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 уголовно-исполнительной системы

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

Тема: **Применение специальных технических средств для защиты конфиденциальной служебной информации в органах и учреждениях уголовно-исполнительной системы Российской Федерации**

Выполнил:
курсант 4 взвода 4 курса
младший сержант
внутренней службы
Батухтин Максим Евгеньевич

Научный руководитель:
доцент кафедры управления и информационно-технического обеспечения деятельности УИС,
кандидат педагогических наук,
полковник внутренней службы
Попов Игорь Вадимович

Рецензент:
начальник ФКУ ЛИУ №19 УФСИН России по Тюменской области
подполковник внутренней службы
Ершов Александр Николаевич

Решение начальника кафедры о допуске к защите допущена

Дата защиты: 23.06.2022 Оценка 4 (хорошо)

Самара
2022

Оглавление

Введение

Актуальность темы. Информация в истории развития цивилизации и человечества в целом всегда играла главную роль и была базовой в принятии решений на всех этапах и уровнях развития государства и общества.

Специфику термина «информация» в учреждениях и органах УИС отражает следующее определение: информация – это собранные, обработанные и проанализированные статистические и оперативные сведения, характеризующие оперативную обстановку, снижающие уровень неопределенности, и оцененные руководителем как полезные для принятия управленческого решения, способствующего выполнению тех или иных задач функционирования УИС.

В соответствии с Законом РФ от 21.07.1993 № 5473-1 «Об учреждениях и органах, исполняющих уголовные наказания в виде лишения свободы» (в ред. 26 мая 2021 г.)[1], также Указом Президента РФ от 13 октября 2004 г. № 1314 «Вопросы Федеральной службы исполнения наказаний»[2] на Федеральную службу исполнения наказаний России (далее – ФСИН России) возложены задачи по исполнению в соответствии с законодательством РФ уголовного наказания в виде лишения свободы, обеспечения правопорядка в местах лишения свободы (далее – МЛС) и охраны осужденных, организации надзора за ними, а также задачи по профилактике правонарушений и преступлений, совершаемых спецконтингентом в учреждения уголовно-исполнительной системы (далее – УИС). На сегодняшний день для выполнения этих задач важное значение играет инженерно-техническое обеспечение служебной деятельности отделов и служб исправительного

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

[2]Вопросы Федеральной службы исполнения наказаний: указ Президента РФ: текст с изменениями и дополнениями на 11 апреля 2022 г. № 201 [принят 13 октября 2004 г. № 1314] // Официальный интернет-портал правовой информации (www.pravo.gov.ru) 11 апреля 2022 г.

учреждения (далее – ИУ), в том числе для получения, хранения и передачи информации различного характера.

Основные направления повышения уровня безопасности ИУ отражены в положениях Концепции развития уголовно-исполнительной системы Российской Федерации до 2030 года[3], которая предусматривает создание целой системы мер по противодействию противоправному поведению осужденных, основываясь на применении новейших инженерно-технических средств, методов и технологий организации безопасности объектов УИС, а также информационной безопасности при выполнении сотрудниками служебных задач, оснащение российских МЛС современными интегрированными системами безопасности, ведение мониторинга за поведением осужденных посредством электронного контроля (беспроводные технологии) и т. д.

Без решения вопроса организации внутреннего и внешнего потока информации невозможно повысить оперативность принятия решения и эффективность контроля за исполнением управленческих решений и, соответственно, успешно выполнить задачи, стоящие перед УИС. Следовательно, информационное обеспечение управленческой деятельности в УИС заключается в осуществлении мероприятий по предоставлению своевременной, достоверной и полной информации (информационных ресурсов) субъекту управления (руководителю) для реализации аналитических и управленческих процедур, обеспечивающих функциональность деятельности УИС, исправление осужденных и предупреждение совершения новых преступлений.

Выбранная тема выпускной квалификационной работы является достаточно актуальной, так как на сегодняшний день «информация» может иметь несколько уровней значимости, важности, ценности, что

---

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

предусматривает соответственно наличие нескольких уровней ее конфиденциальности. Наличие разных уровней доступа к информации предполагает различную степень обеспечения каждого из свойств безопасности информации – конфиденциальность, целостность и доступность.

Защита информации включает в себя целый комплекс организационных и технических мер по обеспечению информационной безопасности техническими средствами. Она должна решать такие задачи, как:

– закрытие доступа постороннего к источникам информации с целью ее ознакомления, распространения;

– предотвращение уничтожения информации в результате разных действий;

– предотвращение самопроизвольной потери информации по техническим каналам связи.

Объектом исследования выступают общественные отношения, связанные с техническим обеспечением и методами по защите конфиденциальной служебной информации в органах и учреждениях УИС.

Предмет исследования составляют научно-теоретические источники, раскрывающие сравнительно-правовой и организационный аспект специальных технических средств информационной безопасности и защиты конфиденциальной служебной информации. В предмет работы также входит система нормативно-правовых актов РФ относительно рассматриваемой тематики, а также практика органов и учреждений УИС в области защиты конфиденциальной служебной информации.

Целью исследования заключается в изучении и анализе законодательства в области информационной безопасности, специальных технических средств и современных методов защиты конфиденциальной служебной информации, применяемых в органах и учреждениях УИС.

Цель определила наличие следующих **задач:**

– определить процесс становления службы по защите информации в структуре ФСИН России;

– изучить правовые и организационные основы применения технических средств в области защиты информации на объектах УИС;

– определить методы по защите конфиденциальной служебной информации и специальные технические средства, применяемые в органах и учреждениях УИС для решения данных задач;

– определить требования к эксплуатации специальных технических средств по защите конфиденциальной служебной информации в учреждениях и органах ФСИН России и порядок аттестации объектов УИС по требованиям информационной безопасности.

Теоретическая база и степень научной разработанности темы. Вопросы применения технических средств и защита информации на объектах ФСИН России не достаточно изучены в виду постоянных новых современных угроз. В работах в основном находит отражение организационно-правовой аспект деятельности служб по защите информации. Проблемам защиты информации в разное время посвятили свои труды С. В. Видов, А. Н. Лепехин, В. В. Теняев, М. И. Купцова А. В. Душкин, В. П. Корячко, В. И. Ярочкин, С. Н. Кленовым, Г. А. Бузов, С. В. Калинин, А. В. Кондратьев, А. А. Хорев и др.

Методы исследования. При подготовке работы автором использовались общенаучные, частнонаучные и специальные методы познания, в том числе диалектический, комплексный, целевой, логические, общесоциологические, статистический, историко и сравнительно-правовой и другие методы.

Структура работы. Выпускная квалификационная работа состоит из введения, двух глав, объединяющих четыре параграфа, заключения, библиографического списка и приложений.

Глава 1. НОРМАТИВНО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ ИСПОЛЬЗОВАНИЯ СПЕЦИАЛЬНЫХ ТЕХНИЧЕСКИХ СРЕДСТВ ДЛЯ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ СЛУЖЕБНОЙ ИНФОРМАЦИИ В ОРГАНАХ И УЧРЕЖДЕНИЯХ ФСИН РОССИИ

1.1. Становление службы по технической защите информации в структуре ФСИН России и порядок применения специальных технических средств защиты конфиденциальной служебной информации

В Федеральном законе «Об информации, информационных технологиях и о защите информации», принятом в июле 2006 года, определено, что информация – это сведения (сообщения, данные) независимо от формы их представления. В зависимости от категории доступа информация подразделяется на общедоступную и ограниченного доступа[4].

Наличие государственных информационных ресурсов, отнесенных законом к категории ограниченного доступа, предполагает наличие вполне определенного режима защиты, установленного соответствующими законами. Защите подлежит информация как речевая, так обрабатываемая техническими средствами, а также существующая в виде информативных электрических сигналов, физических полей, носителей на бумажной, магнитной, оптической и иной основе. Поэтому с целью исключения или существенного затруднения в добывании информации техническими средствами разведки, а также ради предотвращения её утечки по техническим каналам, защиты её от несанкционированного доступа в процессе обработки и передачи информации в территориальных органах уголовно-исполнительной системы, в штатной структуре узлов связи центров

[4]Об информации, информационных технологиях и защите информации: федеральный закон: текст с изменениями и дополнениями на 30 декабря 2021 г. № 441-ФЗ [принят 27 июля 2006 г. № 149-ФЗ] // Официальный интернет-портал правовой информации (http://pravo.gov.ru) 30 декабря 2021 г.

инженерно-технического обеспечения было предписано создать подразделения технической защиты информации.

Техническая защита информации (далее – ТЗИ) стала важным направлением деятельности в УИС. На созданные подразделения возложены функции организации и проведения работ по оборудованию, технической защите и аттестации объектов информатизации территориальных органов УИС, ведомственного контроля соблюдения установленных правил и требований безопасности информации при обработке сведений, составляющих государственную и служебную тайну, на средствах вычислительной техники.

Вопросы защиты информации требуют наличия в структуре УИС подразделений, укомплектованных компетентными и высокопрофессиональными специалистами в области защиты информации. Поэтому одним из важнейших направлений деятельности является обучение сотрудников современным методам и способам обеспечения информационной безопасности. Подготовка специалистов в области технической защиты информации на первоначальном этапе проводилась на курсах повышения квалификации в Межотраслевом специальном учебном центре при Минатоме России, Управлении Федерального казначейства по Волгоградской области, учебном центре безопасности информации «Маском» (Дальний восток). В 2007–2008 годах в территориальные подразделения ТЗИ УИС стали приходить специалисты, прошедшие обучение в высших учебных заведениях России по специализации «Безопасность и техническая защита информации», но таких специалистов были единицы. Таким образом, в период с 2004 по 2008 гг. прошли первичную подготовку и углубили свои знания более 120 сотрудников УИС[5].

Все подразделения ТЗИ территориальных органов УИС и подразделений центрального подчинения принимали участие в сборах по

[5] Средства охраны, безопасности и телекоммуникационного оборудования на службе УИС России: юбилейный сборник: с приложением на CD / [ред. совет Баринов Н. И. – пред. и др.]. – Москва: Информ. мост, 2009. – 188 с.

повышению квалификации на базе Псковского юридического института ФСИН России, прошедших в мае 2008 года. Полученные теоретические и практические навыки в области технической защиты информации помогают специалистам ТЗИ компетентно разрабатывать организационно-распорядительные документы на объекты информатизации, решать поставленные перед ними задачи технической защиты информации. Немаловажным направлением в деятельности по технической защите информации в ФСИН России стало оборудование и аттестация объектов информатизации, предназначенных для обработки сведений, составляющих государственную и служебную тайны, согласно требованиям руководящих и нормативных документов Федеральной службы по техническому и экспортному контролю (ФСТЭК России). По результатам аттестационных испытаний посредством специального документа – «аттестата соответствия» – подтверждается, что объект соответствует требованиям стандартов и иных нормативно-технических документов по безопасности информации. В связи с тем, что проводить аттестационные испытания могут только аккредитованные во ФСТЭК России организации, значительные бюджетные средства ФСИН России уходят на оплату работ сторонних организаций.

В целях решения этой проблемы возникла необходимость создания лабораторий, аккредитованных во ФСТЭК России и способных профессионально решать задачи по аттестации ведомственных объектов информатизации. К тому времени прошли лицензирование и получили аттестат аккредитации две ведомственные лаборатории технической защиты информации ФБУ «Научно-исследовательский институт информационных и производственных технологий» ФСИН России (г. Тверь) и ФБУ Межрегиональный центр инженерно-технического обеспечения ГУФСИН России по Волгоградской области.

Создание собственных аттестационных лабораторий позволило проводить весь комплекс аттестационных работ ведомственных объектов информатизации собственными силами и, в конечном итоге, привести к

существенной экономии финансовых средств при более оперативном решении самых неотложных задач по аттестации объектов информатизации без привлечения сторонних организаций. Созданный в конце 2005 года отдел по противодействию техническим разведкам и технической защите информации (ПДТР и ТЗИ) занимался координацией мероприятий по защите информации во ФСИН России, оказанием консультативной помощи подразделениям ТЗИ территориальных органов УИС, координацией и руководством деятельностью этих подразделений, проведением единой технической политики в данной области. Работа подразделения строилась в тесном взаимодействии с режимно-секретными подразделениями центрального аппарата ФСИН России и ФБУ ГЦИТО ФСИН России. Активное и плодотворное для ФСИН России сотрудничество проводилось с Федеральной службы безопасности (ФСБ России) и ФСТЭК России. Была развернута большая практическая работа по оказанию методической и практической помощи подразделениям ТЗИ территориальных органов УИС. С этой целью для обучения сотрудников и обмена опытом центральным аппаратом ФСИН России, совместно с отделом ПДТР и ТЗИ ФБУ ГЦИТО, на базе Псковского юридического института ФСИН России стали проводится сборы сотрудников подразделений ТЗИ территориальных органов ФСИН России. Так, в мае 2008 года в рамках проведения представителями ФСБ и ФСТЭК России участникам сборов разъяснены основные положения законодательства Российской Федерации по защите государственной тайны в части, касающейся вопросов порядка аттестационных испытаний объектов информатизации и лицензирования по работе с гостайной.

Были также рассмотрены проблемные вопросы организации ТЗИ в территориальных органах УИС. Заслушаны выступления начальника аппарата директора ФСИН России полковника внутренней службы А. Е. Косолапова, заместителя начальника аппарата директора ФСИН России подполковника внутренней службы А. И. Парсегова по вопросам взаимодействия режимно-секретных подразделений и подразделений ТЗИ

при осуществлении мероприятий в области защиты информации, содержащей сведения, составляющие государственную тайну. По вопросам законодательных основ защиты государственной тайны, аттестации объектов информатизации по требованиям информации, лицензирования в области защиты государственной тайны в УИС России представлены доклады сотрудников ФБУ НИИИиПТ ФСИН России полковника внутренней службы Д. В. Зубарева и полковника внутренней службы В. А. Родионова.

В докладе начальника отдела ПДТР и ТЗИ ФБУ ГЦИТО ФСИН России полковника внутренней службы А. А. Важенкова были изложены основные направления информационной безопасности и меры по технической защите информации, рассмотрены вопросы информационной безопасности, изложенные в «Доктрине информационной безопасности Российской Федерации» (утверждена указом Президента Российской Федерации от 5 декабря 2016 г. № 646)[6]. В рамках работы круглого стола были заслушаны выступления сотрудников УФСИН по Чувашской Республике, ГУФСИН по Приморскому краю, УФСИН по Еврейской автономной области, УФСИН по Ульяновской области, ФБУ МЦИТО ФСИН России. По данным выступлениям разъяснены вопросы, касающиеся практической деятельности подразделений ТЗИ, также обсуждены вопросы организации взаимодействия ФСИН России, ФБУ ГЦИТО ФСИН России и территориальных органов УИС, а также проблемные вопросы организации ТЗИ и информационной безопасности в учреждениях и органах УИС.

Сотрудниками ЗАО НПЦ «Модуль» и ОАО ЦБИ «Маском» были представлены образцы новой техники и проведены практические занятия на технике, закупленной по государственным контрактам ФСИН России. Комплекс мероприятий по обеспечению аттестации и контролю эффективности защиты объектов информатизации сотрудниками ПДТР и ТЗИ был представлен в виде стенда организации ЗАО «АННА», на котором

---

[6] Об утверждении Доктрины информационной безопасности Российской Федерации: указ Президента РФ от 05 декабря 2016 г. № 646 // Официальный интернет-портал правовой информации (www.pravo.gov.ru) 5 декабря 2016г.

подробно рассмотрена схема включения и настройки датчиков с применением средств вычислительной техники. Кроме того, была представлена техника, применяемая сотрудниками отдела ПДТР и ТЗИ при выявлении закладочных устройств («Лорнет»), оборудование, выполняющее блокирование телефонов сотовой связи («Мозаика») и блокирование диктофонов речевой записи («Шторм»), а также проведено занятие по установке и инсталляции программного обеспечения «Страж NT».

Значимым направлением развития службы технической защиты информации является проведение единой технической политики по обеспечению подразделений ТЗИ территориальных органов ФСИН России современными сертифицированными техническими и программными средствами защиты информации, а также измерительным и специальным поисковым оборудованием, основанным на различных физических принципах. Для решения этой задачи сотрудники подразделения ПДТР и ТЗИ разрабатывают техническое задание на закупку аппаратуры ТЗИ в рамках государственного оборонного заказа.

В настоящее время отделы по защите информации представлены в учреждениях непосредственно подведомственных ФСИН России, первый орган это федеральное казенное учреждение «Научно-исследовательский институт информационных технологий Федеральной службы исполнения наказаний» (ФКУ НИИИТ ФСИН России) целями деятельности учреждения являются:

– комплексное информационное, программное и нормативно-методическое обеспечение стабильного функционирования, развития и совершенствования УИС в интересах наиболее полного и эффективного выполнения функций, возложенных на нее законодательством Российской Федерации;

– осуществление прикладных научных исследований и разработок в сфере информационных и иных проблем деятельности подразделений УИС;

– проведение работ по созданию и поддержанию в актуальном состоянии информационного ресурса УИС на основе внедрения современных информационных технологий, прогрессивных форм и методов управления, с учетом создаваемой инфраструктуры информационных служб на всех уровнях управления УИС;

– эффективное использование и развитие собственного научно-технического потенциала;

– обеспечение сохранности информационного ресурса ФСИН России;

– иные цели, возложенные на учреждение в соответствии с законодательством Российской Федерации. Основной вид деятельности учреждения это создание и использование баз данных и информационных ресурсов.

Второй орган – это федеральное казенное учреждение «Главный центр инженерно-технического обеспечения и связи Федеральной службы исполнения наказаний» (ФКУ ГЦИТОиС ФСИН России) в соответствии с приказом ФСИН России от 26 ноября 2013 г. № 712 «О внесении изменений в Устав федерального казенного учреждения «Главный центр инженерно-технического обеспечения и связи Федеральной службы исполнения наказаний»[7] в состав учреждения включены 8 филиалов: Волгоградский, Воронежский, Иркутский, Нижегородский, Новосибирский, Санкт-Петербургский, Челябинский и Хабаровский, и приказом ФСИН России от 21 мая 2014 г. № 257 «О внесении изменений в штатные расписания учреждений, непосредственно подчиненных Федеральной службе исполнения наказаний», в состав федерального казенного учреждения «Главный центр инженерно-технического обеспечения и связи Федеральной службы исполнения наказаний» включен Крымский филиал[8].

---

[7] О внесении изменений в Устав федерального казенного учреждения «Главный центр инженерно-технического обеспечения и связи Федеральной службы исполнения наказаний: приказ ФСИН России от 26 ноября 2013 г. № 712(неопубликованный акт).

[8] О внесении изменений в штатные расписания учреждений, непосредственно подчиненных Федеральной службе исполнения наказаний: приказ ФСИН России от 21 мая 2014 г. № 257 (неопубликованный акт).

Предметом и целями деятельности учреждения являются:

– инженерно-техническое и организационно-методическое обеспечение деятельности УИС в области использования инженерно технических средств охраны и надзора (далее – ИТСОН), средств связи, информационных и телекоммуникационных систем, средств вычислительной техники, периферийного оборудования;

– приобретение, получение, хранение материально-технических ресурсов и обеспечение ими учреждений и органов УИС;

– планирование и проведение плановых ремонтов и сезонного технического обслуживания ИТСОН, средств связи УИС;

– сопровождение и контроль за проведением научно-исследовательских и опытно-конструкторских работ, направленных на совершенствование существующих и внедрение новых образцов ИТСОН, средств связи, информационных и телекоммуникационных систем;

– организация работы по внедрению, эксплуатации ИТСОН, средств связи, информационных и телекоммуникационных систем, средств вычислительной техники, периферийного оборудования в учреждениях и органах УИС;

– обеспечение ФСИН России возможности непрерывного управления учреждениями и органами УИС путем предоставления всех видов связи, в том числе и шифрованной;

– предоставление своевременной, надежной, достоверной и скрытой передачи сообщений и информационных данных в любых условиях оперативной обстановки;

– разработка и практическое осуществление мероприятий по организации, обеспечению функционирования и безопасности шифрованной связи, ее развитию и совершенствованию в УИС;

– распространение шифровальных (криптографических) средств, выполнение работ, оказание услуг в области шифрования информации, техническое обслуживание шифровальных (криптографических) средств;

– организация работ в УИС по защите информации;

– организация проведения поверок средств измерений;

– иные цели, возложенные на учреждение в соответствии с законодательством Российской Федерации.

Данные учреждения с момента создания прошли большой путь становления и накопили большой практический опыт, по ведомственной защите информации выполняя все поставленные руководством ФСИН России задачи по защите государственной тайны, предотвращению утечки информации по техническим каналам и предупреждению преднамеренных программно-технических воздействий при автоматизированной обработке информации в Федеральной службе исполнения наказаний, принимают активное участие в организации работ по обеспечению информационной безопасности, внедряют новейшие образцы перспективной техники, построенной на передовых технологиях, привлекая квалифицированных специалистов в данной области с целью надежного обеспечения сохранности государственной и служебной тайны.

1.2. Правовые и организационные основы применения специальных технических средств в области защиты информации на объектах УИС

Россия в сфере информационной безопасности в рамках правового регулирования начала активное развитие в конце XX века. Первоначально были приняты Закон «О правовой охране программ для электронных вычислительных машин и баз данных» от 23 сентября 1992 г. № 3523-1[9] и Концепция защиты средств вычислительной техники и автоматизированных

[9]. О правовой охране программ для электронных вычислительных машин и баз данных: закон от 23 сентября 1992 г. № 3523-1: ред. от 02 февраля 2006 г. // Российская газета. – 1992. – № 229 (утратил силу).

систем от несанкционированного доступа к информации[10], затем Закон «О государственной тайне» от 21 июля 1993 г. № 5485-1 (в редакции 11 июня 2021 г.) [11] и Закон «Об информации, информатизации и защите информации» от 20 февраля 1995 г. № 24-ФЗ[12], а также были разработаны Правила отнесения сведений, составляющих государственную тайну, к различным степеням секретности (1995 г.)[13].

На федеральном уровне власти принимают ряд мер по обеспечению информационной безопасности: формируется единая государственная политика по обеспечению защиты национальных интересов от угроз в информационной сфере, создается баланс между допустимыми ограничениями распространения информации и потребностью в свободном обмене ею, приводится к совершенству законодательство РФ в данной сфере, осуществляется координация деятельности органов государственной власти по обеспечению безопасности в информационной среде, защищаются государственные информационные ресурсы на оборонных предприятиях, развиваются отечественные информационные и телекоммуникационные средства, совершенствуется информационная структура развития новых информационных технологий, унифицируются средства поиска, сбора, хранения, обработки и анализа информации для вхождения в глобальную информационную инфраструктуру.

---

[10]Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации: утв. решением Гостехкомиссии России 30.03.1992 (неопубликованный акт).

[11]О государственной тайне: закон: текст с изменениями и дополнениями на 11 июня 2021 г. № 170 ФЗ [принят 21 июля 1993 № 5485-115] // Официальный интернет-портал правовой информации (www.pravo.gov.ru) 11 июня 2021 г.

[12] Об информации, информатизации и защите информации: федеральный закон: текст с изменениями и дополнениями на 10 января 2003 г. № 15-ФЗ [принят 20 февраля 1995 г. № 24-ФЗ] // Официальный интернет-портал правовой информации (www.pravo.gov.ru) 10 января 2003 г. (утратил силу).

[13]Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности: постановление Правительства РФ: текст с изменениями и дополнениями на 30 октября 2021 г. № 1868 [принят 4 сентября 1995 г. N 870] // Официальный интернет-портал правовой информации (www.pravo.gov.ru) 30 октября 2021 г.

С течением времени и развитием государства возникла потребность в дополнении действующего законодательства. В связи с чем вопросы информационной безопасности было решено отразить в Концепции национальной безопасности РФ (1997 г.)[14]. В ее содержание вошли следующие пункты: выявление, оценка и прогнозирование источников угроз информационной безопасности; разработка государственной политики обеспечения информационной безопасности, комплекса мероприятий и механизмов ее реализации; нормативно-правовое обеспечение информационной безопасности, координация деятельности органов государственной власти и управления, а также предприятий по обеспечению информационной безопасности; формирование системы обеспечения информационной безопасности, развитие ее организации, методов, форм и средств парирования, предотвращения и нейтрализации угроз информационной безопасности и ликвидации последствии ее нарушения; обеспечение активного участия России в процессах создания и использования глобальных информационных сетей и систем.

Но в соответствии с указом Президента РФ уже 10 января 2000 года данная Концепция вновь претерпела изменения и была изложена в новой редакции[15]. Это говорит о том, что защита информации в государстве являлась одним из приоритетных направлений деятельности, учитывая тот факт, что Россия в значительной степени отставала от европейских стран в данной сфере.

В 2006 году в России был принят ныне действующий Федеральный закон «Об информации, информационных технологиях и о защите информации», который является основой всего законодательства в сфере защиты информации и сегодня, а в 2016 году – Указ Президента РФ

---

[14] Концепция национальной безопасности Российской Федерации: утв. указом Президента РФ от 17 декабря 1997 № 1300 // Российская газета. – 1997. – № 247 (утратил силу).

[15] Концепция национальной безопасности Российской Федерации: утв. указом Президента РФ от 10 января 2000 г. № 24 // Собр. законодательства Рос. Федерации. – 2000. – № 2, ст. 170 (утратил силу).

«Об утверждении Доктрины информационной безопасности Российской Федерации».

Стоит отметить, что современное российское законодательство устроено таким образом, что, кроме специальных нормативных актов, регулирующих какую-то одну сферу деятельности, отдельные нормы по регламентации встречаются и в других нормативных актах. Например, ряд статей Уголовного кодекса Российской Федерации (далее – УК РФ) направлены на защиту информации[16]. Так в гл. 28 УК РФ «Преступления в сфере компьютерной информации» включены статьи, а именно:

1) Ст. 272. Неправомерный доступ к компьютерной информации.

Эта норма содержит много признаков, которые являются обязательными для квалификации по данной статье. Непосредственным объектом выступают общественные отношения в сфере обеспечения безопасности компьютерной информации и нормальной работы ЭВМ, их сети или системы. Состав преступления считается материальным, при этом если деяние в форме действия четко определено (неправомерный доступ к компьютерной информации, охраняемой законом), то последствия могут быть разнообразными:

1) уничтожение информации,

2) блокирование ее,

3) модификация,

4) копирование.

В ч. 2 ст. 272 в качестве квалифицирующих предусмотрены 2 признака: если деянием причинен крупный ущерб (сумма ущерба более 1 млн рублей) или если деяние совершено из корыстной заинтересованности.

Кроме того, также отмечены и другие квалифицирующие признаки: если деяния из ч. 1 и ч. 2 совершены группой лиц по предварительному

[16] Уголовный кодекс Российской Федерации: федеральный закон: текст с изменениями и дополнениями на 25 марта 2022 г. № 63-ФЗ [принят 13 июня 1996 г. № 63-ФЗ] // Официальный интернет-портал правовой информации (www.pravo.gov.ru) 25 марта 2022 г.

сговору или организованной группой либо лицом с использованием своего служебного положения (ч. 3) и если деяния из ч. ч. 1 -3 повлекли тяжкие последствия или создали угрозу их наступления (ч. 4).

2) Ст. 273. Создание, использование и распространение вредоносных компьютерных программ. Непосредственным объект – это общественные отношения по безопасному использованию ЭВМ, ее программного обеспечения и информационного содержания. Эта норма накладывает запрет на совершение одного из следующих действий: создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации.

Также предусмотрены квалифицирующие признаки: если деяние совершено группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно причинившие крупный ущерб или совершенные из корыстной заинтересованности (ч. 2) и если они повлекли тяжкие последствия или создали угрозу их наступления (ч. 3).

3) Ст. 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей. Цель этой нормы заключается в предупреждении неисполнения пользователями своих обязанностей, которые влияют на сохранность хранимой и перерабатываемой информации и соблюдение определенных правил эксплуатации (технической документации на приобретаемые компьютеры, правил внутреннего распорядка, которые приняты в определенной организации или учреждении, нормативно оформлены и подлежат доведению до сведения соответствующего персонала. Непосредственный объект преступления – это отношения по соблюдению правил эксплуатации ЭВМ, системы или их сети.

Квалифицирующий признак только один: если деяние повлекло тяжкие последствия или создало угрозу их наступления.

4) Ст. 274.1. Неправомерное воздействие на критическую информационную инфраструктуру РФ. Эта норма накладывает запрет на:

– создание, распространение и (или) использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для неправомерного воздействия на критическую информационную инфраструктуру РФ, в том числе для уничтожения, блокирования, модификации, копирования информации, содержащейся в ней, или нейтрализации средств защиты указанной информации (ч. 1);

– неправомерный доступ к охраняемой компьютерной информации, которая содержится в критической информационной инфраструктуре РФ, в том числе с использованием компьютерных программ либо иной компьютерной информации, предназначенных для неправомерного воздействия на критическую информационную инфраструктуру РФ, или иных вредоносных компьютерных программ, повлекший причинение вреда критической информационной инфраструктуре РФ (ч. 2);

– нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, которая содержится в критической информационной инфраструктуре РФ, или информационных систем, автоматизированных систем управления, информационно-телекоммуникационных сетей, сетей электросвязи, относящихся к критической информационной инфраструктуре РФ, либо правил доступа к указанной информации, информационно-телекоммуникационным сетям, информационным системам, автоматизированным системам управления, сетям электросвязи, повлекшее причинение вреда критической информационной инфраструктуре РФ (ч. 3).

Кроме того, предусмотрены квалифицирующие признаки: если вышеуказанные действия совершены группой лиц по предварительному

сговору или организованной группой, или лицом с использованием своего служебного положения (ч. 4), а также если они повлекли тяжкие последствия.

Таким образом, в России на сегодняшний день существует достаточно развитая правовая база в сфере регулирования информационной безопасности, позволяющая управлять современными процессами, обеспечивающими оборот информационных ресурсов от их создания до организации доступа к ним и защиты от несанкционированного использования.

ФСИН России является федеральным органом исполнительной власти, осуществляющим правоприменительные функции, функции по контролю и надзору в сфере исполнения уголовных наказаний в отношении осужденных, функции по содержанию лиц, подозреваемых либо обвиняемых в совершении преступлений, и подсудимых, находящихся под стражей, их охране и конвоированию, а также функции по контролю за поведением условно осужденных и осужденных, которым судом предоставлена отсрочка отбывания наказания. ФСИН России подведомственна Министерству юстиции Российской Федерации. Повышение эффективности управления уголовно-исполнительной системой, использование инновационных разработок и научного потенциала предполагают[17]:

– совершенствование ведомственного контроля, создание и использование комплексной системы непрерывного мониторинга и оценки деятельности учреждений и органов уголовно-исполнительной системы;

– регулярное проведение мониторинга состава осужденных и персонала в целях получения объективных данных для принятия решений о дальнейшем реформировании уголовно-исполнительной системы;

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

– интеграцию автоматизированных систем уголовно-исполнительной системы с автоматизированными системами судебных и правоохранительных органов;

– совершенствование инфраструктуры информационно телекоммуникационного и других видов обеспечения функционирования и развития системы передачи и обработки данных, систем информационной безопасности и защиты информации;

– создание резервного центра управления сетевыми ресурсами, позволяющего повысить надежность работы информационно телекоммуникационной сети, хранения и защиты информации;

– обеспечение пользователям информационными ресурсами уголовно-исполнительной системы возможности доступа к сети связи общего пользования, сетям взаимодействующих федеральных органов исполнительной власти на основе межведомственных регламентов и соглашений;

– интегрирование средств связи и передачи данных в телекоммуникационную инфраструктуру органов исполнительной власти, судебных и правоохранительных органов с учетом проблем труднодоступных районов России;

– предоставление осужденным и лицам, содержащимся под стражей, технической возможности использования широкого спектра телекоммуникационных услуг, в том числе средств видеоконференцсвязи, электронной почты и др.;

– дальнейшее развитие сети специальной связи в целях обеспечения информационной безопасности уголовно-исполнительной системы, участие в создании и развитии межведомственных сетей передачи шифрованной информации органов государственной власти, организация на их основе межведомственного электронного документооборота, комплексов информационного взаимодействия;

– активное использование научного потенциала научно исследовательских институтов, образовательных организаций высшего образования Федеральной службы исполнения наказаний и организаций дополнительного профессионального образования во взаимодействии с другими образовательными организациями высшего образования и научными организациями, обеспечение приоритетности диссертационных исследований, направленных на научный анализ актуальных проблем практической деятельности учреждений и органов уголовно-исполнительной системы, повышение требований к контролю качества образования;

– проведение научных исследований, соответствующих современному уровню развития пенитенциарных систем иностранных государств, на базе лабораторий, научных центров и других подразделений, сформированных по предусмотренным Концепцией направлениям развития уголовно исполнительной системы.

По мнению Черешкина Д. С., Вирткovского В. А., основными объектами защиты информации являются[18]:

– информационные ресурсы, содержащие сведения, отнесенные к государственной тайне, и конфиденциальную информацию;

– средства и системы информатизации (средства вычислительной техники, информационно-вычислительные комплексы, сети и системы), программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение), автоматизированные системы управления, системы связи и передачи данных, технические средства приема, передачи и обработки информации ограниченного доступа (звукозапись, звукоусиление, звукосопровождение, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки

[18] Концепция информационной безопасности Российской Федерации (проект): Препринт. / Под ред. Д. С. Черешкина и В. А. Вирткovского. – М.: Институт системного анализа РАН, 1994. – 44 с.

графической, смысловой и буквенно-цифровой информации), их информативные физические поля.

Техническое мероприятие – это мероприятие по защите информации, предусматривающее применение специальных технических средств, а также реализацию технических решений. Технические мероприятия направлены на закрытие каналов утечки информации путем ослабления уровня информационных сигналов или уменьшением отношения сигнал/шум в местах возможного размещения портативных средств разведки или их датчиков до величин, обеспечивающих невозможность выделения информационного сигнала средством разведки, и проводятся с использованием активных и пассивных средств.

С целью оптимизации видов информации, относящейся к конфиденциальной, Президент Российской Федерации своим Указом от 6 марта 1997 года № 188 утвердил Перечень сведений конфиденциального характера, в котором выделены шесть основных категорий информации[19]:

1. Персональные данные.
2. Тайна следствия и судопроизводства.
3. Служебная тайна.
4. Профессиональные виды тайн (врачебная, нотариальная, адвокатская и т.д.).
5. Коммерческая тайна.
6. Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

В настоящее время ни один из перечисленных институтов не урегулирован на уровне специального закона, что, естественно, не способствует улучшению защиты указанных сведений. Основную роль в

[19] Об утверждении перечня сведений конфиденциального характера: указ Президента РФ: текст с изменениями и дополнениями на 13 июля 2015 г. № 357 [принят 6 марта 1997 г. № 188] // Официальный интернет-портал правовой информации (www.pravo.gov.ru) 13 июля 2015 г.

создании правовых механизмов защиты информации играют органы государственной власти РФ.

Проникая во все сферы деятельности общества и государства, информация приобретает конкретные политические, материальные и стоимостные выражения. С учетом усиления роли информации на современном этапе, правовое регулирование общественных отношений, возникающих в информационной сфере, является приоритетным направлением процесса нормотворчества в Российской Федерации (РФ), целью которого является обеспечение информационной безопасности государства.

Для изучения данного вопроса следует рассмотреть следующую структуру нормативно-правовых актов, которые ориентированы на защиту информации в настоящее время:

– международные правовые акты;

– нормы Конституция Российской Федерации, используемые в сфере защиты информации (ст. 2, 23, 24, 29, 33, 41, 42, 44 Конституции РФ)[20];

– отдельные отрасли законодательства, акты которых посвящены вопросам защиты информации;

– отрасли законодательства, акты которых содержат в себе отдельные нормы, применяемые в области защиты информации и информационных технологий.

Конституция РФ является основным источником права в области обеспечения информационной безопасности в России. Согласно Конституции РФ:

– каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений (статья 23);

---

[20] 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.

– сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются (статья 24);

– каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом, перечень сведений, составляющих государственную тайну, определяется федеральным законом (статья 29);

– каждый имеет право на достоверную информацию о состоянии окружающей среды (статья 42).

Нормативно-правовую базу России в сфере безопасности информационной деятельности, которая непосредственно используется в УИС, может представить как совокупность законов:

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

В данном законе закреплены основные термины, используемые в данной сфере деятельности, определен правовой режим использования информации, работы с ней, закреплена ответственность в сфере защиты информации в системах ее обработки, закреплен порядок правовой защиты и гарантии реализации прав и ответственности субъектов информационных взаимоотношений, ограничительные меры и т. д. Эти положения являются основой всего законодательства в данной сфере жизнедеятельности.

2. Закон РФ от 21 июля 1993 г. № 5485-1 «О государственной тайне», используемый в УИС довольно часто, особенно в работе подразделений специального назначения, оперативного аппарата, отделов собственной безопасности, ГО и ЧС и других служб.

На основании ст. 1 данного Закона субъекты правоотношений в информационной сфере – это органы государственного управления, а также юридические лица (учреждения, предприятия и организации, независимо от их организационно-правовых форм деятельности и видов собственности).

Свое действие закон распространяет только на должностных лиц и граждан, взявших на себя обязательства либо обязанных выполнять

требования законодательства о государственной тайне по своему статусу. Физическое лицо на основании этой нормы представляет собой субъект данных правоотношений только в том случае, если в добровольном порядке имеет допуск к закрытым сведениям на договорной основе. В ином случае при наличии доступа к таким сведениям, это может быть расценено как нарушение норм законодательства.

Объекты правоотношений представляют собой сведения из внешнеполитической, разведывательной, военной, контрразведывательной, оперативно-розыскной и экономической областей государственной деятельности. В законе дано подробное описание этих сведений. В частности, в сферах техники, науки и экономики к государственной тайне относятся сведения:

– о научно-исследовательских, проектных и опытно-конструкторских работах, технологиях, которые имеют важное экономическое или оборонное значение;

– о средствах и методах защиты информации;

– о государственных программах и мероприятиях в области защиты государственной тайны.

Нормативно-правое регулирование порядка засекречивания сведений, содержащих государственную тайну, заключается в установлении следующих принципов:

– законность;

– обоснованность;

– своевременность.

Принцип законности определяет, что законом устанавливается перечень сведений, которые подлежат засекречиванию, так и перечень сведений, не подлежащих засекречиванию. Лица, виновные в нарушении законодательных норм, должностные лица могут быть привлечены к дисциплинарной, уголовной или административной ответственности.

Каждый гражданин имеет право обжаловать эти действия в суде.

Принцип обоснованности состоит в установлении целесообразности засекречивания конкретных сведений посредством экспертной оценки, основываясь на жизненно-важных интересах государства, общества и граждан.

Принцип своевременности заключается в том, что ограничения по распространению информации должны быть установлены не позднее момента их получения.

В российском законодательстве закреплены три степени секретности, им соответствуют определенные грифы для носителей информации: секретно, совершенно секретно, особой важности. Порядок определения степени и грифа устанавливается нормативным актом Правительства РФ, а именно это Правила отнесения сведений, составляющих государственную тайну, к различным степеням секретности[21]. Этот нормативный является сопутствующим Закону «О государственной тайне».

При работе с документами используется определенная структура объектов законодательства о государственной тайне.

1) На федеральном уровне сформирован перечень, который утвержден президентом РФ и подлежит открытому опубликованию. В нем также указываются федеральные органы управления, наделенные правомочиями по распоряжению конкретными сведениями.

2) В соответствии с общегосударственным перечнем, данными органами управления разрабатываются развернутые перечни и устанавливаются степени их секретности.

3) Отдельные перечни сведений по решению заказчиков также могут быть разработаны в целевых комплексных программах.

По причине того, что засекречивание информации, как следствие, приводит к ограничению прав собственника на пользование и

[21] Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности: постановление Правительства РФ: текст с изменениями и дополнениями на 30 октября 2021 г. № 1868 [принят 4 сентября 1995 г. № 870] // Официальный интернет-портал правовой информации (www.pravo.gov.ru) 30 октября 2021 г. 26 мая 2021 г.

распространение данных, то в законодательстве предписано за счет государства возмещение материального ущерба собственнику, при этом его размер определен в договоре между органом государственного управления и собственником, также в нем предусмотрено обязательство собственника информации по ее нераспространению. Возникновение конфликтных ситуаций решается в судебном порядке.

В законодательстве установлен механизм дополнения действующих перечней, если они не дают возможности идентификации или отнесения новых сведений к секретной информации. В такой ситуации администрация структуры-разработчика обеспечивает предварительное засекречивание и направляет в месячный срок уполномоченному должностному лицу, который утвердил конкретный перечень, предложения по его дополнению и применению, решение по которым принимается в трехмесячный срок.

3. Федеральный закон РФ от 28 декабря 2010 г. № 390-ФЗ «О безопасности»[22], который закрепляет правовые основы по обеспечению безопасности личности, общества и государства и определяющий систему безопасности и ее функции, а также в нем установлен порядок организации и финансирования органов обеспечения безопасности, надзора и контроля за законностью их деятельности.

Основными объектами безопасности являются: личность – ее права и свободы; общество – его материальные и духовные ценности; государство – его конституционный строй, суверенитет и территориальная целостность.

На основании этого Закона основным субъектом обеспечения безопасности является государство, которое осуществляет функции через органы законодательной, исполнительной и судебной властей. Государство, в нашем случае в лице сотрудников УИС, на основании действующего законодательства обеспечивает безопасность осужденных, заключенных под стражу, находящихся в исправительных учреждениях.

---

[22] О безопасности: федеральный закон: текст с изменениями и дополнениями на 9 ноября 2020 г. № 365-ФЗ [принят 28 декабря 2010 г. № 390-ФЗ] // Официальный интернет-портал правовой информации (www.pravo.gov.ru) на 9 ноября 2020 г.

Граждане, общественные и иные организации и объединения являются субъектами безопасности, обладают правами и обязанностями по участию в обеспечении безопасности в соответствии с законодательством РФ, законодательством республик в составе РФ, нормативными актами органов государственной власти и управления краев, областей, автономной области и автономных округов, принятыми в пределах их компетенции в данной сфере. Государство обеспечивает правовую и социальную защиту гражданам, общественным и иным организациям и объединениям, оказывающим содействие в обеспечении безопасности в соответствии с Законом.

Также в данном Законе применяется термин «угроза безопасности» – совокупность факторов и условий, которые создают опасность жизненно важным интересам личности, общества и государства.

Безопасность достигается путем проведения единой государственной политики в данной сфере, системой мер политического, экономического, организационного и иного характера. Для создания и поддержания необходимого уровня защищенности объектов безопасности в РФ разработана целая система правовых норм, которые регулируют отношения в области безопасности, определяют основные направления деятельности органов государственной власти и управления в этой сфере, формируют или реформируют органы обеспечения безопасности и механизм надзора и контроля за их деятельностью.

В ст. 2 данного Закона закреплены основные принципы обеспечения безопасности, которыми являются:

– законность;

– соблюдение баланса жизненно важных интересов личности, общества и государства;

– взаимная ответственность личности, общества и государства по обеспечению безопасности;

– интеграция с международными системами безопасности.

Не допускается при обеспечении безопасности ограничивать права и свободы граждан, за исключением случаев, предусмотренных законодательством. Содержание в МЛС является одним из таких случаев и не является нарушением Законов.

Осужденные, лица, заключенные под стражу, имеют право получать разъяснения по фактам ограничения их прав и свобод от государственных органов, в чьи функции входит обеспечение безопасности. По их требованию разъяснения должны быть даны в письменной форме и в установленные сроки.

4. Постановление Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»[23];

5. Постановление Правительства Российской Федерации от 16 апреля 2012 г. № 313 «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем»[24].

6. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»[25].

7. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к

---

[23] Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных: постановление Правительства Рос. Федерации от 1 ноября 2012 г. № 1119 // Собр. законодательства Рос. Федерации. – 2012. – № 45, ст. 6257.

[24] Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем: постановление Правительства: текст с изменениями и дополнениями на 28 декабря 2021 г. № 2518 [принят 16 апреля 2012 г. № 313] // Официальный интернет-портал правовой информации (www.pravo.gov.ru) 28 декабря 2021 г.

[25] О персональных данных: федеральный закон: текст с изменениями и дополнениями на 2 июля 2021 г. № 331-ФЗ [принят 27 июля 2006 г. № 152-ФЗ] // Официальный интернет-портал правовой информации (www.pravo.gov.ru) 2 июля 2021 г.

информации (далее – Концепция)[26] – идейная основа ряда существующих руководящих документов. Она включает в себя систему основных принципов, взглядов, закладывающихся в основу при решении проблем, возникающих при защите информации от несанкционированного доступа (далее – НСД).

В Концепции различают термины «средства вычислительной техники» (далее – СВТ) и «автоматизированная система» (далее – АС) по аналогии с тем, как в Европейских Критериях проводится деление на системы и продукты. Более конкретно, Концепция включает 2 отличающихся и относительно самостоятельных направления в проблеме защиты информации от НСД: направление, связанное с АС, и направление, которое связано с СВТ.

Их отличие появилось по той причине, что СВТ на рынок поставляются и разрабатываются только как элементы, из которых в последующем будут построены функционально ориентированные АС, при этом не решаются прикладные задачи, СВТ не содержат пользовательской информации.

При создании АС, кроме пользовательской информации, появляются такие характеристики АС, отсутствующие при разработке СВТ, как технология обработки информации, модель нарушителя, полномочия пользователей.

На сегодняшний день есть разные способы покушения на информационную безопасность – акустические, радиотехнические, программные и т. п. НСД среди них выделяется как «доступ к информации, нарушающий установленные правила разграничения доступа с использованием штатных средств, предоставляемых СВТ или АС. При этом

[26] Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации: утв. Решением Гостехкомиссии России 30 марта 1992 г. (неопубликованный акт).

штатные средства стоит понимать как совокупность микропрограммного, программного и технического обеспечения АС или СВТ»[27].

В Концепции сформулированы следующие принципы защиты информации от НСД:

1) Защита СВТ обеспечивается комплексом программно-технических средств.

2) Защита АС обеспечивается комплексом программно-технических средств и поддерживающих их организационных мер.

3) Защита АС должна быть обеспечена во всех режимах функционирования и на всех технологических этапах обработки информации, в том числе при проведении регламентных и ремонтных работ.

4) Программно-технические средства защиты существенно не должны негативно влиять на основные функциональные характеристики АС (возможность изменения конфигурации АС, быстродействие, надежность).

5) Оценка эффективности средств защиты – неотъемлемая часть работ по защите информации, которая осуществляется по методике, учитывающей совокупность технических характеристик оцениваемого объекта, в том числе практическую реализацию средств защиты и технические решения.

6) Защита АС должна предусматривать контроль эффективности средств защиты от НСД, который может осуществляться периодически, а может быть инициирован контролирующими органами или пользователем АС по мере необходимости.

Концепция ориентирована на защищенную физически среду, проникновение посторонних лиц в которую считается невозможным, на основании этого правонарушитель определяется как субъект с доступом к работе со штатными средствами АС и СВТ как части АС.

---

[27] Введение в специальность «Организация и технология защиты информации» по курсу «Теория и методология защиты информации» / под ред. Е. Л. Монаховой: метод. пособие. – Таганрог: Изд-во Таганрогского государственного радиотехнического университета, 2000. – С. 27.

Нарушители классифицируются по уровню возможностей, предоставляемых им штатными АС и СВТ. Выделяется 4 уровня этих возможностей.

Классификация является иерархической, т. е. каждый следующий уровень включает в себя функциональные возможности предыдущего.

Первый уровень определяет самый низкий уровень возможностей ведения диалога в АС – запуск задач (программ) из фиксированного набора, реализующих заранее предусмотренные функции по обработке информации.

Второй уровень определяется возможностью создания и запуска собственных программ с новыми функциями по обработке информации.

Третий уровень определяется возможностью управления функционированием АС, т. е. воздействием на базовое программное обеспечение системы и на состав и конфигурацию её оборудования.

Четвертый уровень определен объемом всех возможностей лиц, которые осуществляют проектирование, реализацию и ремонт технических средств АС до включения в состав СВТ собственных технических средств с новыми функциями по обработке информации.

Также Концепция включает наличие обеспечивающих средств для СРД, выполняющих функции:

– идентификацию и опознание (аутентификацию) субъектов и поддержание привязки субъекта к процессу, выполняемому для субъекта;

– регистрацию действий субъекта и его процесса;

– предоставление возможностей исключения и включения новых субъектов и объектов доступа, а также изменение полномочий субъектов;

– реакцию на попытки НСД, например, сигнализацию, блокировку, восстановление после НСД;

– тестирование;

– очистку оперативной памяти и рабочих областей на магнитных носителях после завершения работы пользователя с защищаемыми данными;

– учет выходных печатных и графических форм и твердых копий в АС;

– контроль целостности программной и информационной части как СРД, так и обеспечивающих ее средств.

В соответствии с Концепцией технические средства от НСД должны быть оценены по параметрам:

– степень полноты охвата ПРД реализованной СРД и ее качество;

– состав и качество обеспечивающих средств для СРД – гарантии правильности функционирования СРД и обеспечивающих ее средств.

Выводы по первой главе.

Наиболее важным является тот факт, что самая совершенная аппаратура не принесет положительных результатов без профессиональной, интеллектуальной деятельности сотрудников УИС. Необходимо применять и личностный метод защиты конфиденциальной служебной информации, так как специфика деятельности УИС выдвигает ряд требований к поведению сотрудников, особенно, по мнению автора данной работы, это касается сотрудников оперативных служб и специалистов службы ИТОСиВ.

Правовые мероприятия включают в себя исполнение существующих и разработку новых норм законодательства, которые обеспечивают правовую защиту конфиденциальной служебной информации от различного вида угроз и находятся под постоянным контролем государства.

Таким образом, мы видим, что положения, отраженные в российском законодательстве, регулирующие сферу обеспечения информационной безопасности, являются универсальными и применяются в УИС наравне с другими структурами и органами. Что касается совершенствования законодательства субъектов Российской Федерации, то оно направлено на формирование в рамках единой системы обеспечения информационной безопасности Российской Федерации региональных систем обеспечения информационной безопасности и защиты конфиденциальной служебной информации субъектов Российской Федерации.

Глава 2. ИСПОЛЬЗОВАНИЕ ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ В ОРГАНАХ И УЧРЕЖДЕНИЯХ ФСИН РОССИИ

2.1. Современные методики и специальные технические средства защиты конфиденциальной информации, используемые на объектах УИС

В России в последние годы выявлено и нейтрализовано свыше 50 миллионов компьютерных атак. Для сравнения в 2015 году их было 14,4 миллиона, – отметил секретарь Совета Безопасности РФ Патрушев Н.П[28]. По данным Совбеза, цель таких атак – получить информацию ограниченного доступа и нарушить режим функционирования технических средств. В то же время защищенность информационных систем от компьютерных атак и средств компьютерной разведки остается недостаточной и в большинстве случаев не отвечает существующим угрозам, – подчеркнул секретарь Совета Безопасности РФ. Также, по его словам, угрозу информационной безопасности несет несанкционированное подключение рабочих компьютеров к Интернету, низкая квалификация пользователей в области защиты информации, использование зарубежных информационных технологий и отсутствие разграничения информационных потоков.

Кроме того, отмечаются случаи передачи информации ограниченного распространения без соблюдения требований безопасности, а еще не хватает квалифицированного персонала, который обслуживает информационные системы органов власти. В то же время Патрушев напомнил, что согласно президентскому указу до конца 2017 года все государственные информационные системы и сети должны быть подключены к российскому государственному сегменту Интернета.

---

[28] Патрушев Н. П. Количество кибератак на сайты госорганов РФ выросло в четыре раза / Н. П. Патрушев // Российская газета. 2017. – 5 марта.

Рассматривая методы защиты информации в учреждениях и органах УИС, необходимо отметить, что в настоящее время имеются большие возможности по ее несанкционированному съему. Следовательно, при отсутствии должного внимания к защите каналов связи важная информация может стать достоянием злоумышленников.

Автор данной работы отмечает, что эффективная защита в уголовно-исполнительной системе конфиденциальной информации возможна лишь при условии, если соответствующие мероприятия будут носить всесторонний и непрерывный характер. Это достигается осуществлением совокупности мер по ее защите в ходе всего процесса подготовки, обсуждения, обработки, передачи и хранения такой информации.

Защита информации в целом представляет собой комплекс мероприятий организационного и технического характера. Методы защиты информации полностью зависят от факторов, обусловливающих их. К методам защиты информации можно отнести следующие:

– организационный, связанный с выработкой и применением конкретных методик проведения мероприятий по предотвращению утечки конфиденциальной информации;

– нормативно-правовой, опирающийся на соблюдение требований нормативных и правовых актов по хранению конфиденциальной информации;

– личностный, обусловленный морально-психологическими характеристиками конкретного лица;

– физический, связанный с расположением и устройством помещения или местности, где циркулирует конфиденциальная информация;

– технический, зависящий от наличия специальной техники и технологий защиты информации и владения сотрудниками навыками в их применении.

Проводя мероприятия по защите от несанкционированного доступа к информации, не следует стремиться обеспечить защиту всего здания от

технического проникновения. Главное – ограничить доступ в те места и к той технике, где сосредоточена конфиденциальная информация. Использование качественных замков, средств сигнализации, хорошая звукоизоляция стен, дверей, потолков и пола, звуковая защита вентиляционных каналов, отверстий и труб, проходящих через эти помещения, демонтаж излишней проводки, а также применение специальных устройств защиты в существенной мере затруднят или сделают бессмысленными попытки внедрения специальной техники съема информации.

Основными направлениями защиты информации от утечки по техническим каналам являются:

– предотвращение утечки обрабатываемой информации за счет побочных электромагнитных излучений и наводок, создаваемых функционирующими техническими средствами, а также за счет электроакустических преобразований;

– выявление внедренных на объекты и в технические средства электронных устройств перехвата информации (закладных устройств);

– предотвращение перехвата с помощью технических средств речевой информации из помещений и объектов.

Средства защиты информации – это совокупность инженерно-технических, электрических, электронных, оптических и других устройств и приспособлений, приборов и технических систем, а также иных вещных элементов, используемых для решения различных задач по защите информации, в том числе предупреждения утечки и обеспечения безопасности защищаемой информации.

В целом средства защиты информации в части предотвращения преднамеренных действий в зависимости от способа реализации можно разделить на группы:

Технические (аппаратные) средства защиты информации. Это различные по типу устройства (механические, электромеханические, электронные и др.), которые аппаратными средствами решают задачи защиты

информации, например, такую задачу, как защита помещения от прослушивания. Они либо препятствуют физическому проникновению, либо, если проникновение все же состоялось, доступу к информации, в том числе с помощью ее маскировки. Первую часть задачи решают замки, решетки на окнах, защитная сигнализация и др. Вторую - генераторы шума, сетевые фильтры, сканирующие радиоприемники и множество других устройств, «перекрывающих» потенциальные каналы утечки информации (защита помещения от прослушивания) или позволяющих их обнаружить.

Программные и технические средства защиты информации включают программы для идентификации пользователей, контроля доступа, шифрования информации, удаления остаточной (рабочей) информации типа временных файлов, тестового контроля системы защиты и др.

Смешанные аппаратно-программные средства защиты информации реализуют те же функции, что аппаратные и программные средства в отдельности, и имеют промежуточные свойства, такие как защита помещения от прослушивания.

Организационные средства защиты информации и технические средства защиты информации складываются из организационно-технических (подготовка помещений с компьютерами, прокладка кабельной системы с учетом требований ограничения доступа к ней и др.) и организационно-правовых (национальные законодательства и правила работы, устанавливаемые руководством конкретного предприятия).

Техническая защита информации как часть комплексной системы безопасности во многом определяет успешность ведения бизнеса. Основной задачей технической защиты информации является выявление и блокирование каналов утечки информации (радиоканал, ПЭМИН, акустические каналы, оптические каналы и др.). Решение задач технической защиты информации предполагает наличие специалистов в области защиты информации и оснащение подразделений специальной техникой обнаружения и блокирования каналов утечки. Выбор спецтехники для

решения задач технической защиты информации определяется на основе анализа вероятных угроз и степени защищенности объекта.

Блокираторы сотовой связи (подавители сотовых телефонов), в просторечье называемые глушителями сотовых – эффективное средство борьбы с утечкой информации по каналу сотовой связи. Суть работы глушителя сотовых сводиться к подавлению радиоканала трубка – база, в диапазоне которого работает блокиратор против утечки информации.

Глушители сотовых телефонов различают по стандарту подавляемой связи (AMPS/N-AMPS, NMT, TACS, GSM900/1800, CDMA, IDEN, TDMA, UMTS, DECT, 3G, универсальные), мощности излучения, габаритам. Как правило, при выборе мощности излучения выпускаемых глушителей сотовых учитывается безопасность находящихся в защищаемом помещении людей, поэтому радиус эффективного подавления составляет от нескольких метров до нескольких десятков метров. Применение блокираторов сотовой связи должно быть строго регламентировано, так как может создать неудобства для третьих лиц.

В территориальных органах ФСИН России на примере УФСИН России по Тюменской области проводятся ряд мероприятий по защите информации согласно нормативно-правовых актов, ведомственных приказов и наставлений[29]. Некоторые мероприятия требуют правильного выбора специальных технических средств по защите конфиденциальной информации – в этом они руководствуются своим практическим опытом и опытом своих коллег, и выбирают продукцию надежных производителей. В этих вопросах себя с положительной стороны зарекомендовал ряд организаций:

– Группа компаний «МАСКОМ»;

– НПО «АННА»;

– Компания «Сюртель»;

[29] Материалы преддипломной практики в ФКУ ЛИУ-19 УФСИН России по Тюменской области / М. Е. Батухтин (неопубликованный акт).

Фирма «Сюртель», опираясь на 20 летний опыт в создании технических средств защиты информации, применив научный системный подход к проблеме и новейшие цифровые технологии, разработала и развернула промышленное производство технических систем, полностью отвечающих как новым требованиям ФСТЭК и ФСБ по защите информации, так и нормам Государственного комитета по радиочастотам, СанПин, требованиям электромагнитной совместимости. Для предотвращение утечки обрабатываемой информации за счет ПЭМИН (побочные электромагнитные излучения и наводки) от технических средств, обрабатывающих служебную (секретную) информацию предлагает ряд систем «Шифон» и «Шагрень» в которых были применены общие структурные, функциональные и эргономические принципы конструирования средств защиты информации, сочетающие как традиционные и проверенные временем наработки, так и уникальные новые решения, которые в настоящее время прошли процедуру патентования. Заложенный при разработке конструктивный технический задел, значительно перекрывающий действующие на данный период требования и нормы, позволяет увеличить срок службы средств защиты информации (далее – СЗИ) до 10 лет и более.

Цифровые технологии управления и контроля за параметрами СЗИ значительно упрощают процессы настройки и обслуживания систем, что позволит в дальнейшем эти процессы автоматизировать.

Функциональные характеристики систем:

– конструктивно каждая система состоит из центрального генераторного блока формирователей шумового сигнала и подключаемых к выходам генератора различных оконечных устройств активной защиты;

– центральный генераторный блок представляет собой несколько размещённых в одном унифицированном корпусе независимых генераторов маскирующего шума с цифровым многополосным частотным эквалайзером и регулировками выходных уровней в пределах не менее 30 дБ;

– возможность соединения по сети Ethernet позволяет объединять СЗИ в единую IP–сеть для формирования распределенной системы защиты информации любого объекта для мониторинга и управления с одного операторского места посредством специализированного программного обеспечения УСЗИ «Шлюз»;

– контроль и индикация нормального режима работы или возникновения аварийной ситуации (визуальная, звуковая, текстовая) позволяют получать информацию о функционировании системы в режиме реального времени на панели управления генераторным блоком или мониторе персонального компьютера;

– автоматическая непрерывная самодиагностика системы;

– интегрированный счётчик наработки системы в режиме генерации помех с хранением данных в энергонезависимой памяти;

– запоминание настроек в энергонезависимой памяти. Обнаружение и защита от несанкционированного доступа к настройкам системы (цифровой пароль);

– работа в необслуживаемом круглосуточном режиме работы;

– электропитание систем сетевое 220 В 50 Гц или через резервный источник постоянного тока 12 В/1,5А.

НПО «АННА» предоставляет аппаратуру защиты от акустической разведки «Соната АВ» (Модель 3М) – это система виброакустической и акустической защиты с централизованным возбуждением излучателей (ЦВИ) «Соната-АВ» модель 3М, предназначена для активной защиты речевой информации в выделенных (защищаемых) помещениях, от утечки по акустическим и виброакустическим каналам. Сертификат ФСТЭК удостоверяет, что система виброакустической и акустической защиты «Соната-АВ» модель 3М, является техническим средством защиты акустической речевой информации, обрабатываемой в выделенных помещениях до 1 категории включительно, от утечки по акустическому и виброакустическому каналам путем постановки помех в диапазоне частот 90-

11200 Гц не создает технических каналов утечки информации и может устанавливаться в выделенных помещениях до 1 категории включительно без применения дополнительных мер защиты. Система виброакустической и акустической защиты «Соната-АВ» (модель 3М) сертифицирована в системе в системе сертификации ГОСТ Р Госстандарта России и на него есть Санитарно-эпидемиологические заключения Роспотребнадзора России.

Устройства для защиты линий электропитания, заземления от утечки информации «Соната-РС1» (сертифицировано ФСТЭК) и «Соната-РС2» (сертифицировано ФСТЭК) предназначены для защиты объектов ВТ (объектов вычислительной техники) от утечки информации за счет наводок на линии электропитания и заземления и могут использоваться в выделенных помещениях до 1 категории включительно.

Также компания «Сюртель» предлагает систему «Secret Net» – это сертифицированное средство защиты информации от несанкционированного доступа на рабочих станциях и серверах, которое предназначено для защиты информации, составляющей коммерческую или государственную тайну или относящейся к персональным данным. Является эффективным средством защиты от внутренних (инсайдерских) угроз, может применяться как на автономных станциях, так и в информационных сетях.

Преимущества СЗИ от НСД «Secret Net»:

1) Сертифицированное средство защиты «Secret Net» позволяет привести автоматизированные системы в соответствие с требованиями регулирующих документов. Сертификаты ФСТЭК России позволяют использовать «Secret Net» для защиты:

– конфиденциальной информации и государственной тайны в автоматизированных системах до класса 1Б включительно;

– информационных систем обработки персональных данных до класса К1 включительно.

2) Надежность и масштабируемость «Secret Net» обеспечивает защиту отдельных рабочих станций в небольших организациях и вычислительных

инфраструктур класса Enterprise. Сетевой вариант «Secret Net» может быть успешно развернут в сложной доменной сети (domain tree/forest) с большим количеством филиалов.

3) Гибкая ценовая политика. Комплектность поставки зависит от размера защищаемой инфраструктуры и требований по безопасности.

4) Удобство администрирования. Централизованное управление политиками безопасности и аудита, средства оперативного управления интегрированы со встроенными средствами управления операционных систем.

Профессиональный детектор нелинейных переходов («нелинейный локатор») NR-T предназначен для обследования элементов строительных конструкций и предметов интерьера. Применяется для выявления и локализации скрыто установленных средств негласного съёма информации, в том числе аппаратуры, содержащей полупроводниковые радиоэлементы. При этом не имеет значения, находятся ли эти устройства в режиме передачи, выключенном или сторожевом режимах. Высокий энергетический потенциал позволяет использовать детектор дистанционного обнаружения, самодельных взрывных устройств с приёмниками дистанционного управления или электронными таймерами.

Отличительные особенности:

поиск электронных средств связи (СИМ-карт, миниатюрных средств звукозаписи, сотовых телефонов, радиостанций) в местах, где пользование ими запрещено (СИЗО, места лишения свободы);

выявление средств связи (сотовых телефонов, радиостанций) и других радиоэлектронных устройств независимо от их функционального состояния «включено/выключено», в сторожевом или ждущем режиме;

Преимущества:

эффективно обнаруживает малоразмерные цели (СИМ-карты, миниатюрные электронные устройства);

повышенная помехоустойчивость к откликам от строительных конструкций и элементов интерьера (контакты МОМ);

дополнительно усиленные разъемные соединения, дополнительные меры по защите от влаги и коррозии для сложных условий эксплуатации;

облегченная батарея повышенной емкости, встроенная в блок приемопередатчика, продолжительное время непрерывной работы без замены источника питания;

специальный подсумок для размещения аппаратуры на теле оператора.

– Современный дизайн и совершенная эргономика;

– Простота управления;

– Высокое качество и надёжность компонентов и блоков;

– Высокая помехозащищённость, абсолютная невосприимчивость к сигналам сотовой связи любых стандартов;

– Полное отсутствие внутренних аппаратных помех.

Акустический сейф «Ларец 4» предназначен для защиты речевой информации, циркулирующей в помещении, от перехвата с использованием телефонов сотовой связи путем создания в звукоизолирующем контейнере нормированного отношения сигнал/помеха на входе приемного датчика (микрофона) сотового телефона.

Устройство обеспечивает на входах приемников телефонов сотовой связи нормированное отношение акустическая помеха/сигнал в октавных частотных полосах.

Конструкция устройства рассчитана на размещение 4 телефонов сотовой связи.

Уровень акустической помехи на расстоянии 0,5 м от устройства не превышает предельного спектра, соответствующего ПС-40.

Диапазон частот маскирующей помехи 175 – 10000 Гц.

Устройство не влияет на работоспособность телефонов сотовой связи в штатных режимах.

Устройство обеспечивает отключение акустической шумовой помехи при открывании контейнера.

Устройство обеспечивает два режима световой индикации при открытом и закрытом контейнере.

Питание устройства осуществляется от сети переменного тока частотой 50 Гц и напряжением (220±22) В.

Рассмотрим организационные аспекты защиты информации в ФКУ ЛИУ №19 УФСИН России по Тюменской области[30].

На 2016 г. – по штату численность сотрудников 73 человека, фактически 70 недокомплект 3, из них количество женщин 11, декретный отпуск 1, командировка 0, стажеры 0.

На 2017 г. – по штату численность 73 человека, по списку 67, недокомплект 6, из них количество женщин 9, декретный отпуск 1, командировка 0, стажеры 0.

На 2018 г. – по штату численность 73 человека, фактически 71 недокомплект 2, из них количество женщин 14, декретный отпуск 1, командировка 0, стажеры 2.

На 2019 г. – по штату численность 73 человека, фактически 72 недокомплект 1, из них количество женщин 14, декретный отпуск 0, командировка 0, стажеры 1.

На 2020 г. – по штату численность 73 человека, фактически 73 недокомплект 0, из них количество женщин 14, декретный отпуск 0, командировка 0, стажеры 0.

На 2021 г. – по штату численность 73 человека, фактически 73 недокомплект 0, из них количество женщин 14, декретный отпуск 0, командировка 0, стажеры 0.

За 2021 год в ФКУ ЛИУ №19 не было выявлено нарушений должностных обязанностей при несении службы сотрудниками отдела

---

[30] Материалы преддипломной практики в ФКУ ЛИУ-19 УФСИН России по Тюменской области / М. Е. Батухтин (неопубликованный акт).

охраны в области защиты сведений конфиденциального характера. Для этого используются технические средства. В некоторых рабочих помещениях размещены устройства защиты объектов информатизации и системы виброакустической и акустической защиты в целях недопущения утечки конфидециальнной информации. Например «Соната-Р2» предназначено для защиты объектов ВТ (вычислительной техники) до 1-й категории включительно от утечки по каналам побочных электромагнитных излучений и наводок на линии электропитания и заземления, инженерные коммуникации и линии вспомогательных технических средств или системы виброакустической и акустической защиты выделенных помещений до 1 категории «Соната-АВ 2Б» ее основная особенность – отсутствие общего для всех излучателей генераторного блока: генераторы шумового сигнала встроены непосредственно в каждый излучатель.

Система «Камертон-5» предназначена для обеспечения защиты акустической речевой информации от утечки по акустическому и вибрационному каналам, за счет акустоэлектрических преобразований во вспомогательных технических средствах и системах, блокирует применение направленных и лазерных микрофонов.

Имеется возможность создания физических (механических) препятствий на пути проникновения к носителям информации (решетки, сейфы, металлические двери, жалюзи на стеклах, замки и др.).

Отметим, что к методам средств защиты конфиденциальной информации можно отнести разграничение доступа, шифрования защищаемых данных, защита программ от несанкционированного использования, контроль целостности информации, организация пропускного режима.

Важной является и процедура прохождения соответствия требования безопасности объекта охраны УИС, которая включает в себя:

– Проверку соответствия представленных данных реальным условиям размещения и эксплуатации объекта информатизации.

– Изучение технологического процесса обработки и хранения защищаемой информации, анализ информационных потоков, каналов утечки и угроз безопасности информатизации;

– Оценку состояния организации работ и выполнения организационно-технических требований по защите информации.

– Испытания на соответствие требованиям по защите информации от утечки за счет побочных электромагнитных излучений и радиоизлучений.

– Проверку выполнения требований по защите информации от утечки по цепям заземления и электропитания и за счет изменения тока потребления, обусловленного обрабатываемыми техническими средствами информативными сигналами.

– Проверку выполнения требований по отсутствию в технических средствах специальных электронных устройств перехвата информации.

При аттестации объекта информатизации подтверждается его соответствие требованиям по защите информации от несанкционированного доступа.

2.2. Требования к эксплуатации технических средств по защите конфиденциальной служебной информации в учреждениях и органах ФСИН России и порядок аттестации объектов УИС по требованиям информационной безопасности

Аттестация объектов информатизации – это комплекс организационно-технических мероприятий, в результате которых посредством специального документа – «Аттестата соответствия» подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации, утверждённых ФСТЭК России.

Аттестация предусматривает комплексную проверку (аттестационные испытания) защищаемого объекта информатизации в реальных условиях

эксплуатации с целью оценки соответствия применяемого комплекса мер и средств защиты требуемому уровню безопасности информации.

Обязательной аттестации подлежат объекты информатизации, предназначенные для обработки информации, составляющей государственную тайну, управления экологически опасными объектами, ведения секретных переговоров. В остальных случаях аттестация является добровольной и может осуществляться по инициативе заказчика или владельца объекта информатизации.

Аттестация по требованиям безопасности информации предшествует началу обработки подлежащей защите информации и вызвана необходимостью официального подтверждения эффективности комплекса используемых на конкретном объекте информатизации мер и средств защиты информации.

При аттестации объекта информатизации подтверждается его соответствие требованиям по защите информации от несанкционированного доступа, в том числе от компьютерных вирусов, от утечки за счёт побочных электромагнитных излучений и наводок при специальных воздействиях на объект (высокочастотное навязывание и облучение, электромагнитное и радиационное воздействие), от утечки или воздействия на неё за счёт специальных устройств, встроенных в объекты информатизации. После утверждения заключения по результатам аттестации оформляется и выдаётся заявителю «Аттестат соответствия».

Наличие на объекте информатизации действующего «Аттестата соответствия» даёт право обработки информации с уровнем секретности (конфиденциальности) и на период времени, установленными в «Аттестате соответствия». Рассмотрим виды специальных работ проводимые лицензированными организациями на объектах ФСИН России:

– специальные обследования помещений целью проведения специального обследования является поиск с помощью специальной техники возможно внедрённых конкурирующими предприятиями или

злоумышленниками устройств съёма информации («закладных устройств»), выявление каналов возможной утечки информации, обусловленных особенностями ограждающих конструкций помещений и проходящих в них коммуникаций, определение зоны безопасности защищаемого помещения, а также выдачей рекомендаций по созданию или доработке существующей системы защиты информации, циркулирующей на объекте. Перечень проводимых работ, выполняемых при специальных обследованиях, зависит от категории защищаемых помещений. Специальные обследования могут выполняться периодически или по отдельным заявкам. Специальное обследование помещений (выделенных для проведения закрытых мероприятий) является сложным организационно-техническим мероприятием;

– специальные проверки технических средств целью проведения специальной проверки является поиск возможно внедрённых в защищаемые технические средства и изделия специальных радиоэлектронных средств перехвата ведущихся в выделенном (защищаемом) помещении разговоров или обрабатываемой информации ограниченного доступа, ее разрушения или вывода технических средств из строя. Специальная проверка проводится, как правило, в лабораторных условиях перед установкой технических средств в защищаемое помещение. По результатам специальной проверки технических средств по выявлению специальных электронных устройств перехвата информации составляется акт, на основании которого заказчику выдается заключение;

– специальные исследования технических средств целью специальных исследований является проверка технических средств на соответствие требованиям по защите информации от возможной утечки по техническим каналам с выдачей соответствующих рекомендаций по усилению защиты. Специальные исследования технического средства проводится в лабораторных условиях перед его установкой в выделенное (защищаемое) помещение и (или) непосредственно в самом помещении после завершения

монтажа и настройки на месте установки. Периодически могут проводиться контрольные специальные исследования технических средств.

По результатам проведения специальных исследований оформляется протокол и предписание на эксплуатацию технического средства, в которых сформулированы требования по размещению исследуемого технического средства, а также требования по применению средств пассивной и активной защиты, при выполнении которых утечка информации по исследуемым каналам будет исключена.

В целях решения своих задач более оперативно в области защиты информации ФСИН России создали свои лаборатории и отделы успешно прошедших испытания в надзорных органах России имеющие право на выдачу лицензий и свидетельств, и стали способны профессионально решать задачи по аттестации ведомственных объектов информатизации. К тому времени прошли лицензирование и получили аттестат аккредитации две ведомственные лаборатории технической защиты информации – федеральное казенное учреждение «Научно-исследовательский институт информационных технологий Федеральной службы исполнения наказаний» ФКУ НИИИТ ФСИН России (г. Тверь) и федеральное казенное учреждение «Главный центр инженерно-технического обеспечения и связи Федеральной службы исполнения наказаний» ФКУ ГЦИТОС ФСИН России (г. Москва) и 9 его филиалов в субъектах РФ. Создание собственных аттестационных лабораторий позволило проводить весь комплекс аттестационных работ ведомственных объектов информатизации собственными силами и в конечном итоге, привести к существенной экономии финансовых средств при более оперативном решении самых неотложных задач по аттестации объектов информатизации без привлечения сторонних организаций.

Работы по аттестации АС включают в себя:

– анализ и оценка исходных данных;

– проверка соответствия представленных исходных данных реальным условиям размещения и эксплуатации объекта информатизации;

– изучение (проверка) технологического процесса обработки и хранения защищаемой информации, анализ информационных потоков, каналов утечки и угроз безопасности информатизации;

– оценка (проверка) состояния организации работ и выполнения организационно-технических требований по защите информации;

– испытания АС на соответствие требованиям по защите информации от утечки за счет побочных электромагнитных излучений и радиоизлучений;

– испытания АС на соответствие требованиям по защите информации от утечки за счет наводок на вспомогательные средства и системы;

– проверка выполнения требований по защите информации от утечки по цепям заземления и электропитания и за счет изменения тока потребления, обусловленного обрабатываемыми техническими средствами информативными сигналами;

– комплексные испытания АС на соответствие требованиям по защите информации от утечки по техническим каналам;

– разработка заключения по результатам испытаний на соответствии требований по защите информации от утечки по техническим каналам;

– проверка выполнения требований по отсутствию в технических средствах специальных электронных устройств перехвата информации;

– испытания АС на соответствие требованиям по защите информации от несанкционированного доступа в части испытаний подсистемы управления доступом;

– разработка заключения по результатам испытаний на соответствие требований по защите информации от несанкционированного доступа;

– подготовка отчетной документации и оценка результатов испытаний АС.

Прохождение аттестации на объектах информатизации органов и учреждений УИС ведомственными лабораториями и отделами ТЗИ по мнению ведомственных специалистов делается более оперативно и с наименьшими силами и финансовыми затратами которые оплачиваются

исполнителю (фирме) оказанных услуг. В настоящее время ФСТЭК России выдано более 4000 лицензий на деятельность по технической защите информации и на деятельность по разработке и/или производству средств защиты конфиденциальной информации.

При эксплуатации новой техники по защите информации привлекаются более подготовленные сотрудники, которые осуществляют проверку технического состояния, установку, наладку и регулировку аппаратуры и приборов, их профилактические осмотры и текущий ремонт.

Выполняют работы по эксплуатации средств защиты и контроля информации, следят за работой аппаратуры и другого оборудования.

Ведут учет работ и объектов, подлежащих защите, установленных технических средств, журналы нарушений их работы, справочники.

Готовят технические средства для проведения всех видов плановых и внеплановых контрольных проверок, аттестации оборудования, а также в случае необходимости к сдаче в ремонт.

Проводят наблюдения, выполняет работу по оформлению протоколов специальных измерений и другой технической документации, в том числе отчетной, связанной с эксплуатацией средств и контроля информации. Выполняют необходимые расчеты, анализирует и обобщает результаты, составляет технические отчеты и оперативные сведения.

Определяют причины отказов в работе технических средств, готовит предложения по их устранению и предупреждению, обеспечению высокого качества и надежности используемого оборудования, повышению эффективности мероприятий по контролю и защите информации.

Участвуют во внедрении разработанных технических решений и проектов, оказании технической помощи при изготовлении, монтаже, наладке, испытаниях и эксплуатации проектируемой аппаратуры.

В рамках проведения Всероссийского семинара-совещания[31] с руководителями служб делопроизводства и сотрудниками подразделений по защите государственной тайны учреждений и органов уголовно-исполнительной системы проведены лекционные занятия по теме «Работа с обращениями граждан, в том числе осужденных и лиц, содержащихся под стражей», «Нормативно-правовое регулирование», «Работа в СЭД».

В учреждениях ФСИН России должны применяться только сертифицированные технические средства по защите информации, под сертификацией понимается форма осуществляемого органом по сертификации подтверждения соответствия объектов требованиям технических регламентов положениям стандартов, сводов правил или условиям договоров согласно Федерального закона от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании»[32]. Сертификация средств защиты информации прежде всего подразумевает проверку их качественных характеристик для реализации основной функции – защиты информации на основании государственных стандартов и требований по безопасности информации. Статья 5 Федерального закона от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании» ставит особняком вопросы технического регулирования в отношении оборонной продукции (работ, услуг), поставляемой по государственному оборонному заказу, продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа, продукции (работ, услуг), сведения о которой составляют государственную тайну. Тем самым, различные виды сведений, отнесенных к

---

[31] Доклад о результатах и основных направлениях деятельности на 2015 – 2017 годы Федеральной службы исполнения наказаний [Электронный ресурс] // ФСИН России. Главная. Статистические данные: офиц. сайт. 20.03.2017. – Режим доступа: https://fsin.gov.ru/structure/inspector/iao/statistika/Kratkaya%20har-ka%20UIS (дата обращения: 20.03.2022).

[32] О техническом регулировании: федеральный закон: текст с изменениями и дополнениями на 2 июля 2021 г. № 351-ФЗ [принят 27 декабря 2002 г. № 184-ФЗ] // Официальный интернет-портал правовой информации (www.pravo.gov.ru) 2 июля 2021 г.

категории ограниченного доступа, предполагают наличие нормативных документов для соответствующих средств защиты информации. Так, например, закон Российской Федерации от 21 июля 1993 г. № 5485-I «О государственной тайне» определяет сертификацию как единственную форму оценки соответствия средств защиты информации. Статья 28 Закона гласит, что средства защиты информации должны иметь сертификат, удостоверяющий их соответствие требованиям по защите сведений соответствующей степени секретности. При этом организация сертификации средств защиты информации возлагается на федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации, федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности и федеральный орган исполнительной власти, уполномоченный в области обороны, в соответствии с функциями, возложенными на них законодательством Российской Федерации.

Каждый экземпляр сертифицированного средства защиты информации имеет пакет документов государственного образца о том, что данный продукт является сертифицированным, включая голографический специальный защитный знак соответствия с уникальным номером, который идентифицирует данный экземпляр средства защиты информации в системе государственного учета сертифицированных продуктов.

Выводы по 2 главе.

Контроль сертификации средств защиты информации и их правильная эксплуатация даёт главную цель, а именно создания надежной «бесперебойной» системы защиты информации в служебной деятельности служб по технической защите информации.

Таким образом, следует подчеркнуть, что организационные мероприятия по совершенствованию комплексного обеспечения информационной безопасности на объектах УИС могут состоять в следующем:

– для каждой информационной системы, используемой в пенитенциарных учреждениях, на этапе ее создания или модернизации должна быть разработана модель угроз, базирующаяся на основе методов математического моделирования с привлечением экспертных оценок;

– помещения, в которых размещены объекты информатизации, должны соответствовать требованиям по обеспечению их сохранности, пожарной безопасности, а также защиты от несанкционированного проникновения посторонних лиц;

– при обработке информационных потоков должно быть обеспечено проведение мероприятий, направленных на предотвращение несанкционированного доступа к конфиденциальной служебной информации или передача их лицам, не имеющим права доступа к такой информации, а также должен повсеместно осуществляться контроль за обеспечением информационной защиты;

– для обеспечения сохранности информационных ресурсов информационной системы органа или учреждения УИС должно производиться их резервное копирование на учтенный материальный носитель, обеспечивающее возможность восстановления содержащихся в информационной системе сведений. Порядок и периодичность проведения резервного копирования информации определяются ведомственными документами.

Возрастающая роль специальных технических средств в деятельности правоохранительных органов, накопленный положительный опыт по их применению создают предпосылки для научного осмысления и совершенствования правовой основы применения специальной техники в обеспечении защиты конфиденциальной служебной информации.

Заключение

Одной из значимых трудностей внедрения в деятельность УИС новых информационных технологий информации считается применение в деятельности ФСИН конфиденциальной информации, к которой предъявляется условие не передавать подобную информацию третьим лицам в отсутствие согласия её владельца, а кроме того её защита с применением специальных технических средств и организационных мер по ограничению беспрепятственного допуска к информации.

В результате проведённого исследования можно сделать ряд выводов.

Во-первых, проблемы, связанные с повышением безопасности информационной сферы в УИС России, являются сложными, многоплановыми и взаимосвязанными. Они требуют постоянного, неослабевающего внимания со стороны государства и персонала учреждения. Развитие информационных технологий побуждает к постоянному приложению совместных усилий по совершенствованию методов и средств, позволяющих достоверно оценивать угрозы безопасности информационной сферы и адекватно реагировать на них.

Во-вторых, предотвращение несанкционированного доступа к конфиденциальной информации, циркулирующей в телекоммуникационных сетях является важной задачей обеспечения безопасности служебной информации.

Защите информации в последнее время уделяется все большее внимание на самых различных уровнях – государства, общества и личности.

Можно выделить несколько основных задач, решение которых в информационных системах и телекоммуникационных сетях обеспечивает защиту информации. Это:

– организация доступа к информации только допущенных к ней лиц;

– подтверждение истинности информации;

– защита от перехвата информации при передаче ее по каналам связи;

– защита от искажений и ввода ложной информации.

Таким образом, в работе исследованы и проанализированы современные требования к организации защиты конфиденциальной служебной информации, рассмотрены критерии и технологии построения и использования систем защиты информационных ресурсов учреждениях ФСИН России, на основе анализа современных технических средств и информационных технологий в области защиты конфиденциальной служебной информации, даны рекомендации по рационализации существующей в учреждениях и органах УИС системы защиты информационных ресурсов. Так как на сегодняшний день «информация» во УИС может иметь несколько уровней значимости, важности, ценности, данный факт предусматривает наличие нескольких уровней ее конфиденциальности. Наличие разных уровней доступа к информации предполагает различную степень обеспечения каждого из свойств безопасности информации – конфиденциальность, целостность и доступность. Приобретение конкретным учреждением или централизованная поставка в учреждения УИС сертифицированных специальных технических средств защиты информации у проверенных отечественных изготовителей позволяет службам по защите информации более качественно и оперативно выполнять свои служебные обязанности в деле защиты государственной тайны.

В заключение отметим, что простой набор мер и специальных технических средств защиты информации нейтрализует лишь отдельные угрозы ее безопасности, оставляя бреши для внутренних и внешних угроз.

Только постоянно развивающаяся ведомственная система информационной безопасности может сдержать натиск непрерывно совершенствующихся средств и методов преступного посягательства на безопасность информации.

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. Уголовный кодекс Российской Федерации: федеральный закон: текст с изменениями и дополнениями на 25 марта 2022 г. № 63-ФЗ [принят 13 июня 1996 г. № 63-ФЗ] // Официальный интернет-портал правовой информации (www.pravo.gov.ru) 25 марта 2022 г.

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

4. Об информации, информационных технологиях и защите информации: федеральный закон: текст с изменениями и дополнениями на 30 декабря 2021 г. № 441-ФЗ [принят 27 июля 2006 г. № 149-ФЗ] // Официальный интернет-портал правовой информации (http://pravo.gov.ru) 30 декабря 2021 г.

5. О государственной тайне: закон: текст с изменениями и дополнениями на 11 июня 2021 г. № 170 ФЗ [принят 21 июля 1993 № 5485-115] // Официальный интернет-портал правовой информации (www.pravo.gov.ru) 11 июня 2021 г.

6. О безопасности: федеральный закон: текст с изменениями и дополнениями на 9 ноября 2020 г. № 365-ФЗ [принят 28 декабря 2010 г. № 390-ФЗ] // Официальный интернет-портал правовой информации (www.pravo.gov.ru) на 9 ноября 2020 г.

7. О техническом регулировании: федеральный закон: текст с изменениями и дополнениями на 2 июля 2021 г. № 351-ФЗ [принят 27 декабря 2002 г. № 184-ФЗ] // Официальный интернет-портал правовой информации (www.pravo.gov.ru) 2 июля 2021 г.

8. О персональных данных: федеральный закон: текст с изменениями и дополнениями на 2 июля 2021 г. № 331-ФЗ [принят 27 июля 2006 г. № 152-ФЗ] // Официальный интернет-портал правовой информации (www.pravo.gov.ru) 2 июля 2021 г.

9. Об утверждении Доктрины информационной безопасности Российской Федерации: указ Президента РФ от 05 декабря 2016 г. № 646 // Официальный интернет-портал правовой информации (www.pravo.gov.ru) 5 декабря 2016г.

10. Вопросы Федеральной службы исполнения наказаний: указ Президента РФ: текст с изменениями и дополнениями на 11 апреля 2022 г. № 201 [принят 13 октября 2004 г. № 1314] // Официальный интернет-портал правовой информации (www.pravo.gov.ru) 11 апреля 2022 г.

11. Об утверждении перечня сведений конфиденциального характера: указ Президента РФ: текст с изменениями и дополнениями на 13 июля 2015 г. № 357 [принят 6 марта 1997 г. № 188] // Официальный интернет-портал правовой информации (www.pravo.gov.ru) 13 июля 2015 г.

12. О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы: указ Президента РФ [принят 2 июля 2021 г. № 400] // Официальный интернет-портал правовой информации (www.pravo.gov.ru) 10 мая 2017 г.

13. О Стратегии национальной безопасности Российской Федерации: указ Президента РФ: [принят 2 июля 2021 г. № 400] // Официальный интернет-портал правовой информации (www.pravo.gov.ru) 3 июля 2021 г.

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

Правительства РФ от 29 апреля 2021 г. № 1138-р // Официальный интернет-портал правовой информации (www.pravo.gov.ru) 17 мая 2021 г.

15. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных: постановление Правительства Рос. Федерации от 1 ноября 2012 г. № 1119 // Собр. законодательства Рос. Федерации. – 2012. – № 45, ст. 6257.

16. Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем: постановление Правительства: текст с изменениями и дополнениями на 28 декабря 2021 г. № 2518 [принят 16 апреля 2012 г. № 313] // Официальный интернет-портал правовой информации (www.pravo.gov.ru) 28 декабря 2021 г.

17. Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности: постановление Правительства РФ: текст с изменениями и дополнениями на 30 октября 2021 г. № 1868 [принят 4 сентября 1995 г. N 870] // Официальный интернет-портал правовой информации (www.pravo.gov.ru) 30 октября 2021 г.

18. Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности: постановление Правительства РФ: текст с изменениями и дополнениями на 30 октября 2021 г. № 1868 [принят 4 сентября 1995 г. № 870] // Официальный интернет-портал правовой информации (www.pravo.gov.ru) 30 октября 2021 г. 26 мая 2021 г.

19. О внесении изменений в Устав федерального казенного учреждения «Главный центр инженерно-технического обеспечения и связи Федеральной службы исполнения наказаний: приказ ФСИН России от 26 ноября 2013 г. № 712 (неопубликованный акт).

20. О внесении изменений в штатные расписания учреждений, непосредственно подчиненных Федеральной службе исполнения наказаний: приказ ФСИН России от 21 мая 2014 г. № 257 (неопубликованный акт).

21. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации: утв. Решением Гостехкомиссии России 30 марта 1992 г. (неопубликованный акт).

22. Концепция национальной безопасности Российской Федерации: утв. указом Президента РФ от 17 декабря 1997 № 1300 // Российская газета. – 1997. – № 247 (утратил силу).

23. Концепция национальной безопасности Российской Федерации: утв. указом Президента РФ от 10 января 2000 г. № 24 // Собр. законодательства Рос. Федерации. – 2000. – № 2, ст. 170 (утратил силу).

24. О правовой охране программ для электронных вычислительных машин и баз данных: закон от 23 сентября 1992 г. № 3523-1: ред. от 02 февраля 2006 г. // Российская газета. – 1992. – № 229 (утратил силу).

25. Об информации, информатизации и защите информации: федеральный закон: текст с изменениями и дополнениями на 10 января 2003 г. № 15-ФЗ [принят 20 февраля 1995 г. № 24-ФЗ] // Официальный интернет-портал правовой информации (www.pravo.gov.ru) 10 января 2003 г. (утратил силу).

Научные, учебные, справочные издания

26. Абалмазов Э. И. Методы и инженерно-технические средства противодействия информационным угрозам / Э. И. Абалмазов. – М.: Гротек, 1997. – 248 с.

27. Адрианов В. И., Бородин В. А., Соколов А. В. «Шпионские штучки» и устройства защиты объектов и информации / Под общ. ред. Золотарева С. А. – СПб., «Лань», 1996. – 530 с.

28. Бойков К. К. Инженерно-технические средства охраны и надзора, применяемые в УИС: учебное пособие для дополнительного профессионального образования сотрудников ФСИН России / К. К. Бойков, С. Н. Леонов. – Томск: ООО «РГ-Графика», 2014. – 283 с.

29. Бузов Г. А., Калинин С. В., Кондратьев А. В. Защита от утечки информации по техническим каналам: Учеб. пособие для подготовки экспертов системы Гостехкомиссии России. М.: Горячая линия-Телеком, 2005. – 416 с.

30. Василевский И. В. Способы и средства предотвращения утечки информации по техническим каналам / И. В. Василевский. – М.: НПЦ «Нелк», 1998. – 200 с.

31. Введение в специальность «Организация и технология защиты информации» по курсу «Теория и методология защиты информации» / под ред. Е. Л. Монаховой: метод. пособие. – Таганрог: Изд-во Таганрогского государственного радиотехнического университета, 2000. – С. 27.

32. Зарубский В. Г. Проблемные вопросы подготовки часовых операторов ФСИН России по вопросам использования интегрированных систем охраны: учебное пособие / В. Г. Зарубский, П. А. Леонтьев. – Пермь: Пермский институт ФСИН России, 2011. – 25 с.

33. Зегжда Д. П. Основы безопасности информационных систем / Д. П. Зегжда, А. М. Ивашко. – М.: Горячая линия-Телеком, 2000. – 452 с.

34. Казак Б. Б. Безопасность уголовно исполнительной системы: монография / Под ред. С. Н. Пономарева, С. А. Дьячковского. – Рязань: академия права и управления Минюста России, 2001. – 324 с.

35. Компьютерная преступность и информационная безопасность / А. П. Леонов [и др.]; под общ. Ред.А. П. Леонова. – Минск: АРИЛ, 2000. – 552 с.

36. Концепция информационной безопасности Российской Федерации (проект): Препринт. / Под ред. Д. С. Черешкина и В. А. Вирткovского. – М.: Институт системного анализа РАН, 1994. – 44 с.

37. Леонов С. И. Специальная техника правоохранительных органов. Курс лекций / С. И. Леонов, В. Г. Попов. – Томск: Томский филиал ФГОУ ВПО Кузбасский юридический институт ФСИН России, 2010. – 345 с.

38. Средства охраны, безопасности и телекоммуникационного оборудования на службе УИС России: юбилейный сборник: с приложением на CD / [ред. совет Баринов Н. И. – пред. и др.]. – Москва: Информ. мост, 2009. – 188 с.

39. Хорев А. А. Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации / А. А. Хорев. – М.: Гостехкомиссия РФ, 1998. – 320 с.

40. Ярочкин В. И. Информационная безопасность. Учебник для студентов вузов / 3-е изд. / В. И. Ярочкин. – М.: Академический проект: Трикста, 2005. – 544 с.

Материалы периодической печати

41. Белкин В. Ю. Безопасность в учреждениях уголовно-исполнительной системы / В. Ю. Белкин // Ведомости уголовно-исполнительной системы. – 2015. – № 8. – С. 27.

42. Белокуров С. В. Математическое моделирование показателей защищенности информационных процессов в инфокоммуникационных системах / С. В. Белокуров, Д. Г. Зыбин, О. А. Кондратов, А. А. Змеев // Вестник Воронежского института ФСИН России. – 2014. – №2. – С. 19-23.

43. Одинцов А. И. Некоторые проблемы обеспечения информационной безопасности учреждений и органов Федеральной службы исполнения наказаний // Уголовно-исполнительная система: право, экономика, управление. – 2008. – № 4. – С. 7.

44. Патрушев Н. П. Количество кибератак на сайты госорганов РФ выросло в четыре раза / Н. П. Патрушев // Российская газета. 2017. – 5 марта.

Материалы юридической практики

45. О состоянии надежности охраны исправительных учреждений и следственных изоляторов в 2020 году и мерах по ее совершенствованию: информационное письмо ФСИН России от 31.03.2021 исх. № 08-21157 (неопубликованный акт).

46. Материалы преддипломной практики в ФКУ ЛИУ-19 УФСИН России по Тюменской области / М. Е. Батухтин (неопубликованный акт).

Электронные ресурсы

47. Бочкарев В. В. Совершенствование использования в исправительных учреждениях инженерно-технических средств [Электронный ресурс] / В. В. Бочкарев // Актуальные проблемы российского права. – 2016. – №4 (65). – Режим доступа: https://cyberleninka.ru/article/n/sovershenstvovanie-ispolzovaniya-v-ispravitelnyh-uchrezhdeniyah-inzhenerno-tehnicheskih-sredstv (дата обращения: 23.02.2022).

48. Доклад о результатах и основных направлениях деятельности на 2015 – 2017 годы Федеральной службы исполнения наказаний [Электронный ресурс] // ФСИН России. Главная. Статистические данные: офиц. сайт. 20.03.2017. – Режим доступа: https://fsin.gov.ru/structure/inspector/iao/statistika/Kratkaya%20har-ka%20UIS (дата обращения: 20.03.2022).

49. Соната АВ – модель 3М [Электронный ресурс] // НПО АННА. Главная. Продукция. Аппаратура защиты от акустической разведки: офиц. сайт. – Режим доступа: http://www.npoanna.ru/Content.aspx?name=models.sonata-avm (дата обращения: 23.04.2022).

50. Нелинейный локатор NR-T [Электронный ресурс] // Специальная техника и технологии. Главная. Продукция / Наша продукция / Поисковое оборудование / Нелинейные локаторы / NR-T: офиц. сайт. – Режим доступа: http://detektor.ru/prod/self/srch/nelinejnaya_lokaciya/nr-t/(дата обращения: 23.04.2022).

51. Ларец 4 (акустический сейф) [Электронный ресурс] // Специальная техника и технологии. Главная. Продукция / Наша продукция / Защита информации / Ларец-4 акустический сейф: офиц. сайт. – Режим доступа: http://detektor.ru/prod/self/protect/larec4/ (дата обращения: 23.04.2022).

Приложения

Приложение 1

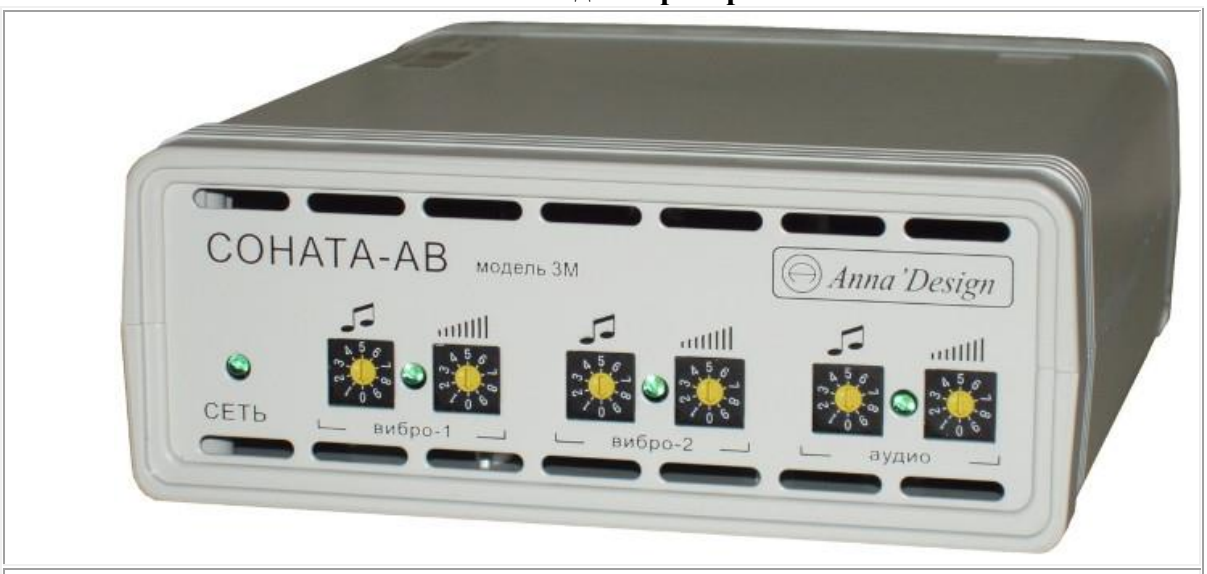
Аппаратура защиты от акустической разведки «Соната АВ» модель 3М[33]

Система виброакустической и акустической защиты с централизованным возбуждением излучателей (ЦВИ) «Соната-АВ» модель 3М, предназначена для активной защиты речевой информации в выделенных (защищаемых) помещениях, от утечки по акустическим и виброакустическим каналам.

Сертификат ФСТЭК удостоверяет, что система виброакустической и акустической защиты «Соната-АВ» модель 3М, разработанная и производимая ЗАО «АННА», является техническим средством защиты акустической речевой информации, обрабатываемой в выделенных помещениях до 1 категории включительно, от утечки по акустическому и виброакустическому каналам путем постановки помех в диапазоне частот 90- 11200 Гц, не создает технических каналов утечки информации и может устанавливаться в выделенных помещениях до 1 категории включительно без применения дополнительных мер защиты.

Система виброакустической и акустической защиты «Соната-АВ» (модель 3М) сертифицирована в системе в системе сертификации **ГОСТ Р Госстандарта России** и на него есть Санитарно-эпидемиологические **заключения Роспотребнадзора России.**

Внешний вид генераторного блока:



Генераторный блок (Модель 3М)

Системным признаком модели 3М аппаратуры «Соната-АВ» является построение по принципу “единый источник электрического шумового сигнала + электроакустические преобразователи (см рис. 1).

[33] «Соната АВ» модель 3М [Электронный ресурс] // НПО АННА. Главная. Продукция. Аппаратура защиты от акустической разведки: офиц. сайт. – Режим доступа: http://www.npoanna.ru/Content.aspx?name=models.sonata-avm (дата обращения: 23.04.2022).

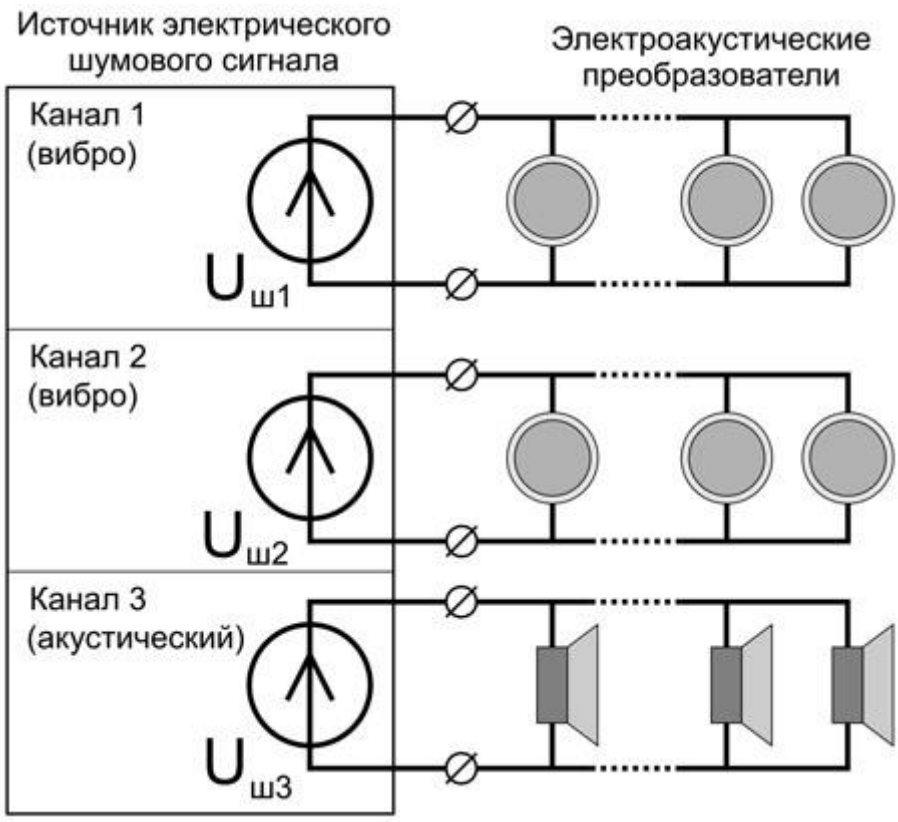


Рис. 1

Основным *положительным следствием такого построения* аппаратуры является потенциально более низкая стоимость системы при большом количестве излучателей, т.к. наиболее массовый элемент (излучатель) содержит только электроакустический преобразователь и является предельно простым устройством.

Основными *отрицательными следствиями такого построения* аппаратуры являются:

А) потенциально более высокое мешающее действие системы из-за отсутствия возможности регулировки интегрального уровня и корректировки спектра шума в каждом излучателе;

Б) относительно высокая стоимость системы при малом количестве и/или большом разнообразии типов нагрузок.

Состав аппаратуры Соната-АВ модели 3М:

Базовый элемент	**Тип базового элемента**	
	Модель 3М	
Аудиоизлучатель	АИ-65 или АИ-3М	
"Тяжелый" виброизлучатель	ВИ-45 или ВИ-3М	
"Легкий" виброизлучатель ("пьезоизлучатель"")	ПИ-45 или ПИ-3М	
Генераторный блок	Соната-АВ модель 3М	

Основные технические характеристики генераторных блоков:

Параметр	Значение
	Модель 3М
Полоса генерируемых частот	90 – 11 200 Гц(7 октав)
Количество независимых каналов [1)]	3 (2 вибро + 1 аудио)
Максимальное [2)] количество одновременно подключаемых:	
- аудиоизлучателей	5
- виброизлучателей	30 (15+15)
- легких виброизлучателей	30 (15+15)
Регулировка уровня шумового сигнала	в каждом канале
Регулировка спектра шумового сигнала	в каждом канале
Входа ДУ (интерфейс)	"Сухой" НР контакт
Электропитание изделия	сеть ~220 В / 50 Гц
Габариты блока, не более	142x60x167 мм
Вес блока, не более	0,6 кг
Условия эксплуатации: - температура окружающей среды - относительная влажность воздуха	 от 5 до 40°С до 70 % при t = 25° С
Продолжительность непрерывной работы Изделия, не менее	24 час

Примечания.

1) «Независимость» понимается,

– в наличии отдельного генератора в каждом канале устройства, что позволяет увеличить стойкость системы виброакустической защиты за счет использования на одном и том же элементе конструкции помещения излучателей подключенных к разным каналам генератора;

– в возможности изменения выходного напряжения и спектрального профиля шумового сигнала независимо на каждом канале;

– в возможности установки вида нагрузки отдельно для каждого канала;

Дистанционное включение/отключение каналов осуществляется одновременно.

2) Значение указано на наихудший случай – когда все без исключения излучатели, подключенные к генераторному блоку должны обеспечивать максимально возможный интегральный уровень.

Основные особенности модели 3М аппаратуры «Соната-АВ»:

1) Добавлен 3-й, «акустический» канал (нагрузка - до 5 излучателей) и исключены переключатели вида нагрузки, в результате:

– снижена вероятность ошибок при настройке и повышена надежность работы при эксплуатации;

– существенно улучшены технико-экономические показатели системы виброакустической защиты – один генераторный блок позволяет полностью обеспечить небольшое выделенное помещение защитой от акустической разведки.

2) Реализована коррекция спектра шумового сигнала по каждому каналу, благодаря чему появилась возможность оптимизировать параметры системы защиты с целью уменьшения мешающего воздействия.

3) Увеличена нагрузочная способность каждого виброканала до 15 излучателей на канал, что позволяет существенно снизить цену системы защиты для больших выделенных помещений, поскольку для обеспечения работы например 30 излучателей теперь нужно не два, а один генераторный блок. При этом еще остается свободным аудиоканал.

4) Генераторный блок может функционировать как с излучателями модели 1М (АИ-65, ВИ-45, ПИ-45), так и с новыми излучателями АИ-3М, ВИ-3М и ПИ-3М. Это позволит существенно снизить издержки перехода от получившей широкое распространение системы 1М к новой, особенно в случае необходимости реконструкции или расширения установленных на объекте систем виброакустической защиты моделей 1А, 1М и 1К.

5) В соответствии с новыми требованиями ФСТЭК России к системам виброакустической и акустической защиты, в модели 3М расширена полоса частот генерируемого шумового сигнала. Она составляет 7 октав (90 … 11200 Гц), что позволит использовать систему для защиты выделенных помещений до 1 категории, включительно, не только в настоящее время, но и в обозримой перспективе.

6) На основе генераторного блока возможно построение комплексов виброакустической защиты.

Приложение 2

Нелинейный локатор NR-T[34]

Описание

Назначение:

- поиск электронных средств связи (СИМ-карт, миниатюрных средств звукозаписи, сотовых телефонов, радиостанций) в местах, где пользование ими запрещено (СИЗО, места лишения свободы)
- выявление средств связи (сотовых телефонов, радиостанций) и дру-гих радиоэлектронных устройств независимо от их функционального состояния «включено/выключено», в сторожевом или ждущем режиме

Область применения:

- обследование мест содержания задержанных или заключенных, досмотр их личных вещей

Преимущества:

- эффективно обнаруживает малоразмерные цели (СИМ-карты, миниатюрные злектронные устройства)
- повышенная помехоустойчивость к откликам от строительных конструкций и элементов интерьера (контакты МОМ)
- дополнительно усиленные разъемные соединения, дополнительные меры по защите от влаги и коррозии для сложных условий эксплуатации
- облегченная батарея повышенной емкости, встроенная в блок приемопередатчика, продолжительное время непрерывной работы без замены источника питания

---

[34] Нелинейный локатор NR-T [Электронный ресурс] // Специальная техника и технологии. Главная. Продукция / Наша продукция / Поисковое оборудование / Нелинейные локаторы / NR-T: офиц. сайт. – Режим доступа: http://detektor.ru/prod/self/srch/nelinejnaya_lokaciya/nr-t/ (дата обращения: 23.04.2022).

Основные технические характеристики:

Параметры и характеристики	**Значение**
Выходная мощность (средняя)	0,2 Вт
Чувствительность приемника не хуже	125 дБм
Индикация звуковая/визуальная	акустический излучатель/светодиодный индикатор
Точность локализации цели	не хуже 0,1 м
Питание	LiION аккумулятор 7,4 В
Питание	автономное (Li-Ion)
Время работы от одного источника	не менее 4 часов
Масса в рабочем положении	не более 2,2 кг

Приложение 3

Ларец-4 акустический сейф[35]

Акустический сейф "Ларец 4" предназначен для защиты речевой информации, циркулирующей в помещении, от перехвата с использованием телефонов сотовой связи путем создания в звукоизолирующем контейнере нормированного отношения сигнал/помеха на входе приемного датчика (микрофона) сотового телефона.

Устройство обеспечивает на входах приемников телефонов сотовой связи нормированное отношение акустическая помеха/сигнал в октавных частотных полосах.

Конструкция устройства рассчитана на размещение 4 телефонов сотовой связи.

Уровень акустической помехи на расстоянии 0,5 м от устройства не превышает предельного спектра, соответствующего ПС-40.

Диапазон частот маскирующей помехи 175 – 10000 Гц.

Устройство не влияет на работоспособность телефонов сотовой связи в штатных режимах.

Устройство обеспечивает отключение акустической шумовой помехи при открывании контейнера.

Устройство обеспечивает два режима световой индикации при открытом и закрытом контейнере.

Питание устройства осуществляется от сети переменного тока частотой 50 Гц и напряжением (220±22) В.

Масса устройства – 1,5 кг.

---

[35] Ларец 4 (акустический сейф) [Электронный ресурс] // Специальная техника и технологии. Главная Продукция / Наша продукция / Защита информации / Ларец-4 акустический сейф: офиц. сайт. – Режим доступа: http://detektor.ru/prod/self/protect/larec4/(дата обращения: 23.04.2022).