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: **Использование систем идентификации личности на режимных объектах уголовно-исполнительной системы для обеспечения безопасности**

Выполнил:
курсант 3 взвода 4 курса,
рядовой внутренней службы
Костин Артём Михайлович

Научный руководитель:
начальник кафедры управления и информационно-технического обеспечения деятельности УИС, кандидат физико-математических наук, доцент
полковник внутренней службы
Озерский Сергей Владимирович

Рецензент:
начальник ФКУ СИЗО-2 ГУФСИН России по Челябинской области
подполковник внутренней службы
Арзамасцев Павел Сергеевич

Решение начальника кафедры о допуске к защите допущена

Дата защиты: 23.06.2021 Оценка 5 (отлично)

Самара
2021

Оглавление

Введение

Актуальность темы. Обусловлена тем, что интерес к системам идентификации личности на режимных объектах уголовно-исполнительной системы в последние годы расширился благодаря тому, что эти системы нашли свое применение в разработках новых и перспективных технологий безопасности, сущность которых сводится к использованию электронных и информационных систем распознавания личности по уникальным в своем роде свойствам биометрических параметров человека, такие как черты лица, папиллярные узоры на пальцах рук или сетчатка глаза. Сами технологии идентификации личности на объектах уголовно–исполнительной системы (далее – УИС) находятся на стадии внедрения, которое происходит с учетом развития отечественных программных средств, а также действующего законодательства, которое определяет круг биометрических характеристик, которые нужно будет относить как к обязательной регистрации для непосредственной безопасности, а также для недопущения преступлений и правонарушений осужденными, подозреваемыми и обвиняемыми, и иными лицами на территориях учреждений и объектов УИС. Поэтому система контроля и управления доступа (далее – СКУД) является лучшим решением в обеспечении безопасности и контрольно–пропускного режима в учреждениях уголовно – исполнительной системы. На данный момент СКУД считается самым инновационным решением проблем учёта, наблюдения и охраны учреждений и объектов УИС. СКУД представляет собой систему сложных подконтрольных функций, в которую входит обеспечение в учреждении линии связи, системы видеонаблюдения и возможность ограничения прохода на определенные участки учреждения.

Главной задачей СКУД является исключение подмены подозреваемых, обвиняемых и осужденных при проходе через контрольно-пропускной пункт (далее – КПП) объекта Федеральной службы исполнения наказаний (далее –

ФСИН), тем самым, совершить побег при использовании таких систем считается практический невозможным. Кроме того, эти системы так же могут защитить лиц, находящихся на территории, от несанкционированного проникновения лица, целью которого может быть дезорганизация деятельности учреждений и объектов УИС путем противоправных или даже преступных действий, что в свою очередь может повлечь к более серьезным последствиям. Именно это как раз и дает стимул к модернизации и установки таких систем во все учреждения и объекты ФСИН России.

На современном этапе развития, цифровая биометрия является одним из точных и быстрых способов идентифицировать лицо с помощью сопоставления полученных данных с уже хранящейся информацией в системе. В 95% случаев биометрия по своей сути – это математическая статистика, которая в свою очередь является точной наукой, алгоритмы которой используются везде, включая УИС. Обилие биометрических методов поражает. Поэтому на объектах УИС все чаще можно заметить систему контроля и управления доступом, работающую именно на основе биометрических данных зарегистрированного в системе лица.

Объектом исследования являются общественные отношения, связанные с особенностями и проблематикой применения систем идентификации личности на режимных объектах уголовно-исполнительной системы для обеспечения безопасности.

Предметом исследования являются нормативно-правовые акты, регулирующие организационно-правовые и практические аспекты применения систем идентификации личности на режимных объектах уголовно-исполнительной системы.

Цель исследования заключается в анализе организационно-правовых аспектов применения систем идентификации личности на режимных объектах уголовно-исполнительной системы, обосновании теоретических положений и практических рекомендаций по их совершенствованию.

Для достижения указанной цели исследования необходимо решить следующие **задачи:**

1) рассмотреть средства обеспечения безопасности в исправительных учреждениях и следственных изоляторах;

2) охарактеризовать состояние правового регулирования применения систем идентификации личности на режимных объектах УИС;

3) представить обзор современных систем идентификации личности;

4) проанализировать практику применения современных систем идентификации личности на режимных объектах УИС для обеспечения безопасности;

5) выделить проблемы и перспективы применения систем идентификации личности на режимных объектах УИС.

Методы исследования выбраны, исходя из поставленных в работе целей и задач исследования, с учетом объекта и предмета исследования. Методологическую основу исследования составили диалектический, формально-логический, системно-структурный методы, метод сравнительного анализа и др.

Теоретическая база исследования и степень научной разработанности темы.

Проблематике применения систем идентификации личности для контроля управления доступом на режимные объекты УИС уделялось значительное внимание в работах А. В. Василькова, И. А Василькова, В. А. Ворона, А. Гинце, Д. П. Зегжды, А. К Крахмалева, А. Мальцева, И. В. Мальцева, В. Моржакова, Н. В. Татарченко, С. В. Тимошенко, О. Р. Юсупова и др.

Структура работы определена целью и задачами исследования. Работа состоит из введения, двух глав, включающих четыре параграфа, заключения, библиографического списка и приложения.

ГЛАВА 1. ПРАВОВЫЕ АСПЕКТЫ ПРИМЕНЕНИЯ СИСТЕМ ИДЕНТИФИКАЦИИ ЛИЧНОСТИ, КАК СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

1.1. Средства обеспечения безопасности в ИУ и СИЗО: правовые основы

В современных обстоятельствах правовое обеспечение развития и функционирования отечественной УИС и поддержания ее безопасности включает в себя международно-правовую составляющую, которая в свою очередь представлена комплексом созданных и действующих в пенитенциарной сфере, а также юридически обязательных и рекомендательных международных правовых положений, как универсального, так и регионального уровня. Они в свою очередь ориентируют национального законодателя и правоприменителя на гуманизацию уголовно-исполнительной сферы, и сочетании с повышением ее эффективности в демократическом обществе. При этом конкретная часть отмеченных положений, а именно общепринятые принципы и нормы международного права, которых в рассматриваемой сфере нет необходимой внятности, а также международные договоры Российской Федерации (далее – РФ) в параметрах положения ч. 4 ст. 15 Конституции РФ и положения ч. 1 ст. 3 Уголовно-исполнительного кодекса РФ (далее – УИК РФ) должны рассматриваться (наряду с Конституцией РФ) в черте правовых основ законодательства России, а также и в сфере безопасности УИС и деятельности ее институциональных компонентов. При этом является несомненным, что при анализе вопросов правового регулирования безопасности УИС, оценке нынешнего состояния ее правового обеспечения нужно принимать во внимание, как выводные от правового статуса лиц, правового режима охраняемых (подлежащих защите) их интересов отличия отмеченных аспектов, так и их взаимосвязь, принимая

во внимание характер угроз, общую конечную нацеленность вышеназванного процесса.

Правовое предоставление безопасности осужденных базируется на положениях Конституции РФ, в которой фиксируются основные права человека (ст. 2 гл. 2 Конституции РФ). Необходимо выделить, что на этом верховном конституционно-правовом уровне выявляется органичная взаимосвязь правовых основ обеспечения безопасности с одной стороны – осужденных, подозреваемых и обвиняемых, с другой стороны – лиц работающих или служащих в исправительных учреждениях (далее – ИУ), а также членов семей сотрудников и всех лиц, пребывающих на территории объектов УИС, поскольку ряд из отмеченных конституционных положений имеет универсальный характер (например, положения ч. 1 ст. 20, ст. 21, ст. 42, ст. 46 Конституции РФ) [1].

Кроме этого, согласно ст. 13 Закона РФ № 5473-1 «Об учреждениях и органах, исполняющих уголовные наказания в виде лишения свободы» к числу обязанностей, которые обеспечивают безопасность в ИУ, отнесены следующие:

– обеспечение исполнения уголовно-исполнительного законодательства РФ;

– формирование условий для обеспечения правопорядка и законности, безопасности осужденных, а также персонала, должностных лиц и граждан, прибывающих на территориях и объектах УИС[2].

Непосредственно здесь выявляется указанная ранее связь различных нюансов безопасности УИС.

---

[1] Конституция Российской Федерации: текст с изменениями и дополнениями на 14 марта 2020 г. № 1-ФКЗ: [принята всенародным голосованием 12 декабря 1993 г.] // Официальный интернет-портал правовой информации (www.pravo.gov.ru) 4 июля 2020 г.

[2] Об учреждениях и органах, исполняющих уголовные наказания в виде лишения свободы: закон РФ текст с изменениями и дополнениями на 5 апреля 2021 г. № 78-ФЗ [принят 21 июля 1993 г. № 5473-1] // Официальный интернет-портал правовой информации (www.pravo.gov.ru) 5 апреля 2021 г.

Эта взаимосвязь также выражается в том, что ИУ проводит постоянную ежедневную профилактическую работу, не позволяя осужденным совершать новые преступления и другие правонарушения, направленные как на безопасность других осужденных, так и на безопасность персонала и членов семей сотрудников этих учреждений. В то же время, профилактика, организованная в соответствии с ведомственным нормативным правовым актом (далее – НПА), представляет собой единый институт, который включает комплекс мероприятий самой различной направленности. Поэтому в профилактической работе участвуют отделы безопасности и режима, оперативные отделы, службы охраны, отделы воспитательной работы, медицинские части, психологические и производственно-технические службы, а также другие службы в соответствии с функциональными обязанностями.

И, как уже упоминалось выше, одним из ключевых критериев нормального функционирования УИС является её безопасность, что в наиболее обобщенном виде можно понимать, как особый уровень защиты общественных отношений, складывающихся при исполнении уголовных наказаний, от связанных с этим опасностей, гарантируя последующее постепенное формирование этих самых общественных отношений.

При данном подходе безопасность УИС можно рассматривать в двух аспектах. Во-первых, как постоянное явление, полученное в результате мер различного характера, обеспечивающих защиту, целостность многих объектов, в том числе личности сотрудников и служащих учреждений, осуществляющих наказания осужденных, других граждан, находящихся на территории учреждений, а также безопасность структурной целостности подразделений, их способность осуществлять свою полноценную деятельность и т.д.

Во-вторых, в качестве явления, имеющего динамические свойства, отражающиеся в понятии «обеспечение безопасности УИС». Если в первом случае безопасность является целью, то при обеспечении безопасности

предполагается конкретный перечень средств получения такой цели. А. Г. Перегудов подмечал, что к обеспечению этого явления касается осуществление организационно-управленческой и оперативно-тактической деятельности по осуществлении, установленного нормами права, порядка в ИУ, а также условий и событий, нацеленных на предотвращение вероятной и устранение очевидной опасности, угрожающей спокойствию, жизни и здоровью сотрудников ИУ, осужденных, иных граждан, причастных к деятельности ИУ в целом и его подразделений в частности[3].

В данный период, исходя из закона, в деятельности УИС можно отметить последующие главные средства обеспечения безопасности:

– режим как установленный порядок исполнения и отбывания наказания;

– охрана;

– надзор за осужденными, подозреваемыми и обвиняемыми;

– фортификация;

– применение физической силы, специальных средств, оружия и связи;

– раздельное содержание разных категорий осужденных;

– оперативно-розыскная деятельность;

– воспитательная работа, проводимая с осужденными, и меры дисциплинарного воздействия, оказываемые на них;

– иные специально-предупредительные средства противоправных действий, совершаемых осужденными и иными лицами;

– трудовая занятость осужденных;

– жизнеобеспечение персонала, осужденных, подозреваемых и обвиняемых, а так же иных лиц;

– охрана здоровья осужденных подозреваемых и обвиняемых, и оказание им медицинской помощи;

---

[3] Перегудов А. Г. Проблемы правовой защищенности осужденных к лишению свободы в реформировании и гуманизации исправительной системы // Материалы научно–теоретической конференции. – Уфа: УВШ МВД РФ. – 1993. – № 1. – С 129.

– общее образование и профессиональное образование (обучение) осужденных;

– контрольно-надзорные средства за обеспечением безопасности;

– социально-правовая и профессиональная защищенность персонала[4].

Сам по себе, режим является определяющим средством обеспечения безопасности в учреждениях УИС, как для персонала, так и для спецконтингента и иных лиц[5]. В настоящий момент на законодательном уровне понятие «режим» применительно к тому или иному виду ИУ, где находит свое отражение в уголовно-исполнительном законодательстве РФ.

Так, ч. 1 ст. 82 УИК РФ говорит следующее: режим в ИУ – установленный законом и соответствующими закону НПА порядок исполнения и отбывания лишения свободы, обеспечивающий охрану и изоляцию осужденных, постоянный надзор за ними, исполнение возложенных на них обязанностей, реализацию их прав и законных интересов, личную безопасность осужденных и персонала, раздельное содержание разных категорий осужденных, различные условия содержания в зависимости от вида ИУ, назначенного судом, изменение условий отбывания наказания[6].

Режим является той самой средой, в которой работают все ИУ. В этой среде есть особые правила и методы. Это касается абсолютно всех лиц, постоянно и временно находящихся на территории исправительного учреждения. Соблюдение этими людьми определенных правил гарантирует безопасность ИУ и их объектов. Помимо персонала учреждения и осужденных, требования режима в качестве меры безопасности

---

[4] Зегжда Д. П. Основы безопасности информационных систем. – М: Горячая Линия – Телеком, 2000. – С. 123.

[5] Якунин Д. В., Павлов И. Н. Обеспечение надлежащего надзора за осужденными, как фактор, влияющий на укрепление режима в исправительных колониях: метод. рек. – Уссурийск, 2007. – С. 99.

[6] Уголовно-исполнительный кодекс Российской Федерации: федеральный закон: текст с изменениями и дополнениями на 5 апреля 2021 г. № 78-ФЗ [принят 08 января 1997 г. № 1-ФЗ] // Официальный интернет-портал правовой информации (www.pravo.gov.ru) 5 апреля 2021 г.

распространяются на и территории, которые прилегают к исправительным учреждениям. В соответствии с правовыми нормами, в рамках обеспечения безопасности от внешних угроз, предполагается, что правовые нормы, регулирующие защиту от различных нападений на учреждения и объекты, а также последствия деятельности организованных преступных группировок, целью которых является дезорганизация деятельности, предусмотрены уголовные санкции.

В этом случае безопасность уголовно – исполнительной системы достигается за счет реализации целого блока правовых норм из разных отраслей права. При этом нормы гражданского права регулируют порядок возмещения вреда; административное законодательство регламентирует деятельность администрации учреждений и органов, исполняющих наказания, в чрезвычайных условиях, вызванных стихийными бедствиями и противоправными действиями второстепенных лиц; уголовное право принимает во внимание решение вопросов об обеспечении безопасности путем определения уголовной ответственности за совершение тех или иных преступлений против личности работников УИС и осужденных, а также за отдельные действия, дезорганизующие деятельность учреждений и органов УИС.

При решении вопросов, связанных с обеспечением внешней безопасности УИС, следует иметь в виду, что УИС – это особый государственный механизм, который отражает все процессы, происходящие в обществе в целом[7].

Внутренняя безопасность УИС заключается в обеспечении защиты от угроз, которые возникают непосредственно в учреждениях исполняющих уголовные наказание. Регулирование процесса обеспечения внутренней безопасности осуществляется в основном нормами уголовного и уголовно – исполнительного права. Сам процесс направлен на предотвращения

---

[7] Анисимков В. М. Организация управления в уголовно-исполнительной системе: учебник. – Рязань: Академия права и управления Минюста России, 2002. – С. 536.

и устранения появления возможных угроз такие как массовые беспорядки, захват заложников и т.д. Помимо этого регулируется и вопрос нарушения законности со стороны сотрудников и персонала ИУ, а также пресечение противоправной деятельность «воров в законе» и прочих лидеров отрицательных группировок осужденных.

К объектам безопасности в рамках данного правового института относятся:

– сотрудники УИС, имеющие специальные звания рядового и начальствующего состава (далее – сотрудники УИС);

– рабочие и служащие учреждений, исполняющих уголовные наказания, органов управления УИС, а также следственных изоляторов (далее – СИЗО), научно-исследовательских, проектных, лечебных, учебных и иных учреждений, входящих в УИС;

– лица, осуществляющие должностные или общественные полномочия в учреждениях и органах УИС: представители органов власти, общественных и религиозных организаций;

– подозреваемые и обвиняемые в совершении преступлений, находящиеся в СИЗО;

– осужденные, отбывающие уголовные наказания;

– учреждения, исполняющие уголовные наказания, иные учреждения и органы УИС;

– предприятия, производства и имущество учреждений, исполняющих наказания, других учреждений и органов УИС[8].

Учреждения и органы, исполняющие наказания, перечислены в ст. 16 УИК РФ. Однако когда речь идет об обеспечении безопасности функционирования названных учреждений и органов силами их администрации, то в первую очередь имеется в виду безопасность ИУ (исправительных колоний (далее – ИК), воспитательных колоний (далее –

[8] Упоров А. Г. Основы безопасности государства и личности: учебное пособие. – Новокузнецк: ФГОУ ВПО Кузбасский институт ФСИН России, 2009. – С. 26.

ВК), тюрем, лечебно-исправительных учреждений), затем – СИЗО, исправительных центров, уголовно-исполнительных инспекций и арестных домов. При этом подразумевается, что при обеспечении безопасности названных учреждений и органов достигаются их устойчивое функционирование и нормальная (на уровне, установленном законодательством) жизнедеятельность в целом. Так же помимо объектов, существуют и субъекты обеспечения безопасности. К субъектам обеспечения безопасности в УИС можно отнести:

– государство, которое через органы законодательной, исполнительной и судебной власти обеспечивает безопасность УИС в целом;

– служба охраны учреждений, исполняющих наказания, которая, обеспечивая изоляцию осужденных, также обеспечивает безопасность этих учреждений, в особенности от воздействия внешних угроз (от нападений на учреждения, диверсий и т.д.);

– служба безопасности учреждений, исполняющих наказания, которая обеспечивает установленный нормами права режим в учреждениях, предупреждение и пресечение противоправных действий, осужденных и, тем самым, решает вопросы обеспечения безопасности данных учреждений;

– оперативные аппараты учреждений и органов УИС, а также органов внутренних дел, для которых обеспечение безопасности граждан является одной из задач, подлежащих решению;

– сотрудники учреждений, исполняющих наказания, при осуществлении надзора и контроля за осужденными;

– общественные и религиозные организации, граждане, принимающие участие в процессе исправления осужденных;

– отряды специального назначения территориальных органов управления УИС, а также МВД и ФСБ России;

– иные правоохранительные органы, в частности прокуратура и суд, а также подразделения МЧС России, службы санэпиднадзора и др.[9]

Так же следует отметить, что содержания права, осужденного на его безопасность и особенности его реализации при наличии весомых угроз со стороны других осужденных и иных лиц, раскрываются в соответствующей главе Правил внутреннего распорядка (далее – ПВР) ИУ[10]. Кроме того, отдельно можно выделить меры, которые предпринимает администрация учреждения для обеспечения непосредственной безопасности спецконтингента:

– перевод осужденного и заключенного в безопасное место;

– медицинские меры, направленные на охрану здоровья и жизни осужденных;

– правила поведения осужденных в ИУ;

– меры, предусмотренные Законом РФ «Об оперативно - розыскной деятельности» и ведомственных нормативных актах. Это меры обеспечения безопасности лиц, сотрудничающих с оперативными аппаратами ИУ на конфиденциальной основе, оперативно-розыскные мероприятия, проводимые с целью профилактики конфликтов и преступлений, обеспечения безопасности конкретных осужденных и заключенных[11],

– меры профилактики, направленные на выявление и устранение условий, способствующих совершению преступлений;

– меры пресечения, являющиеся средством прекращения, устранения различного рода правонарушений и эксцессов, несущих опасность. Эти меры имеют охранительную направленность и применяются исключительно в

---

[9] Громов М. А. Организация безопасности в исправительных учреждениях: учебное пособие. – Рязань: Академия ФСИН России, 2005. – С. 114.

[10] Об утверждении Правил внутреннего распорядка исправительных учреждений приказ Минюста России: текст с изменениями и дополнениями на 29 января 2021 г. № 6 [принят 16 декабря 2016 г. № 295] // Официальный интернет-портал правовой информации (www.pravo.gov.ru) 9 февраля 2021 г.

[11] Об оперативно-розыскной деятельности: федеральный закон: текст с изменениями и дополнениями на 30 декабря 2020 г. № 515-ФЗ [принят 12 августа 1995 г. № 144-ФЗ] // Официальный интернет-портал правовой информации (www.pravo.gov.ru) 30 декабря 2020 г.

связи с правонарушениями и только до момента устранения угрожающей опасности;

– меры, применяемые в особых условиях деятельности ИУ и СИЗО: при возникновении стихийных бедствий и иных чрезвычайных происшествий.

Меры безопасности уголовно-исполнительного характера можно подразделить на меры общего характера и специальные меры.

Общие меры обеспечения безопасности являются составным элементом трех специфических видов деятельности администрации ИУ и СИЗО: обеспечение режима, охраны и надзора.

Специальные меры безопасности – это меры, принятые для обеспечения безопасности определённых защищаемых субъектов. В случае возникновения опасности для осужденного или заключенного, начальник исправительного учреждения или следственного изолятора, по заявлению самого лица, которому угрожает опасность, может принять решение о его переводе

в безопасное место (помещение). Специально для этих случаев такие помещения во многих учреждениях не оборудованы. Соответственно осужденные содержатся в камерах штрафного изолятора (далее – ШИЗО) (помещений камерного типа (далее – ПКТ)), куда они переводятся по постановлению начальника учреждения на срок не свыше 30 суток. При этом безопасность осужденного на какое-то время обеспечивается, но вместе с тем ухудшаются условия его содержания. Существующее оборудование учреждений и условия содержания осужденных и заключенных таковы, что перевод осужденного в безопасное место (в камеру) обязательно предполагает его изоляцию, объективно связанную с определенными правовыми ограничениями. Отсюда следует, что меры безопасности, наряду с защитой, приносят охраняемому лицу и какие-то ограничения в правах, создают определенные неудобства. Это общая черта мер безопасности, независимо от того в какой сфере и в отношении кого они применяются.

Так же в основе безопасности стоит охрана объектов УИС как совокупность правовой, организационной, охранной, так и режимной, технической и иной деятельности. Кроме того, функции и задачи по управлению силами и средствами охраны предназначены для защиты объектов УИС, от нападения, преступных посягательств и несанкционированного проникновения на территорию[12]. Непосредственную охрану учреждений УИС и объектов осуществляет личный состав караула.

Караулом является вооруженная группа сотрудников отдела охраны, которая назначается для охраны объектов УИС, их защиты от преступных действий, а также для организации пропускного режима на территорию учреждений и органов УИС. Это связанно и с тем, что размещение на прилегающей к ИК режимной территории торговых точек, разведение огня, приведение в действие салютов, фейерверков и т. д. может привести к нарушению режима в ИК, а значит, поставит (может поставить) под угрозу безопасность учреждения в целом или его часть.

Следует также отметить, что содержание права, осужденного на безопасность и особенности его реализации при наличии угроз осужденного со стороны других осужденных и иных лиц раскрываются в соответствующем разделе ПВР ИУ.

1.2 Правовые аспекты применения систем идентификации личности

С 1992 г. осуществляется процесс реформирования УИС, и его приоритетным направлением является приведение законодательства в соответствие с Конституцией РФ и международными правовыми актами.

---

[12] Ковалев О. Г. Организация действий учреждений УИС Министерства юстиции РФ в особых условиях. – Москва, 2004. – С. 31.

Принятые законы и указы Президента РФ, постановления Правительства РФ, приказы ФСИН и Министерства юстиции РФ обеспечивают поддержку и развитие системы исполнения уголовных наказаний. Конституция РФ провозглашает право каждого на свободу и личную неприкосновенность, право на неприкосновенность частной жизни. Наряду с этим, в ч. 3 ст. 55 Конституции указано, что права и свободы человека и гражданина могут быть ограничены федеральным законом в той мере, в какой это необходимо в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности других лиц. В ч. 2 ст. 10 УИК РФ, предусмотрено, что при исполнении наказаний осужденным гарантируются права и свободы граждан РФ с изъятиями и ограничениями, установленными уголовным, уголовно-исполнительным и иным законодательством. В отношении лиц, заключенных под стражу, данные ограничения предусмотрены Федеральным законом № 103-ФЗ «О содержании под стражей подозреваемых и обвиняемых в совершении преступлений», где в ст. 6 указанно, что подозреваемые и обвиняемые пользуются правами и свободами и несут обязанности, установленные для граждан РФ, с ограничениями, предусмотренными федеральными законами[13].

Данный НПА дал возможность в целях осуществления надзора использовать в отношении подозреваемых обвиняемых аудио- и видеотехнику (ст. 34). Впервые в федеральном законе применение технических средств надзора и контроля в учреждениях УИС в отношении осужденных было урегулировано в 1997 г. УИК РФ (ст. 83). Правовое закрепление данных норм позволило администрации ИУ и СИЗО при осуществлении своей деятельности на законных основаниях применять различные технические средства в целях профилактики и пресечения побегов

[13] О содержании под стражей подозреваемых и обвиняемых в совершении преступлений: федеральный закон: текст с изменениями и дополнениями на 5 апреля 2021 г. № 78-ФЗ [принят 15 июля 1995 г. № 103-ФЗ] // Официальный интернет-портал правовой информации (www.pravo.gov.ru) 5 апреля 2021 г.

и других преступлений, нарушений установленного порядка содержания и отбывания наказания, а также в целях получения необходимой информации о поведении осужденных.

Одной из приоритетных задач, стоящих перед учреждениями УИС, является обеспечение надежной охраны и изоляции осужденных и лиц, содержащихся под стражей, с соблюдение требований законности. В связи с этим вопросы повышения эффективности осуществления надзора и контроля за осужденными и заключенными в учреждениях ФСИН всегда актуальны.

В настоящее время не представляется возможным обеспечение нормального функционирования учреждений ФСИН России при помощи одного «человеческого фактора». Успешное выполнение задач по содержанию осужденных и лиц, содержащихся под стражей, возможно только в сочетании рационального использования человеческого ресурса совместно

с применением современных аудиовизуальных, электронных и иных технических средств надзора и контроля.

Кроме того, применение данных средств позволяет создать условия, обеспечивающие правопорядок и законность, безопасность осужденных, персонала, а также должностных лиц и граждан, находящихся на территории учреждений ФСИН России, что в соответствии с п. 2 ст. 12 Закона «Об учреждениях и органах, исполняющих уголовные наказания в виде лишения свободы» является их обязанностью. Применение технических средств надзора и контроля позволяет учреждениям, исполняющим наказания, осуществлять контроль за соблюдением режимных требований на объектах учреждений и территориях, прилегающих к ним, требовать от осужденных и иных лиц исполнения ими обязанностей, ПВР (п. 1 и 3 Закона «Об учреждениях и органах, исполняющих наказания в виде лишения свободы»).

Как уже упоминалось выше, непосредственная правовая регламентация применения в отношении осужденных и заключенных технических средств

надзора и контроля закреплена в ст. 83 УИК РФ и Федеральном законе «О содержании под стражей подозреваемых и обвиняемых в совершении преступлений». В ч. 2 ст. 83 УИК РФ указано, что осужденные под расписку уведомляются о применении на территории ИУ технических средств надзора и контроля. В ПВР ИУ и ВК предусмотрено, что во время содержания в карантинном отделении с осужденными проводятся занятия по специальной программе, которая предусматривает ознакомление с порядком и условиями отбывания наказания, мерами ответственности за их нарушения, правами и обязанностями осужденных, порядком обращения с предложениями, ходатайствами, заявлениями и жалобами, в том числе они информируются о применении в ИУ и ВК аудиовизуальных, электронных и иных технических средств надзора и контроля.

Таким образом, осуществление в учреждения ФСИН России надзора и контроля за осужденными, заключенными и иными лицами при помощи технических средств является законным, поскольку такое право данным учреждения предоставлено федеральным законодательством. Оснащение объектов УИС техническими средствами надзора и контроля в целях повышения уровня их функционирования осуществляется ФСИН. Была разработана Концепция развития охраны учреждений УИС на период до 2020 года, в соответствии с которой планировалось оснащение объектов ФСИН России новыми техническими средствами надзора и контроля[14]. Также во ФСИН России разработано Руководство по технической эксплуатации технических средств, применяемых для оборудования объектов УИС. В руководстве регламентировано содержание эксплуатации технических средств надзора и контроля, их ремонт. Эксплуатация технических средств надзора и контроля предусматривает:

– плановое техническое обслуживание;

---

[14] Об уотверждении Концепции развития уголовно-исполнительной системы Российской Федерации до 2020 года: распоряжение Правительства РФ: текст с изменениями и дополнениями на 23 сентября 2015 г. № 1877-р [принят 14 октября 2010 г. № 1772-р] // Собрание законодательства РФ. – 2010. – № 43. – Ст. 5544 (утратил силу).

– внеплановое техническое обслуживание;

– плановый ремонт (средний, капитальный);

– внеплановый ремонт (текущий, восстановительный).

Успешное выполнение мероприятий по технической эксплуатации и обслуживанию технических средств надзора и контроля достигается прежде всего за счет:

– достаточного количества квалифицированных специалистов;

– наличия твердых знаний и точного выполнения специалистами инженерно-технического обеспечения учреждений и органов ФСИН возложенных на них обязанностей;

– постоянного поддержания технических средств в исправном состоянии, а также четкой организации и качественного выполнения всего комплекса мероприятий по технической эксплуатации данных средств;

– закрепления технических средств надзора и контроля за ответственными лицами;

– знания специалистами устройства, принципа работы и тактики применения технических средств надзора и контроля; – систематического контроля со стороны руководства за состоянием технических средств, качеством их эксплуатации, выявления недостатков и своевременного их устранения;

– анализа, обобщения и внедрения передового опыта технического обслуживания и тактики применения технических средств[15].

Для обучения сотрудников работе с техническими средствами надзора и контроля, получения навыков их правильной эксплуатации в учреждениях используются учебные технические средства. Органы ФСИН России обеспечиваются данным оборудованием за счет технических средств,

---

[15] Об утверждении Наставления по оборудованию инженерно-техническими средствами охраны и надзора объектов уголовно-исполнительной системы: приказ Минюста России: текст с изменениями и дополнениями на 17 июня 2013 г. № 94 [принят 04 сентября 2006 г. № 279] // Официальный интернет-портал правовой информации (www.pravo.gov.ru) 17 июня 2013 г.

выпускаемых промышленностью в качестве учебных и технических средств, переведенных установленным порядком из служебных в учебные. Данное оборудование позволяет сотрудникам приобрести навыки работы с техническими средствами надзора и контроля, обучиться приемам технического обслуживания и ремонта, связанного с искусственным вводом неисправностей, обучиться приемам разборки, демонтажа аппаратуры.

Данное руководство определяет порядок ввода в эксплуатацию технических средств надзора и контроля. В этих целях создается приемная комиссия, которая назначается приказом территориального органа ФСИН России. Данная комиссия осуществляет комплексную проверку исполнительной документации, соответствия выполненных монтажных работ утвержденному проекту, проверяет работу установленных технических средств надзора и контроля в течение 10 дней. В этот период осуществляется подготовка специалистов, которым предстоит эксплуатировать данную аппаратуру и оборудование. В конце обучения сдается зачет по знанию должностных обязанностей, правил и мер техники безопасности. В соответствии с приказом № 325 «Об установлении оценки деятельности территориальных органов ФСИН при инспектированиях» осуществляется оценка деятельности учреждений ФСИН, в том числе оценка состояния обеспечения надежности охраны подразделений, подведомственных территориальному органу ФСИН России.

Предметом оценки выступает соблюдение мер безопасности при эксплуатации инженерно-технических средств охраны и надзора (далее – ИТСОН), проведение инструктажей, наличие у сотрудников УИС, эксплуатирующих ИТСОН, соответствующей квалификационной группы по электробезопасности и удостоверения на право эксплуатации данных средств, состояние учета и отчетности по вопросам инженерно-технического обеспечения, состояние технической эксплуатации ИТСОН, работоспособность технических средств, выполнение норм технических осмотров и проверок ИТСОН, наличие и качество необходимой

документации интегрированной системы безопасности (далее – ИСБ), качество монтажных и пусконаладочных работ ИСБ, наличие, степень оснащенности и качество функционирования элементов ИСБ, наличие специалистов для эксплуатации ИСБ[16].

Данная деятельность проводится в целях стимулирования активности работников территориального органа ФСИН России и подведомственных ему подразделений УИС в повышении эффективности своей деятельности, служебно-боевой, мобилизационной готовности и готовности к действиям при чрезвычайных обстоятельствах[17].

Наряду с этим осуществляется допуск специалистов к работе с техническими средствами надзора и контроля: они проходят медицинское обследование, получают удостоверение на право эксплуатации технических средств. Начальники учреждений и органов ФСИН осуществляют планирование эксплуатации технических средств надзора и контроля. На современном этапе развития УИС РФ ведется целенаправленная работа по формированию единой технической политики по оснащению объектов ФСИН комплексами технических средств надзора и контроля. Понятие «техническая политика УИС» означает систему действий государства, направленных на оснащение техническими средствами учреждения и органы УИС, совершенствование техники и способов ее применения для успешного решения стоящих перед ними задач. Имеющиеся проблемы эффективности функционирования учреждений УИС являются главным фактором

---

[16] Об установлении оценки деятельности территориальных органов Федеральной службы исполнения наказаний при инспектированиях: приказ ФСИН России: [принят 14 июня 2012 г. № 325] // Официальный интернет-портал правовой информации (www.pravo.gov.ru) 14 июня 2012 г.

[17] Об утверждении Концепции развития уголовно-исполнительной системы Российской Федерации на период до 2030 г.: распоряжение Правительства РФ: [принят 29 апреля 2021 г. № 1138-р] // Официальный интернет-портал правовой информации (www.pravo.gov.ru) 5 мая 2021 г.

разработки новых подходов к решению вопросов, связанных с повышением уровня работы данных учреждений.[18]

Постепенно ведется замена морально и физически устаревшей аппаратуры, происходит внедрение в учреждения ФСИН ИСБ, активно используются системы видеоконтроля. В настоящее время доказана высокая степень их эффективности в осуществлении надзора за осужденными, заключенными и иными лицами. В соответствии с приказом Минюста России № 94 «О внесении изменений в приказ Министерства юстиции Российской Федерации № 279 «Об утверждении Наставления по оборудованию ИТСОН объектов УИС» урегулировано оборудование объектов УИС ИСБ, в основу которых так же включается и СКУД, который в свою очередь обеспечивает безопасность лиц, находящихся на территории ИУ или СИЗО. В данном приказе было не мало уделено моментам улучшения и усовершенствования уже имеющихся технических средств. Например, в данном приказе говорится о том, что СКУД должен оснащаться не менее тремя функциями, которые обеспечивают проход, как на территорию, так и внутри территории учреждения, а именно для прохода через КПП по пропуску людей (далее – КПП-Л), данная система должна оснащаться переговорным устройством, цветной видеокамерой с обеспечением отождествления личности и датчиком блокировки. Данное оборудование устанавливается так же и на проходных коридорах, в сборном отделении изолятора, локальных участках, караульных помещениях, комнатах хранения оружия, на постах в корпусах СИЗО и тюрем, ШИЗО, ПКТ и ЕПКТ.

Выводы по первой главе.

Таким образом, можно сказать, что представление безопасности базируется на основах положений Конституции РФ, в которой зафиксированы основные права человека. Так же безопасность непосредственно в УИС регламентирует Закон РФ. №5473-1

[18] Сабынин В. Н. Организация пропускного режима первый шаг к обеспечению безопасности и конфиденциальности информации // Информост радиоэлектроники и телекоммуникации. – 2001. – № 3. – С. 32.

«Об учреждениях и органах, исполняющих уголовные наказания в виде лишения свободы». В нем прописаны обязанности, которые обеспечивают безопасность в ИУ. При этом профилактика, организуемая в соответствии с ведомственным НПА, является единым институтом, включающим комплекс мероприятий самой различной ориентированности, поэтому в профилактической работе участвуют отделы безопасности и режима, оперативные отделы, службы охраны, отделы воспитательной работы, медицинские части, психологические и производственно-технические службы, а также другие службы в соответствии с функциональными обязанностями.

И как ранее уже было сказано, что одним из ключевых критериев нормального функционирования уголовной системы является её безопасность, что в наиболее обобщенном виде можно понимать, как особый уровень защиты общественных отношений, складывающихся при исполнении уголовных наказаний, от связанных с этим опасностей, гарантируя последующее постепенное формирование этих самых общественных отношений.

При таком подходе безопасность УИС можно анализировать в двух аспектах. Во-первых, как постоянное явление, полученное в результате мер различного характера, обеспечивающих защиту, целостность многих объектов, в том числе личности сотрудников и служащих учреждений, осуществляющих наказания осужденных, других граждан, находящихся на территории учреждений, а также безопасность структурной целостности подразделений, их способность осуществлять свою полноценную деятельность и т.д.

Во-вторых, в качестве явления, имеющего динамические свойства, отражающиеся в понятии «обеспечение безопасности УИС». Если в первом случае безопасность является целью, то при обеспечении безопасности предполагается конкретный перечень средств получения такой цели.

Помимо этого, УИК РФ так же можно отнести к НПА, обеспечивающие безопасность как спецконтингента, так и сотрудников и иных лиц, присутствующих на территории ИУ. УИК РФ обеспечивает режим,

а выполнение и соблюдение этими лицами определенных правил обеспечивает безопасность ИУ и объектов. Кроме персонала ИУ и осужденных, требования режима как средства безопасности распространяются на прилегающие к ИУ территории.

В этом случае безопасность УИС получается благодаря реализации целого блока правовых норм различных отраслей права. Кроме того, УИК РФ позволило администрации ИУ и СИЗО при осуществлении своей деятельности на законных основаниях применять различные технические средства в целях профилактики и пресечения побегов и других преступлений, нарушений установленного порядка содержания и отбывания наказания, а также в целях получения необходимой информации о поведении осужденных. Благодаря этому, в учреждениях ФСИН России стало возможно появление СКУД, которое помогает обеспечивать режим и безопасность. В свою очередь, данные технические средства регулируется своими НПА, в котором устанавливаются требования к СКУД, порядок их эксплуатации и выполнение технического регламента.

ГЛАВА 2. СОВРЕМЕННЫЕ СИСТЕМЫ ИДЕНТИФИКАЦИИ ЛИЧНОСТИ, ПРИМЕНЯЕМЫЕ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ НА РЕЖИМНЫХ ОБЪЕКТАХ УИС

2.1. Обзор современных систем идентификации личности

Сейчас невозможно представить современный мир без систем, которые могут отождествить личность по определенными, неповторимыми особенностям.

Они давно уже активно участвуют в нашей жизни и без них невозможны современные и довольно обыденные действия. Сканеры отпечатков пальцев, которые в свою очередь уже стали привычным атрибутом смартфона, технологии распознавания лиц и прочие инструменты. Все это постепенно приходит на замену традиционным методам. Бумажные документы, по своей сути, не имеют возможности абсолютно точно подтвердить личность владельца, и, следовательно, они постепенно превращаются в так называемый анахронизм. На данном этапе развития их вытесняют все более и более современные виды пропусков – начиная всеми известными смарт-картами и заканчивая сложнейшими системами биометрической идентификации личности.

Простой электронный пропуск или, проще говоря, смарт-карта – компактный чип, сделанный в виде маленькой пластиковой карты, которая зачастую напоминает визитную карточку или, скажем, брелока. Существует множество видов этих карт, но их принцип работы во всех случаях будет одинаков: карта вставляется в ридер, и совершается так называемая идентификация. Но может случиться, что эта карта может попасть в руки злоумышленников и это может создать определённую опасность, в виде прохода иного лица на режимную территорию. На самом деле многое зависит от типа этой самой смарт-карты. Простейшие её разновидности

смарт-карт (вроде карточек для таксофона) дают минимальную защиту для охраняемого объекта. В более продвинутых моделях смарт-карт могут применяться такие степени защиты, как PIN-код и даже криптографическая защита.

Зачастую смарт-карты и ридеры для них применяют как средство для защиты персонального компьютера от злоумышленников. Таким образом, существуют подключаемые к ПК модули, которые позволяют включить машину или загрузить операционную систему только одобренному системой пользователю – владельцу данной смарт-карты, знающему PIN-код доступа или пароль. И всё же, пройти такую защиту, будет достаточно легко: стоит только извлечь из компьютера жесткий диск – и можно будет воспользоваться информацией, которая находилась на нем по своему желанию, поскольку запрет действует лишь в период включения и загрузки самой операционной системы персонального компьютера.

Еще один тип простых и распространенных электронных пропусков – «цифровая кнопка» (iButton), которая, прикладывается к приемному устройству, и таким образом передает единственный в своем роде идентификационный код вместе с определенным напряжением тока, запрашиваемым с «базы». Выглядит такое устройство как маленькая металлическая таблетка[19].

В качестве дополнительной гарантии iButton может использовать криптографию, но все зависит от конструкции самой «цифровой кнопки». Но такие «кнопки» в основном применяют военные и силовые ведомства, а в обычной жизни широкое популяризацию получили лишь их базовые варианты[20].

Более защищенными, в отличии от смарт-карт и «кнопок», являются так называемые токены (eToken). Данные устройства обычно выглядят

---

[19] Барсуков В. С. Безопасность: технологии, средства, услуга. – М.: Куниц-образ, 2001. – С. 213.

[20] Барсуков В. С. Интегральная защита информации // Системы безопасности. – 2002. – № 5. – С. 47.

как самые обыкновенные небольшие брелоки, использующие для аутентификации разнообразные виды беспроводной (обычно защищенной) связи. Имеется множество видов токенов – от самых простых до очень сложных. Владелец современной модели должен помнить свой личный PIN, после ввода которого сам токен в зашифрованном виде обменивается информацией с базой данных и получает от нее уникальный код, высвечивающийся затем на дисплее самого брелка[21].

Доступ предоставляется только после ввода этого кода (который, кстати, изменяется каждые несколько минут) в принимающее устройство разрешения доступа. Вариант усложнения механизма защиты – имплантация бесконтактного чипа в организм. Понятно, что потерять такой пропуск будет уже невозможно. Такие устройства могут значительно решить определенные проблемы тяжело больных людей: даже если человек потеряет сознание посреди улицы, приехавшие работники медицинской службы смогут считать из имплантированного в тело больного чипа личные данные, информацию об заболеваниях, состоянии здоровья и медицинскую карту, чтобы оказать неотложную помощь, не тратя ценные минуты на выяснение диагноза и поиск близких родственников[22].

Еще одно использование таких электронных имплантатов может значительно облегчить слежение за такой категорией как досрочно освобожденными или, к примеру, за условно осужденными лицами. В этом случае чипы дают правоохранительным структурам возможность определить местонахождение лица и передают сигнал тревоги на пульт управления при попытке «хозяина» пересечь границу разрешенной зоны. Тем самым это может оказаться достойной заменой уже имеющимся браслетам СЭМПЛ.

Биометрические системы имеют ряд преимуществ по сравнению с традиционными методами, так как они, в свою очередь, предусмотрены

---

[21] Злотник Е. TouchMemory – новый электронный идентификатор // Монитор. – 1994. – № 6. – С. 26.

[22] Ярочкин, В. И. Информационная безопасность: учебник для студентов вузов. – 3-е изд. – М.: Академический Проект: Трикста, 2005. – С. 321.

под идентификацию личности без возможности передачи ключа и во многом являются более удобными с точки зрения пользователя.

Биометрическая идентификация – это процесс сравнения и определения сходства между данными человека и его биометрическим «шаблоном» [23]. Именно биометрия способна считать более надежным за счет сравнения набора специфических и уникальных черт, которые присуще человеку

от рождения. Этот метод распознавания принято считать одним из самых надежных, так как в отличие от стандартного логина и пароля биометрическими данными гораздо сложнее несанкционированно воспользоваться. Интересно, что подпись и голос человека можно отнести к тем самым биометрическим параметрам, но как первый параметр, так и второй могут довольно заметно изменяться под воздействием множества факторов: волнения, стресса, недомогания, времени суток, влажности окружающей среды. Человек не может фотографический создать точную копию подписи и каждый раз произносить пароль по ключевому слову точно так же, с такой же интонацией и акцентом, как это требуют системы идентификации. Но отпечатки пальцев каждого человека достаточно уникальны и не зависят от погоды и других посторонних условий.

Существующие сегодня устройства распознавания отпечатков пальцев можно подразделить на два типа. Простые устройства сканируют папиллярный рисунок только оптически, а затем сравнивают полученное изображение с образцов в базе данных. Более сложные системы имеют сверхчувствительный элемент, на который помещается палец, а папиллярный узор распознается по разнице электрических потенциалов на впадинах и неровностях кончика пальца[24].

---

[23] Барсуков В. С. Интегральная защита информации // Системы безопасности. – 2002. – № 5. – С. 47.

[24] Горлицин И. Контроль и управление доступом – просто и надежно. – КТЦ «Охранные системы», 2002. – С. 169.

Но гораздо важнее другое: такая система не позволит злоумышленнику использовать отрубленный палец с желаемым отпечатком пальца пили просто отпечатком пальца, поскольку в этом случае электрические потенциалы будут сильно отличаться от эталонных. Так же сам сканер может не распознать отпечаток пальца лица, который находится в алкогольном опьянении. Одним словом, этот тип идентификации в сочетании с PIN – кодом обеспечивает безопасность на достаточно высоком уровне.

Другой распространенный метод биометрической идентификации – анализ формы руки и линий на её поверхности. До недавнего времени распознавание ладоней выполнялось так же, как и про простом сканировании отпечатков пальцев – сравнение фотографии из базы данных отсканированного изображения.

Однако в последнее время используются всё более новые технологии: устройство сканирует как кисть, так и край кисти, после чего на основе полученных данных создается трехмерная модель. Трехмерные индикаторы рук недешевы, пока они востребованы лишь спецслужбами и крупными корпорациями[25].

Достаточно точный и не самый дорогой вид биометрической идентификации – сканирование глаза. Как и в случае с отпечатками пальцев, есть два очень разных варианта этой идентификации.

Первый сканирует радужную оболочку глаза. Этот метод основан на уникальности рисунка радужной оболочки, который невероятно сложно, если невозможно, подделать. Оптический сканер с высоким разрешением анализирует ваш зрачок и сравнивает изображение с эталонным с учетом внешних факторов: изменения освещения или физиологических свойств зрачка, который может еще и менять цвет в зависимости от настроения человека или времени суток. Эта технология имеет множество преймуществ. С одной стороны, она отличается высокой точностью идентификации.

[25] Гинце А. Новые технологии в СКУД // Системы безопасности. – 2005. – № 6. – С. 35.

С другой стороны, нет необходимости сосредотачиваться на каком – либо объекте во время сканирования. Кроме того, процесс обнаружения может происходить на расстоянии до 90 см, что очень удобно: для полной идентификации, человек должен остановиться посреди коридора на несколько секунд. Тот, кто не знает необходимости такой процедуры, просто проходит мимо и активирует тем самым сигнал тревоги без сканирования[26].

Важно, что проблемы со зрением – например, катаракта – никоим образом не влияет на точность распознавания с помощью этого метода. Вот почему сегодня сканирование радужной оболочки глаза – один из самых надежных способов идентификации человека. Второй вариант – сканирование сетчатки глаза. В этом случае инфракрасный лучи низкой интенсивности проходит через зрачок и попадает в кровеносные сосуды на задней стенке глаза, а сканирующий элемент считывает изображение, которое отразилось от глазного дна. Этот метод распознавания имеет невероятно низкий процент ошибок, поэтому его часто используют специальные службы. Однако эту технологию пока нельзя называть идеальной – сама катаракта может крайне негативно сказаться на результатах идентификации личности помощью этого метода[27].

Сканирование лица – один из наиболее технических сложных процессов идентификации, требующий максимальной адаптируемости системы. Прямое сравнение отсканированного изображения с эталоном неуместно,
так как слегка изменений угол или иное выражение полностью меняют изображение.

Таким образом, процесс распознавания включает в себя первое долгосрочное сканирование лица и создание шаблона лица по так

---

[26] Васильков А. В., Васильков И. А. Безопасность и управление доступом в информационных системах: учебное пособие. – М.: Форум, 2017. – С. 214.

[27] Девянин П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. – 2-е изд., испр. и доп. – М.: Наука, 2017. – С. 233.

называемым «стабильным зонам», которые не меняются с возрастом (например, края рта и верхней челюсти, часть глазницы.). Этот шаблон сохраняется в базе данных. И уже при сканировании ID полученное изображение лица посетителя конвертируется с аналогичным цифровым форматом, а затем распознается по «стабильным зонам» с учетом внешних факторов. Также системы идентификации чрезвычайно дороги, поэтому их могут себе позволить только правоохранительные органы и успешные компании[28].

Системы биометрической идентификации постепенно становятся более точным и менее ресурсоёмкими устройствами. Уже сейчас, руководители аэропортов, вокзалов и крупных предприятий всерьез задумываются об оснащении своих территорий комплексами доступа на основе биометрических систем. По прогнозам аналитиков, ближайшие годы спрос на такие системы идентификации может стать достаточно высоким. Не исключено, что очень скоро даже полиция на улицах потребует от нас не паспорт, а отпечаток указательного пальца. Какие бы методы идентификации не были выбраны, все они имеют как недостатки, так и достоинства. Биометрические признаки, используемые для идентификации должны обладать следующими свойствами:

– Универсальность: каждый человек должен иметь эту характеристику.

– Достоинства: характеристика не должна меняться.

– Измеримость: характеристика должна иметь количественную меру и измеряться достаточно просто.

– Эффективность: идентификационная способность, скорость, гибкость, потребность в ресурсах, обеспечивающих желаемую точность и скорость идентификации, а также факторы, возникающие в процессе идентификации, и внешние факторы, влияющие на точность и скорость идентификации.

---

[28] Ворона В. А., Тихонов В. А. Системы контроля и управления доступом. – М.: Горячая линия – Телеком, 2010. – С. 145.

– Доступность: готовность людей использовать биометрический метод в повседневной жизни.

– Защищенность от подделки: отражает защищенность системы от обмана[29].

Каждый из описанных выше биометрических методов имеет свои преимущества и недостатки. В таблице (*приложение 1*) представлено сравнение этих методов по шести ранее перечисленным свойствам для различных биометрических характеристик.

В дополнение существует несколько частных требований к разработке биометрических методов:

– Цена: аппаратное обеспечение (сенсор) и программное обеспечение требуется каждому пользователю.

– Удобство использования: простота использования средств идентификации (программных и аппаратных);

– Возможность удаления уже имеющегося пользователя.

– Эксплуатационные характеристики: сам прибор должен работать в довольно длительный период.

В зависимости от критерия идентификации методы биометрической идентификации делятся на две группы:

– статические – критерием являются физиологические характеристики человека, уникальные и неизменные на протяжении всей жизни (отпечатки пальцев, сетчатка, ДНК, форма ладони, термограмма лица и т. д.);

– динамические – критерием являются действия, совершаемые человеком, подсознательные движения, которые могут меняться в разные периоды, в том числе осознанно (почерк и написание на клавиатуре, голос, динамика поворота ключа в замке и т. д.)

Биометрические системы могут работать в режиме верификации и в режиме идентификации.

---

[29] Зегжда Д. П. Основы безопасности информационных систем. – М: Горячая Линия – Телеком, 2000. – С. 452.

Верификация – сравнение математической модели только что считанного и обработанного биометрического признака с конкретной математической моделью, хранящейся на карте доступа или соответствующей определенному паролю, или коду[30].

Идентификация – поиск в базе данных математической модели, идентичной только что созданной[31].

Важно учитывать имеющиеся в биометрических системах ошибки первого и второго типа: показатели по этим параметрам обратно пропорциональны друг другу.

Ошибка первого рода (false reject rate – FRR, вероятность ложного отказа) – это процентное соотношение случаев ложного отказа в допуске к общему количеству попыток идентификации. Ошибка второго рода (false acceptance rate – FAR, вероятность ложного допуска) – это вероятность того, что система примет чужого человека за зарегистрированного пользователя.

Если в системе предусмотрена такая возможность, администратор может установить необходимые значения FRR и FAR. Итак, чтобы минимизировать вероятность ошибки при идентификации, рекомендуется устанавливать большое значение FAR, для увеличения скорости идентификации – до низкого. Также, если мы говорим об отпечатках пальцев, статистика VeriFinger SDK, полученная с помощью сканера отпечатков пальцев DP U.are.U, использовалась в качестве источника данных для FAR и FRR.

За последние 5-10 лет алгоритмы распознавания пальцев не сильно изменились, поэтому приведенные цифры достаточно хорошо показывают среднее значение современных алгоритмов. Сам алгоритм VeriFinger в течение нескольких лет выигрывал Международный конкурс по проверке отпечатков пальцев, где соревновались алгоритмы распознавания пальцев.

---

[30] Мальцев И. В. Системы контроля доступом // Системы безопасности. – 1996. – № 1. – С. 43.

[31] Татарченко Н. В., Тимошенко С. В. Биометрическая идентификация в интегрированных системах безопасности // Специальная техника. – 2002. – № 2. – С. 44.

Типичное значение FAR для метода распознавания отпечатков пальцев составляет 0,001%. Из формулы получим, что стабильная работа системы идентификации при FAR=0,001% возможна при численности персонала N≈300[32].

Несмотря на современность метода идентификации личности, он все же имеет достоинства и недостатки. Преимущества метода. Высокая надежность – статистические показатели метода лучше показателей методов идентификации по лицу, голосу, подписи. Низкая стоимость устройств, сканирующих изображение отпечатка пальца. Достаточно простая процедура сканирования отпечатка пальца.

Недостатки: папиллярный рисунок отпечатка пальца очень легко повредить мелкими царапинами и порезами. Люди, которые использовали сканеры на фабриках с несколькими сотнями сотрудников, сообщают о большом количестве ошибок сканирования. Многие сканеры не подходят для сухой кожи и не позволяют людям пожилого возраста пройти идентификацию. При общении на последней выставке MIPS начальник службы безопасности крупного химического предприятия рассказывал, что их попытка ввести сканеры пальцев на предприятии (пробовались сканеры различных систем) провалилась – минимальное воздействие химических реактивов на пальцы сотрудников вызывало сбой систем безопасности сканеров – сканеры объявляли пальцы подделкой. Так же присутствует недостаточная защищённость от подделки изображения отпечатка, отчасти вызванная широким распространением метода. Для некоторых людей с «неподходящими» пальцами (особенности температуры тела, влажности) вероятность отказа в доступе может достигать 100 %. Количество таких людей варьируется от долей процентов для дорогих сканеров до десяти процентов – для недорогих.

---

[32] Абрамова О. Ф. Сравнительный анализ программных продуктов оценки инвестиционных проектов // Волгоград: ВПИ ВГТУ (филиал). – 2017. – № 60-2. – С. 81.

Что касается радужной оболочки, то она является так же уникальной характеристикой человека. Рисунок радужки формируется на восьмом месяце внутриутробного развития, окончательно стабилизируется в возрасте около двух лет и практически не изменяется в течение жизни, кроме как в результате сильных травм или резких патологий. Метод является одним из наиболее точных среди биометрических методов.

Система идентификации личности по радужной оболочке логически делится на две части: устройство захвата изображения, его первичной обработки и передачи вычислителю и вычислитель, производящий сравнение изображения с изображениями в базе данных, передающий команду об отпуске исполнительному устройству[33].

Время первичной обработки изображения в современных системах примерно 300-500мс, скорость сравнения полученного изображения с базой имеет уровень 50000-150000 сравнений в секунду на обычном ПК. Такая скорость сравнения не накладывает ограничений на применения метода в больших организациях при использовании в системах доступа. При использовании же специализированных вычислителей и алгоритмов оптимизации поиска становится даже возможным идентифицировать человека среди жителей целой страны.

Характеристики FAR и FRR для радужной оболочки глаза наилучшие в классе современных биометрических систем (за исключением, возможно, метода распознавания по сетчатке глаза). Здесь стоит отметить немаловажную особенность, отличающую систему распознавания по радужной оболочке от других систем. В случае использования камеры разрешения от 1.3 МП можно захватывать два глаза на одном кадре[34].

Преимущества метода – статистическая надёжность алгоритма. Захват изображения радужной оболочки можно производить на расстоянии

---

[33] Хвощ С. Т. Микропроцессоры и микроЭВМ в системах автоматического управления. Справочник. – М.: Машиностроение, 2018. – С. 143.

[34] Крахмалев А. К. Средства и системы контроля и управления доступом: учебное пособие. – М.: НИЦ «Охрана» ГУВО МВД России, 2003. – С. 156.

от нескольких сантиметров до нескольких метров, при этом физический контакт человека с устройством не происходит. Радужная оболочка защищена от повреждений – а значит, не будет изменяться во времени

Так же в УИС в последнее время широко используется метод по распознаванию лица. Причем, стоит отметить, что их существует достаточно много и все они основаны на том, что черты лица и форма черепа каждого человека индивидуальны. Эта область биометрии многим кажется привлекательной, потому что мы узнаем друг друга в первую очередь по лицу. Данная область делится на два направления: 2-D распознавание и 3-D распознавание.[35]

2-D распознавание лица – один из самых статистически неэффективных методов биометрии. Появился он довольно давно и применялся, в основном, в криминалистике, что и способствовало его развитию. В последствие появились компьютерные интерпретации метода, в результате чего он стал более надёжным, но, безусловно, уступал и с каждым годом все больше уступает другим биометрическим методам идентификации личности. Преимущества метода. При 2-D распознавании, в отличие от большинства биометрических методов, не требуется дорогостоящее оборудование. При соответствующем оборудовании возможность распознавания на значительных расстояниях от камеры.

Недостатки – низкая статистическая достоверность. Предъявляются требования к освещению (например, не удается регистрировать лица входящих с улицы людей в солнечный день). Для многих алгоритмов неприемлемость каких-либо внешних помех, как, например, очки, борода, некоторые элементы прически. Обязательно фронтальное изображение лица, с весьма небольшими отклонениями. Многие алгоритмы не учитывают

---

[35] Мальцев А., Моржаков В. Современные биометрические методы идентификации // Безопасность. Достоверность. Информация. – 2009. – № 2. – С. 44.

возможные изменения мимики лица, то есть выражение должно быть нейтральным[36].

Переходным от 2-D к 3-D методом является метод, реализующий накопления информации о лице. Этот метод имеет лучшие характеристики, чем 2-D метод, но также как и он использует всего одну камеру. При занесении субъекта в базу субъект поворачивает голову, и алгоритм соединяет изображение воедино, создавая 3-D шаблон. А при распознавании используется несколько кадров видеопотока. Данный метод является экспериментальным и доля его практической реализации в системах СКУД очень мала. Наиболее классическим методом является метод проецирования шаблона. Он состоит в том, что на объект (лицо) проецируется сетка. Далее камера делает снимки со скоростью десятки кадров в секунду, и полученные изображения обрабатываются специальной программой. Луч, падающий на искривленную поверхность, изгибается – чем больше кривизна поверхности, тем сильнее изгиб луча. Изначально при этом применялся источник видимого света, подаваемого через «жалюзи». Затем видимый свет был заменен на инфракрасный, который обладает рядом преимуществ. Обычно на первом этапе обработки отбрасываются изображения, на котором лица не видно вообще или присутствуют посторонние предметы, мешающие идентификации. По полученным снимкам восстанавливается 3-D модель лица, на которой выделяются и удаляются ненужные помехи (прическа, борода, усы и очки). Затем производится анализ модели – выделяются антропометрические особенности, которые в итоге и записываются в уникальный код, заносящийся в базу данных[37].

Все выше описанные методы, так или иначе, находят свое применение, как и на объектах УИС, так и непосредственно на территориях своих учреждений. Данные методы зарекомендовали себя по большей части

---

[36] Барсуков В. С. Интегральная защита информации // Системы безопасности. – 2002. – № 5. – С. 47.

[37] Татарченко И. В., Соловьев Д. С. Концепция интеграции унифицированных систем безопасности // Системы безопасности. – 2007. – № 1 (73). – С. 86.

с положительной стороны. Приведенная выше таблица показывает всю картину методов и их критерий.

2.2. Практика применения современных систем идентификации личности на режимных объектах УИС для обеспечения безопасности: эффективность, основные проблемы и перспективы

Глядя на неуклонный рост интереса к СКУД и перспективу широкого их применения в ближайшем будущем, не следует забывать, что СКУД лишь упрощает процесс идентификации, экономит время и повышает эффективность работы служб безопасности и охраны, но, при этом, все равно требует контроля со стороны человека. От уровня вероятных угроз и поставленных перед системой задач, зависит необходимость подбора оптимального соотношения между сотрудниками и техническими ресурсами системы.

СКУД стандартно состоит из четырех видов устройств, отвечающих за идентификацию, контроль доступа и управление, центральное и исполнительное управление. Однако, в зависимости от СКУД, используемой на объекте, они могут быть объединены в одно общее устройство, или же вовсе отсутствовать.[38]

Устройства контроля и управления доступом – электронные устройства, контролирующие работу считывателей и управляющие исполнительными устройствами. Эти устройства называются контроллерами, которые делятся на два типа: однофункциональные и многофункциональные.

Управление основными устройствами, получение и обработка информации от считывателя, хранение кодов доступа пользователей, принятие решений о доступе пользователя на основе полученной

[38] Крахмалев А. К. Средства и системы контроля и управления доступом: учебное пособие. – М.: НИЦ «Охрана» ГУВО МВД России, 2003. – С. 187.

информации, программирование разных режимов работы – вот их основное предназначение на объектах. Чаще всего используется контроллеры, управляющие от 1 до 8 считывателей. Если контроллеры работают на одном объекте, то их возможно подключить к компьютеру, который в свою очередь будет контролировать их работу, или к главному контроллеру. Также к нему возможно подключить принтер, сканер, управляющий компьютер и другую технику.

Многофункциональные контроллеры помогают создавать сложные комплексы, связанные с другими подсистемами, такими как система видеонаблюдения и т.д. Главный контролер связывается с компьютером через стандартный интерфейс RS-232. А для связи между контроллерами используется интерфейс RS-485. Многофункциональные контроллеры весьма примитивны, как правило они выполняют свою работу только в автономном режиме и выполняют функцию обычного кодового замка, в отличие от многофункциональных контроллеров, которые в основном работают в сетевом режиме (централизованное управление и контроль доступа)[39].

Центральные устройства управления предназначены для получения информации о пользователях самой системы, поиска необходимой информации и программирования СКУД. Как правило, это ЭВМ или проще говоря персональные компьютеры (далее – ПК) с нужным для выполнения этих задач программным обеспечением. ПК предназначен для программирования, но вместе с этим, он также может выполнять операции по СКУД. Компьютер, с помощью специального специализированных под эту задачу программ, управляет СКУД, помимо этого создает общую базу данных, собирает информацию с контроллеров и формирует все возможные различные отчеты.

Программа записывает данные для всех операций которые осуществляет компьютер. Это помогает пользователю получить

---

[39] Тарасов. Ю. А. Контрольно-пропускной режим на предприятии. Защита информации // Конфидент. – 2002. – № 1. – С. 55.

необходимую информацию в любое время. Состояние СКУД отображается в виде таблицы с возможностью мониторинга, которая выводится на информационный дисплей. Введенный в ПК план охраняемой территории, дает возможность узнать состояние любого механизма в нужный момент. Благодаря этому в случае возникновения нештатной ситуации, можно будет быстро принять все возможные необходимые меры для их немедленного устранения[40].

Исполнительные устройства они же приводы, получают сигнал от контроллеров и могу как блокировать, так и разблокировать двери и любые другие запорные механизмы, подключенные к контроллерам. Это способствует наилучшей защите объекта от нарушителей. В основе устройств лежит принцип электромеханического и электромагнитного действия.

В механизмах с электромагнитным способом работы нет движимых частей, функционирования этих механизмов основано на силах магнитного притяжения, создаваемых магнитом.

Электромеханические принцип работы подразумевает под собой подвижные части, называемые запорными ригелями, которые в свою очередь подключаются к электроприводу и за счет электродвигателя они обретают возможность двигаться, выполняя функцию запирания и отпирания дверей.

В большинстве случаев мы видим исполнительные механизмы с электромагнитными принципами действия. Не секрет, что они оснащены так называемыми доводчиками, которые позволяют после открытия двери, вернуться в исходное положение, тем самым выполняя основную функцию – ограничение доступа[41].

Однако функция дверного доводчика не ограничивается гарантией закрытия той самой двери, это устройство пассивной безопасности, то есть

---

[40] Абрамов А. М. Системы управления доступом. – М.: Оберег-РБ, 1998. – С. 88.

[41] Мащенов Р. Г. Системы охранной сигнализации: основы теории и принципы построения: учебное пособие. – М.: Горячая линия – Телеком, 2004. – С. 118.

в случае пожара он должен автоматически открывать все двери, тем самым способствую наиболее эффективной эвакуации лиц.

Доводчики так же делятся на классы: электромеханические, пневматические, пружинные и гидравлические. Так же доступны дверные доводчики с тормозной системой подтягивания. Принцип этой системы заключается в том, что створка двери сначала ускоряется, затем немного замедляется, чтобы не было громкого стука, а в самом конце резко подтягивает створку на место, обеспечивая тем самым надежное и почти бесшумной закрытие двери.

В целом, составляющая часть системы биометрической регистрации осужденных очень сильно экономят время сотрудников УИС при проведении таких мероприятий, как общие проверки наличия спецконтингента, что, несомненно, оптимизирует большую часть работы и позволяет рационально выполнять свои служебные обязанности[42]. Одни из первых к этому пришли в ГУФСИН России по Красноярскому краю. Данные системы были введены в эксплуатацию начиная с 2010 года и по сей день. Данная система на сегодняшний день работает достаточно стабильно и стала полностью автоматизированной, но в ходе эксплуатации данной системы не может не обойтись и без недостатков, который не давал гарантированно отслеживать отметку спецконтингента на 100%.

Существующая система «Biosmart» не мог проводить отметку лиц, которые были с деформированными отпечатками пальцев или при отсутствии их на руках, но при всём необходимом, учет такой группы лиц вести просто необходимо. Исходя по субъектам РФ, количество таких осужденных, а также подозреваемых и обвиняемых в среднем составляет от 1% и до 4% от всей общей численности спецконтингента. Но решение данного вопроса нашло отражение в осуществлении проверки осужденного на стационарном терминале, путем отождествления личности по 2-D

[42] Тихонов В. А., Райх В. В. Информационная безопасность: концептуальные, правовые, организационные и технические аспекты: уч. пособие для вузов. – М.: Гелиос АРВ, 2006. – С. 227.

геометрии лица. Лицо осужденного, который не смог пройти проверку при помощи отпечатка пальца, фотографируется и проходит идентификацию личности при помощи ранее вставленному в базу данных его снимка лица. Сам же фотоснимок этого лица, а также все его данные заносятся в базу данных учреждения, которая имеется на компьютере дежурного помощника начальника учреждения.

Помимо системы «Biosmart» существует, и довольно успешно применяется такая система как СПО «Синергет СКДЛ» (далее – «Синергет»). Данная система имеет те же основные принципы работы и те же функции, что и выше названная система, но она благодаря своей новизне и новаторством, она использует уже весьма современные и высокотехнологические составляющие. Исходя из Приказа Минюста России от 17.06.2013 № 94 «О внесении изменений в приказ Министерства юстиции Российской Федерации от 04.09.2006 № 279 «Об утверждении Наставления по оборудованию ИТСОН объектов УИС», все подобные системы должны отвечать достаточно высоким уровнем безопасности, а именно, все системы на объектах и учреждениях УИС должны осуществлять идентификацию лица с помощью не менее трех, так называемых, «рубежей». И данная система «Синергет» использует и обеспечивает исключение несанкционированного выхода спецконтингента путем:

– Проверки сходства 3-D модели лица в момент входа и выхода;

– Автоматической проверки степени сходства изображения 2-D лица спецконтингента с изображения, которая выдает камера видеонаблюдения;

– Идентификации личности осужденного, подозреваемого и обвиняемого, путем использования отпечатка пальца;

– Считывания EMM Card сотрудников и лиц, посещающих объекты и учреждения УИС. Так же на данный момент она отвечает всем требованиям и целям, которая ставит перед собой Распоряжение Правительства РФ от 29 апреля 2021 г. № 1138-р «Об утверждении Концепции развития УИС РФ на период до 2030 г.».

Данный комплекс применяется в учреждении для контроля и управление доступом трех категорий лиц, а именно: посетителей, сотрудников и спецконтингента. «Синергет» распознает личности по биометрическим параметрам и выводит основную информацию о субъекте на монитор. Так же система «Синергет» применяет современные высокоэффективные биометрические алгоритмы, которые исключают попытку несанкционированного выхода спецконтингента с территории учреждения через КПП-Л.

«Синергет» работает в круглосуточном режиме для контроля трех категорий лиц, которые были указаны выше. Главной особенностью комплекса является то, что он контролирует прохождение через КПП-Л при помощи различных технических средств, таких как сканер отпечатков пальцев, считыватель прокси – карт и средств фотографирования лица прибывшего человека. Проверяет все проходящие лица через пост контроля и без участия оператора фиксирует в базе данных дату, время, фотографию лица и его установочные данные, которые были заранее занесены туда. В дальнейшем это помогает определить, кто и в какое время проходил через данный пост. Система так же имеет возможность обработки фотоизображения очень низкого качества, которые не соответствуют требованиям ГОСТа 19794-5-2006. Имеющаяся система предоставляет возможность сравнения изображений, отобранных оператором при помощи поиска вручную. Кроме того, она не нуждается в ярком освещении, чтобы идентифицировать лицо, т.к. использует уникальный алгоритм, в котором отсутствует необходимость «кодирования» изображений и выбора определенных антропометрических точек. Применения высокоэффективных алгоритмов биометрии позволяют исключить побег заключенного путем подмены его на схожего по внешним признакам гражданина.

Организация контроля доступа по результатам проверки осуществляется следующим образом:

– при формировании сообщения «задержать», «совершение подмены идентификационной карты», «совершение подмены специального контингента» контроллер управления замковыми устройствами производит блокировку цепей управления замковыми устройствами дверей отсекающего тамбура проходного коридора КПП-Л;

– разблокировку цепей управления замковыми устройствами дверей отсекающего тамбура проходного коридора КПП осуществляется пользователями комплекса, имеющими на данную операцию права доступа.

Таким образом, работа «Синергет» обеспечивает:

– протоколирование действий пользователя: вход (выход) из системы, открытие (закрытие) экранных форм, создание (изменение, удаление, просмотр) объектов учета данных, выполнение поиска по биометрическим параметрам, сохранение истории о создании и удалении объекта учетных данных;

– возможность восстановления ошибочно удалённой информации и протоколирование операций удаления;

– возможность разграничения доступа пользователей по уровням с ограничением на просмотр (изменение, удаление) различных объектов данных комплекса;

– возможность ограничения доступа ранее зарегистрированных пользователей;

– возможность ограничения диапазона IP-адресов, допустимых для подключения к комплексу.

Периодически проводятся проверки работоспособности комплекса по следующим параметрам:

– сотрудники меняются электронными картами до считывания параметров лица;

– головной убор не снимается;

– активная мимика лица (в некоторых случаях может распознать);

– ограничения считывания параметров пальцев[43].

Как показала практика, процесс ввода в эксплуатацию «Синергет» занимает до двух месяцев. Помимо этого, во время эксплуатации были выявлены определенные недостатки в работе, а именно:

– отсутствие возможности перезакрепления за сотрудниками EMM Card;

– отсутствие возможности корректировки отпечатков пальцев в созданной дактилокарте с АРМ;

– при изменении геометрии лица, (появлении шрамов, глубоких порезов, опухоли) становится невозможным идентифицировать личность.

Кроме того, существенными минусом всех подобных систем является: отсутствие единой базы данных подозреваемых, обвиняемых и осужденных. Именно эта проблема порождает конфликтные ситуации между спецконтингетом и сотрудниками. Во время приема обвиняемых и подозреваемых, они обязаны пройти регистрацию, путем занесения личных установочных данных в базу системы «Синергет». Это требует снятия отпечатков пальцев и ладони, фотографирования и занесения геометрии лица, что приводит к длительному ожиданию в сборном отделении. И такая процедура проходит в каждом учреждении, куда прибывает спецконтингент. Даже для транзитно-пересыльных осужденных, эта процедура является обязательной. Именно из-за длительного ожидания и самого процесса неоднократной перерегистрации могут рождаться конфликтные ситуации, которые в дальнейшем могут перерасти в противоправные действия.

Выводы по второй главе.

Мы выяснили, что существует довольно много систем идентификации личности, которые могут, как обеспечить должный уровень безопасности, так и не обеспечить его вовсе, в силу прогресса современных технологий. Одним из самых надежных и эффективных методов является использование биометрии. Именно потому, что за счет сравнения набора специфических

[43] Абрамов А. М. Системы управления доступом. – М.: Оберег-РБ, 1998. – С. 76.

и уникальных черт, которые присущи человеку от рождения, она является авангардом среди систем безопасности. Интересно, что к биометрическим параметрам можно отнести подпись и голос человека, однако, как первая, так и второй могут весьма заметно изменяться под влиянием многих факторов: волнения, стресса, недомогания, времени суток, влажности воздуха. Еще один распространенный способ биометрической идентификации – анализ формы ладони и линий на ее поверхности. До недавнего времени распознавание ладони производилось так же, как и при простом сканировании отпечатков пальцев – путем сравнения фотографии из базы и снимка, полученного в результате сканирования. Помимо всего прочего существуют сканирование глаза, лица, рисунка вен, сетчатки и папиллярного узора на пальцах рук. Так же в УИС в последнее время широко используется метод по распознаванию лица. Причем, стоит отметить, что их существует достаточно много и все они основаны на том, что черты лица и форма черепа каждого человека индивидуальны. Все выше описанные методы, так или иначе, находят свое применение, как и на объектах УИС, так и непосредственно на территориях своих учреждений. Данные методы зарекомендовали себя по большей части с положительной стороны. Приведенная выше таблица показывает всю картину методов и их критерий.

Так же, мы выяснили, что на объектах и учреждениях УИС используются такие системы как «Biosmart» и СПО «Синергет». Которые отвечают современным требованиям и концепции развития УИС до 2030 года, где говорится, что нужно оснащать данные объекты современными системами. В свою очередь Приказ Минюста России от 17.06.2014г №94 «О внесении изменений в приказ Министерства юстиции Российской Федерации от 04.09.2006 № 279 – «Об утверждении Наставления по оборудованию ИТСОН объектов УИС» вносит определенные критерии, которым должны отвечать эти системы. Также эти системы являются зачастую автономными и интегрируются в ИСБ, что позволяет сотруднику рационально использовать свое время при выполнении служебных

обязанностей и облегчает сам процесс выполнения. Но также мы могли заметить, что данные системы не связаны между собой и не имеют единой базы данных, которая может заметно упростить прием осужденных, подозреваемых и обвиняемых в учреждения УИС и снизить риск появления конфликтных ситуаций между спецконтингентом и сотрудниками администрации.

Заключение

Итак, подводя итоги проведенного исследования, можно сделать следующие выводы.

1. Правовое предоставление безопасности осужденных базируется на положениях Конституции РФ, в которой фиксируются основные права человека, так же за обеспечение безопасности как спецконтингента, так и персонала, и иных лиц отвечают основные положения УИК, где говорится, что режим это такая среда, где существуют определенные правила, как для осужденных, так и для персонала и тех лиц, которые находятся на режимных объектах УИС. К ним так же можно отнести те самые прилегающие территории, на которых, так же действуют требования того или иного объекта или ИУ.

2. Режим – это среда, в которой работают все ИУ. В них есть свои особые правила и свой уклад, которые распространяются на всех лиц находящихся

на территории, как постоянно, так и временно. Выполнение и соблюдение этими лицами определенных правил, как факт, обеспечивает безопасность учреждений и объектов УИС. Помимо прочего, кроме персонала ИУ и осужденных, определенные требования режима как средство безопасности распространяются и на прилегающие к учреждениям территориям.

3. При правовом регулировании под обеспечением безопасности от внешних угроз предполагается осуществление правовых норм, регулирующих вопросы защиты от различного рода стихийных бедствий, эпидемий, диверсий, нападений на учреждения и органы УИС, а также от воздействий организованных преступных групп, обладающих такой целью, как дезорганизацию процесса исполнения уголовных наказаний.

4. Сами меры безопасности уголовно-исполнительного характера можно разделить на так называемые меры общего характера и специального характера.

– Общие меры обеспечения безопасности считаются сложными составляющими трех специфических видов деятельности администрации ИУ и СИЗО: обеспечение режима, охраны и надзора.

– Специальные меры безопасности – это меры, принимаемые в целях предоставления безопасности конкретным защищаемым субъектам, и случае возникновения, какой – либо, опасности для осужденного или заключенного под стражу, начальник ИУ или СИЗО по собственному заявлению от осужденного либо по собственной инициативе принимает решение о его переводе в безопасное место (помещение), которое может быть определено администрацией того самого учреждения.

5. В целях профилактики и пресечения побегов и других преступлений, нарушений установленного порядка содержания и отбывания наказания, а также в целях получения необходимой информации о поведении осужденных, администрацией ИУ было разрешено пользоваться аудио – видео аппаратурой, а правовое закрепление данной нормы было отражено в ст.83 УИК РФ и в ст. 34 Федерального закона от 15.07.1995 № 103-ФЗ «О содержании под стражей подозреваемых и обвиняемых в совершении преступлений».

6. Ведется активное внедрение в ИСБ СКУД, которые в свою очередь регулируются в соответствии с приказом Минюста России от 17.06.2013 № 94 «О внесении изменений в приказ Министерства юстиции Российской Федерации от 04.09.2006 № 279 «Об утверждении Наставления по оборудованию ИТСОН объектов УИС». В данных приказе говорится, что СКУД, находящийся в учреждениях должен обладать не менее тремя видами идентификации личности.

7. В самой работе мы установили, что существует достаточно много систем идентификации личности, которые различны по своим алгоритмам,

степеням защиты от несанкционированного взлома и надежности. Некоторые уже перестали быть актуальными из-за того, что их функционал достаточно устарел, а некоторые наоборот набирают популярность, как и в сложных системах безопасности, так и в простых, обиходных, для человека устройствах.

Например, применение биометрии для защиты личных данных стало частым явлением в простой жизни почти каждого человека. Методы сканирования отпечатка пальца, или лица используются даже в самых простых устройствах как смартфон или же дверной замок.

8. Анализ методов идентификации личности, которые были приведены в Таблице 1, показал, что самым удобным в использовании и распространенным является метод отождествления путем сканирования отпечатка пальца или ладони самого носителя. Так же этот метод имеет более широкое распространение, нежели все другие.

9. Помимо прочего, большинство биометрических систем могут работать в режиме верификации и в режиме идентификации.

Верификация – это своего рода сравнение математической модели, которую только что считали и обработали её биометрический признак с конкретной математической моделью, хранящейся в виде данных на карте доступа или на соответствующему определенному паролю, или коду.

Идентификация – поиск в базе данных математической модели, идентичной только что созданной.

Так же в УИС в последнее время широко используется метод по распознаванию лица. Причем, стоит отметить, что их существует достаточно много и все они основаны на том, что черты лица и форма черепа каждого человека индивидуальны.

К основным элементам безопасности относится СКУД, но стоит помнить, что она лишь упрощает процесс идентификации, экономит время и повышает эффективность работы служб безопасности и охраны, но, при этом, все равно требует контроля со стороны персонала учреждения.

От уровня вероятных угроз и поставленных перед системой задач, зависит необходимость подбора оптимального соотношения между сотрудниками и техническими ресурсами системы.

10 В УИС основными СКУД являются непосредственно «Biosmart» и СПО «Синергет». Данные системы зарекомендовали себя с положительной стороны и отвечают всем требованиям ФСИН России. Кроме того, они имеют достаточные хорошие алгоритмы методов идентификации личности, что непосредственно помогает администрации предотвратить преступления и провести профилактику их предотвращения.

Но не стоит забывать, что у каждой системы есть изъян. В данном случае в качестве одного из больших минусов стоит отметить отсутствие единой базы данных подозреваемых, обвиняемых и осужденных по всей России, где могли бы быть указаны их регистрационные данные и вся возможная информация исчерпывающего характера. Это бы заметно упростило работу администрации и заметно снизило риск возникновения конфликтных ситуаций при прибытии по приговору суда в места лишения свободы или в места содержания под стражей. Также к проблеме можно отнести определенные алгоритмы методов, по которым тоже возникает затруднение в отождествлении. Например, если рассматривать метод отпечатка пальцев, то главным минусом является то, что папиллярные узоры очень легко повредить, и идентифицировать лицо станет невозможным определенный промежуток времени. Если же мы возьмем метод отождествления при помощи лица, то тут так же возникает проблема, а именно: субъект, который находился под стражей за определенный промежуток времени, изменился во внешности. Либо он сбросил определенный вес, либо набрал, в связи с чем, его фотография, которую сохранил алгоритм в своей базе данных с самого начала, перестала быть актуальной. И, исходя из этого, субъект, которого пытаются идентифицировать при помощи сканера, просто напросто не проходит идентификацию.

Библиографический список

Нормативные правовые акты

1. Конституция Российской Федерации: текст с изменениями и дополнениями на 14 марта 2020 г. № 1-ФКЗ: [принята всенародным голосованием 12 декабря 1993 г.] // Официальный интернет-портал правовой информации (www.pravo.gov.ru) 4 июля 2020 г.

2. Уголовно-исполнительный кодекс Российской Федерации: федеральный закон: текст с изменениями и дополнениями на 5 апреля 2021 г. № 78-ФЗ [принят 8 января 1997 г. № 1-ФЗ] // Официальный интернет-портал правовой информации (www.pravo.gov.ru) 5 апреля 2021 г.

3. О содержании под стражей подозреваемых и обвиняемых в совершении преступлений: федеральный закон: текст с изменениями и дополнениями на 5 апреля 2021 г. № 78-ФЗ [принят 15 июля 1995 г. № 103-ФЗ] // Официальный интернет-портал правовой информации (www.pravo.gov.ru) 5 апреля 2021 г.

4. Об оперативно-розыскной деятельности: федеральный закон: текст с изменениями и дополнениями на 30 декабря 2020 г. № 515-ФЗ [принят 12 августа 1995 г. № 144-ФЗ] // Официальный интернет-портал правовой информации (www.pravo.gov.ru) 30 декабря 2020 г.

5. Об учреждениях и органах, исполняющих уголовные наказания в виде лишения свободы: закон РФ: текст с изменениями и дополнениями на 5 апреля 2021 г. № 78-ФЗ [принят 21 июля 1993 г. № 5473-1] // Официальный интернет-портал правовой информации (www.pravo.gov.ru) 5 апреля 2021 г.

6. Об утверждении Концепции развития уголовно-исполнительной системы Российской Федерации на период до 2030 г.: распоряжение

Правительства РФ: [принят 29 апреля 2021 г. № 1138-р] // Официальный интернет-портал правовой информации (www.pravo.gov.ru) 5 мая 2021 г.

7. Об утверждении Наставления по оборудованию инженерно-техническими средствами охраны и надзора объектов уголовно-исполнительной системы: приказ Минюста России: текст с изменениями и дополнениями на 17 июня 2013 г. № 94 [принят 4 сентября 2006 г. № 279] // Официальный интернет-портал правовой информации (www.pravo.gov.ru) 17 июня 2013 г.

8. О внесении изменений в приказ Министерства юстиции Российской Федерации от 4 сентября 2006 г. № 279 «Об утверждении Наставления по оборудованию инженерно-техническими средствами охраны и надзора объектов уголовно-исполнительной системы»: приказ Минюста России: [принят 17 июня 2013 г. № 94] // Официальный интернет-портал правовой информации (www.pravo.gov.ru) 4 сентября 2006 г.

9. Об утверждении Правил внутреннего распорядка исправительных учреждений приказ Минюста России: текст с изменениями и дополнениями на 29 января 2021 г. № 6 [принят 16 декабря 2016 г. № 295] // Официальный интернет-портал правовой информации (www.pravo.gov.ru) 9 февраля 2021 г.

10. Об установлении оценки деятельности территориальных органов Федеральной службы исполнения наказаний при инспектированиях: приказ ФСИН России: [принят 14 июня 2012 г. № 325] // Официальный интернет-портал правовой информации (www.pravo.gov.ru) 14 июня 2012 г.

11. Об утверждении Концепции развития уголовно-исполнительной системы Российской Федерации до 2020 года: распоряжение Правительства РФ: текст с изменениями и дополнениями на 23 сентября 2015 г. № 1877-р [принят 14 октября 2010 г. № 1772-р] // Собрание законодательства РФ. – 2010. – № 43. – Ст. 5544 (утратил силу).

Научные, учебные, справочные издания

12. Абрамов А. М. Системы управления доступом / А. М. Абрамов, О. Ю. Никулин, А. И. Петрушин. – М.: Оберег-РБ, 1998. – 190 с.

13. Анисимков В. М. Организация управления в уголовно-исполнительной системе: учебник / под ред. Ю. Я. Чайки, В. М. Анисимкова, А. А. Аксенова. – Рязань: Академия права и управления Минюста России, 2002. – С. 536.

14. Барсуков В. С. Безопасность: технологии, средства, услуга / В. С. Барсуков. – М.: Куниц-образ, 2001. – 489 с.

15. Васильков А. В., Васильков И. А. Безопасность и управление доступом в информационных системах: учебное пособие / А. В. Васильков, И. А. Васильков. – М.: Форум, 2017. – 368 с.

16. Ворона В. А., Тихонов В. А. Системы контроля и управления доступом / В. А. Ворона, В. А. Тихонов. – М.: Горячая линия – Телеком, 2010. – 272 с.

17. Горлицин И. Контроль и управление доступом – просто и надежно / И. Горлицин. – КТЦ «Охранные системы», 2002. – 369 с.

18. Громов М. А. Организация безопасности в исправительных учреждениях: учебное пособие / М. А. Громов. – Рязань: Академия ФСИН России, 2005. – 240 с.

19. Девянин П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками / П. Н. Девянин. – 2-е изд., испр. и доп. – М.: Наука, 2017. – 338 с.

20. Зегжда Д. П. Основы безопасности информационных систем / Д. П. Загжда, А. М. Ивашко. – М: Горячая Линия – Телеком, 2000. – 452 с.

21. Ковалев О. Г. Организация действий учреждений УИС Министерства юстиции РФ в особых условиях / О. Г. Ковалев. – Москва, 2004. – 77 с.

22. Крахмалев А. К. Средства и системы контроля и управления доступом: учебное пособие / А. К. Крахмалев. – М.: НИЦ «Охрана» ГУВО МВД России, 2003. – 272 с.

23. Мащенов Р. Г. Системы охранной сигнализации: основы теории и принципы построения: учебное пособие / Р. Г. Мащенов. – М.: Горячая линия – Телеком, 2004. – 314 с.

24. Тихонов В. А., Райх В. В. Информационная безопасность: концептуальные, правовые, организационные и технические аспекты: уч. пособие для вузов / В. А. Тихонов, В. В. Райх. – М.: Гелиос АРВ, 2006. – 528 с.

25. Упоров А. Г. Основы безопасности государства и личности: учебное пособие / А. Г. Упоров. – Новокузнецк: ФГОУ ВПО Кузбасский институт ФСИН России, 2009. – 52 с.

26. Хвощ С. Т. Микропроцессоры и микроЭВМ в системах автоматического управления. Справочник / С. Т. Хвощ, Н. Н. Варлинский, Е. А. Попов. – М.: Машиностроение, 2018. – 642 с.

27. Якунин Д. В., Павлов И. Н. Обеспечение надлежащего надзора за осужденными, как фактор, влияющий на укрепление режима в исправительных колониях: метод. рек / Д. В. Якунин, И. Н. Павлов. – Уссурийск, 2007. – 168 с.

28. Ярочкин, В. И. Информационная безопасность: учебник для студентов вузов / В. И. Ярочкин. – 3-е изд. – М.: Академический Проект: Трикста, 2005. – 544 с.

Материалы периодической печати

29. Абрамова О. Ф. Сравнительный анализ программных продуктов оценки инвестиционных проектов / О. Ф. Абрамова, А. Р. Галкин, А. А. Рыбанов // Волгоград: ВПИ ВГТУ (филиал). – 2017. – № 60-2. – С. 81–86.

30. Барсуков В. С. Интегральная защита информации / В. С. Барсуков // Системы безопасности. – 2002. – № 5. – С. 47–54.

31. Гинце А. Новые технологии в СКУД / А. Гинце // Системы безопасности. – 2005. – № 6. – С. 35–39.

32. Злотник Е. TouchMemory – новый электронный идентификатор / Е. Злотник // Монитор. – 1994. – №6. – С. 26–31.

33. Мальцев А., Моржаков В. Современные биометрические методы идентификации / А. Мальцев, В. Моржаков // Безопасность. Достоверность. Информация. – 2009. – № 2. – С. 44–48.

34. Мальцев И. В. Системы контроля доступом / И. В. Мальцев // Системы безопасности. – 1996. – № 1. – С. 43–45.

35. Сабынин В. Н. Организация пропускного режима первый шаг к обеспечению безопасности и конфиденциальности информации / В. Н. Сабынин // Информост радиоэлектроники и телекоммуникации. – 2001. – № 3. – С. 32–35.

36. Тарасов. Ю. А. Контрольно-пропускной режим на предприятии. Защита информации / Ю. А. Тарасов // Конфидент. – 2002. – № 1. – С. 55–61.

37. Татарченко И. В., Соловьев Д. С. Концепция интеграции унифицированных систем безопасности / И. В. Татарченко, Д. С. Соловьев // Системы безопасности. – 2007. – № 1 (73). – С. 86–89.

38. Татарченко Н. В., Тимошенко С. В. Биометрическая идентификация в интегрированных системах безопасности / Н. В. Татарченко, С. В. Тимошенко // Специальная техника. – 2002. – № 2. – С. 44–47.

39. Перегудов А. Г. Проблемы правовой защищенности осужденных к лишению свободы – в реформировании и гуманизации исправительной системы / А. Г. Перегудов // Материалы научно – теоретической конференции. – Уфа: УВШ МВД РФ. – 1993. – № 1. – С 129–133.

40. Юсупов О. Р. Сравнительный анализ возможности использования технологий биометрической идентификации / О. Р. Юсупов // Молодой ученый. – 2016. – № 19. – С. 118–121.

Материалы юридической практики

41. Материалы преддипломной практики в ФКУ СИЗО-2 ГУФСИН России по Челябинской области / А. М. Костин (неопубликованный акт).

Приложения

Приложение 1

Сравнение методов биометрической идентификации личности по степени выраженности различных свойств[44]

Биометрия	Универ-сальность	Посто-янство	Измери-мость	Эффектив-ность	Доступ-ность	Защищен-ность
Отпечатки пальцев	С	В	С	В	С	В
Лицо	В	С	В	Н	В	Н
Форма кисти	С	С	В	С	С	С
Радужка	В	В	С	В	Н	В
Сетчатка	В	С	Н	В	Н	В
Динамика подписи	Н	Н	В	Н	В	Н
Распознавание голоса	С	Н	С	Н	В	Н
Клавиатурный почерк	Н	Н	С	Н	С	С
Сосуды ладони	С	С	С	С	С	В
Термография лица	В	Н	В	С	В	В

Н – низкая, С – средняя, В – высокая.

[44] Зегжда Д. П. Основы безопасности информационных систем. – М: Горячая Линия – Телеком, 2000. – С. 453.