всех подразделений и органов УИС;

- в-четвертых, имеющиеся в распоряжении администрации учреждений и органов УИС технические средства и новшества информационных технологий весьма достоверно фиксируют все происходящее на территории исправительного учреждения (ИУ), что положительно влияет не только на осужденных, но и должным образом требует от персонала надлежащего исполнения ими закона и своих служебных обязанностей;

- в-пятых, необходимо отметить, что исследуемые технические и информационные новации пусть не напрямую, но опосредованно положительно влияют на правозащитную деятельность должностных лиц и организаций, которые осуществляют правоохранительные функции в учреждениях и органах ФСИН России.

Названные факторы подчеркивают объективную целесообразность электронной фиксации правонарушений, имеющих место в пенитенциарных учреждениях и при ограничении свободы осужденных.

Необходимо также отметить, что в наиболее развитых странах мира имеет место все более широкое использование информационных технологий, методов дистанционного аудиовизуального контроля в учреждениях закрытого и открытого типа. В России наше Правительство так же уделяет первостепенное внимание вопросам «цифровизации» и внедрения «искусственного интеллекта». Не стала исключением и пенитенциарная система Российской Федерации.

Актуальность и значимость применения передовых информационных технологий для обеспечения управления в УИС тесно связана с решением важнейшей задачи по оптимизации имеющейся и формирование единой модели информационно-телекоммуникационного обеспечения ФСИН России.

В информационных технологиях УИС имеется опережающее техническое развитие в сравнении с процессами их нормативно-правового обеспечения.

Сегодня крайне мало нормативных актов, посвященных данной проблематике. Много правовых норм, регламентирующих особенности приема, использования, хранения и передачи данных. Они рассредоточены по различным актам, обладающим различной юридической силой. Это вызывает потребность активизации работы с целью создания глобального нормативно-правового массива регулирования информационной деятельности в УИС.

Таким образом, очевидна низкая теоретическая исследованность проблематики использования информационных технологий, не достаточная четкость в трактовке отдельных норм уголовно-исполнительного законодательства в данной сфере, потребность в дальнейших исследованиях, объективно отражающих сущность, смысл и назначение информационных технологий в УИС. Этим обусловлен выбор темы выпускной квалификационной работы.

**Объектом исследования** выступают общественные отношения, связанные с применением передовых информационных технологий в уголовно–исполнительной системе Российской Федерации.

**Предметом исследования** являются организационно–правовые аспекты использования информационных технологий в деятельности уголовно–исполнительной системы.

**Целью** выпускной квалификационной работы является осмысление теоретических, правовых и организационных основ применения современных информационных технологий в исправительных учреждениях УИС, а также обоснование предложений и рекомендаций в рассматриваемой области исследования.

В этой связи исследование направлено на решение следующих задач:

- изучить понятие «информационные технологии», определив виды, свойства, компоненты организации информационных технологий;
- проанализировать нормативно–правовую базу, обеспечивающую регулирование информационных технологий в сфере деятельности УИС;
- представить классификацию информационных технологий, используемых в различных сферах деятельности УИС;
- изучить особенности применения информационных технологий в УИС на примере Зеленодольского филиала ФКУ УИИ УФСИН России по Республике Татарстан.

**Методы исследования.** При проведении исследований использовались:

- общенаучные методы (системного и логического подхода, анализа и синтеза, дедуктивный, структурно-функциональный), позволяющие выявить основные тенденции и закономерности развития изучаемого объекта;

частно-научные методы (формально-юридический, сравнительно-правовой), позволяющие выявить и описать исследуемые явления, сопоставить их для определения сходства и различия.

**Теоретическая база исследования и степень научной разработанности темы** определена тем, что информационные технологии активно исследуются в различных областях науки и практики. Однако в УИС вопросы информационного обеспечения освещены лишь в отдельных предметных областях. Различные аспекты информационного обеспечения управления УИС исследовались И. И. Мироновым (информационное обеспечение производственно–экономической деятельности), Н. Д. Андреевым (информационное обеспечение непромышленной деятельности), С.Н. Кленовым (организационно–правовые основы защиты информации), В. А. Дуленко (система информационной поддержки принятия решений в экстремальных условиях), М. А. Нагимовым (количественные методы в управлении), В. Т. Вербовым (информационно–аналитическая работа оперативных аппаратов), Ю. И. Андреевым (информационно–аналитическая работа по изучению и оценке оперативной обстановки).

Степень разработанности темы исследования. Учитывая актуальность темы исследования, ее различные аспекты анализировались многими отечественными и зарубежными учеными и практическими работниками. Общие вопросы государственного и социального управления с использованием информационных технологий, отражены в работах Г. В. Атаманчука, В. Г. Афанасьева, С. М. Галузина, В. В. Грибакина, А. А. Горбунова, И. И. Гальцева, О. А. Городова, Т. В. Закупени, В. А. Копылова, М. Н. Костомарова, В. Н. Лопатина и др.

**Структура** выпускной квалификационной работы определена целью и задачами исследования. Работа состоит из введения, двух глав, четырех параграфов, заключения, библиографического списка.

## **ГЛАВА 1. ПРАВОВЫЕ АСПЕКТЫ РАЗВИТИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ДЕЯТЕЛЬНОСТИ УИС**

### **1.1 Понятие «информационные технологии» и их роль в деятельности УИС**

Информационные технологии – технологические процессы, включающие информационную деятельность управленческого персонала, связанную с подготовкой и принятием управленческих решений.

Как и все технологии, информационные технологии постоянно развиваются и совершенствуются. Это способствует появлению новых технических средств, разработке новых концепций и методов организации, передачи, хранения и обработки данных, форм взаимодействия пользователей с техническими и другими компонентами информационных и компьютерных систем.

Разделяют информационные технологии (ИТ) по видам: ИТ обработка данных, ИТ управление, ИТ автоматизация офиса, ИТ сопровождение решений в области управления, ИТ экспертных оценок и т.п.

До начала 1990–х гг. понятие «информация» не используется в национальном законодательстве, поэтому современное российское право и юриспруденция адаптировали это понятие сравнительно недавно – чуть более двадцати лет назад.

Наиболее распространенное использование термина «информация» связано с Конституцией Российской Федерации 1993 года, в содержание положений которой данный термин использовался пять раз. Статья 29 Конституции Российской Федерации устанавливает право граждан на информацию. В этой статье говорится, что каждый имеет право свободно

искать, получать, передавать, производить и распространять информацию любым законным способом<sup>1</sup>.

Недостатком широкого использования термина «информация» является то, что в российском прецедентном праве он в основном относится к документу. Следовательно, право на информацию также связано с правом просматривать документ.

Однако количество секторов, включенных в информационную сферу общества, с каждым годом растет. На данный момент их более десяти:

- 1) зона международного обмена информацией;
- 2) реализация основных информационных прав и свобод человека и гражданина, интересов общества и государства в области информации;
- 3) организация и деятельность СМИ;
- 4) коммуникация и массовые коммуникации;
- 5) обеспечение информационной безопасности России;
- 6) электронный документооборот;
- 7) электронная коммерция и бизнес с использованием информационных технологий;
- 8) формирование и обработка персональных данных;
- 9) библиотека, архивирование;
- 10) рассмотрение конфликтов и информационных споров.

В соответствии с Федеральным законом от 27 июля 2006 г. № 149–ФЗ «Об информации, информационных технологиях и защите информации» статья 2 разъясняет основные понятия информации и информационных технологий.

- 1) информация – это сообщения, данные независимо от вида их представления;

---

<sup>1</sup> Конституция Российской Федерации: текст с изменениями и дополнениями на 14.03.2020 № 1-ФКЗ: [принята 12 декабря 1993 г.] // Официальный интернет-портал правовой информации ([www.pravo.gov.ru](http://www.pravo.gov.ru)) 04 июля 2020 г.

2) информационные технологии – это процессы, методы поиска, сбора, хранения, обработки, представления, распространения информации и способы реализации таких процессов и методов;

3) информационная система – это совокупность информации, содержащейся в базе данных, и технических средств, обеспечивающих информационную технологию и ее обработку;

4) информационные и телекоммуникационные сети – это технологическая система передачи информации о сетях связи, доступ к которой осуществляется с помощью компьютерных технологий<sup>2</sup>.

Понятие информационных технологий – это совокупность методов, производственных процессов и программного и аппаратного обеспечения, интегрированных в технологическую цепочку, обеспечивающих обработку информации для снижения трудоемкости процессов с использованием информационных ресурсов.

Другими словами, информационные технологии – это процесс, который использует набор инструментов и методов для сбора, обработки и передачи данных для получения высококачественной информации<sup>3</sup>.

Когда новые информационные технологии внедряются в организацию деятельности, необходимо оценивать риск отставания от конкурентов из-за их «устаревания», поскольку информационные продукты имеют очень высокую скорость перехода на новые типы или возможности. Срок оборота от нескольких месяцев до года. Если этот фактор не будет должным образом учтен при внедрении новой информационной технологии, он может устареть

---

<sup>2</sup> Об информации, информационных технологиях и о защите информации: Федеральный закон: текст с изменениями и дополнениями на 9 марта 2021 г. № 43-ФЗ, № 39-ФЗ [принят 27 июля 2006 г. № 149-ФЗ] // Официальный интернет-портал правовой информации ([www.pravo.gov.ru](http://www.pravo.gov.ru)) 10 марта 2021 г.

<sup>3</sup> Информатика и информационные технологии в профессиональной деятельности: учебник / А. В. Душкин [и др.]; под ред. В. П. Корячко, М. И. Купцова. – Рязань: Академия ФСИН России, 2016. – С. 231.

до того, как будет завершен переход к новой информационной технологии, и необходимо предпринять шаги для его обновления.

Подобные ошибки при внедрении информационных технологий обычно связаны с несовершенными техническими средствами, а основной причиной ошибок является отсутствие или плохое обращение с информационными технологиями.

Современные информационные системы, обеспечивающие функционирование баз данных в УИС, обрабатывают большие объемы информации. Универсальным техническим средством обработки любой информации является компьютер, который действует как усилитель интеллектуального потенциала человека и общества в целом, а средства связи, используемые компьютерами, используются для передачи и обработки информации. Развитие компьютеров – необходимая часть информационного процесса для общественности<sup>4</sup>.

Информатизация общества – один из законов современного социального прогресса. Этот термин заменяет широко использовавшийся до недавнего времени термин «компьютеризация общества». Несмотря на схожесть этих понятий, между ними есть существенные различия.

Основным направлением информатизации общества является разработка и внедрение технической базы компьютеров, которая обеспечивает быстрый поиск и компиляцию результатов обработки информации.

Особое внимание уделяется комплексу мер, направленных на обеспечение полноценного использования достоверных, всеобъемлющих и своевременных знаний во всех видах человеческой деятельности в условиях информатизации общества<sup>5</sup>.

---

<sup>4</sup> Бачило И. Л. Информационное право / И. Л. Бачило, В. Н. Лопатин, М. А. Федотов. – СПб.: Изд-во Р. Асланова «Юридический центр Пресс», 2015. – С. 394.

<sup>5</sup> Лопатин В.Н. Понятие и структура информационной сферы / В. Н. Лопатин // Актуальные проблемы права: теория и практика. – 2017. – №26. – С. 65.

Таким образом, «информатизация общества» является более широким понятием, чем «компьютеризация общества», и направлена на получение информации в кратчайшие сроки для удовлетворения своих потребностей. В понятии «информатизация общества» акцент надо делать не столько на технических средствах, сколько на сущности и цели социально-технического прогресса. Компьютеры являются базовой технической составляющей процесса информатизации общества.

Важнейшие особенности использования информационных технологий при работе с информацией являются:

- содействие в решении глобальных проблем человечества через систематизацию баз данных и информационных ресурсов.
- получение и накопление данных для последующего использования;
- эффективное использование информационных ресурсов общества для всех сфер жизнедеятельности;
- оптимизация и автоматизация информационных систем для предоставления услуг по поиску, обработке, хранению и обеспечения безопасности.

Целесообразность использования информационных технологий является главной целью реализации данной информационной технологии на базе использования современных компьютеров и технических средств.

Информационные технологии позволяют оптимизировать и во многих случаях автоматизировать растущие информационные процессы в жизни общества в последние годы.

Известно, что развитие цивилизации движется в сторону формирования информационного общества, в котором предметами и результатами труда для большинства занятого населения становятся уже не материальные ценности, а в первую очередь информация и научные знания.

Информационные процессы являются важными элементами в других сложных производственных или социальных процессах, поэтому они часто

выступают составной частью соответствующих производственных или социальных технологий.

Информационные технологии сейчас играют очень важную роль в обеспечении взаимодействия между людьми, а также в системе подготовки и распространения информации.

Цель использования информационных технологий является получение информации для анализа и на ее основе разработки управленческого решения, основанные на каком-либо действии.

Отличительной особенностью новых информационных технологий является активное вовлечение конечных пользователей (непрофессионалов в области компьютерных технологий и программирования) в процесс подготовки управленческих решений путем внедрения современных ПК на своих рабочих местах.

С одной стороны, это позволяет специалистам по управлению использовать свой творческий потенциал, опыт, интуицию в процессе подготовки и принятия решений (автоматизация незавершенных задач), а также повысить эффективность получения информации о результатах, связанных с устранением, посредники в технологической цепочке снижают вероятность отказа.

С другой стороны, особенности работы конечных пользователей – специалистов по работе с информационными ресурсами требовали от них создания инструментов и методов для связи с компьютерными системами, знаниями архитектуры и принципов работы ПК.

Новые информационные технологии взаимодействия конечных пользователей и компьютерных систем основаны на принципиально иной организации пользовательского интерфейса с компьютерной системой, которая заключается в следующем:

– обеспечение права пользователя на ошибку за счет защиты системной информации и ресурсов обработки данных от непрофессиональных действий на компьютере;

– широкий набор иерархических меню, система вызовов и упражнений, что упрощает процесс взаимодействия пользователя с ПК;

– возможности вернуться в предыдущее состояние информационной системы при наличии возвратного действия, последствия которой по каким-то причинам не удовлетворяют пользователя при выполнении регламентированного действия<sup>6</sup>.

В этой связи современные информационные технологии основаны на концепции использования специального оборудования и программного обеспечения (от скремблеров до сложных криптографических методов) для обеспечения информационной безопасности<sup>7</sup>.

Рассмотрение возможностей и особенностей использования информационных технологий можно констатировать, что их основное предназначение - это получение, сбор и анализ информации для принятия управленческих решений. Правоохранительные органы как часть социальной системы не исключение. В пенитенциарной системе России проблема информационного обеспечения всей деятельности исполнения наказаний подчиняется решению стоящих перед ней задач, которые можно и нужно решать с использованием новейших информационно-технических средств и информационных технологий.

Основанная в начале 90-х годов система информационного обеспечения надзора, охраны и обеспечения безопасности постоянно совершенствуется, что соответствовать требованиям системы уголовного правосудия и постоянно растущему уровню преступности в рыночной

---

<sup>6</sup> Волков Ю. В. Информационное право. Информация как правовая категория / Ю. В. Волков. – М.: Юрайт, 2019. – С. 96.

<sup>7</sup> Специальная техника и информационная безопасность. Учебник / под ред. В. И. Кирина. – М.: Академия управления МВД России, 2000. – С. 279.

экономике. Поэтому задача руководства Федеральной службы уголовного судопроизводства России – подготовить персонал органов и учреждений УИС к использованию современных компьютерных технологий в своей работе и внедрению новейших информационных технологий в повседневную работу<sup>8</sup>.

При этом особая роль отводится созданию автоматизированных информационных систем для сотрудников уголовно-исполнительной системы, осуществляющих процессы сбора, обработки, накопления, хранения, поиска, распространения, мониторинга информации.

Реальным проявлением использования информационных технологий в пенитенциарной системе являются, прежде всего, процедуры управления. Информация используется практически во всех сферах оперативно-служебной деятельности для выполнения различных регистрационных функций (учет нарушений режима), расчетных функций (начисление заработной платы, планирование материально-технического обеспечения), для ведения оперативно-розыскных учетов (нераскрытые преступления, похищенные вещи), оперативных, следственных, поисковых и других дел<sup>9</sup>.

В настоящее время происходит широкое развитие в деятельности УИС системы электронного документооборота (СЭД). Наиболее часто используемыми приложениями к официальным входящим и исходящим документам являются файлы Microsoft Office, содержащие текстовую, графическую и статистическую (на уровне MS Excel) информацию.

Существенно сокращает длительность оперативных мероприятий, совещаний и иных режимных мероприятий и делает их более

---

<sup>8</sup> Рачков В. Е. Информационные технологии в управлении: Лекция 14 [Электронный ресурс]/ В. Е. Рачков // Фондовые лекции СтГАУ, 2014. – Режим доступа: <http://www.stgau.ru/company/personal/user> (дата обращения: 23.04.2021г.).

<sup>9</sup> Жеребцова Н. И. Применение информационных технологий в деятельности правового управления ФСИН России/ Н. И. Жеребцова, А. Б. Маслова // Информационно-техническое обеспечение деятельности уголовно-исполнительной системы на современном этапе: материалы научно-практического семинара, Вологодский институт права и экономики ФСИН. – Вологда, 2017. – С. 40.

результативными обращение к СЭД, которая позволяет сразу же, обращаться к прикрепленным массивам данных о спецконтингенте, о мониторинге оперативной обстановки, о выпускаемой продукции и т. д.

Для подлинной экономии бумаги в процессе документооборота при осуществлении режимных мероприятий - оперативных, надзорных, воспитательных - нужна интеграция в СЭД элементов ПТК АКУС и других элементов специального программного обеспечения УИС.

Программно-технический комплекс автоматизированного картотечного учета спецконтингента (ПТК АКУС) АКУС был создан в 2000 году Научно-исследовательским институтом ФСИН России в г. Твери. Прототипом ПК АКУС был Картотечный учет, созданный Омским ЦИТОС в 1998 году. Семейство ПК АКУС разрабатывалось в течение 2000–2008 годов<sup>10</sup> для всех видов исправительных учреждений и органов (ПТК АКУС СИЗО в 2000 году; ПТК АКУС ИК (КП) в 2003 году; ПК АКУС УИИ в 2005 году; ПК Интегратор в 2008 году). Таким образом, информационная система обеспечения наполнения, обработки и хранения массива базы данных спецконтингента, находящегося в местах лишения свободы и без изоляции от общества реализуется с применением «удобной» и качественно эффективной в использовании ПТК АКУС.

Обновления для всех типов ПТК АКУС постоянно выпускаются в соответствии с новыми требованиями. Также на официальном сайте НИИ информационных технологий ФСИН России выданы свидетельства о регистрации программ для всех типов ПТК АКУС.

АКУС ПК предназначен для решения задач по обеспечению текущей работы с сервисами в рамках документооборота путем сбора и обработки данных об абонентах (заключенный, заключенный). Умение использовать разные типы представления информации позволяет

---

<sup>10</sup> Программно-технический комплекс «Автоматизированный картотечный учет спецконтингента»: руководство администратора. – Тверь: ФБУ НИИИиПТ ФСИН России, 2014. – С. 83.

быстро получить необходимую информацию, данные, статистику и ссылки на документы<sup>11</sup>.

В исполнении наказаний без изоляции от общества показало свою целесообразность применение системы электронного мониторинга подконтрольных лиц (СЭМПЛ). По мере развития хозяйственной и приносящей доход деятельности исправительных учреждений, развития внешних связей системы будет возрастать необходимость мониторинга аналогичным образом всех важнейших объектов, перемещаемых внутри инфраструктуры ФСИН России. Поэтому представляется необходимым и вполне возможным интегрировать СЭМПЛ с ГЛОНАСС. Согласование информационных и технических характеристик этих систем позволит отслеживать маршрут передвижения автомобилей, перевозящих осужденных, и грузовых автомобилей<sup>12</sup>.

Появление электронного мониторинга впервые было продемонстрировано в пенитенциарной системе США в конце 20 века. В 1983 году Верховный суд Нью-Мексико одобрил использование электронных браслетов для домашнего ареста. За 35 лет технология использования электронных браслетов в США претерпела серьезные изменения.

Самые простые передатчики с приемниками, работающими в радиусе 10 метров, высокотехнологичные электронные браслеты со сложными ключами доступа с зоной контроля стали использоваться в обеспечение ограничения свободы в Российской Федерации<sup>13</sup>.

---

<sup>11</sup> Купцов, М. И. Информационно-аналитические технологии государственного и муниципального управления: учебное пособие / М. И. Купцов, В. Н. Ручкин, В. В. Фомин. – Рязань: Академия ФСИН России, 2014. – С.48.

<sup>12</sup> Бобылев О.В. Электронный мониторинг в уголовно-исполнительной системе: монография / О. В. Бобылев. – М.: НИИ ФСИН России, 2010. – С. 81.

<sup>13</sup> Кузнецов П.У. Информационные технологии в юридической деятельности / П. У. Кузнецов. — М.: Юрайт, 2018. – С. 246.

Информационные технологии широко используются в исправительных учреждениях Российской Федерации для обеспечения надлежащего режима, надзора, охраны и конвоирования.

Сегодня есть все основания полагать, что невозможно обеспечить режим лишения свободы в пенитенциарной системе России без применения технических средств контроля и надзора. Постоянное совершенствование технических средств контроля и наблюдения требует глубоких знаний и навыков управляющего ими персонала, творческого подхода к решению новых проблем и задач.

Технические средства охраны и надзора (ТСОН) – это устройства и технологии, предназначенные для обнаружения физического воздействия создаваемой ими чувствительной зоны, превышения стандартизованного уровня и подачи сигнала (информации) об этом событии.

В систему технических средств охраны и надзора в исправительном учреждении относят<sup>14</sup>:

- 1) системы и устройства сбора и обработки информации;
- 2) средства обнаружения;
- 3) приборы контроля и досмотра;
- 4) средства тревожной сигнализации (далее – СТС);
- 5) средства оперативной связи;
- 6) средства видеонаблюдения.

Системы и устройства для сбора и обработки информации – это компьютерные системы для сбора, обработки и документирования информации от периферийных устройств, датчиков, детекторов, блоков контроля доступа, блоков управления и мониторинга. Концентраторы предназначены для сбора и обработки информации от периферийных устройств, датчиков, детекторов, элементов управления.

---

<sup>14</sup> Майоров А.М. Инженерно-технические средства охраны в УИС: учебное пособие / А. М. Майоров // Специальная техника. – 2005. – С. 35.

Системы контроля управления доступом (СКУД) предназначены для соблюдения требований режима в исправительном учреждении, увеличения пропускной способности контрольно-пропускного пункта и обеспечения безопасности дежурного персонала.

Средства обнаружения нарушителей предназначены для сбора информации об обнаружении несоответствия в деятельности по обеспечению режима и надзора. Информация о данных нарушениях передается на пульт дежурной части и в караульное помещение. Система СКУД устанавливается по периметру охраняемого объекта, на контрольно-пропускных пунктах, специальных зданиях и помещениях.

Для реагирования на перемещение объектов в исправительных учреждениях используются датчики обнаружения. Данные устройства состоят из чувствительного элемента, который использует определенные физические принципы обнаружения и схемы для передачи и преобразования сигнала, предназначенного для дальнейшей обработки.

Роль приборов контроля и досмотра оценивается эффективностью их использования для досмотра на предмет запрещенных предметов спецконтингента, сотрудников и транспортных средств.

Средствами контроля и досмотра оборудуются помещения для обыска и приема лиц под стражу, санитарные пункты пропуска, между жилыми и промышленными зонами, контрольно-досмотровые пункты.

Изучая информационные технологии, применяемые в различных сферах организации оперативно-служебной деятельности УИС, отдельно выделяются рабочие средства связи. Система связи в органах и учреждениях УИС объединяет абонентские устройства, громкоговорители, телефоны и другие формы связи в системе с другими средствами защиты.

Средства тревожной сигнализации предназначены для подачи светового и звукового сигналов о чрезвычайных обстоятельствах на объектах

охраны, вызова должностных лиц, а также для сбора сотрудников учреждения по тревоге.

К средствам оперативной связи относятся соединительные линии связи, абонентские устройства, установки громкоговорящей связи, устройства телефонной и других видов связи в системах технических средств охраны.

Обеспечение бесперебойного мониторинга оперативной обстановки в пенитенциарных учреждениях реализуется с помощью системы видеонаблюдения, которое используется для удаленного наблюдения за обстановкой в охраняемых зонах, на территории объекта, в режимных зданиях и помещениях, на подступах к территории учреждения. Использование систем видеонаблюдения обеспечивает следующие функции контроля и надзора:

- 1) наблюдение различных контролируемых зон с оценкой их текущего состояния;
- 2) обнаружение вторжения в охраняемые зоны;
- 3) запись изображения контролируемых зон с возможностью последующего анализа происшедшего и идентификации личности нарушителя;
- 4) осуществление визуальной проверки охраняемой зоны при срабатывании систем охранно-пожарной сигнализации<sup>15</sup>.

Таким образом, информационные технологии в УИС, это комплекс инженерно-технических, программных и прикладных информационных ресурсов, которые обеспечивают получение, обработки, хранение и передачу оперативной информации. С помощью информационных технологий реализуются и организуются охрана и обеспечение безопасности режимных объектов.

---

<sup>15</sup> Щербаков Г. Н. Инженерно-технические средства охраны и надзора / Г. Н. Щербаков // Специальная техника. – 2000. – № 2. – С. 19-20.

Для обеспечения дистанционного надзора за осужденными к ограничению свободы и домашним арестом уголовно-исполнительными инспекциями используется СЭМПЛ, который постоянно модифицируется и обновляется.

Для эффективного взаимодействия между подразделениями УИС используется система электронного документооборота, система автоматического заполнения статистических данных и ведения бухгалтерского учета.

## **1.2. Нормативно–правовое регулирование использования информационных технологий в деятельности пенитенциарной системы**

Анализ нормативных правовых документов в области регулирования информационных технологий показал, что в настоящее время на территории РФ действуют более 40 федеральных законов в области информации, более 80 актов Президента, около 200 актов Правительства Российской Федерации<sup>16</sup>. Так, обеспечение правовых основ глобализирующегося информационного общества, осуществляется следующими правовыми источниками:

- Конституция РФ;
- Всеобщая декларация ООН «О правах человека» 10 декабря 1948 г.;
- Уголовный кодекс РФ;
- Уголовно–процессуальный кодекс РФ;
- Гражданский кодекс РФ;

---

<sup>16</sup> Кусова Е.А. Нормативно-правовое регулирование общественных отношений в информационной сфере / Е. А. Кусова // Правовое государство: теория и практика. – 2015. – № 6. – (16). – С. 63.

– ФЗ «Об информации, информационных технологиях и защите информации»;

– ФЗ «Об электронной цифровой подписи»;

– ФЗ «Об обязательном экземпляре документов»;

– ФЗ «О связи»;

– ФЗ «О персональных данных»;

– Закон РФ «О государственной тайне».

– Указы Президента РФ («Перечень сведений конфиденциального характера», «О некоторых вопросах государственного управления в сфере связи, информационных технологий и массовых коммуникаций» и др.);

– Постановления Правительства РФ («О Правительственной комиссии по федеральной связи и информационным технологиям», «О государственной аккредитации организаций, осуществляющих деятельность в области информационных технологий» и др.);

– Доктрина информационной безопасности РФ.

Правовым фундаментом, регулирующим в РФ отношения в области информации, являются федеральные законы, направленные, на обеспечение защиты информации: Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149–ФЗ, Федеральный закон «О связи» от 07.07.2003 № 126–ФЗ, Федеральный закон «О безопасности» от 28.12.2010 № 390–ФЗ, Федеральный закон «Об электронной подписи» от 06.04.2011 № 63–ФЗ, Федеральный закон «О персональных данных» от 27.07.2006 № 152–ФЗ, Федеральный закон «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных» от 19.12.2005 № 160–ФЗ<sup>17</sup>.

---

<sup>17</sup> Андреев В. В. Правовое регулирование информационной сферы / В. В. Андреев, Н. В. Киркина // Пробелы в российском законодательстве. – 2015. – № 8. – С. 22.

Так же за последнее время в уголовно-исполнительной системе Российской Федерации произошли серьезные изменения как в нормативно-правовой базе, так и в штатной структуре пенитенциарных учреждений, занимающихся внедрением и обслуживанием информационных технологий.

Данные изменения вызваны процессом гуманизации и совершенствования всей системы. В рамках реализации «Концепции федеральной целевой программы «Развитие уголовно-исполнительной системы (2017 - 2025 годы)»<sup>18</sup> в деятельность исправительных учреждений и органов активно внедряются информационные технологии, соответствующие Российским и международным стандартам, применяемые при разработке информационных платформ.

За последнее десятилетие пенитенциарная система России претерпела значительные изменения, направленные на реформирование принципов, методов, правовой базы, концепции исполнения наказаний, внедрение новых информационных и коммуникационных технологий в практику исполнения наказаний. В то же время растет потребность в анализе современных информационных технологий и их использовании в процессе обеспечения режима, надзора, охраны и конвоирования.

Не все существующие методы и инструменты информационных технологий используются в контексте российских исправительных учреждений. Это зависит от субъективных и объективных причин.

К субъективным причинам относятся следующие причины: недостаточное техническое оснащение, несовершенная законодательная база, особенности исполнения наказаний, связанных с лишением свободы, и другие.

---

<sup>18</sup> Об утверждении Концепции федеральной целевой программы «Развитие уголовно-исполнительной системы (2017 - 2025 годы): распоряжение Правительства РФ: принят 23 декабря 2016 г. № 2808-р // Официальный интернет-портал правовой информации ([www.pravo.gov.ru](http://www.pravo.gov.ru)) 29 декабря 2016 г.

К объективным причинам можно отнести особенности работы с определенными категориями осужденных, которые относятся негативно к использованию технических средств для их ресоциализации<sup>19</sup>.

Реформа системы уголовного правосудия как одного из важнейших социальных и правовых институтов в государстве, усиление законности в области исполнения приговоров судов также повлияла на использование информационных технологий в исправительных учреждениях.

Это связано с возрастающей ролью, которую правовой фактор играет в технической реализации деятельности УИС, поскольку закон «не может и не должен отставать от достижений науки и техники в современном обществе, он должен своевременно регулировать условия, возникающие в результате использования современных технологий».

В то же время вопросы правового регулирования использования технических средств и информационных технологий в пенитенциарных учреждениях еще недостаточно проработаны.

Важнейшим нормативным актом, регулирующим общественные отношения в связи с непосредственным применением информационно-технических средств в исправительных учреждениях при исполнении уголовного наказания в виде лишения свободы осужденных, является статья 83 Уголовно–процессуального кодекса Российской Федерации, в которой регулируется применение аудиовизуальных, электронных и других средств наблюдения и контроля для предотвращения нарушений правил и получения необходимой информации о поведении в исправительных учреждениях. Данная статья введена с целью закрепления законодательства о порядке

---

<sup>19</sup> Устинкина А. В. Использование современных информационных технологий для организации режима и надзора в УИС/ А. В. Устинкина // Уголовно-исполнительная система Российской Федерации в условиях модернизации: современное состояние и перспективы развития: доклады участников Международной научно-практической конференции, Академия ФСИН России (22–23 ноября 2012 г.). – Рязань, 2013, – Т. 3. – С. 105.

использования технических средств в исправительных учреждениях при организации исполнения наказания<sup>20</sup>.

Среди законов, регулирующих исполнение приговоров с использованием технических средств в отношении осужденных, выделим Закон Российской Федерации от 21 июля 1993 г. «Об учреждениях и органах исполнения уголовных наказаний в виде лишения свободы».

Важно, чтобы рассматриваемый акт, как и УИК РФ, был фундаментальной «основой» для правового регулирования исполнения наказания в виде лишения свободы и создавал объективные условия для улучшения правового обеспечения такого обращения. Текст закона отражает основные принципы пенитенциарной системы, ее организацию, права и обязанности входящих в ее состав исполнительных институтов, правовой статус персонала, порядок использования технических средств и оружия, физической силы и специальных средств в исправительных учреждениях.

В контексте рассматриваемого вопроса следует отметить, что ст. 14 «Права учреждений, исполняющих наказания» в ч. 7 разрешает «осуществлять регистрацию осужденных, а также их фотографирование, звукозапись, кино– и видеосъемку»<sup>21</sup>.

В настоящее время использование и развитие информационных технологий в пенитенциарной системе регулируется положениями новой Концепции развития пенитенциарной системы в Российской Федерации до 2030 года<sup>22</sup> и является основным документом, определяющим задачи

---

<sup>20</sup> Елифанов С.С. О целесообразности внесения изменений и дополнений в статью 83 Уголовно-исполнительного кодекса Российской Федерации «Технические средства надзора и контроля» // Актуальные проблемы исполнения уголовных наказаний: материалы научно-практического семинара. Рязань, 2005. – С. 95.

<sup>21</sup> Об учреждениях и органах, исполняющих уголовные наказания в виде лишения свободы: закон РФ № 5473-1: текст с изменениями и дополнениями на 26 мая 2021 г. № 154-ФЗ, № 155-ФЗ [принят от 21 июля 1993 г. № 5473-1] // Официальный интернет-портал правовой информации" ([www.pravo.gov.ru](http://www.pravo.gov.ru)) 26 мая 2021 г.

<sup>22</sup> Концепция развития уголовно–исполнительной системы Российской Федерации до 2030 года: распоряжение Правительства Российской Федерации: текст от 29 апреля

уголовно–исполнительной системы Российской Федерации в соответствии с законодательством Российской Федерации, а также цели и приоритеты ее развития на определенный период с учетом международных норм и стандартов при использовании информационных технологий.

Следует отметить, что руководством ФСИН России приняты меры по упорядочению процедуры подключения исправительных учреждений к сети Интернет, разработаны рекомендации по соблюдению оперативно-режимных требований, инструкции по порядку защиты информации и предотвращению несанкционированного доступа осужденных к информационным ресурсам.

Также ежегодно директором ФСИН России утверждаются годовые планы с учетом задач, поставленных в ведомственной целевой программе, и предложений управлений и служб центрального аппарата ФСИН России. В настоящее время в соответствии с Приоритетным национальным проектом «Образование» Федеральная служба исполнения наказаний и Федеральное агентство по образованию проводят работы по оснащению и подключению к сети Интернет исправительных учреждений России. В соответствии с рассматриваемой программой осужденные 303 вечерних образовательных школ при исправительных учреждениях получают доступ в Интернет.

Рассмотрев нормативно-правовое регулирование использования информационных технологий в деятельности пенитенциарной системы, можно утверждать, что законодательные акты регулируют все виды деятельности, осуществляемой в учреждениях и органах УИС: создание, обработку, хранение и использование документов, требования к оформлению различных документов, требования к легализации документов, созданию, хранению и защите информации, а также основные концепции и процессы по обеспечению защиты информации.

Уголовно-исполнительный кодекс (УИК РФ) содержит основные положения уголовно-исполнительного законодательства, нормы об исполнении конкретных наказаний. В основе уголовно-исполнительного законодательства заложен ряд принципов - это законность, гуманизм, демократизм, средств исправления осужденных и стимулирование их правопослушного поведения, соединение наказания с исправительным воздействием<sup>23</sup>.

*Выводы по первой главе.*

Анализируя основные информационные технологии ФСИН России: их характеристики, цели, историю развития, можно сделать следующие выводы:

– информационные технологии, применяемые во ФСИН России, соответствуют предъявляемым к ним требованиям Российской Федерации.

- информационные технологии, применяемые во ФСИН России, разнообразны, охватывают множество направлений деятельности ФСИН России и соответствуют современным требованиям, предъявляемым к программно-техническим разработкам.

Необходимо систематизировать и унифицировать терминологию, употребляемую в действующих и разрабатываемых нормативных актах (особого внимания требуют понятия «информационные технологии», «информационная система», «информационное общество», «информационная услуга», «электронная торговля» и т.д.

Существующие информационные технологии для режима исполнения наказаний и его информационно-техническое обеспечение должны быть унифицированы, и в территориальных органах ФСИН России под руководством центрального органа остается еще широкое поле для совершенствования организационной деятельности структур, обеспечивающих работу с информационными технологиями и средствами.

---

<sup>23</sup> Барабанов Н. П. Обеспечение безопасности информации в уголовно-исполнительной системе: монография/ Н. П. Барабанов. – Рязань: Акад. права и упр., 2003. – С. 65.

Для осуществления режима в исправительных учреждениях должны применяться интегрированные системы безопасности, причем интеграция осуществляется на программно-аппаратном уровне.

Информационные технологии в УИС и их влияние на режим исполнения наказания можно рассматривать только с использованием специальной техники. Технические усовершенствования должны быть неразрывно связаны с организационно-правовыми усовершенствованиями. В ч. 3 ст. 83 УИК РФ необходимо изменить формулировку: термин «технические средства надзора» следует заменить на термин «программно-технические средства» или «технические средства и их программное обеспечение».

Законодательство Российской Федерации об информации, информационных технологиях и о защите информации основывается на Конституции Российской Федерации, международных договорах Российской Федерации и состоит из Федерального закона «Об информации, информационных технологиях и о защите информации» и других регулирующих отношения по использованию информации федеральных законов.

## **ГЛАВА 2. ОРГАНИЗАЦИОННЫЕ АСПЕКТЫ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ДЕЯТЕЛЬНОСТИ УИС (НА ПРИМЕРЕ ЗЕЛЕНОДОЛЬСКОГО ФИЛИАЛА ФКУ УИИ УФСИН РОССИИ ПО РЕСПУБЛИКЕ ТАТАРСТАН)**

### **2.1. Классификация информационных технологий, используемых в различных сферах деятельности УИС**

В настоящее время актуальной задачей является создание системы физической защиты объектов безопасности в пенитенциарной системе Российской Федерации, оценка эффективности комплексов ИТСОН и формирование общей информационной политики при внедрении и использовании технической защиты.

Реализация предложенного метода состоит из следующих этапов. При решении задачи оценки эффективности системы безопасности учреждения из полного списка угроз выбирается набор угроз, характерных для данного защищаемого объекта. Далее важность рисков, коэффициенты ущерба различных видов возможных последствий, выявление локальных объектов защиты, определение допустимого и остаточного уровня риска.

Модель защиты объекта включает информацию об установленных технических средствах, принципах обнаружения, вероятности обнаружения, возможностях маскировки, устойчивости к помехам и условиям эксплуатации, стоимости, возможности блокировки определенных типов и типов зон, размере заблокированные зоны, условия использования и т.п.

Залогом успешной оценки эффективности системы физической защиты объектов УИС является использование качественной базы данных для анализа поступающей оперативно-служебной информации. Без информации невозможно оценить состояние системы безопасности учреждения. В

некоторых случаях может использоваться экспертная информация, но нелогично ограничивать оценку информационных технологий только экспертными заключениями<sup>24</sup>.

Количественные данные о системе безопасности, используемые для качественной оценки эффективности системы безопасности, типы и примеры используемых информационных технологий, их тактико–технические характеристики должны быть урегулированы нормативными положениями.

Информация, необходимая для оценки эффективности систем безопасности, собирается из различных источников. При этом важно отразить его актуальность и истинное состояние технической и технологической составляющей исправительного учреждения. Поскольку система безопасности охраняемого объекта является результатом нескольких взаимосвязанных факторов, должен быть набор информационных блоков, доступных для анализа информации, необходимой для его оценки. Используемая оценочная информация должна соответствовать ряду требований: она должна быть надежной, актуальной и всеобъемлющей.

Информационные системы и программное обеспечение, применяемые в служебной деятельности сотрудников УИС, могут обеспечить надежную информационную поддержку для качественного анализа эффективности комплексов ИТСОН в УИС. Эти системы являются надежным средством сбора, хранения и обработки данных о различных видах деятельности учреждений и органов в УИС.

Существующие ведомственные информационные системы ФСИН России в настоящее время образуют мощное информационное пространство, аккумулирующее важные статистические и другие данные, в том числе, необходимые для анализа эффективности безопасности исправительного учреждения, такие как автоматизированные системы ПТК АКУС или

---

<sup>24</sup> Щербаков Г. Н. Инженерно-технические средства охраны и надзора / Г. Н. Щербаков // Специальная техника. – 2000. - № 2. – С. 18.

«Электронный паспорт исправительного учреждения» и «Электронный паспорт следственного изолятора, тюрьмы».

Автоматизированные системы «Электронный паспорт исправительного учреждения» (АС ЭПИУ) и «Электронный паспорт следственного изолятора, тюрьмы» (АС ЭПСТ) формируют базы данных информации, характеризующей состав объектов, зданий и помещений исправительных учреждений, следственных изоляторов и тюрем ФСИН России, их оборудование и обеспечение ИТСОН.

Эти автоматизированные системы обеспечивают ввод, хранение, обработку информации о технических и технологических возможностях учреждения, дают возможность оценить надежность зданий, строений и помещений исправительных учреждений, следственных изоляторов (колоний) в пенитенциарной системе, их оборудование<sup>25</sup>.

Расположение объектов на закрытой территории, сохраненная информация о свойствах объектов, позволяет непрерывно во времени анализировать безопасность участка периметра, когда нарушитель пытается преодолеть физические препятствия. Информация, полученная из перечня средств ИТСОН, зависит от параметров надежности, тактико-технических характеристик, климатических условий на режимном объекте, условий эксплуатации сотрудниками учреждения и позволяет анализировать данные для своевременного реагирования со стороны руководителей подразделений органа или учреждения УИС.

С 2017 года передана в опытную эксплуатацию информационная система «Учет состояния инженерно-технического обеспечения служебной деятельности учреждений и органов ФСИН России» (форма 30-ИТО), целью разработки которой является создание системы полноценного учета ИТСОН,

---

<sup>25</sup> Царькова Е.Г. Чем измерить эффективность: методы оценки эффективности систем физической защиты охраняемых объектов УИС / Е. Г. Царькова // Актуальные вопросы информатизации Федеральной службы исполнения наказаний на современном этапе развития уголовно-исполнительной системы: сборник материалов круглого стола (24 июня 2019 года). Тверь, 2019. - С. 189.

позволяющей систематизировать подробную информацию о наличии, качественном состоянии и движении ИТСОН, в том числе, применительно к интегрированной системе безопасности (ИСБ), СКУД, биометрическим системам идентификации, различным системам видеонаблюдения, специальному транспорту и т.п.

Разработанная информационная система позволяет автоматизировать существующий процесс учета инженерно-технических средств охраны и надзора в системе инженерно-технического обеспечения ФСИН России, формируя по каждому учреждению перечень размещенных ИТСОН.

В системе включены разделы для хранения информации об отдельных тактико–технических характеристиках специальных средств обеспечения безопасности, длине периметра и других параметрах, важных для оценки эффективности системы надзора и охраны исправительного учреждения.

Разработанный Интернет–портал «Дежурная служба ФСИН России» применяется для сбора, обработки и хранения информации о зарегистрированных в учреждениях и органах УИС происшествиях. Данная информационный портал реализуется на ведомственном интернет–портале «Дежурная служба», который был внедрен в деятельность дежурных служб в 2009 году.

Основное назначение интернет-портала «Дежурная служба ФСИН России» является создание комплексной системы предоставления оперативной информации о событиях и преступлениях, произошедших в учреждениях и органах пенитенциарной системы.

Интернет-портал создан на основе web-технологий и обеспечивает подготовку ежедневной и еженедельной оперативной сводки, формирование донесений дежурным по территориальным органам, размещение донесений (и вторичных сообщений по происшествиям, находящимся на контроле руководства ФСИН России) в дежурную службу ФСИН России ответственным дежурным по территориальному органу; формирование

ежесуточной, еженедельной оперативной сводки, контроль за происшествиями, влияющими на обстановку в УИС; контроль и получение результатов служебных проверок; получение отчетов и выборок информации из базы данных системы.

В настоящее время программное обеспечение используется во всех учреждениях и территориальных органах пенитенциарной системы Российской Федерации и позволяет анализировать статистическую информацию о происшествиях по всей стране, по каждому региону и учреждению<sup>26</sup>.

Современное направление поддержки ИТСОН в конвоировании связано с работой программного комплекса «Охрана и конвоирование», обеспечивающего взаимодействие управления по конвоированию (УОК) ФСИН России и исправительных учреждений.

В 2018 году была создана часть запланированных подсистем программного комплекса «Охрана и конвоирование», включающая подсистемы контроля, подсистемы учета безопасности учреждений и их объектов, подсистемы учета караулов. С 2019 года ведется дальнейшая разработка программного обеспечения «Охрана и конвоирование».

Наиболее востребованной возможностью программного комплекса, в том числе, и для оценки эффективности системы охраны, является автоматический расчет объема службы подразделений охраны и конвоирования, формирование данных о численности караула, а также возможность мониторинга объема службы в разрезе учреждений на уровне территориального органа и УОК ФСИН России. Рассматриваемая функция позволяет руководителям подразделений охраны и конвоирования

---

<sup>26</sup> Царькова Е.Г. Чем измерить эффективность: методы оценки эффективности систем физической защиты охраняемых объектов УИС / Е. Г. Царькова // Актуальные вопросы информатизации Федеральной службы исполнения наказаний на современном этапе развития уголовно-исполнительной системы: сборник материалов круглого стола (24 июня 2019 года). Тверь, 2019. - С. 202.

разрабатывать, принимать и организовывать качественные управленческие решения, касающиеся несения службы подразделений караулов.

Уникальность разработанной системы заключается в ее системности и комплексности реализации, предполагающей впервые полностью автоматизировать деятельность управления ФСИН России в целом <sup>27</sup>.

Сформированные массивы данных по организации охраны учреждения являются значимой входной информацией для оценки результативности организационных мероприятий по обеспечению системы физической защиты охраняемого объекта УИС.

Для сбора, обработки и анализа статистической информации в УИС используется Автоматизированная информационная система электронной обработки статистической информации «Статистика УИС» (ФГИС АИС «Статистика УИС»), которая позволяет централизованно формировать базы данных статистической информации о деятельности территориальных органов и учреждений, непосредственно подчиненных ФСИН России.

Система позволяет автоматизировать отправку, получение и обработку статистических отчетов, а также создание формы на основе информации из центральной базы данных, агрегированных, оперативных и ежедневных аналитических отчетов.

АИС «Статистика УИС» также формирует отчеты, которые позволяют получить информацию, необходимую для оценки эффективности безопасности учреждения: состояние служебной дисциплины; состояние работы с кадрами; сведения о происшествиях среди сотрудников; сведения о фактах злоупотребления спиртными напитками сотрудниками; данные о фактах применения, использования и утраты огнестрельного боевого оружия и спецсредств; сведения о случаях нарушения законности; результаты деятельности органов воспитательной работы; результаты служебной

---

<sup>27</sup> Чураков Д.Ю. Создание базы данных технических средств обнаружения, используемых в учреждениях и органах УИС / Д. Ю. Чураков// Информационные технологии в УИС. – 2019. – № 1. – С. 32.

деятельности специальных подразделений уголовно-исполнительной системы по конвоированию; сведения по основным показателям служебной деятельности, а также один из важнейших блоков данных – информацию об оперативной обстановке на объекте<sup>28</sup>.

Таким образом, анализ информационных технологий, применяемых в деятельности УИС, позволяет выделить классификацию рассматриваемых технологий по функциональному критерию:

- 1) совершенствование цифровой интегрированной сети передачи данных, включая связь уголовно-исполнительной системы;
- 2) развитие информационной системы учета кадров УИС;
- 3) автоматизирование системы делопроизводства УИС;
- 4) автоматизирование системы управления бюджетными платежами ФСИИ России;
- 5) автоматизация бухгалтерского учета и бюджетной дисциплины;
- 6) реализация «Единой автоматизированной системы картотечного учета подозреваемых, обвиняемых и осужденных»;
- 7) автоматизация статистической отчетности подразделениями УИС в рамках ведомственной информационной системы;
- 8) автоматизация системы формирования электронного паспорта исправительного учреждения;
- 9) аттестация информационных объектов подразделений собственной безопасности ФСИИ России;
- 10) автоматизация служебной деятельности персонала подразделений собственной безопасности УИС;
- 11) внедрение системы «Электронного мониторинга» за осужденными к ограничению свободы;

---

<sup>28</sup> Рачков В. Е. Информационные технологии в управлении: Лекция 14 [Электронный ресурс]/ В. Е. Рачков // Фондовые лекции СтГАУ, 2014. – Режим доступа: <http://www.stgau.ru/compra№y/perso№al/user> (дата обращения 23.04.2020).

12) внедрение системы географического слежения и контроля подвижных объектов УИС на базе спутниковой группировки «ГЛОНАСС».

## **2.2 Особенности использования электронных средств надзора и контроля в деятельности УИС (на примере Зеленодольского филиала ФКУ УИИ УФСИН России по Республике Татарстан)**

В целях обеспечения дистанционного надзора за осужденными без изоляции от общества, в том числе за подозреваемыми или обвиняемыми в месте исполнения меры пресечения в виде домашнего ареста, а также контроля выполнения ими предписанных судом ограничений, путем индивидуальной идентификации и проверки местонахождения в установленных местах (в том числе по сигналам GPS/ГЛОНАСС), а также снижения вероятности повторных преступлений уголовно-исполнительными инспекциями (УИИ) используются средства электронного мониторинга подконтрольных лиц (СЭМПЛ).

Аудиовизуальные, электронные и иные технические средства контроля применяются к подозреваемому и обвиняемому в форме постановления об использовании в отношении лица, которому избрана мера пресечения в виде домашнего ареста, аудиовизуальных, электронных и иных технических средств контроля, которое объясняют подозреваемому и обвиняемому в отношении которых избрана мера пресечения в виде домашнего ареста, а так же лицам, проживающим с ним, разъясняя при этом ответственность подозреваемого и обвиняемого в отношении, которых избрана мера пресечения в виде домашнего ареста за порчу оборудования. С момента вынесения постановления осуществляется установка соответствующего оборудования, подозреваемому и обвиняемому в отношении которых избрана мера пресечения в виде домашнего ареста, разъясняются особенности

эксплуатации технических средств контроля, вручается инструкцию эксплуатации под роспись<sup>29</sup>.

Контроль за исполнением ограничений, наложенных судом на подконтрольных лиц, осуществляется с помощью электронного мониторинга.

Электронная система контроля для контролируемых лиц – это набор средств персонального контроля и мониторинга, технических средств и устройств, используемых региональными информационными центрами посредством идентификации личности и контроля местоположения в обозначенных местах, включая сигналы GPS / ГЛОНАСС, обеспечение удаленного контроля над подозреваемым (подсудимым) и контроль за выполнением установленных им запретов (ограничений).

Целью системы электронного наблюдения за контролируемыми лицами является обеспечение контроля территориальными органами ФСИН России за подозреваемыми или обвиняемыми путем сбора, накопления, обработки, хранения и предоставления УИИ информации о выполнении подконтрольными лицами предписанных им запретов (ограничений).

Состав комплекта оборудования в каждом конкретном случае определяется, исходя из особенностей организации контроля за соблюдением подозреваемым (обвиняемым) ограничений, установленных судом.

Функциональные возможности элементов системы электронного мониторинга подконтрольных лиц позволяют гибко конфигурировать их состав при реализации задач контроля за подконтрольными лицами,

---

<sup>29</sup> О порядке применения аудиовизуальных, электронных и иных технических средств контроля, которые могут использоваться в целях осуществления контроля за нахождением подозреваемого или обвиняемого в месте исполнения меры пресечения в виде домашнего ареста и за соблюдением им наложенных судом запретов и (или) ограничений: постановление Правительства РФ: текст с изменениями и дополнениями на 15 ноября 2018 г. № 1377 [принят 18 февраля 2013 г. № 134] // Собрание законодательства РФ. – 2018. – № 48. – Ст. 7419.

определении их места нахождения и соблюдения ими установленных запретов (ограничений).

Назначение комплекса задач состоит:

- 1) в получении информации о местонахождении подконтрольного лица
- 2) путем контроля за соблюдением установленных запретов (ограничений) подконтрольных лиц;
- 3) в формировании уведомлений и сообщений о нарушениях контролируемым лицом установленных ограничений;
- 4) в электронной системе управления контролируемыми лицами обеспечивается:
  - регистрация подконтрольных лиц и технических средств контроля;
  - определение местонахождения подконтрольного лица в каждый конкретный момент времени с использованием технических средств контроля;
  - анализ данных о местонахождении подконтрольного лица по соблюдению установленных запретов (ограничений);
- 5) формирование сообщений о выявленных случаях несоответствия данных местонахождения и предписанных ограничений;
- 6) оперативную и периодическую диагностику неисправностей в блоках технических устройств электронного мониторинга<sup>30</sup>.

Система электронного мониторинга подконтрольных лиц состоит из серверного и клиентского компонента.

Серверный компонент, устанавливается на постоянно включенном сервере мониторинга территориального органа ФСИН России. Клиентский

---

<sup>30</sup> Использование системы электронного мониторинга подконтрольных лиц (СЭМПЛ-2) в деятельности уголовно- исполнительных инспекций: методические рекомендации / Е. Л. Зарембинская, С. А. Грязнов, О. Н. Ежова; под общ. ред. К. В.Талакина. – Самара: Самарский юридический институт ФСИН России, 2015. – С. 95.

компонент, устанавливается на персональной электронно–вычислительной машине оператора<sup>31</sup>.

После установки и активации электронного браслета сотрудник уголовно-исполнительной инспекции, ответственный за использование технических средств контроля и наблюдения, периодически осуществляет сбор информации (оператор – не реже двух раз в рабочий день, администратор – не реже одного раза в день) о соблюдении подозреваемым (обвиняемым) установленных ограничений при помощи стационарного пульта мониторинга.

Чтобы своевременного реагирования на нарушения со стороны подконтрольных лиц и принятия мер, оператор системы электронного мониторинга контролируемых лиц ежедневно отправляет отчеты об нарушениях руководителю УИИ, который обеспечивает еженедельную сверку и анализ информации, полученной администратором и операторами.

Процесс контроля за соблюдением подозреваемым (обвиняемым) установленных запретов (ограничений) осуществляется сервером управления и передается на стационарный пульт управления в автоматическом режиме.

Программа мониторинга, установленная на стационарном пульте мониторинга, содержит конструктор отчетов, формирование которых происходит автоматически в заданный интервал времени либо по запросу сотрудника уголовно-исполнительной инспекции в любое время.

Отчет с координатами местонахождения контролируемого лица может быть создан автоматически через определенный промежуток времени, а затем в последующем архивирован в отчетный файл, который будет храниться в течение заданного промежутка времени на сервере мониторинга территориального органа ФСИН России.

---

<sup>31</sup> Система электронного мониторинга подконтрольных лиц ФСИН РОССИИ. Специальное программное обеспечение стационарного пульта мониторинга: руководство системного программиста. – М.: ФГУП ЦИТОС ФСИН России, 2010. – С. 20.

Сигнал о допущенных подозреваемым (обвиняемым) нарушениях или потере точки на экране отображается в отдельном окне в виде сообщения об ошибке в окне монитора.

Протокол о нарушениях, допущенных подконтрольным лицом, может быть автоматически оформлен в виде текстового файла или в виде электронной таблицы, которая хранится на СМ территориального органа ФСИН России в течение определенного периода времени.

Сведения о нарушениях, полученные при помощи системы электронного мониторинга подконтрольных лиц, предназначенные для использования сотрудниками УИИ при применении в установленном порядке мер взыскания и направления в суд представлений для принятия решения о дальнейшем порядке отбывания наказания.

Внедрение оборудования СЭМПЛ в практику работы Зеленодольского филиала ФКУ УИИ УФСИН России по Республике Татарстан проводилось поэтапно, с 2010-го по 2012 гг. В настоящее время оборудование успешно внедрено во всех филиалах ФКУ УИИ ФСИН России по РТ и используется в отношении осужденных, отбывающих наказание в виде ограничения свободы; в отношении подозреваемых или обвиняемых в месте исполнения меры пресечения в виде домашнего ареста.

В 2020 г. по учетам УИИ территориальных органов ФСИН России обеспечен контроль за 13252 лицами, в отношении которых избрана мера пресечения в виде домашнего ареста (АППГ – 9180 + 30,73%).

По состоянию на 31 декабря 2020 г. на учете в филиалах УИИ состояло 4215 подозреваемых (обвиняемых), в отношении которых избрана мера пресечения в виде домашнего ареста (АППГ – 2730). Оборудование СЭМПЛ применялось в отношении 3673 лиц, находящихся под домашним арестом, что составило 86,3% (плановый – 70%).

Всего по состоянию на 31 декабря 2020 г. под электронным контролем СЭМПЛ находились 10985 подконтрольных лиц, состоящих на учете

в филиалах УИИ, из них 3789 (90%) лиц, в отношении которых избрана мера пресечения в виде домашнего ареста.

За весь период использования СЭМПЛ под электронным контролем находились более 128 тыс. подозреваемых (обвиняемых), в отношении которых избрана мера пресечения в виде домашнего ареста.

При помощи контрольных устройств СЭМПЛ выявлено 5244 фактов нарушения условий исполнения меры пресечения в виде домашнего ареста (с 2018 г.).

В отношении лиц, находящихся под домашнем арестом, сотрудниками УИИ выявлено 1932 нарушения, из них 1650 – при помощи СЭМПЛ (85,3%).

Рассмотрим процесс обеспечения дистанционного надзора за осужденными без изоляции от общества, в том числе за подозреваемыми или обвиняемыми в месте исполнения меры пресечения в виде домашнего ареста, а также контроля выполнения ими предписанных судом ограничений, путем индивидуальной идентификации и проверки местонахождения в установленных местах (в том числе по сигналам GPS/ГЛОНАСС).

После того, как начальником филиала УИИ будет подписано постановление о применении СЭМПЛ в отношении подозреваемого (обвиняемого), инспектор по СЭМПЛ посещает лицо, в отношении которого избрана мера пресечения в виде домашнего ареста, по месту исполнения данной меры пресечения. При посещении подконтрольного лица, инспектор филиала УИИ объясняет правила эксплуатации оборудования, которое применяется к данному лицу, ответственность за порчу оборудования и проводится первоначальная беседа.

После установки технических средств контроля и надзора в отношении подозреваемого (обвиняемого) в месте исполнения меры пресечения в виде домашнего ареста, инспектор филиала УИИ осуществляет контроль с помощью проверки подконтрольного лица по месту исполнения меры пресечения в виде домашнего ареста - не реже двух раз в неделю; с помощью

телефонных разговоров - не реже двух раз в неделю с отражением результатов в месячной ведомости контроля.

Перечень аудиовизуальных, электронных и технических средств, которые применяются филиалами УИИ предусмотрен Постановлением Правительства РФ от 18 февраля 2013 г. № 134<sup>32</sup>.

1) Электронный браслет (далее – БД) – электронное устройство со встроенной системой управления, предназначенное для длительного ношения на теле (более 3 месяцев), которое носит подозреваемый или обвиняемый при опознании и отслеживании его местонахождения. для снятия и вскрытия корпуса без разрешения.

ЭБ используется в комплекте с СКУ и МКУ, он не имеет дисплея, или какого-либо индикатора заряда поэтому если произойдет разряд батареи браслета, инспектор филиала УИИ может не заметить этого, и поэтому приходящие сообщения на пульт СЭМПЛ о потере связи с оборудованием будут изначально рассматриваться как нарушение условий меры пресечения подозреваемым (обвиняемым). Вся информация передается через спутник на станцию электронного мониторинга.

В процессе эксплуатации электронных браслетов выявились серьезные недостатки, связанные с тем, что, когда ЭБ одет подконтрольному лицу, то его нельзя подвергать ударным воздействиям, но как быть в том случае, если работа сопряжена с риском ударного воздействия, к примеру, строительство, либо монтажные работы – это остается проблемой. Кроме того, еще одним проблемным вопросом в применении СКУ является его значительно маленький радиус действия - от 50 до 100 метров, в зависимости от установленной мощности передатчика.

---

<sup>32</sup> О порядке применения аудиовизуальных, электронных и иных технических средств контроля, которые могут использоваться в целях осуществления контроля за нахождением подозреваемого или обвиняемого в месте исполнения меры пресечения в виде домашнего ареста и за соблюдением им наложенных судом запретов и (или) ограничений: постановление Правительства РФ: текст с изменениями и дополнениями на 15 ноября 2018 г. № 1377 [принят 18 февраля 2013 г. № 134] // Собрание законодательства РФ. – 2018. – № 48. – Ст. 7419.

2) Мобильное контрольное устройство (далее МКУ) с установленной периодичностью определяет свое местоположение по навигационным спутниковым сигналам ГЛОНАСС/GPS и передает эту информацию на сервер мониторинга. Все случаи потери и восстановления приема навигационного сигнала фиксируются СЭМПЛ, при необходимости предоставляя необходимую информацию или тревожное сообщение сотруднику УИИ, который обменивается информацией с сервером мониторинга по беспроводным каналам связи (по каналам GSM, использующим передачу данных GPRS).

МКУ уведомляет сервер мониторинга о несанкционированном доступе к электронному браслету или МКУ, включая попытки вскрыть ЭБ и МКУ.

Изучая особенности применения оборудования СЭМПЛ в деятельности УИИ можно выделить проблемы в применении МКУ в Зеленодольском филиале ФКУ УИИ УФСИН России по Республике Татарстан<sup>33</sup>:

- слабость удержания заряда батареи в МКУ;
- износ комплектующих деталей МКУ;
- до сегодняшнего дня карта Зеленодольского района не отображается, что не позволяет дистанционно отслеживать местоположения подконтрольного лица через спутниковую навигационную систему ГЛОНАСС/GPS.

3) Устройство - Ретранслятор применяется в случаях, когда необходимо расширение контролируемой зоны более 100 метров от СКУ. Ретранслятор размещается в местах проживания подконтрольных лиц путем установки стационарно на стене или неподвижной горизонтальной поверхности.

---

<sup>33</sup> Аналитическая записка о состоянии использования электронных средств надзора и контроля в деятельности Зеленодольского филиала ФКУ УИИ УФСИН России по Республике Татарстан от 30. 12. 2020 г // Материалы преддипломной практики в ФКУ ИК -19 УФСИН России по Республике Татарстан / В. В. Ласточкин (неопубликованный акт).

Ретранслятор осуществляет прием, усиление и переизлучение сигналов ЭБ, обеспечивая тем самым расширение зон приема контрольных устройств. Ретранслятор имеет возможность настройки чувствительности радиоприемного модуля, а также уровня мощности излучаемого радиосигнала для точного задания требуемых границ контрольных зон.

Использование ретрансляторов при осуществлении контроля за нахождением подозреваемых (обвиняемых) в месте исполнения меры пресечения в виде домашнего ареста и за соблюдением ими наложенных судом запретов и (или) ограничений в Зеленодольском филиале ФКУ УИИ УФСИН России выявило следующую проблему:

- на территории обслуживания Зеленодольского района много сельских поселений и частного сектора, где сотовая сеть GSM имеет слабый сигнал, что приводит к ложному срабатыванию на пульте СЭМПЛ<sup>34</sup>.

4) Персональный трекер – электронное устройство для удаленного мониторинга местоположения контролируемого лица через систему спутниковой навигации ГЛОНАСС / GPS. Это устройство имеет встроенную систему контроля несанкционированного снятия и вскрытия корпуса. Устройство можно носить не более трех месяцев.

Вместо меры пресечения в виде домашнего ареста использование персонального трекера для наблюдения за соблюдением подозреваемыми (подсудимыми) запретов и (или) ограничений, установленных судом в Зеленодольском отделении выявило проблемы:

- по искажению сигнала в подвалах, а также в больших зданиях (радиационный контроль);

– недостатки спутниковой связи - при неблагоприятных погодных условиях (снегопад, сильная облачность) сигнал может прекращаться, что

---

<sup>34</sup> Аналитическая записка о состоянии использования электронных средств надзора и контроля в деятельности Зеленодольского филиала ФКУ УИИ УФСИН России по Республике Татарстан от 30. 12. 2020 г // Материалы преддипломной практики в ФКУ ИК -19 УФСИН России по Республике Татарстан / В. В. Ласточкин (неопубликованный акт).

приводит к потере СЭМПЛ подозреваемого (обвиняемого) лица на какое-то время.

5) В деятельности филиалов УИИ также используются аудиовизуальные блоки управления – электронное устройство для визуальной и голосовой идентификации подозреваемого или обвиняемого.

Практика применения устройств аудиовизуального контроля при осуществлении контроля за нахождением подозреваемых (обвиняемых) в месте исполнения меры пресечения в виде домашнего ареста и за соблюдением ими наложенных судом запретов и (или) ограничений<sup>35</sup> в Зеленодольском филиале ФКУ УИИ УФСИН России по Республике Татарстан выявил следующие проблемы:

– видеорегистратор тяжелый и имеет относительно короткое время работы (невозможно полностью зарядить его при интенсивном использовании, так как для полной зарядки требуется много времени);

6) Технические средства и оборудование из региональных информационных центров:

- сервер мониторинга — это программно-аппаратный комплекс, предназначенный для обеспечения работы системы дистанционной идентификации, получения, обработки, хранения и передачи информации;

- сервер аудиовизуального контроля — программно-аппаратный комплекс для обеспечения функционирования системы визуальной и голосовой идентификации, записи, обработки, хранения и передачи информации;

- стационарный пульт мониторинга - обеспечивает представление инспектору филиала УИИ результатов контроля в текстовом и графическом виде, в том числе отображение местоположения подконтрольного лица в виде яркостной метки и/или маршрутов его перемещения в виде ломаной

---

<sup>35</sup> Новожилов С.А. Опыт применения системы электронного мониторинга при исполнении уголовных наказаний: научно-аналитический обзор / С. А. Новожилов, А. В. Лапенков. – Псков: Псковский филиал Академии ФСИН РОССИИ, 2014. – С. 43.

линии на электронной карте местности с обозначенными границами зон, где подконтрольное лицо может или должно находиться, а также зон, куда вход для него запрещен;

- мобильный пульт мониторинга — это портативный компьютер, предназначенный для контроля за наблюдаемыми лицами (прием и идентификацию сигналов электронных браслетов, их обработку и отображение информации о соблюдении подозреваемым или обвиняемым наложенных судом запретов и (или) ограничений), а также работой СКУ, трекеров и ретрансляторов и для их замены в случае необходимости.

Практика применения технических средств и устройств региональных информационных центров при осуществлении контроля за нахождением подозреваемых (обвиняемых) в месте исполнения меры пресечения в виде домашнего ареста и за соблюдением ими наложенных судом запретов и (или) ограничений в Зеленодольском филиале ФКУ УИИ УФСИН России по Республике Татарстан выявило следующие проблемы:

- нехватка некоторых размеров ремешков и предохранительных защелок к ЭБ;

- отсутствие последних версий электронных карт местности;

- низкий уровень комплектующих устройств;

- использование старого оборудования (70 %)

- техническая недоработка средств контроля, что в свою очередь влияет на их дальнейший срок службы использования (при этом возникают частые поломки и скопления большого количества оборудования СЭМПЛ, требующего ремонта);

- использование информационно - телекоммуникационной сети «Интернет» подконтрольным лицом, если судом наложено ограничение на её использование (подконтрольное лицо осуществляет выход в «Интернет» с мобильного телефона родственников или друзей, которые проживают совместно с ним).

Несмотря на достаточно подробно регламентированные порядок и основания для избрания меры пресечения в виде домашнего ареста, при его осуществлении возникает ряд проблем. В отдаленных районных центрах не хватает штата сотрудников по контролю исполнения домашнего ареста. Исполнение решения суда по избранию меры пресечения в виде домашнего ареста происходит на основе федерального законодательства, однако не урегулирован процесс действия данного приказа и реализации данной меры пресечения так же продолжает происходить по внутриведомственным актам УФСИН России по территориальным органам.

На данный момент проблемы возникают при приведении документов к новому образцу.

В связи с реформированием УИС необходимо постоянно проводить курсы переподготовки и повышения квалификации сотрудников УИИ, необходимо совершенствование профессионального обучения кадров, рост их профессионального уровня, для чего требуются:

- разработка и внедрение действенного механизма подбора кадров;
- совершенствование управления профессиональным развитием кадров УИИ;
- создание системы непрерывного профессионального образования сотрудников УИИ, совершенствование программ подготовки и профессионального развития кадров УИИ.

Что касается модернизации оборудования для СЭМПЛ, то следует отметить, что с 2015 году всеми территориальными органами ФСИН России были получены модернизированные электронные браслеты, и в настоящее время УИИ активно их используют. Однако целесообразно постоянно повышать и увеличению мощности ЭБ и встроенной аккумуляторной батареи, которой, как заявлено производителем, должно хватить на семь лет работы устройства, в отличие от трех лет работы предыдущих моделей. Более того, в новой модели электронных браслетов полностью изменена

конструкция крепления ремня и замка, благодаря чему производителям удалось исключить вероятность ложного срабатывания датчика целостности ремня.

Анализ проблем использования СЭМПЛ в материалах юридической практики показывает, что основной проблемой является процедура взыскания материального ущерба с подозреваемого или обвиняемого в случаях повреждения (утрате) ими комплектующих частей оборудования СЭМПЛ. В связи с этим, представляется целесообразным внести в действующее законодательство Российской Федерации поправки и изменения, предусматривающие материальную ответственность подозреваемого или обвиняемого, находящегося в качестве меры пресечения под домашним арестом, в случаях повреждения, уничтожения (утраты) применяемых к ним аудиовизуальных, электронных и иных технических средств надзора и контроля.

*Выводы по второй главе.*

Изучение организационных аспектов использования информационных технологий в деятельности пенитенциарной системы позволяет сделать следующие выводы:

1. Разработанные и применяемые информационные технологии в различных сферах деятельности органов и учреждений УИС можно классифицировать по функциональному критерию:

- 1) совершенствование цифровой интегрированной сети передачи данных, включая связь уголовно-исполнительной системы;
- 2) развитие информационной системы учета кадров УИС;
- 3) автоматизирование системы делопроизводства УИС;
- 4) автоматизирование системы управления бюджетными платежами ФСИН России;
- 5) автоматизация бухгалтерского учета и бюджетной дисциплины;

6) реализация «Единой автоматизированной системы картотечного учета подозреваемых, обвиняемых и осужденных»;

7) автоматизация статистической отчетности подразделениями УИС в рамках ведомственной информационной системы;

8) автоматизация системы формирования электронного паспорта исправительного учреждения;

9) аттестация информационных объектов подразделений собственной безопасности ФСИН России;

10) автоматизация служебной деятельности персонала подразделений собственной безопасности УИС;

11) внедрение системы «Электронного мониторинга» за осужденными к ограничению свободы;

12) внедрение системы географического слежения и контроля подвижных объектов УИС на базе спутниковой группировки «ГЛОНАСС».

2. Анализ особенностей использования электронных средств надзора и контроля в деятельности УИС на примере Зеленодольского филиала ФКУ УИИ УФСИН России по Республике Татарстан выделил проблемы использования технических средств контроля и надзора за осужденными без изоляции от общества, связанные с техническими характеристиками рассматриваемых устройств; со своевременным реагированием за осужденными, которые допускают несанкционированное снятие и вскрытия корпуса электронного устройства, предназначенного для дистанционного отслеживания местоположения подконтрольного лица через спутниковую навигационную систему ГЛОНАСС/GPS и с общением с определенными лицами; отправкой и получением почтово-телеграфных отправок; использованием средств связи и информационно-телекоммуникационной сети «Интернет».

Сделанные выводы и предложения по решению проблемных вопросов, возникающих при исполнении меры пресечения в виде домашнего ареста

и ограничения свободы, позволят оптимизировать применение электронных средств мониторинга, имеющихся в распоряжении УИИ и более качественно выполнять служебные задачи, поставленные перед пенитенциарной системой России.

## Заключение

Согласно проведенного исследования организационно-правовых аспектов использования информационных технологий в деятельности уголовно-исполнительной системы можно сделать следующие выводы.

Современные информационные технологии можно определить, как операционную систему для сбора, хранения, обработки и передачи информации по каналам связи с использованием компьютерных технологий.

Важные принципы современных информационных технологий – интерактивный, «дружественный» рабочий интерфейс; интеграция с другими программными продуктами; гибкость в процессе изменения данных и постановки целей.

Пенитенциарная система на современном этапе обладает необходимым техническим и технологическим потенциалом для применения и обновления информационных ресурсов при обеспечении исполнения наказаний как с ограничением свободы, так и без изоляции от общества.

Однако в настоящее время отсутствует специальное программное обеспечение для отдельных подразделений и служб различных учреждений ФСИН России, которое крайне необходимо.

Для развития системы информационного обеспечения институтов исполнения наказаний целесообразно:

1. Внедрение ускоренных информационных технологий, компьютерных технологий и телекоммуникаций, локальных вычислительных сетей, стандартного программного обеспечения и автоматизированных рабочих мест для обобщения и анализа информации, информационного обеспечения операционных служб.

2. Обеспечение единообразия и совместимости компьютерных технологий и телекоммуникаций, общесистемного и прикладного программного обеспечения, его адаптация с учетом особенностей автоматизированных систем обработки информации.

3. Изучение передового опыта в области компьютеризации наряду с совершенствованием информационных технологий позволили автору исследования выделить классификацию информационных технологий, применяемых в деятельности органов и учреждений уголовно-исполнительной системы по функциональному критерию. Представленная в работе классификация реализуется постоянным совершенствованием инженерно-технических средств обеспечения режима, надзора, охраны, конвоирования и повышением результатов служебной деятельности всех подразделений УИС, способствует своевременному и качественному принятию и организации управленческих решений руководителями отделов и служб органов и учреждений пенитенциарной системы.

4. Анализ политики информационного обеспечения исполнения наказаний должна включать как централизованные, так и децентрализованные компоненты. Централизованная составляющая должна быть нацелена на достижение стратегических целей ведомства и должна финансироваться в первую очередь из государственного бюджета. Она должна быть направлена на формирование комплексной научно-технической политики, которая будет способствовать реализации всех областей информационного процесса с целью развития научно-технических достижений как сейчас, так и в будущем.

Децентрализованный компонент должен быть нацелен на создание среды, которая отвечает текущим потребностям учреждений и органов ведомства по внедрению информационных технологий, с целью повышения производительности и улучшения условий оперативно-служебной деятельности, и ориентироваться на добровольность и заинтересованность пользователей.

Помимо задач по управлению учреждениями, отделами, службами, созданию ведомственной инфраструктуры, решению финансовых проблем, централизованное управление в ведомственных структурах должно

сочетаться с действиями по созданию необходимых условий для нормальной работы децентрализованной составляющей.

Такая интеграция позволяет осуществлять обмен информацией с территориальными органами других федеральных органов исполнительной власти, государственными органами субъектов Российской Федерации, правоохранительными органами, органами местного самоуправления, а также обмениваться последними достижениями науки и технологий, исследования и применения опыта пенитенциарных систем других стран мира.

Таким образом, создание единого информационного пространства УИС и внедрение новых информационных технологий в деятельность подразделений, отделов и служб в настоящее время является актуальной задачей, в решении которой должны активное участие принимать образовательные и научно-исследовательские учреждения, подведомственные ФСИН России. Основные задачи формирования и функционирования единого информационного пространства УИС позволяют:

- внедрять комплекс мероприятий, обеспечивающий механизм функционирования и эксплуатационных особенностей ИТСОН, средств связи, информационных потоков и телекоммуникационных магистралей в разветвленной сети пенитенциарных учреждений страны, комплексов вычислительной техники и периферийного оборудования;

- обеспечивать ФСИН Российской Федерации механизмом постоянного, непрерывного во времени управления ведомственными учреждениями и органами посредством предоставления достоверных, своевременных и качественных вариантов связи, в том числе и кодированной версии;

- предоставлять оперативную, достоверную и качественную информацию в виде трансляции простых текстовых файлов, оцифрованных и закодированных информационных потоков в любых условиях, включая чрезвычайные;

- внедрять в обеспечение практических мероприятий, обуславливающих должное функционирование и «закрытость» (как от внешних, так и от внутренних посягательств) шифрованной связи, ее развитие и совершенствование в масштабах ФСИН России;

- использовать криптографические механизмы, исчерпывающего перечня сервиса, работ и услуг, касающихся зашифрованных сведений, информации и данных, их техническое обслуживание;

- обеспечивать единый механизм защиты информационных потоков в УИС.

## Библиографический список

### Нормативные правовые акты

1. Конституция Российской Федерации: текст в редакции на 14 марта 2020 г. № 1–ФКЗ: [принята всенародным голосованием 12 декабря 1993 г.] // Официальный Интернет–портал правовой информации ([www.pravo.gov.ru](http://www.pravo.gov.ru)) 4 июля 2020 г.

2. Всеобщая декларация прав и свобод человека (принята Генеральной Ассамблеей ООН 10 декабря 1948 года) // Российская газета. – 1998. – 10 декабря.

3. Уголовный кодекс Российской Федерации: федеральный закон: текст с изменениями и дополнениями на 5 апреля № 59-ФЗ [принят 13 июня 1996 г. № 63-ФЗ] // Официальный Интернет–портал правовой информации ([www.pravo.gov.ru](http://www.pravo.gov.ru)) 5 апреля 2021 г.

4. Уголовно–исполнительный кодекс Российской Федерации: федеральный закон: текст с изменениями и дополнениями на 26 мая 2021 г. № 154–ФЗ [принят 8 января 1997 г. № 1–ФЗ] // Официальный Интернет–портал правовой информации ([www.pravo.gov.ru](http://www.pravo.gov.ru)) 26 мая 2021 г.

5. Гражданский кодекс Российской Федерации (часть вторая): федеральный закон: текст с изменениями и дополнениями на 30 декабря 2020 г. № 258-ФЗ [принят 26 января 1996 г. № 14-ФЗ] // Официальный Интернет–портал правовой информации ([www.pravo.gov.ru](http://www.pravo.gov.ru)) 30 декабря 2020 г.

6. Гражданский кодекс Российской Федерации (часть четвертая): федеральный закон: текст с изменениями и дополнениями на 30 апреля 2021 г. № 107-ФЗ [принят 18 декабря 2006 г. № 230-ФЗ] // Официальный Интернет–портал правовой информации ([www.pravo.gov.ru](http://www.pravo.gov.ru)) 30 апреля 2021 г.

7. Об информации, информационных технологиях и защите информации: Федеральный закон: текст с изменениями и дополнениями на 9 марта 2021 г. № 43–ФЗ, № 39–ФЗ [принят 27 июля 2006 г. № 149–ФЗ] // Официальный Интернет–портал правовой информации ([www.pravo.gov.ru](http://www.pravo.gov.ru)) 10 марта 2021 г.

8. Об электронной подписи: федеральный закон: текст с изменениями и дополнениями на 24 февраля 2021 г. № 20-ФЗ [принят 6 апреля 2011 г. №63-ФЗ] // Официальный Интернет–портал правовой информации ([www.pravo.gov.ru](http://www.pravo.gov.ru)) 24 февраля 2021 г.

9. Об обязательном экземпляре документов: федеральный закон: текст с изменениями и дополнениями на 8 июня 2020 № 166-ФЗ [принят 29 декабря 1994 г. №77-ФЗ] // Официальный Интернет–портал правовой информации ([www.pravo.gov.ru](http://www.pravo.gov.ru)) 8 июня 2020 г.

10. О связи: федеральный закон: текст с изменениями и дополнениями на 30 декабря 2020 № 533-ФЗ [принят 7 июля 2003 г. №126-ФЗ] // Официальный Интернет–портал правовой информации ([www.pravo.gov.ru](http://www.pravo.gov.ru)) 30 декабря 2020 г.

11. О персональных данных: Федеральный закон: текст с изменениями и дополнениями на 30 декабря 2020 г. № 519-ФЗ [принят 27 июля 2006 г. №152-ФЗ] // Официальный интернет-портал правовой информации ([www.pravo.gov.ru](http://www.pravo.gov.ru)) 30 декабря 2020 г.

12. Об использовании глобальной навигационной спутниковой системы ГЛОНАСС в интересах социально–экономического развития Российской Федерации: указ Президента Российской Федерации: текст в редакции от 12 апреля 2019 г. № 161 [принят в мае 17, 2007 № 638] // Официальный Интернет–портал правовой информации ([www.pravo.gov.ru](http://www.pravo.gov.ru)) 12 апреля 2019 г.

13. Об утверждении перечня аудиовизуальных, электронных и иных технических средств надзора и контроля, используемых уголовно-исполнительными инспекциями для обеспечения надзора за осужденными

к наказанию в виде ограничения свободы: постановление Правительства РФ на 31 марта 2010 г. № 198 // Собрание законодательства РФ. – 2010. – № 14. – Ст. 1663.

14. Об утверждении Концепции федеральной целевой программы «Развитие уголовно-исполнительной системы (2017 - 2025 годы)»: распоряжение Правительства РФ: принят 23 декабря 2016 г. № 2808-р // Официальный интернет-портал правовой информации ([www.pravo.gov.ru](http://www.pravo.gov.ru)) 29 декабря 2016 г.

15. Об утверждении перечня аудиовизуальных, электронных и иных технических средств надзора и контроля, используемых администрациями исправительных центров для предупреждения преступлений, нарушений порядка и условий отбывания принудительных работ и для получения необходимой информации о поведении осужденных к принудительным работам: распоряжение Правительства Российской Федерации: принят 31 декабря 2016 г. № 2932-р // Официальный Интернет–портал правовой информации ([www.pravo.gov.ru](http://www.pravo.gov.ru)) 6 января 2017 г.

16. О порядке использования аудиовизуальных, электронных и иных технических средств контроля, которые могут быть использованы для контроля нахождения подозреваемого или обвиняемого по месту применения меры пресечения в виде домашнего ареста и др. соблюдение запретов и (или) ограничений, установленных судом: постановление Правительства Российской Федерации: текст в редакции на 15 ноября 2018 г. № 1377 [принят 18 февраля 2013 г. № 134] // Официальный интернет-портал правовой информации ([www.pravo.gov.ru](http://www.pravo.gov.ru)) 16 ноября 2018 г.

17. Концепция развития уголовно–исполнительной системы Российской Федерации до 2030 года: распоряжение Правительства Российской Федерации: текст от 29 апреля 2021 года № 1138–р [принят 14 октября 2020 года № 1772–р] // Официальный Интернет–портал правовой информации ([www.pravo.gov.ru](http://www.pravo.gov.ru)) 12 мая 2021 г.

18. О государственной тайне: закон Российской Федерации: текст в редакции на 9 марта 2021 г. № 39–ФЗ [принят 21 июля 1993 № 5485–1] // Официальный Интернет–портал правовой информации ([www.pravo.gov.ru](http://www.pravo.gov.ru)) 9 марта 2021 г.

19. Об учреждениях и органах, исполняющих уголовные наказания в виде лишения свободы: закон Российской Федерации: текст в редакции на 26 мая 2021 г. № 154–ФЗ, № 155–ФЗ [принят в 21 июля 1993 № 5473–1] // Официальный Интернет–портал правовой информации ([www.pravo.gov.ru](http://www.pravo.gov.ru)) 26 мая 2021 г.

20. О введении в действие федеральной государственной информационной программы «Электронный документооборот ЕИС»: приказ ФСИН России от 30 декабря 2015 г. № 1278 // Официальный Интернет–портал правовой информации ([www.pravo.gov.ru](http://www.pravo.gov.ru)) 30 декабря 2015 г.

### **Учебные, научные и справочные издания**

21. Авсянский В. А. Применение современных технологий в деятельности органов безопасности пенитенциарной системы, проблемные вопросы и пути их решения / В. А. Авсянский // Пенитенциарная система и общество: опыт взаимодействия: материалы IV Международной научно–практической конференции. Пермский институт ФСИН России (4–6 апреля 2017 г.) / сост. Тарасов В.А. – Пермь, 2017. – 89 с.

22. Барабан Н. П. Обеспечение информационной безопасности в пенитенциарной системе: монография / Н. П. Барабанов. – Рязань: Акад. Право и управл., 2003. – 95 с.

23. Бачило И. Л. Информационное право / И. Л. Бачило, В. Н. Лопатин, М. А. Федотов. – СПб.: Издательство Р. Асланова «Правовой центр Пресс», 2015. – 434 с.

24. Бобылев О.В. Электронный мониторинг в пенитенциарной системе: монография / О.В. Бобылев. – М.: НИИ ФСИН России, 2010. – 128 с.

25. Волков Ю. В. Информационное право. Информация как правовая категория / Ю. В. Волков. – М.: Юрайт, 2019. – 243 с.

26. Епифанов С.С. О целесообразности внесения изменений и дополнений в статью 83 УК РФ «Технические средства наблюдения и контроля» // Актуальные проблемы исполнения уголовных наказаний: материалы научно–практического семинара. ... Рязань, 2005. – 121 с.

27. Жеребцова Н.И. Применение информационных технологий в деятельности Юридического управления ФСИН России / Н.И. Жеребцова, А. С. Маслова // Информационно–техническое обеспечение деятельности уголовно–исполнительной системы на современном этапе: материалы науч. и практический семинар, Вологодский юридический и экономический институт ФСИН / Отв. изд. А.А. Бабкин – Вологда, 2017. – 78 с.

28. Использование системы электронного мониторинга подконтрольных лиц (СЭМПЛ–2) в деятельности уголовно–исполнительных инспекций: методические указания / Е.Л. Зарембинская, С.А. Грязнов, О.Н. Ежова; под общ. изд. К.В. Талакина. – Самара: Самарский юридический институт ФСИН России, 2015. – 164 с.

29. Информатика и информационные технологии в профессиональной деятельности: учебник / А. В. Душкин [и др.]; изд. В.П. Корячко, М. Купцов. – Рязань: Академия ФСИН России, 2016. – 321 с.

30. Организационно–правовые и технические основы деятельности операторов SEMPL: учебное пособие / И.Л. Бедняков, С.А.Грязнов, А.В. Мусалева, К.А. Насреддинова, Д.А. Приходько. – Самара: Самарский юридический институт ФСИН России, 2013. – 165 с.

31. Программно–технический комплекс «Автоматизированное делопроизводство спецконтингента»: пособие администратора. – Тверь: ФБУ НИИиПТ ФСИН России, 2014. – 184 с.

32. Специальная техника и информационная безопасность: Учебник / Под ред. В. И. Кирина. – М., Академия управления МВД России, 2000. – 356 с.

33. П. Ю. Кузнецов Информационные технологии в юридической деятельности / П.Ю. Кузнецов. – М.: Юрайт, 2018. – 321 с.

34. Купцов М.И. Информационно–аналитические технологии государственного и муниципального управления: учебник / М.И. Купцов, В.Н. Ручкин, В.В. Фомин. – Рязань: Академия ФСИН России, 2014. – 76 с.

35. Новожилов С.А. Опыт использования электронной системы мониторинга при исполнении уголовных наказаний: научно–аналитический обзор / С.А. Новожилов, А.В. Лапенков. – Псков: Псковский филиал Академии ФСИН России, 2014. – 74 с.

36. Система электронного мониторинга контролируемых лиц ФСИН России. Специальное программное обеспечение для стационарной станции мониторинга: руководство системного программиста. – М.: ФГУП ЦИТОС ФСИН России, 2010. – 54 с.

37. Устинкина А. В. Использование современных информационных технологий для организации режима и надзора в пенитенциарной системе / А. В. Устинкина // Пенитенциарная система Российской Федерации в условиях модернизации: современное состояние и перспективы развития: доклады участников Международная научно–практическая конференция Академии ФСИН России (22–23 ноября 2012 г.). – Рязань, 2013, – Т. 3. – 164 с.

38. Царькова Е.Г. Как измерить эффективность: методы оценки эффективности систем физической защиты охраняемых объектов пенитенциарной системы/ Е. Г. Царькова // Актуальные вопросы информатизации ФСИН на современном этапе развития пенитенциарной системы: сборник материалов круглого стола (24 июня 2019 г.). Тверь, 2019. – 269 с

### **Материалы периодических изданий**

39. Андреев В. В. Правовое регулирование информационной сферы / В. В. Андреев, Н. В. Киркина // Пробелы в российском законодательстве. – 2015. – № 8. – С. 21–25.

40. Кусова Е.А. Нормативно–правовое регулирование общественных отношений в информационной сфере / Е. А. Кусова // Правовое государство: теория и практика. – 2015. – № 6. – (16). – С. 72–75.

41. Лопатин В.Н. Понятие и структура информационной сферы / В. Н. Лопатин // Актуальные проблемы права: теория и практика. – 2017. – №26. – С. 63–67.

42. Майоров А.М. Инженерно–технические средства охраны в УИС, учебное пособие / А. М. Майоров // Специальная техника. – 2005. – С. 30–36.

43. Чураков Д.Ю. Создание базы данных технических средств обнаружения, используемых в учреждениях и органах УИС / Д. Ю. Чураков// Информационные технологии в УИС. – 2019. – № 1. – С. 30–42.

44. Щербаков Г. Н. Инженерно–технические средства охраны и надзора / Г. Н. Щербаков // Специальная техника. – 2000. – № 2. – С. 19–24.

### **Материалы юридической практики**

45. Аналитическая записка о состоянии использования электронных средств надзора и контроля в деятельности Зеленодольского филиала ФКУ УИИ УФСИН России по Республике Татарстан от 30. 12. 2020 г // Материалы преддипломной практики в ФКУ ИК–19 УФСИН России по Республике Татарстан / В. В. Ласточкин (неопубликованный акт).

## Электронные ресурсы

46. Рачков В. Е. Информационные технологии в управлении: Лекция 14 [Электронный ресурс]/ В. Е. Рачков // Фондовые лекции СтГАУ, 2014. – Режим доступа: <http://www.stgau.ru/company/personal/user> (дата обращения 23.04.2021).