

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ»

КАФЕДРА № 33

ОТЧЕТ
ЗАЩИЩЕН С ОЦЕНКОЙ
ПРЕПОДАВАТЕЛЬ

доцент, канд. техн. наук
должность, уч. степень, звание

подпись, дата

В.С. Коломойцев
инициалы, фамилия

ОТЧЕТ О ПРАКТИЧЕСКОЙ РАБОТЕ № 1

Построение защищенной организации

по курсу: Основы управления информационной безопасностью

РАБОТУ ВЫПОЛНИЛА

СТУДЕНТ ГР. № 3931

подпись, дата

А. А. Крюковская
инициалы, фамилия

Санкт-Петербург, 2022

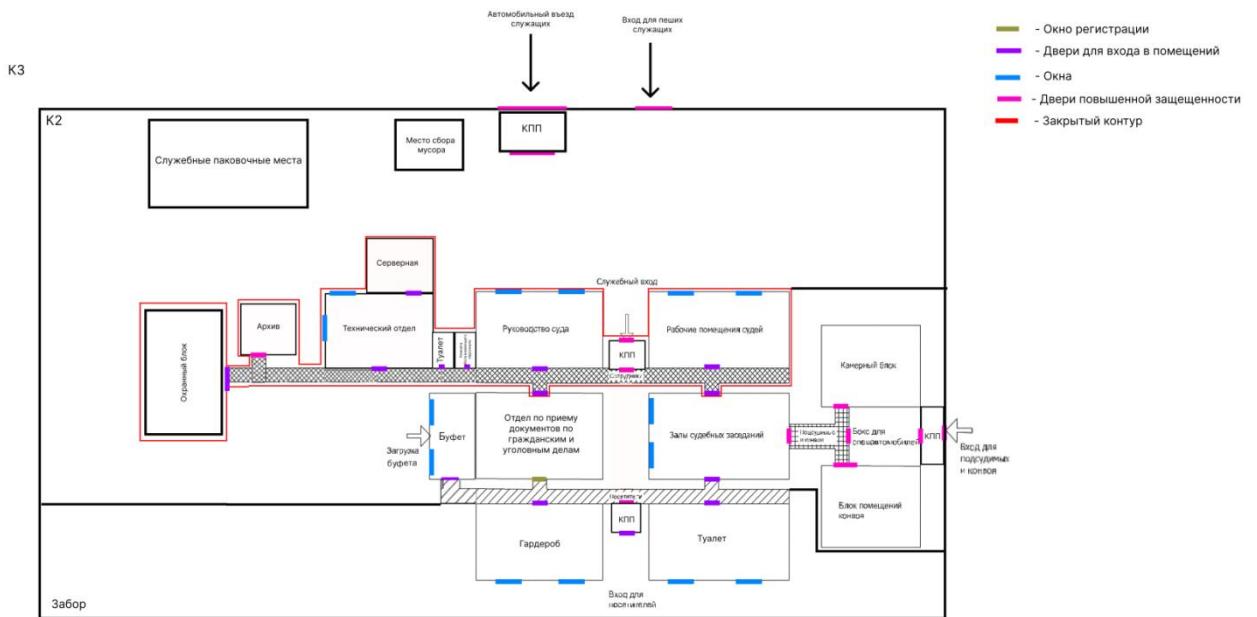


1. Цель работы

Разработка защищенной организации, определение ее информационных потоков, построение взаимодействия ее частей, построение модели защиты и по надобности модификация организации.

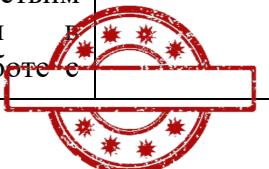
2. Описание объектов защиты

Организация представляет собой областное здание суда XXXX, которое обрабатывает следующие информационные потоки:



Необходимо идентифицировать только те активы, которые определяют функциональность ИС и существенны с точки зрения обеспечения безопасности.

Наименование актива	Критерий определяющий важность актива	Размерность оценки
Аппаратные ресурсы «закрытого» контура: сервер БД, однонаправленный МЭ, оборудование ЛВС, АРМ пользователей.	Нарушение конфиденциальности, доступности (возможность раскрытия содержимого информации третьим лицам, не допущенным в установленном порядке к работе с этой информацией, нарушение доступности путем сбоя работы серверов)	Высокая
Информационные ресурсы «закрытого» и «открытого» контуров: данные о судимостях, приговоры, сведения личной жизни, сведения, касающиеся гос. тайны, персональные данные, базы и файлы данных, контракты и соглашения, системная документация.	Нарушение конфиденциальности, целостности, доступности рассматривается (возможность раскрытия содержимого информации третьим лицам, не допущенным в установленном порядке к работе с	Высокая



	этой информацией. Нарушение двух последних пунктов может произойти из-за сбоев функционирования ИС либо бизнес-подразделений)	
Программные ресурсы «закрытого» и «открытого» контуров: ОС, СУБД, прикладное ПО	Нарушение конфиденциальности, целостности (возможность раскрытия содержимого информации третьим лицам, не допущенным в установленном порядке к работе с этой информацией)	Высокая
Людские ресурсы	Нарушение конфиденциальности и целостности (учитывая доступ сотрудников к информационным ресурсам с правами на чтение и на модификацию)	Высокая
Имидж организации	Репутация организации оценивается в связи с информационными ресурсами: какой ущерб репутации организации будет нанесен в случае нарушения безопасности информации организации.	Высокая

Из всего вышеперечисленного понятно, что данная организация обрабатывает такую информацию как: судимости, приговоры, персональные данные граждан, предоставленные для возбуждения судопроизводства.

Тогда очевидно, что данная организация будет обрабатывать данные согласно уровню защищённости – 1А/ИСПДн-С. Пунктом 1 части 1 статьи 26 ГПК РФ предусмотрено, что в качестве суда первой инстанции гражданские дела, связанные с государственной тайной, рассматривают верховный суд республики, краевой, областной суд, суд города федерального значения, суд автономной области и суд автономного округа. Отсюда и уровень защиты 1А.

Данная ИСПДн обрабатывающая специальные категории ПДн, касающиеся расовой, национальной принадлежности, политических взглядов, судимостей, религиозных и философских убеждений, состояния здоровья, интимной жизни субъектов (ИСПДн-С). Эта система подвержена угрозам 1-го типа (информация имеет высокий уровень значимости (УЗ 1)), а, следовательно, нуждается в повышенной защите данной информации.

Защита информации от несанкционированного доступа является составной частью общей проблемы обеспечения безопасности информации. Мероприятия по защите информации от НСД должны осуществляться взаимосвязано с мероприятиями по специальной защите основных и вспомогательных средств вычислительной техники, средств



и систем связи от технических средств разведки и промышленного шпионажа.

Целью обеспечения информационной безопасности информационной системы (ИС) предприятия является ее надежное и бесперебойное функционирование в условиях возникающих угроз и воздействий, которые могут привести к нарушению работы ее компонент, в т. ч. и подсистемы информационной безопасности.

Подсистема информационной безопасности (ПИБ) ИС реализует требования ПИБ и предназначена для обеспечения ее информационной безопасности за счет комплексного использования организационных, сертифицированных технических и программно-аппаратных средств и мер защиты.

Данное требование определяется целым рядом положений законодательных и нормативных актов в области защиты информации, в том числе нормативными документами ФСТЭК:

- Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации». Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.

- Руководящий документ «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации». Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.

- ФЗ № 152 «О персональных данных».
- Постановление правительства № 1119 от 01.11.2012 «Требования к защите персональных данных при их обработке в информационных системах персональных данных» и др.

В соответствии с законодательством Российской Федерации, в информационных системах ряда организаций использование сертифицированных программных продуктов является обязательным. К таким организациям относятся:

- государственные организации;
- негосударственные организации, работающие со служебной информацией государственных органов;
- организации, работающие с персональными данными.

В большинстве случаев выбор средств защиты информации осуществляется в рамках нескольких десятков сертифицированных решений различных брэндов. На рынке



сертифицированных СЗИ можно приобрести средства, обеспечивающие защиту от любых угроз и с требуемым уровнем защиты. С полным перечнем сертифицированных СЗИ можно ознакомиться на официальном сайте ФСТЭК России в разделе Государственный реестр сертифицированных средств защиты информации.

3. Теоретические сведения

Рассмотрим нормативно-правовые документы, которыми нужно руководствоваться при создании подобной организации.

- Для обеспечения физической защиты здания

Данные нормативные документы обеспечивают нормальное функционирование и защиту самого здания суда. Рассмотрим каждый из них подробнее.

- 1) СП 1.13130.2009 Системы противопожарной защиты. Эвакуационные пути и выходы
- 2) СП 2.13130.2012 Системы противопожарной защиты. Обеспечение огнестойкости объектов защиты
- 3) СП 3.13130.2009 Системы противопожарной защиты. Система оповещения и управления эвакуацией людей при пожаре. Требования пожарной безопасности
- 4) СП 4.13130.2009 Системы противопожарной защиты. Ограничение распространения пожара на объектах защиты. Требования к объемно-планировочным и конструктивным решениям
- 5) СП 5.13130.2009 Системы противопожарной защиты. Установки пожарной сигнализации и пожаротушения автоматические. Нормы и правила проектирования.
- 6) СП 6.13130.2009 Системы противопожарной защиты. Электрооборудование. Требования пожарной безопасности
- 7) СП 30.13330.2012 "СНиП 2.04.01-85* Внутренний водопровод и канализация зданий"
- 8) СП 152.13330.2012. Свод правил. Здания судов общей юрисдикции. Правила проектирования
- 9) СП 60.13330.2012 "СНиП 41-01-2003 Отопление, вентиляция и кондиционирование"
- 10) СП 89.13330.2012 "СНиП II-35-76* Котельные установки"
- 11) СП 113.13330.2012 "СНиП 21-02-99* Стоянки автомобилей"
- 12) СП 118.13330.2012 "СНиП 31-06-2009 Общественные здания и сооружения"
- 13) СП 124.13330.2012 "СНиП 41-02-2003 Тепловые сети"
- 14) СП 132.13330.2011 Обеспечение антитеррористической защищенности зданий и сооружений. Общие требования проектирования
- 15) СП 139.13330.2012 Здания и помещения с местами труда для инвалидов. Правила проектирования



- 16) ГОСТ Р 50571.1-2009 Электроустановки низковольтные. Часть 1. Основные положения, оценка общих характеристик, термины и определения
- 17) ГОСТ Р 53770-2010 Лифты пассажирские. Основные параметры и размеры
- 18) ГОСТ 30494-2011 Здания жилые и общественные. Параметры микроклимата в помещениях
- 19) СанПиН 2.2.2/2.4.1340-03 Гигиенические требования к персональным электронно-вычислительным машинам и организации работы

- Организационные методы защиты

- 1) Концепцией обеспечения безопасности федеральных судов общей юрисдикции и федеральных арбитражных судов (одобрена постановлением Президиума Совета судей Российской Федерации от 19 октября 2006 г. № 98 и от 23 мая 2011 г. № 262) – Данные мероприятия включают в себя обеспечение физической охраны зданий судов, обеспечение судов техническими средствами охраны.
- 2) В СП 132.13330.2011 «Свод правил. Обеспечение антитеррористической защищённости зданий и сооружений. Общие требования проектирования». Разработаны планы мероприятий по антитеррористической и противодиверсионной защите судов, которые согласованы с органами ФСБ, МВД, ФССП и МЧС на местах. В планах предусматривается порядок действий судей, работников аппарата суда, судебных приставов в чрезвычайной обстановке.
- 3) п. 1 ст. 12 ФЗ «О государственной защите судей, должностных лиц правоохранительных и контролирующих органов» – Применение и осуществление мер безопасности в отношении судей возлагается на органы внутренних дел. выдачу оружия судьям и специальных средств индивидуальной защиты, временное помещение в безопасное место, замену документов, изменение внешности и ряд других мер, направленных на обеспечение защиты их жизни и здоровья.

- Аппаратно-технические методы защиты

- 1) Приказом Судебного департамента от 31.12.2016 №258 – Технические средства охраны судов. – Нормы обеспечения техническими средствами безопасности и средствами защиты, утв.: турникеты на входе здания суда; стационарный и ручные металлообнаружители; охранно-пожарная сигнализация, выведенная на пульт централизованного наблюдения органов внутренних дел; система автоматического пожаротушения, устанавливаемая в помещениях, в которых хранятся архивные судебные дела и вещественные доказательства, в канцелярии суда, а также в помещении, где установлен сервер локально-вычислительной сети; стационарные кнопки тревожной сигнализации в залах судебных заседаний и кабинетах судей и мобильные брелоки



тревожной сигнализации, выдаваемые каждому судье; система видеонаблюдения, обеспечивающая возможность наблюдения и фиксации обстановки внутри здания суда и на прилегающей территории.

2) Документ ФСТЭК – Приказ ФСТЭК России от 18.02.2013 № 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных" регламентирует параметры ИС типа ИСПДн-С следующим образом: Требования, предъявляемые к системам данного типа, следующие:

- Меры по идентификации и аутентификации субъектов доступа и объектов доступа должны обеспечивать присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).
- Меры по управлению доступом субъектов доступа к объектам доступа должны обеспечивать управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивать контроль за соблюдением этих правил.
- Меры по регистрации событий безопасности должны обеспечивать сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.
- Меры по обнаружению (предотвращению) вторжений должны обеспечивать обнаружение действий в информационной системе, направленных на несанкционированный доступ к информации, специальные воздействия на информационную систему и (или) персональные данные в целях добывания, уничтожения, искажения и блокирования доступа к персональным данным, а также реагирование на эти действия.
- Меры по контролю (анализу) защищенности персональных данных должны обеспечивать контроль уровня защищенности персональных данных, обрабатываемых в информационной системе, путем проведения систематических мероприятий по анализу защищенности информационной системы и тестированию работоспособности системы защиты персональных данных.

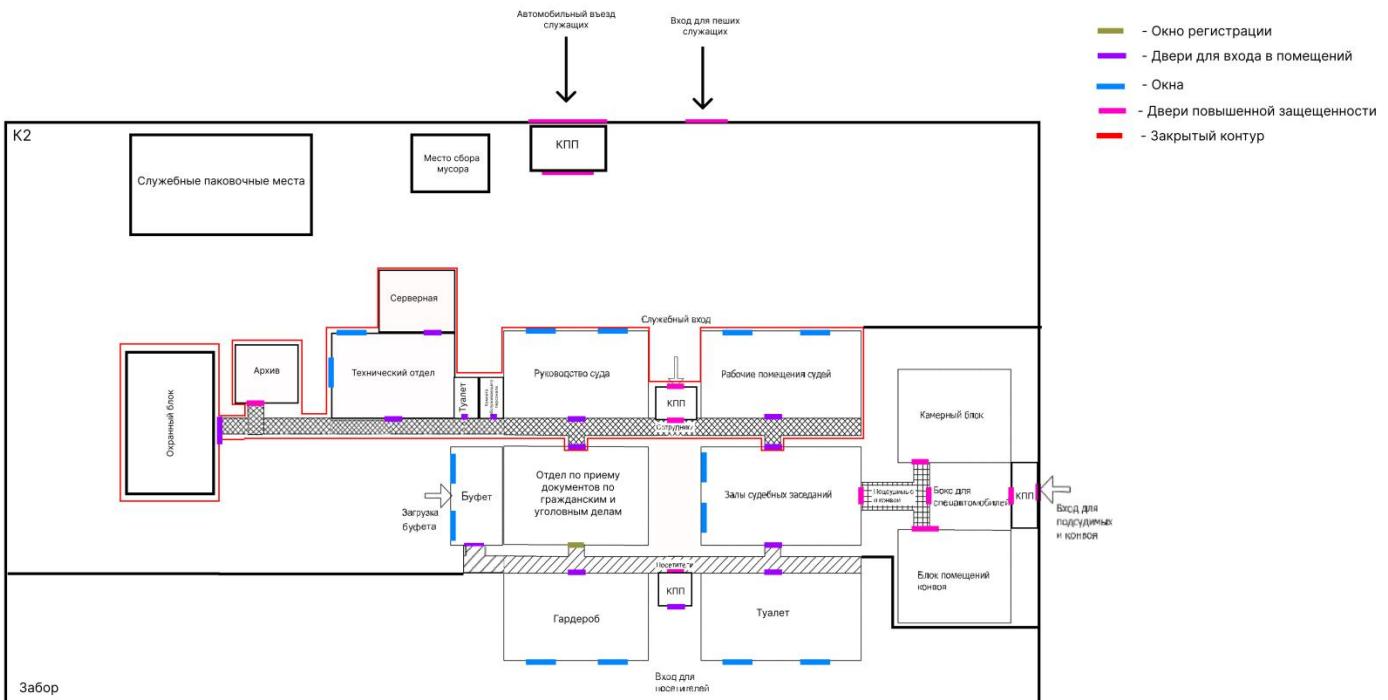


- Меры по обеспечению целостности информационной системы и персональных данных должны обеспечивать обнаружение фактов несанкционированного нарушения целостности информационной системы и содержащихся в ней персональных данных, а также возможность восстановления информационной системы и содержащихся в ней персональных данных.
- Меры по обеспечению доступности персональных данных должны обеспечивать авторизованный доступ пользователей, имеющих права по доступу, к персональным данным, содержащимся в информационной системе, в штатном режиме функционирования информационной системы.
- Меры по защите информационной системы, ее средств, систем связи и передачи данных должны обеспечивать защиту персональных данных при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы и проектных решений, направленных на обеспечение безопасности персональных данных.
- Меры по выявлению инцидентов и реагированию на них должны обеспечивать обнаружение, идентификацию, анализ инцидентов в информационной системе, а также принятие мер по устранению и предупреждению инцидентов.
- Меры по управлению конфигурацией информационной системы и системы защиты персональных данных должны обеспечивать управление изменениями конфигурации информационной системы и системы защиты персональных данных, анализ потенциального воздействия планируемых изменений на обеспечение безопасности персональных данных, а также документирование этих изменений.

4. Архитектура организации и ее взаимодействие

Рассмотрим архитектуру организации областного суда и взаимодействие его компонентов.





Это отдельно построенное одноэтажное здание, находящееся в жилом районе, окруженное парком со всех сторон. Само здание суда окружено двухметровым забором. У данной организации есть три типа входа для разного типа посетителей:

- 1) Проход в заборе, ведущий к общедоступному входу. Пространство общедоступного входа также окружено забором, и данное помещение круглосуточно просматривается камерами видеонаблюдения, запись с которых передается в охранный блок самого здания суда.
- 2) Служебный вход, предназначенный для сотрудников судопроизводства и для обслуживающего персонала. Это зона также выделена внутренним забором. Проход осуществляется либо через забор, либо через автомобильный въезд, если сотрудник прибыл на транспортном средстве. На транспортном средстве имеют право въезжать строго ограниченный круг людей (судья, прокурор, секретарь). При автомобильном въезде стоит КПП, где находится охранник, который проверяет зарегистрированы ли номера в БД (т.е. данные машины могут осуществлять въезд на территорию и осматривают машину на наличие запрещенных предметов (оружие, взрывные устройства и т.д.). Пеший вход на территорию осуществляется по специальным электронным карточкам, которые прикладываются к датчику забора. На территории данной зоны предусмотрена парковка для зарегистрированных автомобилей, специально выделенное место для сбора мусора (каждые 2 дня здание суда посещает мусороуборочная машина, номер которой зарегистрирован так же в БД для возможности въезда на



территорию), специально выделенное место для подъезда машины, обеспечивающей доставку еды в буфет суда, круглосуточно работающие камеры видеонаблюдения.

- 3) Вход для подсудимых и конвоя. Осуществляется с боковой части здания суда и только на спецавтомобилях (АВТОМОБИЛЬНЫЕ ТРАНСПОРТНЫЕ СРЕДСТВА ОПЕРАТИВНО-СЛУЖЕБНЫЕ ДЛЯ ПЕРЕВОЗКИ ЛИЦ, НАХОДЯЩИХСЯ ПОД СТРАЖЕЙ), также в данном автомобиле находится конвой минимум из 4-х человек (наряд полиции, осуществляющий охрану подсудимого при доставлении его к месту назначения в спецавтомобиле). Конечно, на входе имеется КПП, которые проверяет номера зарегистрированных спецавтомобилей и полицейские удостоверения.

Рассмотрим порядок взаимодействия лиц в общедоступном контуре:

При входе в здание стоит рамка металлоискатель для проверки проноса несанкционированных предметов и профилактики предотвращения террористической угрозы. На входе есть рентген-сканер, которым проверяется сам человек на наличие в нем запрещенных устройств, которые не уловил металлоискатель (оператор сканера, сидящий рядом в будке, не видит лица, сканированные изображения не сохраняются). А при помощи интроскопа проверяется ручная кладь. Также входной контроль регулируют, стоящие на входе охранники.

После прохода посетителями входного контроля, они могут сдать свои вещи в гардероб или сходить в туалет, около которых расположены камеры видеонаблюдения. Далее посетители либо направляются в зал судебного заседания, либо стоя в живой очереди подают информацию в окно регистрации, чтобы подать документы по делопроизводству. В холле также имеется план эвакуации, система автоматического пожаротушения, огнетушители в размере 3 шт.

Рассмотрим порядок взаимодействия лиц в закрытом контуре:

На входе служащие идентифицируют свой проход по электронным пропускам, проходят рамку металлоискателя и интроскоп. На входе также расположены камеры видеонаблюдения, и находится два охранника. Нужно отметить, что все помещения закрытого контура обустроены: утолщенными стенами с помощью гипсокартона (гипсокартонные перегородки) для предотвращения утечки речевой информации по акустическому и вибравакустическому каналу, матовые стекла для предотвращения утечки по оптическому каналу (зондирующие лазеры). Также в холле и в кабинетах есть план эвакуации, огнетушители, система автоматического пожаротушения (кроме помещения “Архив”, “Серверная” и “Технический отдел”, жалюзи или светонепроницаемые плотные



шторы, система видеокамер и приборов ночного видения. Имеются аварийные выходы и все двери из железа.

Отделы “Руководство суда”, “Рабочее помещение судей”, “Отдел по приему документов по уголовным делам” имеют внутри помещений детектор жучков, находящий в принципе любые радиопередающие устройства: например, аналоговые и цифровые жучки, радио микрофоны, сотовые телефоны, жучки, беспроводные скрытые видеокамеры и т.д., которые работают по включению служащих во время переговоров (защищают от хищения информации при помощи закладных устройств), прибор для генерации ультразвуковых и акустических помех (берегут информацию от утечки от закладных устройств, работающих на ультразвуковом излучении).

Также внутри всех остальных помещений (кроме “Туалет” и “Архив”) находятся как минимум по 2-3 компьютера, предназначенных для занесения информации о прохождении дел судопроизводства. Естественно от компьютера идут провода, по которым идет ток, создающий вокруг себя электромагнитное поле опасного (информационного сигнала), который может быть перехвачен злоумышленником из К2 или соседних помещений, поэтому в качестве решения используем экранирование и создание помех затрудняющих прием и выделение полезной информации из перехваченных злоумышленником сигналов за счет излучения с помощью специальных антенн электромагнитных сигналов в пространство.

Во всех помещениях стоит охранная сигнализация от несанкционированного вторжения в здание суда, сигнал с которой передается в пульт управления охраны и ближайшее отделение полиции.

В помещении архива полностью герметично изолировано в нем имеется аварийный выход и вход в архив осуществляется по электронным карточкам, с помощью которых фиксируется факт посещения архива тем или иным служащим.

Стены помещения “Архив” отделаны с использованием неагрессивных, не пылящихся материалов. В помещении нет газовых и водонесущих магистральных трубопроводов. Архивное помещение телефонизировано и оснащено системами пожарно-охранной сигнализации и пожаротушения. В системах пожаротушения применяются нейтральные, безопасные для документов вещества.

Сами судьи работают в помещении “Рабочие помещения судей”, где на компьютерах они могут изучать дела и документы, также работают с документами из архива, но их переносить они обязаны в черном непрозрачном кейсе (с архивными документами имеют право работать лишь в помещении судей, находиться с ними могут в помещениях: “Архив”, “Рабочие помещения судей”, “Руководство суда” и “Зал судебных заседаний”). Судьи могут посещать все помещения закрытого контура за исключением технического отдела и



серверной. После судебного заседания судьи (или их секретарь) оформляют рассмотренное дело в БД и относят дела в архив.

Обслуживающий персонал находится в помещении “Помещение для персонала”. Обслуживающий персонал имеет допуск во все помещения кроме архива.

Нужно отметить, что служащие суда начиная от судей и руководства и заканчивая обслуживающим персоналом ознакомливаются и подписывают внутреннюю документацию, которая устанавливает правила работы с компьютерной техникой и конфиденциальной информацией, и подписывают бумаги о неразглашении конфиденциальной информации в случае допуска к ней и дополнительные соглашения к трудовым договорам, где указана ответственность за разглашение или неправомерное использование сведений, ставших известных по работе.

Также руководство проводит инструктаж и периодические проверки персонала, внедрение программных продуктов, которые защищают данные от копирования или уничтожения любым пользователем и составляют план восстановления системы на случай выхода из строя по любым причинам.

Рассмотрим порядок взаимодействия в зоне подсудимых и конвоя:

После прохождения входного контроля спецмашина въезжает на специально отведенную зону, по периметру которой стоит охрана. Также здесь ведется система видеонаблюдения и есть датчики контроля движения, вся информация с них приходит на пульт охранного блока.

Все перемещения подсудимого, помимо камерного блока осуществляются в наручниках. Заключенного выгружают из клетки машины и в сопровождении четырех охранников вводят в камерный блок. Камерный блок обустроен следующим образом: на всех оконных проемах камер с наружной стороны следует устанавливать металлические решетки. Со стороны камер оконные стекла защищают металлической сеткой, обеспечивающей возможность открывания форточки. Камера оборудована электрическим потолочным освещением, приточно-вытяжной вентиляцией, отоплением, специальными металлическими дверями, скамьями, раскладным столом для принятия пищи. Также на металлической входной двери расположена сигнализация, при нарушении целостности двери сигнализация сработает и отправит тревожный сигнал на пульт охраны и ближайшее отделение полиции.

Напротив камерного блока расположен блок помещения конвоя, обустроенный аналогичным образом, за исключением дверной сигнализации. В коридоре, связывающем блок помещения конвоя и камерным блоком, расположена система видеонаблюдения и тревожная кнопка, по нажатию которой происходит вызов полиции на объект.



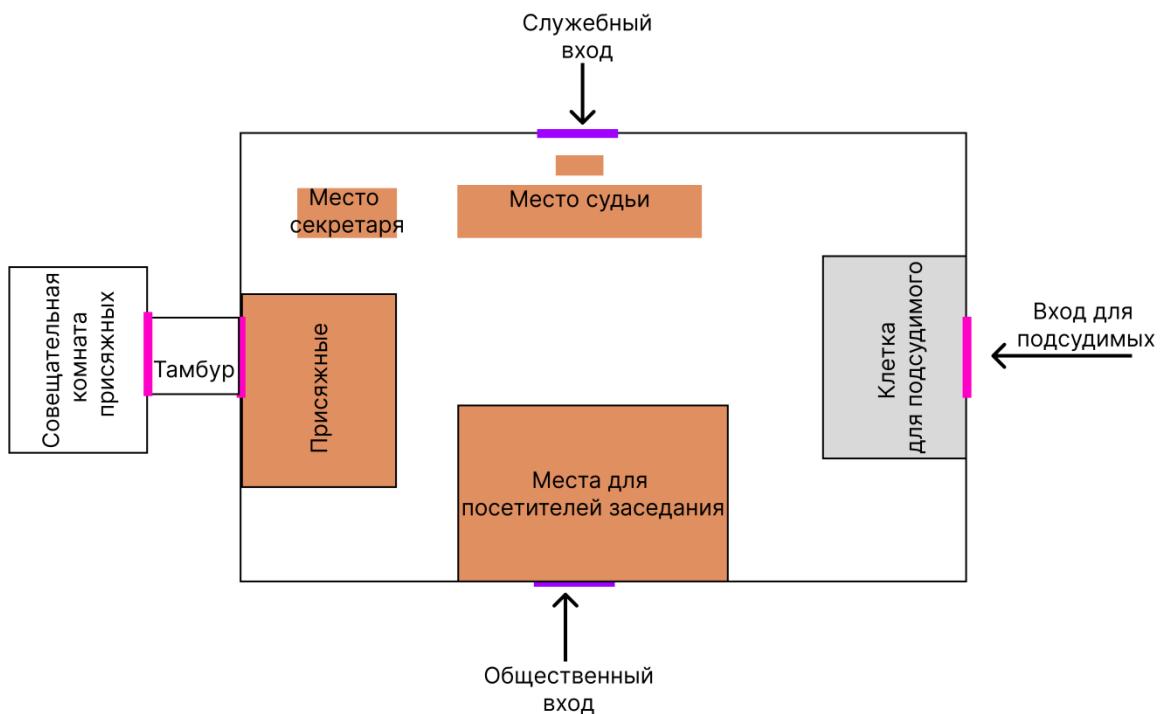
О необходимости доставления подсудимого в зал сообщают с поста охраны в помещение конвоя по телефонным линиям.

Рассмотрим порядок взаимодействия в зоне зала суда:

В зал суда посетители входят с трех входов:

- 1) Подсудимого вводят в зал конвой в специальную железную клетку, из которой можно выйти только к конвою и камерному блоку. Естественно, все перемещения подсудимого, помимо камерного блока осуществляются в наручниках. Около клетки также находятся два охранника.
- 2) Обычные посетители и присяжные заходят с общественного входа и занимают свои места в зале суда (стулья, огороженные деревянной стенкой на уровне груди). Во время судебного заседания для совещания присяжные прямо из зала суда удаляются в отдельную звуконепроницаемую без окон комнату, оснащенную сигнализацией и системой пожаротушения. Особенность в том, что в комнате нет видеонаблюдения.
- 3) Вход для судьи, со стороны служебного входа. Судья садится на трибуну для рассмотрения дела. За судьей стоят два охранника для обеспечения безопасности. Еще у судьи есть тревожная кнопка, по ее нажатию приезжает наряд полиции и передается тревожный сигнал в охранный блок. Судья может несколько раз отлучаться во в рабочие помещения судей для обдумывания и вынесения решения по делу.

Сам зал суда выполнен из звуконепроницаемых материалов, оснащен сигнализацией охранной и противопожарной, имеется кнопка вызова полиции и система видеонаблюдения.



Рассмотрим порядок работы с компьютерами здания суда:



1) Так как каждый из представленных в здании суда компьютеров обрабатывает специальную информацию, то в данной системе предусмотрена система идентификации и аутентификации (авторизации). То есть каждый сотрудник совершает вход в систему по заданному логину и паролю, которые однозначно идентифицируют пользователя.

В данной ситуации нельзя позволять злоумышленнику овладеть логином и паролем (тогда он имеет возможность совершать действия от лица легального пользователя). Поэтому в системе выполнены следующие настройки системы безопасности согласно требованиям ФСТЭК по инженерной защите информации касаемо управления политиками паролей:

- Максимальный срок действия пароля Согласно требованиям ИБ системы руководящего документа, максимальный срок действия пароля должен быть до 60 дней, исходя из этого, производим данную настройку политики ИБ на 60 дней, в результате настройки увеличиваем степень безопасности пароля от взлома, за 31 день злоумышленник при данных параметрах методом полного перебора сможет перебрать максимум 2232 варианта паролей, что мало для подбора шестизначного пароля, соответствующего требованиям безопасности (длительность блокировки исключает непрерывный подбор паролей, что ограничивает производительность злоумышленника). Слишком длинный срок действия ставить не стоит, чем дольше пароль существует, тем выше вероятность того, что он будет скомпрометирован атакой методом подбора, злоумышленником, который получает общие знания о пользователе или пользователем, который использует пароль. А короткий срок действия пароля приведёт к обязательной частой смене пароля, что является неудобным для пользователя. В целях безопасности хранящихся ресурсов, установим максимальный срок на 1 месяц.
- Минимальная длина пароля Согласно требованиям ИБ системы руководящего документа, минимальная длина пароля должен быть не менее 8 символов, исходя из этого, производим настройку политики ИБ на 8 символов, в результате настройки усложняем задачу злоумышленнику по подбору пароля. Нет необходимости делать слишком длинный пароль, который пользователь не сможет запомнить и будет вынужден написать его на бумажке, с которой недоброжелатель может спокойно подсмотреть пароль. Так же банальная потеря бумажки с паролем может подвергнуть систему огромным рискам. Рекомендуемая длина – 8 символов, так как сделав его меньше будет доступна атака на пароль с помощью перебора (даже если использовать требования сложности пароля: заглавные, строчные буквы и т.д.)



- Минимальный срок действия пароля Согласно требованиям ИБ системы руководящего документа, минимальный срок действия пароля должен быть до 30 дней, исходя из этого, производим настройку данного параметра политики ИБ на 14 дней, в результате настройки усложняем задачу злоумышленнику по подбору пароля. За 14 день злоумышленник при данных параметрах методом полного перебора сможет перебрать максимум 1008 варианта паролей, что мало для подбора шестизначного пароля, соответствующего требованиям безопасности (длительность блокировки исключает непрерывный подбор паролей, что ограничивает производительность злоумышленника).
- Пароль должен отвечать требованиям сложности. Согласно требованиям ИБ системы руководящего документа, вход в систему должен осуществляться по паролю условнопостоянного действия длиной не менее восьми буквенноцифровых символов, исходя из этого, производим настройку политики ИБ, в результате настройки пароль будет защищен от атак перебором. Без данного параметра даже пароль очень большой длины будет подвержен атаке с помощью перебора.
- Требование неповторяемости паролей. Согласно требованиям ИБ системы руководящего документа, количество хранимых паролей не менее 5, исходя из этого, производим настройку политики ИБ на значение 5, в результате настройки пользователю необходимо будет придумать как минимум 6 новых паролей, что обеспечит сложность злоумышленнику в качестве постоянной смены паролей. Слишком большой параметр устанавливать не стоит, так как бесконечно изменяющийся поток паролей невозможно запомнить, а, следовательно, пароль будет записан на различные носители (например, бумага), что еще больше подвергает безопасность системы, а если установить слишком маленький порог, то пользователь сможет периодически использовать одни и те же пароли, что делает систему уязвимой для перебора пароля злоумышленником.
- Хранение паролей, используя обратимое шифрование. Согласно требованиям ИБ системы руководящего документа, хранение паролей, используя обратимое шифрование запрещено, исходя из этого, производим настройку политики ИБ отключив этот параметр, в результате настройки исключается взлом пароля через приложения, хранящие не только хэш-код пароля. Использование этой функции аналогично хранению пароля в открытом виде. В настраиваемом компьютере хранящаяся информация, имеет высокий уровень значимости, поэтому мы не можем подвергать нашу систему таким рискам.



2) Каждому из авторизированных пользователей выделен свой ограниченный доступ к системе. Например, идентификация судьи дает возможность работать с БД, но не дает возможности менять системные настройки политики, их может менять только системный администратор.

Так как злоумышленник может быть легитимным сотрудником, имеющим неограниченные возможности при попытке входа в чужой профиль, тогда следует ввести меры по ограничению опасной активности и заблокировать учетную запись, чтобы остановить потенциального нарушителя информационной безопасности. Рассмотрим настройки политик блокировки учетных записей:

- Время до сброса счётчиков блокировки Согласно требованиям ИБ системы руководящего документа, время до сброса счетчиков блокировки должно быть не менее 60 минут, исходя из этого, производим настройку политики ИБ установив этот параметр равным 60 минутам, в результате настройки устанавливается количество минут, которые должны пройти после неудачной попытки для автоматической разблокировки, заданного в параметре времени хватит, чтобы системный администратор при необходимости смог предупредить действия злоумышленника. Если установить большое время, то есть риск, что пользователь может случайно заблокировать свои учетные записи, если они не введут пароль несколько раз. Чтобы установить данный параметр нужно оценивать уровень угроз для организации и баланс между затратами на поддержку службы технической поддержки для сброса паролей.
- Пороговое значение блокировки. Согласно требованиям ИБ системы руководящего документа, пороговое значение блокировки должно быть не более 3 попыток, исходя из этого, производим настройку политики ИБ, установив этот параметр равным 3 попыткам, в результате настройки дается только три попытки на верный ввод пароля, тем самым мы усилили безопасность системы, исключив атаку перебором. Атаки методом подбора пароля могут использовать автоматизированные методы для проверки миллионов сочетаний паролей для любой учетной записи пользователя. Эффективность таких атак можно практически исключить, если ограничить количество неудачных попыток входа, которые могут быть выполнены.
- Продолжительность блокировки учетной записи. Согласно требованиям ИБ системы руководящего документа, продолжительность блокировки учетной записи должна быть не менее 60 минут, исходя из этого, производим настройку политики ИБ установив этот параметр равным 60 минутам, в результате 11 настройки при неверном вводе учетная запись заблокируется на час, этого времени хватит, чтобы



системный администратор при необходимости смог предупредить действия злоумышленника.

Также нарушитель все еще может являться сотрудником организации, имеющим цель нанести ущерб организации через использование своих привилегий, тогда для обеспечения информационной безопасности может пригодиться аудит действий сотрудников, при правильной настройке политики которого будет производиться запись подозрительных действий в журнал. Поэтому необходимо настроить политику аудита:

- Аудит входа в систему. Согласно требованиям ИБ системы руководящего документа, мы должны регистрировать результат попытки входа: успешная или неуспешная – несанкционированная, исходя из этого, производим настройку политики ИБ установив аудит успехов и отказов, в результате настройки “отказ” поможет обнаружить нарушителя, который пытается войти в систему, а “успех” поможет понимать, кто из сотрудников в данный период пользовался конфиденциальной информацией. И в случае ее утечки мы точно будем знать, кто имел к ней доступ, тем самым сузив круг подозреваемых.
- Аудит доступа к объектам. Согласно требованиям ИБ системы руководящего документа, мы должны регистрировать результат попытки доступа к объектам: успешная или неуспешная – несанкционированная, исходя из этого, производим настройку политики ИБ установив аудит успехов и отказов, в результате настройки “отказ” поможет найти проблему или обнаружить нарушителя., а “успех” поможет понимать, кто из сотрудников в данный период пользовался информацией из определенных объектов. И в случае ее утечки мы точно будем знать, кто имел к ней доступ, тем самым сузив круг подозреваемых.
- Аудит доступа к службе каталогов. Согласно требованиям ИБ системы руководящего документа, мы должны регистрировать результат попытки доступа к службе каталогов: успешная или неуспешная – несанкционированная, исходя из этого, производим настройку политики ИБ установив аудит успехов и отказов, в результате настройки “отказ” поможет найти проблему или обнаружить нарушителя., а “успех” поможет понимать, кто из сотрудников изменил политику безопасности, создавал новые учетные записи и т.д. И в данном случае мы можем отследить людей, которые могут умышленно ослабить настроенную политику безопасности.
- Аудит изменения политики. Согласно требованиям ИБ системы руководящего документа, мы должны регистрировать результат попытки изменения политики:



успешная или неуспешная – несанкционированная, исходя из этого, производим настройку политики ИБ установив аудит успехов и отказов, в результате настройки мы сможем избежать потенциальные последствия несанкционированного изменения политик, которые влекут за собой возможности злоумышленника к изменения личной информации, а также к повышению прав пользователя.

- Аудит изменения привилегий. Согласно требованиям ИБ системы руководящего документа, мы должны регистрировать результат попытки изменения привилегий: успешная или неуспешная – несанкционированная, исходя из этого, производим настройку политики ИБ установив аудит успехов и отказов, в результате настройки мы исключаем потенциальные последствия несанкционированного изменения 14 привилегий, например, приложение, обладающее большими полномочиями, чем предполагалось системным администратором, может совершать неавторизированные действия, что повлечет угрозу.
- Аудит отслеживания процессов. Согласно требованиям ИБ системы руководящего документа, мы должны регистрировать результат попытки отслеживания процессов: неуспешная – несанкционированная, исходя из этого, производим настройку политики ИБ установив аудит отказов, в результате настройки мы обеспечиваем нужный уровень, можем не только найти проблему в настройке, но и обнаружить нарушителя.
- Аудит системных событий. Согласно требованиям ИБ системы руководящего документа, мы должны регистрировать результат попытки изменений системных событий: успешная или неуспешная – несанкционированная, исходя из этого, производим настройку политики ИБ, установив аудит успехов и отказов, в результате настройки мы контролируем роль этой политики в поиске проблем и причин неполадок. 15 Данная политика безопасности имеет особую ценность, так как именно при помощи этой политики возможно узнать, перезагружался ли у пользователя компьютер, превысил ли размер журнала безопасности пороговое значение предупреждений, была ли потеря отслеженных событий из-за сбоя системы аудита и даже вносились ли изменения, которые могли повлиять на безопасность системы или журнала безопасности вплоть до изменения системного времени.
- Аудит событий входа в систему. Согласно требованиям ИБ системы руководящего документа, мы должны регистрировать результат попытки событий входа в систему: успешная или неуспешная – несанкционированная, исходя из этого, производим настройку политики ИБ, установив аудит успехов и отказов, в результате настройки аудит отказов поможет найти проблему, а также обнаружить нарушителя. Так как



обрабатываемая информация не является общедоступной, то необходимо включить и аудит успехов (например, для того, чтобы знать, если какой-то пользователь внутри системы пытается зайти под видом другого пользователя).

- Аудит управления учётными записями. Согласно требованиям ИБ системы руководящего документа, должна производиться регистрация управление учетными записями: успешная или неуспешная – несанкционированная, исходя из этого, производим настройку политики ИБ, установив аудит успехов и отказов, в результате настройки в журнал безопасности будут записываться такие действия как создание, перемещение и отключение учётных записей, а также изменение паролей и групп, данная политика играет большую роль в поиске проблем и причин неполадок.
 - Политика назначения прав пользователей. Согласно требованиям ИБ системы руководящего документа, Такие права, как изменение системного времени, завершение работы системы, разрешение входа в систему через службу терминалов должны быть закреплены только за администратором, исходя из этого, производим настройку политики ИБ, в результате настройки обеспечили безопасность системы, так как данные параметры могут существенно повлиять на работоспособность системы.
- 3) Возможность использовать только лишь зарегистрированные носители информации, которые выдаются сотрудникам делопроизводства и администратору уникальным id, привязанным к каждому конкретному человеку. Если же вставить незарегистрированный носитель, то система его не опознает и не даст возможности работы с ним, также будет отправлено тревожное уведомление об этом в технический отдел (защита от инсайдеров).
- 4) Также производится ведение и регистрация событий безопасности в журнал. Согласно требованиям ИБ к ИС типа ИСПДн-С, необходимо вести учет следующей информации:
- дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;
 - идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа;
- Данная информация сохраняется в Журнале событий Windows в журнале безопасности в соответствии с политиками аудита. Так как у нас политики аудита настроены на аудит входа и доступа к системе, то в журнале безопасности появляются следующие записи. При достижении конца журнала, журнал будет затирать записи по необходимости, чтобы при возникновении системных ошибок мог быть проведен аудит и анализ.
- 5) Применение средств антивирусной защиты для избежания утечки данных из внс.



Произведенные настройки были рассчитаны исходя из соответствия данной системы требованиям документа ФСТЭК – Приказ ФСТЭК России от 18.02.2013 № 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных". Текущие настройки системы позволяют обезопасить вход в систему от злоумышленников, однако накладывает некоторые обязательства на пользователей системы (например, ежемесячная смена пароля). Также произведена защита системы от некоторых действий пользователей, которые могут нанести вред системе. Произведена настройка аудита входа и доступа к системе в соответствии с требованиями ИБ. Результатом настроек является повышение защищенности информации, обрабатываемой с помощью компьютера, путем введения и настройки аутентификации по паролю, политики назначения прав пользователей, фиксации событий в журналах событий Windows и ограничение возможности проникновения злоумышленника в систему с помощью политик блокировки учетных записей.

5. Модель защиты

Организация представляет собой областное здание суда XXXX, которое обустроено следующим образом:

4.1 Физическая защита

- Участок размещения здания суда включает следующие функциональные зоны (СП 42.13330 и СП 4.13130):
 - 1) общественную, включающую проходы и проезды, озеленение и стоянки для автомашин (публичная зона здания суда). Также здание суда общей юрисдикции доступно для инвалидов и маломобильных групп населения (СП 59.13330).
 - 2) служебную зону. Служебная зона предназначена для приема специальных транспортных средств, осуществляющих доставку лиц, содержащихся под стражей. Она размещена со стороны въезда в боксы для посадки-высадки лиц, содержащихся под стражей. Данная зона обеспечивает свободный проезд, маневрирование и стоянку специальных транспортных средств. Число мест для стоянки специальных транспортных средств(бокс для спецавтомоблей), организуемых в служебной зоне, устанавливается заданием на проектирование (СП 152.13330.2012).
 - 3) хозяйственную зону. Хозяйственная зона предназначена для парковки закрепленных за судом служебных автомобилей, устройства площадок для размещения мусоросборников и размещение специального входа для сотрудников суда. Площадка для установки мусоросборников соответствует действующим требованиям санитарных норм (СанПиН 2.2.2/2.4.1340-03): имеет твердое (бетонное



или асфальтовое) покрытие, ограниченное бордюром по периметру. К площадке обеспечен удобный подъезд мусороуборочной техники.

4) зону-площадь застройки здания суда.

- Внутри здания суда обеспечено разделение (непересечение) потоков:

- посетителей суда (главный вход в здание суда);
- судей и работников аппарата суда (служебный вход);
- лиц, содержащихся под стражей, и конвоя.

Это требование распространяется также и на горизонтальные коридоры и холлы в здании (СП 152.13330.2012).

- Наличие охранного отдела в здании суда, который осуществляет охрану периметра здания, помещений судов в круглосуточном режиме. Так же наличие охраны с трех основных входов. И контроль охраны по выгрузке еды в буфет и сбора мусора. (Приказ ФССП России от 17.12.2015 № 596 «Об утверждении Порядка организации деятельности судебных приставов по обеспечению установленного порядка деятельности судов (зарег. в Минюсте России 25.12.2015 № 40234)
- Обеспечены выходы пожарной безопасности (Здания судов общей юрисдикции следует проектировать по классу пожарной безопасности Ф3.5. Требования к конструкциям зданий должны соответствовать СП 2.13130).
- В целях недопущения несанкционированного проникновения посторонних лиц на территорию здания федерального суда общей юрисдикции и противоправных действий в отношении объектов, расположенных на данной территории, предусмотрено общее ограждение участка с учетом градостроительных условий размещения. И вдобавок ограждена общественная зона. (СП 132.13330).
- Оконные проемы в наружных стенах всех помещений ограждены металлическими распашными решетками.
- Оконные проемы здания суда, коридоров, выходящие к пожарным лестницам, к крышам прилегающих строений и козырькам, по которым можно проникнуть в охраняемые помещения для размещения подсудимых, должны быть оборудованы металлическими распашными решетками, соответствующими требованиям пожарной безопасности.
- Стены и двери кабинетов судей, совещательных комнат суда, залов судебных заседаний, а также стены помещений облицованы звукоизолирующим материалом. (СП 51.13330).
- Помещения для лиц, задержанных судебными приставами (камерный блок) оборудован запирающейся металлической дверью.
- Двери помещений для хранения вещественных доказательств и архивов имущества от предел огнестойкости не ниже EI 30 в соответствии с СП 2.13130.



- Служебная зона должна иметь контролируемый въезд для специальных транспортных средств, предназначенных для доставки в здание суда лиц, содержащихся под стражей; сплошное ограждение высотой не менее 2,5 м, исключающее доступ посторонних лиц на территорию, а также наблюдение за происходящим в служебной зоне с внешней стороны.

4.2 Организационная защита

Согласно федеральному закону от 27.07.2006 N 149-ФЗ (ред. от 29.12.2022) "Об информации, информационных технологиях и о защите информации".

- разработка внутренней документации, которая устанавливает правила работы с компьютерной техникой и конфиденциальной информацией;
- провождение инструктажа и периодические проверки персонала; подписание дополнительных соглашений к трудовым договорам, где указана ответственность за разглашение или неправомерное использование сведений, ставших известных по работе;
- разграничение зоны ответственности, чтобы исключить ситуации, когда массивы наиболее важных данных находятся в распоряжении одного из сотрудников; организуют работу в общих программах документооборота и следят, чтобы критически важные файлы не хранились вне сетевых дисков;
- внедрение программных продуктов, которые защищают данные от копирования или уничтожения любым пользователем, в том числе топ-менеджментом организации;
- составление плана восстановления системы на случай выхода из строя по любым причинам.

4.3 Техническая защита

- При входе в здание суда установлен КПП (со всех трех основных входов: служебный, для конвоя и заключённых и общественный): турникет, стационарный металлообнаружитель, устройство контроля ручной клади (интроскоп), средства обнаружения взрывчатых и отравляющих веществ (портативные детекторы паров взрывчатых и отравляющих веществ, обнаружители часовых и электронных взрывателей и других необходимых технических средств охраны зданий судов). (СП 132.13330)
- Акустическая отделка залов судебных заседаний и помещений судей выполнена из несгораемых и трудносгораемых материалов, имеющих сертификат соответствия.
- Существует пожарно-охранная сигнализация, которая обеспечивает подачу раздельных сигналов о возникновении пожара в помещениях здания суда и попытках несанкционированного проникновения в здание суда из контролируемых зон на пульт охраны здания суда и пульт централизованной охраны органов внутренних дел. В обязательном порядке пожарно-охранной сигнализацией оснащаются помещения с повышенной опасностью возникновения пожаров и помещения,  несанкционированное

проникновение в которые может привести к возникновению чрезвычайных ситуаций и гибели людей (архивные помещения, помещения котельных, помещения вводно-распределительных устройств систем электроснабжения, встраиваемых в здание трансформаторных подстанций, и источников гарантированного электроснабжения).

Стационарная система охранной и тревожной сигнализаций размещены в следующих помещениях:

- залы судебных заседаний, совещательные комнаты суда и присяжных заседателей;
- рабочие помещения для судей;
- рабочие помещения аппарата суда, в которых ведется прием посетителей, и приемной суда;
- помещение кассы, помещение для хранения вещественных доказательств, помещения отдела государственной службы и кадров, секретного отделения, архив;
- группа помещений для лиц, содержащихся под стражей, и конвоя;
- Помещения охраны и конвоя обеспечиваются прямой телефонной связью с ближайшим отделом полиции.
- Системами автоматического пожаротушения оснащены помещения судей, для хранения вещественных доказательств, кассы, залы суда и все помещения закрытого контура согласно СП 5.13130. А также имеется противопожарная вентиляция по СП 7.13130.
- Также в здании имеются кнопки тревожной сигнализации, установленные в скрытых местах и обеспечивающие подачу сигнала тревоги на пульт в помещение охранного блока и пульт централизованной охраны органов внутренних дел.
- Здание суда снабжено системой видеонаблюдения для обеспечения контроля (наблюдение) за обстановкой внутри и снаружи здания суда. Внутри здания суда контролируются входы в здание, залы судебных заседаний, помещения для лиц, содержащихся под стражей, ограждение участка, конвойные помещения, холлы, коридоры и, при необходимости, другие помещения. Снаружи контролируются периметр здания, въезд и вход в служебную зону, входы в здание суда и отдельно стоящие здания (помещения) вспомогательного назначения.
- Персональные компьютеры в рабочих помещениях здания суда должны быть объединены в локальную сеть. Их размещение должно отвечать требованиям СанПиН 2.2.2/2.4.1340 и дополнениям к нему. ЛВС монтируется в составе общей структурированной кабельной системы СКС (для компьютеризации, телефонизации, видеоконференцсвязи и т.п.).
- Помещения архива должны обеспечивать условия, исключающие возможность появления плесени, насекомых, грызунов, пыли. Отделку помещений проводят с



использованием неагрессивных, не пылящихся материалов. В помещениях не должно быть газовых и водонесущих магистральных трубопроводов. Помещением основного назначения архива является хранилище. Хранилища должны размещаться в изолированных помещениях, которые должны быть безопасными в пожарном отношении, гарантированы от затопления, иметь запасный выход. Архивные помещения должны быть телефонизированы и оснащены системами пожарно-охранной сигнализации и пожаротушения. В системах пожаротушения применяются нейтральные, безопасные для документов вещества. Охранный режим архива и хранилищ обеспечивается выбором места размещения архива в здании, техническими средствами защиты и сигнализации. Наружные двери архива и хранилищ должны иметь металлическую облицовку и прочные запирающие устройства. На доступные извне окна устанавливают запираемые, распашные наружу металлические решетки. Помещения архива оборудуются охранной сигнализацией.(СН 426-82 – Инструкция по проектированию архивов)

4.4 Инженерная защита

Согласно документу ФСТЭК – Приказ ФСТЭК России от 18.02.2013 № 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных":

- использование системы идентификации и аутентификации (авторизации) субъектов, имеющих доступ к ПНд, и объектов ПНд;
- возможность ограничения и управления правами доступа к персональной информации;
- физическая и программная защита носителей информации;
- регистрация событий безопасности и ведение их журнала;
- применение средств антивирусной защиты;
- регулярный контроль защищенности ПНд;
- обнаружение и предотвращение вторжений, несанкционированного доступа;
- обеспечение доступности хранимых сведений, их и информационной системы, базы данных доступности;
- соблюдение требований по защите среды виртуализации, технических средств, информационной системы (ИС), ее средств, каналов и линий связи и передачи данных.

Как мы можем увидеть, спроектированная модель здания суда соответствует всем требованиям информационной безопасности по обработке ИПДн-С.

6. Конкретные инженерные средства



Рассмотрим конкретные аппаратно-технические средства деалтзации безопасной информационной системы.

- Бубен-Ультра

Подавитель "Бубен-Ультра" действует просто и эффективно. По умолчанию он генерирует неслышимый для человеческого уха ультразвуковой сигнал, который воздействует на предварительный усилитель устройств звукозаписи и создает в них нелинейные искажения. В результате шпионская техника (даже дорогая и "навороченная") становится совершенно бесполезной, так как не может выполнить своих задач (снять информацию).

В случае необходимости можно также включить генерацию сложной звуковой и речеподобной помехи, которая позволяет значительно повысить эффективность работы подавителя и гарантировать защиту важных переговоров от записи. Данные виды помех относятся к типу "акустических", то есть их человеческое ухо уже улавливает. Однако такие помехи не мешают нормальному общению собеседников, к тому же встроенный в подавитель "Бубен-Ультра" регулятор позволяет настроить громкость акустических помех.

- BugHunter X8

Это прибор, работающий на основе микропроцессорной системы. Детектор жучков находит в принципе любые радиопередающие устройства: например, аналоговые и цифровые жучки, радио микрофоны, сотовые телефоны, жучки, беспроводные скрытые видеокамеры и т.д. Стационарный подавитель сотовых телефонов GSM, 3G, 4G, GPS, Wi-Fi. Широкополосный 8-ми диапазонный стационарный подавитель сигналов, оснащенный раздельной регулировкой мощности для каждого частотного диапазона. Он парализует работу GSM-жучков, сотовых телефонов, GPS-навигаторов и трекеров, передачу данных, доступ в Интернет. Для каждого из диапазонов имеется своя антенна, что значительно повышает эффективность подавления. Очень прост в настройке и использовании. Прибор оснащен восемью передатчиками, каждый из которых работает на свою antennу и создает в радиусе от 2 до 50 метров «мертвую зону» для всех популярных мобильных устройств. Находясь в зоне действия подавителя, они перестают принимать/отправлять сообщения и звонки, а также теряют возможность выходить в мобильный Интернет. Таким образом, подавитель гарантирует конфиденциальность деловых встреч, бизнес-семинаров, научных конференций, препятствует утечкам ценной информации, а также избавляет от назойливых телефонных звонков.

- Система камер видеонаблюдения RVi

Это система интеллектуального видеонаблюдения. В комплекте также приобретено облачное сервиса видеонаблюдения RVi Cloud RVi Cloud – это современный облачный



сервис видеонаблюдения, благодаря которому для организации системы видеонаблюдения потребуется только IP-камера и доступ в Интернет. При этом пользователю не потребуется покупать у провайдера статический IP-адрес, настраивать DDNS и заниматься маршрутизацией портов (для облачного связывания всех видеокамер).

Также имеются камеры ночного видеонаблюдения той же фирмы.

- Серверы «RVi-Оператор»

Серверные решения на базе ПО «RVi-Оператор» предназначены для построения небольших, распределенных клиент-серверных систем, поддерживающих любые сетевые камеры, работающие по ONVIF. Система позволяет решать следующие задачи:

- 1) Наблюдение за объектом в реальном времени.
- 2) Ведение архива и работа с ним.
- 3) Своевременное оповещение и оперативное реагирование на возникающие ситуации.

С учетом наличия базового функционала и всесторонней интеграции с сетевыми устройствами RVi, данный программный продукт является высоко-оптимизированным с точки зрения построения системы видеонаблюдения. Интеграция ПО «RVi-Оператор» с камерами RVi позволяет задействовать встроенные базовые аналитические детекторы в камере, в том числе и детектор движения, что обеспечивает снижение требований к производительности процессора сервера за счет выполнения базовой аналитики на борту камеры. Благодаря этому уменьшается стоимость сервера. Реализована интеграция с программными обеспечениями A.C. Tech, Global, Firesec, R-Platforma.

- Противопожарная сигнализация CARCAMS T-220

Эта модель универсальной беспроводной сигнализации — простая в настройке и удобная в эксплуатации. Устройство оснащено сенсорной панелью для быстрого доступа и управления всеми функциями. Сигнализация использует новейшую систему обработки цифрового сигнала Ademco ContactID, благодаря которой ложное срабатывание исключено. Устройство обладает расширенным функционалом — помимо предупреждения о пожаре оно способно предотвратить кражу, утечку газа и грабёж со взломом.

Сигнализация будет служить основой для многофункциональной системы безопасности в помещении, поэтому не придется устанавливать несколько разных приборов. Подключается устройство к сети, есть встроенный аккумулятор на случай отключения электричества. Датчики беспроводные, их можно разместить возле окон и дверей. При срабатывании прибор включает громкую сигнализацию. При желании можно купить модификацию с GSM, тогда при срабатывании владельцу дома будет приходить сообщение на телефон.



- Охранная сигнализация MSS

Работает по следующему принципу: злоумышленник пытается проникнуть в помещение, срабатывает охранный комплекс, сигнал поступает на пульт охраны, диспетчер направляет группу быстрого реагирования и сигнал на пульт управления, прибывшая на место ГБР устраняет угрозу. Используется для ввода персональных кодов пользователей при постановке и снятии объекта с охраны. Также имеет дополнительные функции:

- 1) Тревожная кнопка

Предназначена для подачи сигнала экстренной помощи. Устанавливается стационарно в незаметном для посторонних лиц месте.

- 2) Датчик разбития стекла

Реагирует на звук разбитого стекла и посыпает сигнал на контрольную панель.

- 3) Датчик температуры

Измеряет температурные условия в охраняемом помещении и извещает контрольную панель при изменении заданной температуры.

- 4) Датчик протечки воды

При появлении воды на полу или стенах охраняемого помещения и замыкании водой сенсоров, датчик передает сигнал на контрольную панель.

- Система автоматического пожаротушения ESMI

- 1) Система автоматического порошкового пожаротушения ESMI

Предназначена для тушения в помещениях Архив, Серверная и Технический отдел.

Принцип действия – подача в зону горения мелкодисперсного порошкового состава.

- 2) Система автоматического газового пожаротушения ESMI

Используется в помещениях Руководство суда и Помещения работы судей. Принцип действия установок газового пожаротушения основан на снижении концентрации кислорода за счет поступления в зону реакции негорючего газа. В случае применения сжиженных газов, их выпуск из баллона сопровождается снижением температуры, что ведет к уменьшению температуры в зоне возгорания. Автоматические установки газового пожаротушения предназначены для создания защитной среды в определенном объеме. Тушение пожара осуществляется заполнением помещения расчетным количеством огнетушащего вещества.

- 3) Система автоматического спринклерного (водного) пожаротушения ESMI

Используется во всех оставшихся помещениях здания суда. Система, обеспечивающая подачу огнетушащего состава на очаг возгорания и состоящая из трубопроводов, оборудованных спринклерными оросителями с тепловым замком (открывается под воздействием температуры). В зависимости от нормальной (рабочей) температуры в



помещении выбираются тепловые замки с соответствующей температурой открывания (в диапазоне от 57 до 343 °C).

- Программный комплекс по обеспечению деятельности мировых судей "Астрея"

Предназначен для автоматизации процесса судебного делопроизводства, организации электронного документооборота, ведения электронных архивов решений на участках мировых судей и обеспечения надлежащего уровня защиты конфиденциальных данных.

Интерфейс пользователя и форматы представления данных системы полностью соответствуют техническим требованиям, установленным ГАС "Правосудие".

Программный комплекс "Астрея" обеспечивает регистрацию и учет уголовных дел частного обвинения; уголовных дел, поступивших с обвинительным актом (обвинительным заключением); гражданских дел искового производства, судебных приказов; материалов по административным правонарушениям; материалов судебного контроля, исполнения решений и приговоров, разрешаемых мировым судьей.

Использование данного программного комплекса позволяет организовать судебное делопроизводство на качественно высоком уровне за счет снижения затрат времени на оформление и подготовку процессуальных документов, позволит придерживаться единых стандартов делопроизводства на региональном уровне, а наличие развитой поисковой системы — формировать любые статистические отчеты и аналитические справки в кратчайший срок, обеспечивая мирового судью дополнительными информационными и функциональными возможностями.

Данный комплекс связывает все здания суда в одну сеть и позволяет безопасно вносить данные в общую БД, а также обмениваться информацией. Создает защищенные каналы для передачи документов, ещё он используется для шифрования IP-телефонии и конференц-связи. Программа VipNet осуществляет защиту в сетях TCP/IP и, как правило, может одновременно взаимодействовать с несколькими структурами корпоративной сети.

- Kaspersky Free

Camsq известен российский антивирус. С ним можно защитить свой ПК от распространенных угроз. Программа сканирует устройство в реальном времени, обеспечивает безопасность паролям и документам, а также шифрует личные данные в сети. Обеспечивает хорошую степень защиты от вирусов;

7. Анализ контролируемых зон

Технический канал утечки информации – канал передачи информации, реализуемый при помощи технических средств обработки информации.

Контролируемая зона, это территория, на которой исключается несанкционированный доступ к элементам информационной системы посторонними лицами.



К1 – зона самого здания суда (система над которой имеется полный контроль).

К2 – зона между зданием суда и забором (имеется частичный контроль).

К3 – зона за забором суда (не находится под контролем).

Зона К3

- Утечка по оптическому каналу утечки. Например, злоумышленник может пытаться извлечь полезный сигнал поем направленного в окна здания суда зондирующего лазерного луча. Данное действие злоумышленник может делать находясь на зданиях расположенных вблизи здания суда.

Противодействие нашей модели защиты: здание суда огорожено парком с высокими деревьями, что затрудняет беспрепятственному прохождению лазера. Также на всех окнах здания суда расположены кривые стекла и плотные шторы.

- Электромагнитный канал течки. Здесь злоумышленник использует побочное электромагнитное излучение от электрических устройств и проводов, работающих на территории здания суда.

Противодействие нашей модели защиты: использование экранирования и генерации шумовых импульсов для предотвращения возможности распознавания информационного полезного сигнала.

- Электрический канал утечки. Невозможен так как доступ к проводным устройствам возможен лишь на территории К1 и К2.
- Акустические каналы утечки в зоне К3 невозможны.

Зона К2

- Утечка по оптическому каналу утечки. Например, злоумышленник может пытаться подсмотреть конфиденциальную информацию через окна.

Противодействие нашей модели защиты: контролирование территории К2 круглосуточной охраной и система видеонаблюдения.

- Электромагнитный канал течки. Здесь злоумышленник использует побочное электромагнитное излучение от электрических устройств и проводов, работающих на территории здания суда.

Противодействие нашей модели защиты: использование экранирования и генерации шумовых импульсов для предотвращения возможности распознавания информационного полезного сигнала.

- Электрический канал утечки. Злоумышленник может попытаться в выходящие электрические провода клеммы для снятия электрического сигнала, содержащего опасную информацию.



Противодействие нашей модели защиты: контролирование территории К2 круглосуточной охраной и система видеонаблюдения.

- Акустические каналы утечки возможны при прослушивании через отверстия в стенах (розетки) и при помощи СТС.

Противодействие нашей модели защиты: использование звуконепроницаемых стен и во время важных переговоров возможна генерация специальными устройствами ультразвуковых и акустических помех.

Зона К1

- Утечка по оптическому каналу утечки. Например, злоумышленник может подсмотреть конфиденциальную информацию, с которой работает привилегированный сотрудник. В качестве злоумышленника здесь может быть работник-инсайдер.

Противодействие нашей модели защиты: система видеонаблюдения и регистрация журналов безопасности на компьютере и отчет о частоте посещения архива (если злоумышленник высокостоящее лицо).

- Электромагнитный канал течки. Здесь злоумышленник использует побочное электромагнитное излучение от электрических устройств и проводов, работающих на территории здания суда.

Противодействие нашей модели защиты: использование экранирования и генерации шумовых импульсов для предотвращения возможности распознавания информационного полезного сигнала, система видеонаблюдения.

- Электрический канал утечки. Злоумышленник может попытаться в выходящие электрические провода клеммы для снятия электрического сигнала, содержащего опасную информацию.

Противодействие нашей модели защиты: контролирование территории К1 круглосуточной охраной и система видеонаблюдения.

- Акустические каналы утечки возможны при прослушивании через отверстия в стенах (розетки) и при помощи СТС.

Противодействие нашей модели защиты: использование звуконепроницаемых стен и во время важных переговоров возможна генерация специальными устройствами ультразвуковых и акустических помех.

ЗАКЛЮЧЕНИЕ

В результате работы получили защищённый объект – здание областного суда. Согласно нормативно-правовым нормам по обеспечению конфиденциальности, целостности



и доступности ИПДн-С установлены соответствующие уровни защиты: аппаратный, инженерный и организационный.

