Приложение № 1

к приказу №\_\_\_\_\_

от «\_\_\_\_» \_\_\_\_\_\_\_\_2018г.

# Концепция

# информационной безопасности

# судебной системы

**СОДЕРЖАНИЕ**

[ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ 7](#_Toc1458647088)

[1. ОБЩИЕ ПОЛОЖЕНИЯ 10](#_Toc696543436)

[1.1. Назначение Концепции 10](#_Toc1938229788)

[1.2. Сфера применения Концепции 10](#_Toc1023721303)

[1.3. Правовая основа Концепции 10](#_Toc360088921)

[1.4. Цели и задачи обеспечения безопасности информации 10](#_Toc316462064)

[2. ОБЪЕКТЫ ЗАЩИТЫ 12](#_Toc297148517)

[2.1. Объектами защиты судебной системы являются: 12](#_Toc1790869008)

[2.2. Информационные ресурсы судебной системы 12](#_Toc1044392932)

[2.3. Средства и системы обработки информации 13](#_Toc335334970)

[2.4. Средства обеспечения 15](#_Toc295080097)

[3. МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В СУДЕБНОЙ СИСТЕМЕ 16](#_Toc1890238888)

[3.1. Основные факторы, воздействующие на информационную безопасность судебной системы 16](#_Toc1589020093)

[3.2. Угрозы безопасности информации и их источники 16](#_Toc943256759)

[3.3. Классификация способов реализации угроз информационной безопасности 17](#_Toc1553327887)

[3.3.1. Пути реализации непреднамеренных субъективных угроз безопасности информации 17](#_Toc897474635)

[3.3.2. Пути реализации преднамеренных субъективных угроз безопасности информации 18](#_Toc715540757)

[3.3.3. Пути реализации непреднамеренных техногенных угроз безопасности информации 19](#_Toc321387309)

[3.3.4. Пути реализации непреднамеренных стихийных угроз безопасности информации 20](#_Toc1214909546)

[3.4. Классификация нарушителей информационной безопасности судебной системы 20](#_Toc1388923858)

[3.5. Обобщенная модель угроз безопасности информации судебной системы 21](#_Toc175894365)

[4. ОРГАНИЗАЦИЯ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СУДЕБНОЙ СИСТЕМЫ 25](#_Toc680081872)

[4.1. Организационно-штатная структура подразделений отвечающих за обеспечение информационной безопасности судебной системы 25](#_Toc1606918537)

[4.2. Порядок разработки и эксплуатации системы обеспечения информационной безопасности судебной системы 25](#_Toc1044022217)

[4.3. Организация системы комплексного мониторинга и контроля состояния информационной безопасности судебной системы 26](#_Toc1859780025)

[5. МЕРОПРИЯТИЯ ПО РЕШЕНИЮ ЗАДАЧ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СУДЕБНОЙ СИСТЕМЫ 29](#_Toc771853579)

[5.1. Организационно-режимные мероприятия 29](#_Toc1973840207)

[5.2. Мероприятия по физической защите объектов и средств информатизации судебной системы 29](#_Toc1578470215)

[5.3. Мероприятия по обеспечению катастрофоустойчивости информационно-телекоммуникационной системы 33](#_Toc86166336)

[5.4. Мероприятия по решению задач защиты информации от несанкционированного доступа в информационную инфраструктуру. 34](#_Toc1821967970)

[5.5. Мероприятия по обеспечению безопасного информационного взаимодействия судебной системы с организациями, министерствами и ведомствами 36](#_Toc1222483004)

[5.6. Мероприятия по организации криптографической защиты информации 37](#_Toc1544813424)

[5.7. Мероприятия по антивирусной защите информационных ресурсов судебной системы 38](#_Toc371027759)

[5.8. Мероприятия по обнаружению компьютерных атак на информационные ресурсы и телекоммуникационные системы 40](#_Toc1013229144)

[5.9. Мероприятия по совершенствованию организационно-штатной структуры подразделений, отвечающих за обеспечение информационной безопасности 41](#_Toc421051079)

[5.10. Мероприятия по повышению квалификации специалистов в области защиты информации 41](#_Toc731116680)

[5.11. Мероприятия по внутреннему аудиту информационных систем 41](#_Toc1329691208)

## ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

АУТЕНТИФИКАЦИЯ – проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности.

СПЕЦИАЛИСТ ЗАЩИТЫ - субъект доступа, ответственный за защиту автоматизированной системы от несанкционированного доступа к информации

БЕЗОПАСНОСТЬ ИНФОРМАЦИИ -состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системы, от внутренних или внешних угроз.

ВСПОМОГАТЕЛЬНЫЕ ТЕХНИЧЕСКИЕ СРЕДСТВА И СИСТЕМЫ - технические средства и системы, не предназначенные для передачи, обработки и хранения конфиденциальной информации, размещаемые совместно с основными техническими средствами и системами или в защищаемых помещениях

Доступ к информации - ознакомление с информацией, ее обработка, в частности, копирование, модификация или уничтожение информации.

Защита информации (ЗИ) - деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на информацию.

Защита от несанкционированного доступа – деятельность, направленная на предотвращение получения информации заинтересованным субъектом (или воздействия на информацию) с нарушением установленных прав или правил.

Защищаемая информация - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

ЗАЩИЩАЕМЫЕ ПОМЕЩЕНИЯ – помещения, специально предназначенные для проведения конфиденциальных мероприятий (совещаний, обсуждений, конференций, переговоров и т.п.).

ЗАЩИЩЕННОЕ СРЕДСТВО ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ (ЗАЩИЩЕННАЯ АВТОМАТИЗИРОВАННАЯ СИСТЕМА) – средство вычислительной техники (автоматизированная система), в которой реализован комплекс средств защиты.

ИНФОРМАЦИОННЫЕ РЕСУРСЫ – отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах)

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

ИДЕНТИФИКАТОР ДОСТУПА – уникальный признак субъекта или объекта доступа.

КОМПЛЕКС СРЕДСТВ ЗАЩИТЫ – совокупность программных и технических средств, создаваемая и поддерживаемая для обеспечения защиты средств вычислительной техники или автоматизированных систем от несанкционированного доступа к информации.

КОНТРОЛИРУЕМАЯ ЗОНА - пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание сотрудников и посетителей организации, а также транспортных средств.

КОНФИДЕНЦИАЛЬНАЯ ИНФОРМАЦИЯ – информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации

НЕСАНКЦИОНИРОВАННЫЙ ДОСТУП - доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

НАРУШИТЕЛЬ ПРАВИЛ РАЗГРАНИЧЕНИЯ ДОСТУПА – субъект доступа, осуществляющий несанкционированный доступ к информации.

ОБЪЕКТ ДОСТУПА – единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа.

ОРГАНИЗАЦИЯ ЗАЩИТЫ ИНФОРМАЦИИ – содержание и порядок действий по обеспечению защиты информации

ОСНОВНЫЕ ТЕХНИЧЕСКИЕ СРЕДСТВА И СИСТЕМЫ - технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи конфиденциальной информации

ПАРОЛЬ – идентификатор субъекта доступа, который является его (субъекта) секретом.

СИСТЕМА РАЗГРАНИЧЕНИЯ ДОСТУПА – совокупность реализуемых правил разграничения доступа в средствах вычислительной техники или автоматизированных системах

САНКЦИОНИРОВАННЫЙ ДОСТУП К ИНФОРМАЦИИ – доступ к информации, не нарушающий правила разграничения доступа.

СЕРТИФИКАТ ЗАЩИТЫ – документ, удостоверяющий соответствие средства вычислительной техники или автоматизированной системы набору определенных требований по защите от несанкционированного доступа к информации и дающий право разработчику на использование и (или) распространение их как защищенных.

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА - комплекс организационных мер и программно-технических (в том числе криптографических) средств защиты от несанкционированного доступа к информации в автоматизированных системах.

СРЕДСТВО ЗАЩИТЫ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА – программное, техническое или программно-техническое средство, предназначенное для предотвращения или существенного затруднения несанкционированного доступа.

СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ –реализующие алгоритмы криптографического преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы, предназначенные для защиты информации, обеспечивающие безопасность информации при ее обработке, хранении и передаче по каналам связи.

СУБЪЕКТ ДОСТУПА – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

УИТ “АДИЛЕТ СОТ” - учреждение информационных технологий “Адилет сот” при Судебном департаменте при Верховном суде Кыргызской Республики

ЦЕЛОСТНОСТЬ ИНФОРМАЦИИ – устойчивость информации к несанкционированному или случайному воздействию на нее в процессе обработки техническими средствами, результатом которого может быть уничтожение и искажение информации.

### ОБЩИЕ ПОЛОЖЕНИЯ

### Назначение Концепции

Настоящая Концепция определяет систему взглядов на проблему обеспечения комплексной безопасности информации и устанавливает порядок организации и правила обеспечения информационной безопасности в судебной системе, распределение функций и ответственности за обеспечение информационной безопасности в судебной системе и требования по информационной безопасности к информационным средствам, применяемым в судебной системе. Документ представляет собой основу для разработки и реализации комплексных целевых задач обеспечения защиты информации на объектах информатизации судебной системы.

### Сфера применения Концепции

Требования настоящей Концепции обязательны для всех субъектов судебной системы и распространяются на:

* автоматизированные системы;
* средства телекоммуникаций;
* помещения;
* сотрудников судебной системы.

Внутренние документы Судебной системы, затрагивающие вопросы, электронных систем и взаимодействия с IT технологиями должны разрабатываться с учетом положений Концепции и не противоречить им.

### Правовая основа Концепции

Правовую основу Концепции составляют:

* Конституция Кыргызской Республики;
* Закон “О защите государственных секретов Кыргызской Республики” от 14.04.1994 № 1476-XII;
* Закон “Об информатизации и электронном управлении” от 8.10.1999 года № 107;
* Закон “Об электронном документе и электронной цифровой подписи” от 17.07.2004 года № 92;
* Закон “Об информации персонального характера” от 14 апреля 2008 года N 58;
* Закон “Об электронной подписи” от 19 июля 2017 года № 128;
* Закон “Об электронном управлении” от 19 июля 2017 года № 127.

### Цели и задачи обеспечения безопасности информации

Главная цель обеспечения безопасности информации, циркулирующей в судебной системе, - реализация положений законодательных актов КР и нормативных требований по защите информации ограниченного доступа (далее по тексту - конфиденциальной или защищаемой информации) и предотвращение ущерба в результате разглашения, утраты, утечки, искажения и уничтожения информации, ее незаконного использования и нарушения работы информационно-телекоммуникационной системы судебной системы.

Основными целями обеспечения безопасности информации являются:

* предотвращение утечки, хищения, искажения, подделки информации, циркулирующей в судебной системе;
* предотвращение нарушений прав личности граждан КР на сохранение конфиденциальности информации, циркулирующей в судебной системе;
* предотвращение несанкционированных действий по блокированию информации;

Основными задачами обеспечения безопасности информации являются:

* соответствие положениям законодательных актов и нормативным требованиям по защите информации;
* своевременное выявление, оценка и прогнозирование источников угроз информационной безопасности, причин и условий, способствующих нанесению ущерба интересам граждан КР и сотрудникам судебной системы, нарушению нормального функционирования и развития информационной инфраструктуры судебной системы;
* создание механизма оперативного реагирования на угрозы информационной безопасности и негативные тенденции в системе информационных отношений;
* эффективное пресечение незаконных посягательств на информационные ресурсы, технические средства и информационные технологии, в том числе с использованием организационно-правовых и технических мер и средств защиты информации;
* создание условий для максимально возможного возмещения и локализации наносимого интересам судебной системе ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения информационной безопасности;
* разработка нормативно-правовой базы обеспечения информационной безопасности, координация деятельности аппаратов судебной системы по обеспечению защиты информации;
* развитие системы защиты, совершенствование ее организации, форм, методов и средств предотвращения, парирования и нейтрализации угроз информационной безопасности и ликвидации последствий ее нарушения;
* создание и применение защищенных информационных объектов и центров обработки защищаемой информации;
* развитие и совершенствование защищенного юридически значимого электронного документооборота.
* создание механизмов, обеспечивающих контроль системы информационной безопасности и гарантии достоверности выполнения установленных требований информационной безопасности
* создание механизмов управления системой информационной безопасности.

### ОБЪЕКТЫ ЗАЩИТЫ

### Объектами защиты судебной системы являются:

* информационные ресурсы;
* средства и системы обработки информации;
* средства и системы защиты информации, в т.ч. криптографической защиты информации;
* Помещения, здания судебной системы.

### Информационные ресурсы судебной системы

Под информационными ресурсами в судебной системе понимается совокупность сведений в электронном и, бумажном виде (база данных, электронная почтовая система, электронная библиотека, реестр, кадастр, фонд, архив и другие виды информационных массивов), поддерживаемые программно-техническими средствами автоматизированной информационной системы. Информационные ресурсы представляют собой хранилища данных, из которого путем специализированной обработки пользователю предоставляется информация на электронных или бумажных носителях, в том числе в виде отдельных фрагментов баз данных, отчетов и справок.

Технологической основой формирования информационных ресурсов является программно-техническая среда автоматизированных информационных систем, используемых в судебной системе.

Используемые в информационных системах судебной системы технологии взаимодействия при обработке информационных ресурсов включают:

* электронную почту;
* электронный обмен файлами;
* обмен файлами на внешних носителях;
* Доступ к глобальной сети интернет;
* технологию терминального доступа для удаленного взаимодействия с сотрудниками судебной системы;

Основным источником информации для наполнения первичных баз данных являются документы и сообщения, поступающие от субъектов судебной системы.

Информационное и функциональное взаимодействие узлов сетевой инфраструктуры судебной системы осуществляется на основе интегрированных (логически единых) баз данных, обеспечивающих должностных лиц структурных подразделений судебной системы требуемой информацией.

Обмен информацией осуществляется:

* внутри сети судебной системы через зашифрованный канал обмена данными ;
* между узлами судебной системы и информационными системами государтвенных организаций и ведомств в соответствии с соглашениями безопасности и протоколами по обмену информацией.

Вся информация, хранимая, обрабатываемая или передаваемая в рамках судебной системы проходит по каналам связи благодаря использованию средств криптографии (шифрования, аутентификации, инфраструктуры открытых ключей, средств для защиты от повторов и изменений, передаваемых по логической сети сообщений), классифицирована по степени важности и критичности на следующие категории.

Конфиденциальная информация

К конфиденциальной относится информация, составляющая коммерческую тайну, информация о фактах, событиях и обстоятельствах частной жизни гражданина КР, позволяющая идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных законом КР случаях, а также служебная информация, служебные и судебные материалы, судебные дела и любая другая закрытая информация, являющаяся собственностью судебной системы.

При хранении, передаче и обработке данной информации необходимо обеспечить максимальный уровень её защиты.

Служебная информация

К служебной информации могут быть отнесены любые сведения, относящиеся к деятельности аппаратов судебной системы, несанкционированное распространение которых может привести к отрицательным экономическим, этическим или иным последствиям для судебной системы и государства. Хранение, обработка и передача такой информации должна осуществляться в соответствии с требованиями настоящего документа.

Рабочая информация

Рабочая информация включает в себя сведения, имеющие отношение к внутренней деятельности аппаратов судебной системы и не относящиеся к конфиденциальной или служебной информации. При хранении, передаче и обработке такой информации необходимо обеспечить максимальный уровень её целостности и аутентичности в соответствии с положениями настоящего документа.

Прочие виды информации

Для прочих видов информации порядок хранения, передачи и обработки с использованием автоматизированных систем не регламентируется.

### Средства и системы обработки информации

Средства и системы обработки информации представляют собой совокупность программного обеспечения и технических средств обработки и передачи информации, а также систему телекоммуникаций.

Техническое обеспечение включает следующие компоненты:

* серверная инфраструктура;
* рабочие станции сотрудников судебной системы;
* средства ввода/вывода информации;
* система хранения данных и резервное архивирование критически важных данных;
* активное и пассивное сетевое оборудование локальной вычислительной сети;
* сетевая инфраструктура;
* средства бесперебойного электро питания.

Система телекоммуникаций, поддерживает информационный обмен между внутренними абонентами и информационными системами судебной системы, а также информационную связь с гражданами КР. В системной архитектуре телекоммуникаций выделены следующие функциональные подсистемы:

* Транспортная подсистема (система обработки запросов, установления соеденений для обмена данными);
* Ведомственная телефонная сеть;
* Подсистема удаленного доступа к информационным ресурсам;
* Подсистема электронной почты;
* Подсистема сервисов глобальной сети Интернет;
* Подсистема управления, мониторинга и обслуживания системы телекоммуникации.

В состав программного обеспечения информационных систем входят:

* общесистемное программное обеспечение;
* специализированное (прикладное) программное обеспечение.

Общесистемное программное обеспечение включает в себя:

* серверные и клиентские операционные системы;
* система управления базами данных;
* пакеты офисных программ;
* антивирусные программы;
* пакеты программ для групповой работы
* терминальные серверные и клиентские программы
* средства электронной почты;
* средства управления информационной безопасностью;
* средства управления и администрирования системой;

Специальное программное обеспечение является совокупностью аналитических и логических методов и алгоритмов, программ их реализации, отражающих специфику автоматизируемых процессов и предназначенных для обеспечения деятельности должностных лиц судебной системы.

### Средства обеспечения

Под средствами обеспечения понимаются вспомогательные инженерно-технические системы, не участвующие в обработке информации, содержащей конфиденциальные сведения. В общем виде к этим системам относятся:

* системы электропитания и заземления объектов;
* система резервного электропитания;
* системы связи (ведомственной, междугородней, городской, внутренней), не предназначенной для закрытых переговоров;
* системы пожарной и охранной сигнализации;
* электронные системы контроля и управления доступом на территорию и в помещения;
* система контроля и управления доступом в помещения с серверным оборудованием;
* системы громкоговорящей связи и оповещения;
* системы кондиционирования, отопления и воздухоснабжения;
* система цифрового видеонаблюдения.

### 

### МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В СУДЕБНОЙ СИСТЕМЕ

### Основные факторы, воздействующие на информационную безопасность судебной системы

Основными факторами, воздействующими на информационную безопасность судебной системы, являются:

* Природный фактор. Совокупность угроз природного характера, являющихся следствием воздействия естественной непреодолимой силы (стихии) – землетрясения, метеорологические катаклизмы и т.п., приводящие к устойчивому нарушению функционирования информационных и телекоммуникационных ресурсов, вплоть до их утраты или физического уничтожения. Вероятность определяется спецификой территории, на которой дислоцируется защищаемый объект – многолетними метеорологическими наблюдениями, геотектоническими данными и др.
* Техногенный фактор. Совокупность угроз искусственного характера, вызванных результатами человеческой деятельности (цивилизации) – пожары, взрывы, затопления, радиационные и химические заражения, энергетические аварии, разрешение коммуникаций, в том числе – в результате террористических актов, диверсий, массовый беспорядков и ведения боевых действий.
* Системный фактор. Возникновение угрозы целостности информации и (или) функционированию информационно-телекоммуникационных средств, систем и сетей в результате ошибок в их проектировании и разработке или возникновения внутрисистемных сбоев (фатальных ошибок) при их эксплуатации, в том числе – из-за несовершенства или конфликтов программного обеспечения или неисправности оборудования.
* Человеческий фактор. Возникновение угрозы безопасности информации в результате отсутствия профессиональных навыков, недостаточной подготовки, халатности, ненадлежащего исполнения обязанностей или злого умысла персонала, эксплуатирующего информационно-телекоммуникационные средства, системы и сети, разработчиков программного обеспечения и пользователей, имеющих допуск к информации на законном основании. Нарушение правил эксплуатации электронно-вычислительной машины, их систем и сетей лицами, ответственными за эту работу.
* Криминальный фактор. Целенаправленное внешнее воздействие на информационные ресурсы и информационно-телекоммуникационные средства, системы и сети («атаки», вторжения) с целью уничтожения, блокирования или копирования информации, разработка и внедрение вредоносных программ (вирусов, симуляторов, «троянских» программ, клавиатурных перехватчиков и др.) внедрение специальных технических средств для негласного получения информации.

### Угрозы безопасности информации и их источники

Информация, обрабатываемая в инормационной инфраструктуре судебной системы, дает потенциальную возможность для проявления угроз безопасности, вызванных действиями, процессами или явлениями, приводящими к нанесению ущерба судебной системе. Предусматривается два типа угроз безопасности:

* связанные с утечкой информации (разглашение, утечка, несанкционированный доступ); Одним из возможных источников данной угрозы является сеть Wi-Fi. Так как данная технология предназначена для общедоступного доступа к сети интернет, при использовани данной технологии возникают следующие типы угроз для сетевой инфраструктуры судебной системы: возможное подключение неавторизованных пользователей к сети, клонирование точки доступа, атака с целью отказа в обслуживании сетевых устройств и подбор ключей сетевых устройств.
* связанные с несанкционированным воздействием на информацию и ее носители (искажение, уничтожение, копирование, блокирование, утрата, сбой функционирования носителя информации, сбои и ошибки техники, ошибки пользователей, природные явления, другие случайные воздействия).

Основными источниками угроз безопасности информации являются:

* Стихийные: стихийные бедствия, катаклизмы;
* Техногенные: аварии, сбои и отказы оборудования (технических средств);
* Ошибки проектирования и разработки компонентов автоматизированной системы (аппаратных средств, технологии обработки информации, программного обеспечения и т. п.);
* Антропогенные: ошибки эксплуатации;
* Антропогенные: Преднамеренные действия нарушителей и злоумышленников.

### Классификация способов реализации угроз информационной безопасности

Угрозы информационной безопасности по отношению к защищаемым объектам могут быть разделены на:

* угрозы, связанные с применением технических средств;
* угрозы, связанные с использованием программного обеспечения;
* угрозы, связанные с нарушением технологического процесса обмена данными;
* угрозы, связанные с использованием сетей передачи данных.

### Пути реализации непреднамеренных субъективных угроз безопасности информации

Сотрудники судебной системы являются внутренними источниками случайных воздействий, т.к. имеют непосредственный доступ к процессам обработки информации и могут совершать непреднамеренные ошибки и нарушения действующих правил, инструкций и процедур.

Основные пути реализации непреднамеренных искусственных (субъективных) угроз информационной безопасности (действия, совершаемые людьми случайно, по незнанию, невнимательности или халатности, из любопытства, но без злого умысла) следующие:

* Действия сотрудников, приводящие к частичному или полному отказу системы или нарушению работоспособности аппаратных или программных средств: отключению оборудования или изменению режимов работы устройств и программ; разрушению информационных ресурсов системы (неумышленная порча оборудования, удаление, искажение программ или файлов с важной информацией, в том числе системных, повреждение каналов связи, неумышленная порча носителей информации и т.п.)
* Несанкционированный запуск технологических программ, способных при некомпетентном использовании вызывать потерю работоспособности системы (зависания или зацикливания) или осуществляющих необратимые изменения в системе (форматирование или реструктуризацию носителей информации, удаление данных и т.п.)
* Несанкционированное внедрение и использование неучтенных программ (игровых, обучающих, технологических и других, не являющихся необходимыми для выполнения сотрудниками своих служебных обязанностей) с последующим необоснованным расходованием ресурсов (процессорного времени, оперативной памяти, памяти на внешних носителях и т.п.)
* Непреднамеренное заражение компьютера вирусами
* Разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования или эллектронно-цифровой подписи, идентификационных карточек, пропусков и т.п.)
* Игнорирование организационных ограничений (установленных правил) при работе в системе
* Некомпетентное использование системы безопасности или неправомерное отключение средств защиты сотрудниками судебной системы имеющими технический доступ к информационным системам.
* Ввод ошибочных данных
* Ошибки программного обеспечения

### Пути реализации преднамеренных субъективных угроз безопасности информации

Основные возможные пути умышленной дезорганизации работы, вывода информационных систем судебной системы из строя, проникновения в систему и несанкционированного доступа к информации (с корыстными целями, по принуждению, из желания отомстить и т.п.) могут быть следующими:

* Физическое разрушение или вывод из строя всех или отдельных наиболее важных компонентов автоматизированной системы (устройств, носителей важной системной информации, лиц из числа персонала и т.п.), отключение или вывод из строя подсистем обеспечения функционирования вычислительных систем (электропитания, линий связи и т.п.)
* Хищение носителей информации (распечаток, магнитных дисков, лент, микросхем памяти, запоминающих устройств и целых электронно-вычислительных машин), хищение производственных отходов (распечаток, записей, списанных носителей информации и т.п.)
* Несанкционированное копирование носителей информации, чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств.
* Использование чужих прав по доступу к ресурсам автоматизированной системы путем незаконного получение паролей и других реквизитов разграничения доступа (агентурным путем, используя халатность пользователей, путем подбора, путем имитации интерфейса системы программными закладками и т.д.).
* Несанкционированное использование автоматизированного рабочего места пользователей, имеющих уникальные физические характеристики, такие как имя рабочей станции в сети, физический адрес, адрес в системе связи и другие.
* Несанкционированная модификация программного обеспечения – внедрение программных "закладок" и "вирусов" ("троянских коней" и "жучков"), то есть таких участков программ, которые не нужны для осуществления заявленных функций, но позволяющих преодолевать систему защиты, скрытно и незаконно осуществлять доступ к системным ресурсам с целью регистрации и передачи защищаемой информации или дезорганизации функционирования автоматизированной системы
* Перехват данных, передаваемых по каналам связи, и их анализ с целью получения сведений, в том числе ограниченного распространения и выяснения протоколов обмена, правил вхождения в связь и авторизации пользователей и последующих попыток их имитации для проникновения в систему
* Вмешательство в процесс функционирования автоматизированной системы сетей общего пользования с целью несанкционированной модификации данных, доступа к сведениям ограниченного распространения, дезорганизации работы подсистем автоматизированной системы и т.п.

### Пути реализации непреднамеренных техногенных угроз безопасности информации

* закупки несовершенных, устаревших или неперспективных средств информатизации и информационных технологий;
* аварии в системах электропитания;
* аварии в системах отопления и водоснабжения в непосредственной близости к техническим средствам обработки информации;
* нарушение температурного режима в помещениях с критическим оборудованием (серверы, узлы связи);
* неумышленное повреждение внешних кабельных систем связи строительными организациями, физическими лицами и т.п. в результате проведения несогласованных работ в местах прокладки кабелей связи;
* возникновение пожаров в непосредственной близости к техническим средствам обработки информации в результате неисправной электропроводки, неисправных технических средств, нарушения сотрудниками правил противопожарной безопасности.

### Пути реализации непреднамеренных стихийных угроз безопасности информации

* Разрушение зданий, отдельных помещений, в которых установлены технические средства обработки информации, хранилища данных в результате стихийных бедствий (наводнений, землетрясений, ураганов) в районе размещения объекта информатизации судебной системы;
* воздействие атмосферного электричества на технические средства обработки информации и системы обеспечения (электропитание, охранная, пожарная сигнализация и т.п.).

### Классификация нарушителей информационной безопасности судебной системы

При анализе угроз информационной безопасности используется модель нарушителя по признаку принадлежности к судебной системе. В соответствии с этой моделью все нарушители делятся на две основные группы: внутренние и внешние.

Под внутренними нарушителями подразумеваются все сотрудники судебной системы, имеющие санкционированный доступ на территорию объектов судебной системы или к ресурсам автоматизированной системы. Под внешними нарушителями подразумеваются все остальные лица.

Внутренним нарушителем может быть лицо из следующих категорий сотрудников:

* пользователи информационных ресурсов;
* обслуживающий персонал (IT консультанты, специалисты (администраторы) автоматизированной системы, специалисты (администраторы) баз данных);
* сотрудники-программисты, сопровождающие системное, общее и прикладное программное обеспечение;
* другие сотрудники подразделений УИТ “Адилет сот”, имеющие санкционированный доступ в здания, где расположено оборудование передачи и обработки информации автоматизированной системы судебных органов.

Предполагается, что несанкционированный доступ на объекты судебной системы посторонних лиц исключается организационными мерами (охрана территории, организация пропускного режима).

Внешние нарушители информационной безопасности - лица, самостоятельно осуществляющие создание методов и средств реализации атак, а также самостоятельно реализующие атаки, совершающие свои действия с целью нанесения ущерба судебной системе (съем информации, искажение информации, разрушение системного или прикладного программного обеспечения).

Потенциальные нарушители делятся на три группы:

* 1 группа - субъекты, не имеющие доступ в пределы подконтрольных зон судебной системы.
* 2 группа - субъекты, не имеющие доступ к работе штатными средствами автоматизированной системы судебной системы, но имеющие доступ в помещения, где они размещаются.
* 3 группа – субъекты, имеющие доступ к работе со штатными средствами автоматизированной системы судебной системы.

Квалификация потенциального нарушителя.

* А – не является специалистом в области вычислительной техники.
* В – самый низкий уровень возможностей – запуск задач (программ) из фиксированного набора, реализующих заранее предусмотренные функции при обработке информации.
* С – возможности создания и запуска собственных программ с новыми функциями по обработке информации.
* Д – возможность управления функционированием автоматизированной системы, т.е. воздействием на базовое программное обеспечение системы, на конфигурацию ее оборудования.
* Е – включает весь объем возможностей лиц, осуществляющих проектирование, реализацию и ремонт технических средств автоматизированной системы, вплоть до включения в состав автоматизированной системы собственных технических средств с новыми функциями по обработке информации.

Наряду с классификацией, приведенной выше, нарушителей информационной безопасности можно разделить на следующие виды - неосторожные (халатные), манипулируемые, саботажники, нелояльные и мотивируемые извне.

### Обобщенная модель угроз безопасности информации судебной системы

| Угроза информационной безопасности | Источник угроз | Способы реализации угроз |
| --- | --- | --- |
| I. Получение информации | 1. Антропогенный | а) Разглашение, передача или утрата атрибутов разграничения доступа |
| б) Внедрение агентов в число персонала системы |
| в) Хищение носителей информации |
| г) Незаконное получение паролей и других реквизитов разграничения доступа |
| д) Несанкционированная модификация программного обеспечения |
| е) Перехват данных, передаваемых по каналам связи |
| ж) Несанкционированное копирование носителей информации, чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств |
| II. Анализ характеристик информации | 1. Антропогенный | а) Хищение носителей информации  хищение производственных отходов |
| б) чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств |
| в) Несанкционированная модификация программного обеспечения |
| г) Перехват данных, передаваемых по каналам связи, и их анализ |
| III. Изменение (искажение, подмена) информации | 1. Антропогенный | а) Несанкционированный запуск технологических программ, способных при некомпетентном использовании вызывать потерю работоспособности системы (зависания или зацикливания) или осуществляющих необратимые изменения в системе (форматирование или реструктуризацию носителей информации, удаление данных и т.п.) |
| б) Непреднамеренное заражение компьютера вирусами |
| в) Ввод ошибочных данных |
| г) Вмешательство в процесс функционирования АС сетей общего пользования с целью несанкционированной модификации данных |
| 2. Техногенный | а) аварии в системах электропитания |
| б) нарушение температурного режима в помещениях с критическим оборудованием (серверы, узлы связи) в результате неисправности систем кондиционирования |
| IV. Нарушение информации | 1. Антропогенный | а) Действия сотрудников, приводящие к частичному или полному отказу системы или нарушению работоспособности аппаратных или программных средств |
| б) Несанкционированное внедрение и использование неучтенных программ (игровых, обучающих, технологических и других, не являющихся необходимыми для выполнения сотрудниками своих служебных обязанностей) с последующим необоснованным расходованием ресурсов (процессорного времени, оперативной памяти, памяти на внешних носителях и т.п.) |
| в) Непреднамеренное заражение компьютера вирусами |
| г) Игнорирование организационных ограничений (установленных правил) при работе в системе |
| д) Ввод ошибочных данных |
| 2. Техногенный | а) аварии в системах электропитания |
| б) нарушение температурного режима в помещениях с критическим оборудованием (серверы, узлы связи) в результате неисправности систем кондиционирования |
| V. Нарушение работоспособности систем | 1. Антропогенный | а) Действия сотрудников, приводящие к частичному или полному отказу системы или нарушению работоспособности аппаратных или программных средств |
| б) Физическое разрушение или вывод из строя всех или отдельных наиболее важных компонентов автоматизированной системы |
| 2. Техногенный | а) закупки несовершенных, устаревших или неперспективных средств информатизации и информационных технологий; |
| б) аварии в системах электропитания; |
| в) аварии в системах отопления и водоснабжения в непосредственной близости к техническим средствам обработки информации; |
| г) нарушение температурного режима в помещениях с критическим оборудованием (серверы, узлы связи) в результате неисправности систем кондиционирования; |
| д) неумышленное повреждения внешних кабельных систем связи строительными организациями, физическими лицами и т.п. в результате проведения несогласованных работ в местах прокладки кабелей связи; |
| е) возникновение пожаров в непосредственной близости к техническим средствам обработки информации в результате неисправной электропроводки, неисправных технических средств, нарушения сотрудниками правил противопожарной безопасности. |
| 3. Стихийный | а) Разрушение зданий, отдельных помещений |
| б) воздействие атмосферного электричества |
| в) возникновение стихийных очагов пожаров |

Наложение угроз безопасности информации на модель серверной и сетевой инфраструктуры судебной системы позволяет оценить их опасность и методом исключения определить наиболее актуальные для конкретного объекта защиты. Кроме того, можно оценить объемы необходимых работ и выбрать магистральное направление по обеспечению безопасности информации.

[Введите цитату из документа или краткое описание интересного события. Надпись можно поместить в любое место документа. Для изменения форматирования надписи, содержащей броские цитаты, используйте вкладку "Средства рисования".]

[Введите цитату из документа или краткое описание интересного события. Надпись можно поместить в любое место документа. Для изменения форматирования надписи, содержащей броские цитаты, используйте вкладку "Средства рисования".]

### ОРГАНИЗАЦИЯ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СУДЕБНОЙ СИСТЕМЫ

### Организационно-штатная структура подразделений отвечающих за обеспечение информационной безопасности судебной системы

Общее руководство системой информационной безопасности и принятие всех решений по вопросам ее функционирования осуществляет Управляющий УИТ “Адилет сот”.

Руководство и контроль за выполнением мероприятий по защите информации в судебной системе осуществляют их руководитель отдела по информационной безопасности.

Исполнительный отдел Судебной системы - отдел по информационной безопасности УИТ “Адилет сот”.

### Порядок разработки и эксплуатации системы обеспечения информационной безопасности судебной системы

Жизненный цикл системы обеспечения информационной безопасности судебной системы включает этап развертывания и этапы постоянного функционирования и совершенствования.

К моменту начала развертывания системы информационной безопасности должны быть уточнены и утверждены Руководством права и обязанности участников работ по защите информации в соответствии с данной Концепцией. Должен быть разработан и утвержден план-график развертывания системы информационной безопасности судебной системы.

Основные этапы развертывания системы должны включать в себя последовательное проведение следующих мероприятий:

* Издание Приказа об организации системы информационной безопасности.
* Разработка и уточнение функций различных отделов, распределение прав и обязанностей в системе информационной безопасности УИТ “Адилет сот”.
* Уточнение состава из специалистов сетей, баз данных и систем.
* Подготовка к информационному обследованию в субъектах судебной системы.
* Информационное обследование субъектов судебной системы.
* Определение перечня угроз, модели нарушителя, требований к системе информационной безопасности;
* Разработка (доработка) нормативно-методической базы системы обеспечения информационной безопасности;
* Ввод системы обеспечения информационной безопасности в действие;
* Категорирование информационных ресурсов судебной системы;
* Аттестация объектов информатизации судебной системы по требованиям безопасности информации.
* Поддержка системы обеспечения информационной безопасности в работоспособном и актуальном состоянии.

### Организация системы комплексного мониторинга и контроля состояния информационной безопасности судебной системы

Контроль и комплексный мониторинг состояния системы информационной безопасности судебной системы выполняется с целью обеспечения надежности и устойчивости системы информационной безопасности, обеспечения доверия к ней и гарантий выполнения требований по информационной безопасности.

Задачи контроля и комплексного мониторинга состояния информационной безопасности:

* определение критериев для оценки безопасности существующих и создаваемых систем в рамках информационно-телекоммуникационной системы;
* определение соответствия или несоответствие создаваемых и существующих систем этим критериям;
* формулировка обоснованных предложений по совершенствованию существующих методов и систем обеспечения защищенности, безопасности и достоверности информации в тех случаях, когда они не удовлетворяют имеющимся критериям.

Для осуществления контроля выполнения требований должна быть организована система отчетности о выполнении требований по безопасности. Отчетность должна вестись ответственным за информационную безопасность соответствующего рабочего места, процесса, системы или организационной структуры. С заданной периодичностью отчетность должна отправляться руководству. На основании этих данных руководство сможет реально оценивать ситуацию с состоянием безопасности во всех субъектов судебной системы.

Основные операции по учету и контролю выполнения требований должны быть автоматизированы.

Обязанности по контролю распределяются между исполнительными органами системы информационной безопасности следующим образом:

* Отдел по защите информации УИТ “Адилет сот” проводит проверки организации и состояния информационной безопасности в подразделениях организации, контролирует ее состояние специальными средствами;
* специалисты систем, баз данных, сетей контролируют текущее состояние информационной безопасности в системах, баз данных и сетях;
* специалисты отдела информационной безопасности контролируют текущее состояние информационной безопасности на своих рабочих местах.

Мероприятия для организации системы комплексного мониторинга и контроля состояния информационной безопасности.

Должна быть организована система непрерывного контроля за состояние системы информационной безопасности следующим образом:

* определение перечня субъектов, рабочих мест, систем, процессов, по которым должен проводиться контроль выполнения требований.
* определение списка требований, для каждой структурной единицы.
* организация сбора отчетности о выполнении требований по информационной безопасности.
* обработка и анализ собранных форм отчетности выводами о выполнении требований;
* периодический пересмотр системы требований
* контроль полноты и непротиворечивости системы требований.

Решение всех перечисленных задач должно быть автоматизировано путем использования необходимых программных средств контроля выполнения требований.

Помимо постоянного контроля отделом по защите информации УИТ “Адилет сот” должны выполняться плановые мероприятия проверки организации и состояния информационной безопасности.

Проверка состояния информационной безопасности судебной системы и её инфраструктуры проводится отделом информационной безопасности УИТ “Адилет сот” и могут быть:

* плановыми;
* внеплановыми;
* внезапными;
* при выявлении фактов нарушения информационной безопасности.

Плановые проверки проводятся в соответствии с годовым Планом проверок, который составляется отделом по защите информации на очередной год, утверждается управляющим УИТ “Адилет сот” и рассылается во все судебные инстанции. В ходе плановых проверок должна полностью проверяться вся серверная и сетевая инфраструктуры информационной безопасности.

Внезапные проверки проводятся отделом по защите информации УИТ “Адилет сот” в соответствии с внутренними планами работы. Внеплановые проверки проводятся на основании свидетельства, либо подозрения в нарушении работы серверной или сетевой инфраструктур. Внезапные проверки проводятся по отдельным вопросам организации информационной безопасности.

Проверки при выявлении нарушения информационной безопасности проводятся отделом по защите информации после того, как нарушение устранено. Проверка проводится с целью выявление причин и предпосылок нарушения и выработка мер по предупреждению подобных нарушений в дальнейшем. Проверка проводится в обязательном порядке по каждому факту нарушения независимо от его последствий.

Результаты всех проверок оформляются актами, с необходимыми в каждом конкретном случае приложениями.

Контроль отделом по защите информации состояния информационной безопасности с применением специальных средств - это текущий контроль, обеспечивающий независимую от работы информационной системы и сотрудников УИТ “Адилет сот” оценку состояния ее безопасности. Такой контроль применяется в первую очередь с использованием специальных автоматизированных рабочих мест. Также для текущего контроля могут применяться различные технические средства пассивного и активного характера для перехвата информации, позволяющие оценить эффективность применяемых методов и средств обеспечения ее безопасности. На данной основе специалисты информационной безопасности:

* контролируют правильность выполнения сотрудниками действий по доступу к объектам информационной системы;
* анализируют состояние информационной системы с целью выявлений попыток несанкционированного доступа и использования информационных средств и информации;
* контролируют правильность использования имеющихся коллективных и индивидуальных средств информационной защиты.

В случае выявления каких-либо отклонений или нарушений в системе информационной безопасности специалисты безопасности принимают меры к их устранению самостоятельно. Ответственность за принятие этих мер и сообщение о происшедшем несет руководитель отдела информационной безопасности.

Сотрудники отдела информационной безопасности анализируют состояние информационных систем с целью выявления попыток несанкционированного доступа и использования информационных средств и информации. В случае выявления таких попыток сотрудник сообщает об этом своему руководителю отдела информационной безопасности.

Для эффективного контроля состояния информационной безопасности необходимо провести обучение сотрудников одела информационной безопасности УИТ “Адилет сот” с целью повышения уровня их осведомленности в вопросах информационной безопасности.

Для организации контроля и комплексного мониторинга системы информационной безопасности необходимо разработать и внедрить следующие организационно-распорядительные и нормативно-технические документы:

* Регламент расследования инцидентов информационной безопасности;
* Должностные инструкции специалистов систем, систем управления базами данных, сетей (в том числе разделы, касающиеся организации контроля и мониторинга информационной безопасности);
* Памятка сотрудника УИТ “Адилет сот” по информационной безопасности;

### МЕРОПРИЯТИЯ ПО РЕШЕНИЮ ЗАДАЧ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СУДЕБНОЙ СИСТЕМЫ

### Организационно-режимные мероприятия

Выполнение организационно-режимных мероприятий при обеспечении информационной безопасности предполагает:

* категорирование объектов информатизации судебной системы;
* разграничение допуска к информационным ресурсам ограниченного распространения;
* разграничения допуска к программно-аппаратным ресурсам судебной системы;
* ведение учета ознакомления сотрудников с информацией ограниченного распространения;
* включение в функциональные обязанности сотрудников обязательства о неразглашении и сохранении сведений ограниченного распространения;
* организация уничтожения информационных отходов (бумажных, магнитных и т.д.);
* ведение учета отчуждаемых носителей информации;
* организация и осуществление периодического контроля за обеспечением информационной безопасности;
* организация учета средств криптографической защиты информации, ключей шифрования и подписи, их хранения, эксплуатации и уничтожения.

В соответствии с вышеуказанными задачами необходимо разработать или актуализировать комплект следующих организационно-распорядительных документов:

* методика категорирования объектов информатизации судебной информации;
* перечень критичных информационных ресурсов судебной системы;
* регламент предоставления доступа к информационным и программно-аппаратным ресурсам судебной системы;
* должностные обязанности сотрудников УИТ “Адилет сот” по обеспечению информационной безопасности.

### Мероприятия по физической защите объектов и средств информатизации судебной системы

Обеспечение физической безопасности всей информационно-телекоммуникационной системы судебной системы и отдельных ее элементов является одной из основных задач, решаемых подсистемой защиты информации. Физические меры защиты основаны на применении разного рода механических, электро- или электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемой информации, а также технических средств визуального наблюдения, связи и охранной сигнализации.

Физическая защита направлена на обеспечение безопасности:

* периметра информационной системы (защита контролируемой зоны);
* периметра отдельных объектов системы (выделенных территорий, зданий, помещений);
* носителей информации, оборудования и каналов передачи данных, хранящих, обрабатывающих и передающих информацию в открытом виде (магнитных и бумажных носителей информации, экранов мониторов, серверов и рабочих станций, открытых каналов связи и т.п.);
* ключевых элементов криптографических и парольных систем;

Основными направлениями физической защиты судебной системы являются:

* контроль физического доступа к оборудованию, на контролируемую территорию и в помещения;
* обеспечение безопасности кабельной системы;
* обеспечение безопасности при утилизации отработавшего оборудования и носителей информации;
* обеспечение безопасности рабочих мест.

Контроль физического доступа к оборудованию, на контролируемую территорию и в помещения

На территориях центров автоматизации субъектов судебной системы следует установить надлежащий контроль доступа в помещения. Правила доступа на территорию должны регламентироваться соответствующим положением (инструкцией).

Для разграничения доступа в помещения, где располагается серверное оборудование и другие критически важные объекты, целесообразно использовать системы физической защиты. Необходимо соблюдать следующие правила доступа в помещения:

* во всех субъектах судебной системы необходимо исключить несанкционированное нахождение посторонних лиц, дата и время их входа и выхода должны регистрироваться;
* посетители должны носить на одежде хорошо различимые идентификационные карточки;
* необходимо немедленно изъять права доступа в защищенные области (территорию, помещения) у увольняющихся сотрудников.

Кроме того, для предотвращения утечки информации и противодействия потенциальным нарушителям необходимо соблюдать следующие правила:

* Эксплуатация автоматизированных рабочих мест и серверов должна осуществляться в помещениях, оборудованных надежными замками, средствами сигнализации, исключающими возможность бесконтрольного проникновения в помещения посторонних лиц и обеспечивающими физическую сохранность находящихся в помещении защищаемых ресурсов (автоматизированных рабочих мест, документов, реквизитов доступа и т.п.);
* Размещение и установка автоматизированных рабочих мест и серверов должна исключать возможность визуального просмотра вводимой (выводимой) информации лицами, не имеющими к ней доступ;
* Уборка помещений, в которых обрабатывается или хранится конфиденциальная или служебная информация, должна производиться в присутствии ответственного, за которым закреплены технические средства (данные), или дежурного по подразделению с соблюдением мер, исключающих доступ посторонних лиц к защищаемым ресурсам;
* В помещениях во время обработки и отображения на автоматизированных рабочих местах информации ограниченного распространения должен присутствовать только персонал, допущенный к работе с данной информацией. Запрещается прием посетителей в помещениях, когда осуществляется обработка защищаемой информации;
* Для хранения служебных документов и машинных носителей с защищаемой информацией помещения снабжаются сейфами и металлическими шкафами. Помещения должны быть обеспечены средствами уничтожения документов;
* Вспомогательное оборудование (например, копировальные аппараты, факс-машины) должно быть так размещено, чтобы уменьшить риск несанкционированного доступа к защищенным областям или компрометации конфиденциальной информации;
* Физические барьеры должны по необходимости простираться от пола до потолка, чтобы предотвратить несанкционированный доступ в помещение;
* Запрещается без надобности предоставлять посторонним лицам информацию о происходящем в защищенных областях (территории, помещениях);
* Для обеспечения должного уровня безопасности и для предотвращения вредоносных действий запрещается работать в одиночку (без надлежащего контроля) с критически важными компонентами информационной системы;
* В нерабочее время защищенные области (территория, помещения) должны быть физически недоступны (закрыты на замки) и периодически проверяться охраной;
* Персоналу, осуществляющему техническое обслуживание серверов, должен быть предоставлен доступ в защищенные области (территорию, помещения) только в случае необходимости и после получения разрешения. По необходимости доступ такого персонала (особенно к конфиденциальным данным) следует ограничить, а их действия следует отслеживать;
* Запрещается использование фотографической, звукозаписывающей и видео аппаратуры в защищенных областях, за исключением санкционированных случаев;
* По окончании рабочего дня помещения с установленными защищенными автоматизированными рабочими местами должны сдаваться под охрану с включением сигнализации;

Обеспечение безопасности кабельной системы

Защита кабельной системы направлена на снижение вероятности несанкционированного доступа к информации путем гальванического подключения к информационным кабелям или снятия информации через побочные электромагнитные излучения и наводки на другие кабели, а также на обеспечение защиты кабельного оборудования от электромагнитных помех.

Кабели электропитания и сетевые кабели для передачи данных необходимо защищать от вскрытия для целей перехвата информации и повреждения. Для уменьшения такого риска в помещениях организации предлагается реализовать следующие защитные меры:

* Кабели электропитания и линии связи, идущие к информационным системам, должны быть проведены под землей (по возможности) или защищены надлежащим образом с помощью других средств.
* Необходимо рассмотреть меры по защите сетевых кабелей от их несанкционированного вскрытия для целей перехвата данных и от повреждения, например, воспользовавшись экранами или проложив эти линии так, чтобы они не проходили через общедоступные места.
* С целью снижения влияния электромагнитных помех, силовые и коммуникационные кабели должны быть разнесены в пространстве.
* Для исключительно уязвимых или критически важных систем следует рассмотреть необходимость принятия дополнительных мер, таких, как:
  + шифрование данных;
  + установка бронированных экранов и использование запираемых помещений;
  + использование других маршрутов или сред передачи данных.

Надежная утилизация отработавшего оборудования и носителей информации

Оборудование, подлежащее выводу из эксплуатации, и использованные носители информации могут содержать остаточную информацию ограниченного доступа. Регламентация порядка и процедур их утилизации позволяет перекрыть каналы несанкционированного доступа к этой информации:

* устройства хранения информации, содержащие ценную информацию, при выведении из эксплуатации должны быть физически уничтожены, либо должно быть проведено гарантированное стирание с них остаточной информации;
* все оборудование, включая носители информации, перед передачей другому владельцу или списанием должно быть проверено на отсутствие важной информации или лицензионного программного обеспечения;
* дальнейшая судьба поврежденных устройств хранения, содержащих важную информацию, (уничтожение или ремонт) определяется на основе заключения экспертной комиссии.

Безопасность рабочего места сотрудников судебной системы

Рабочие места сотрудников судебной системы - наиболее многочисленная категория объектов информационно-телекоммуникационной системы, через которые возможен несанкционированный доступ к информации. Действия сотрудников сложно контролировать, поэтому в системе защиты информации необходимо предусмотреть автоматизированные механизмы мониторинга за действиями пользователей и сигнализации при обнаружении попыток несанкционированного доступа, а также установлен жесткий регламент доступа к рабочим местам с помощью организационных мер.

Безопасность рабочих мест сотрудников судебной системы предусматривает:

* документы на всех видах носителей и технические средства обработки информации, должны храниться (размещаться) в помещениях, исключающих несанкционированный доступ к ним;
* исключение несанкционированного доступа к информации, хранящейся на различного рода носителях;
* персональные компьютеры, терминалы и принтеры должны защищаться блокираторами клавиатуры, паролями или другими методами на время отсутствия пользователя;
* должны быть приняты надежные меры, исключающие несанкционированное использование копировальной техники;
* распечатки, содержащие информацию ограниченного доступа должны изыматься из печатающего устройства немедленно Необходимо устанавливать печатающие устройства для печати конфиденциальных документов в помещениях, где работают сотрудники, ответственные за их учет, хранение и выдачу исполнителям.

### Мероприятия по обеспечению катастрофоустойчивости информационно-телекоммуникационной системы

Обеспечение катастрофоустойчивости необходимо для сохранения устойчивости и стабильности функционирования судебной системы и ее информационно-телекоммуникационной системы в различных условиях неблагоприятного воздействия внешних и внутренних факторов техногенного и/или природного характера.

Для обеспечения катастрофоустойчивости необходимо выполнить работы, направленных на минимизацию возможных потерь в условиях активного воздействия внутренней и внешней среды.

Важнейшим качеством информационно-телекоммуникационной системы и, в частности, центров обработки данных является способность обеспечивать требуемый уровень отказоустойчивости. Возможно применение следующих технических мероприятий для обеспечения отказоустойчивости:

* Следует внедрять технологии резервирования хранилищ данных.
* Серверное и другое критическое оборудование следует размещать таким образом, чтобы свести к минимуму излишний доступ в рабочие помещения.
* Оборудование необходимо защищать от сбоев в системе электропитании и других неполадок в электрической сети. Источник питания должен соответствовать спецификациям производителя оборудования.
* Следует рассмотреть необходимость использования резервного источника питания. Для оборудования, поддерживающего критически важные производственные сервисы, рекомендуется установить источник бесперебойного питания. План действий в чрезвычайных ситуациях должен включать меры, которые необходимо принять по окончании срока годности источников бесперебойного питания. Оборудование, работающее с источниками бесперебойного питания, необходимо регулярно тестировать в соответствии с рекомендациями изготовителя.
* Следует рассмотреть возможность изоляции областей, требующих специальной защиты, для понижения необходимого уровня общей защиты.

Для создания системы обеспечения катастрофоустойчивости необходимо разработать следующие организационно-распорядительные и нормативно-технические документы:

* Политика резервного копирования и восстановления данных
* План обеспечения непрерывной работы и восстановления работоспособности подсистем автоматизированной системы.

### Мероприятия по решению задач защиты информации от несанкционированного доступа в информационную инфраструктуру.

Основные мероприятия по защите информации от несанкционированного доступа должны предусматривать следующее:

* Разграничение прав доступа к информационным ресурсам на основе доменных учётных записей;
* Обеспечение строгой доменной аутентификации.
* Применение сертифицированных аппаратно-программных средств защиты информации от несанкционированного доступа.
* Механизмы защиты от несанкционированного доступа должны осуществлять защиту системы от возможности посторонних лиц осуществлять работу в системе (механизмы идентификации и аутентификации), а также получать доступ к информационным ресурсам системы (механизмы разграничения доступа в соответствии с полномочиями субъекта). При реализации этих механизмов защиты должна использоваться совокупность организационных, программных (пароли, матрицы доступа и др.), аппаратно-программных и технических методов защиты.
* Защита системы от несанкционированного доступа должна обеспечиваться на всех технологических этапах передачи, обработки и хранения информации и при всех режимах работы системы, в том числе при проведении ремонтных и регламентных работ. При этом реализованные в системе средства защиты от несанкционированного доступа не должны ухудшать основные функциональные характеристики системы.
* Защита системы от несанкционированного доступа с помощью программных, программно-аппаратных и технических методов должна обеспечивать:
  + защиту технических средств обработки информации;
  + защиту баз данных;
  + защиту системы управления.
* Защита от несанкционированного доступа должна строиться на основе системы разграничения доступа пользователей к системе и ее информационным ресурсам. Основными функциями системы разграничения доступа должны являться:
  + реализация правил разграничения доступа пользователей и их процессов к информационным ресурсам;
  + реализация правил разграничения доступа пользователей к устройствам создания твердых копий;
  + исключение возможной эксплуатации ресурсов информационной инфраструктуры судебной системы через технологию Wi-Fi;
  + изоляция программ процесса, выполняемого в интересах пользователя, от других пользователей системы;
  + реализация правил обмена данных между пользователями системы, построенных по сетевым принципам.
* Обеспечивающие средства системы разграничения доступа должны выполнять следующие основные функции:
  + идентификацию и аутентификацию пользователей системы и поддержание привязки к их процессам, выполняемым в их интересах;
  + регистрацию действий пользователей и выполняемых в их интересах процессов, предоставление возможности исключения и включения новых пользователей и объектов доступа, а также изменение полномочий пользователей;
  + реакцию на попытки несанкционированного доступа (сигнализацию, блокировку и т.д.), восстановление механизмов защиты после несанкционированного доступа;
  + тестирование;
  + очистку оперативной памяти и рабочих областей на магнитных носителях после завершения работы пользователя с защищенными данными;
  + учет выходных печатных и графических форм, а также твердых копий в системе;
  + контроль целостности программной и информационной части как системы разграничения доступа, так и обеспечивающих ее средств.
* Практическая реализация системы разграничения доступа должна определяться с учетом конкретных особенностей системы и может включать в себя следующие способы и их сочетания:
  + распределенная система разграничения доступа, локализованная в аппаратно-программном комплексе системы;
  + система разграничения доступа в рамках операционной системы, системы управления базами данных или прикладных программ;
  + система разграничения доступа в средствах реализации сетевых протоколов взаимодействия или на уровне приложений;
  + Программная и (или) техническая реализация системы разграничения доступа;
  + Программная и (или) аппаратная реализация криптографических функций.

В рамках системы защиты от несанкционированного доступа необходимо внедрить комплексную систему защиты баз данных, содержащих критичную к нарушению безопасности информацию.

Для создания системы защиты информации от несанкционированного доступа в информационно-телекоммуникационных системах необходимо разработать следующие организационно-распорядительные и нормативно-технические документы:

* Положение о разграничении прав доступа к информационным ресурсам
* Должностные инструкции IT консультантов и сотрудников УИТ “Адилет сот”.

### Мероприятия по обеспечению безопасного информационного взаимодействия судебной системы с организациями, министерствами и ведомствами

К основным мероприятиям по обеспечению безопасности сетевого информационного взаимодействия судебной системы с гражданами, пользователями веб-ресурсов судебной системы / источниками информации, относятся:

* Предотвращение возможности утечки конфиденциальной информации через внешнюю сеть.
* Обеспечение защиты ресурсов со стороны внешней сети.

Так как ресурсы, предназначенные для доступа из внешней сети (по каналам связи сетей общего пользования), подвержены атакам из внешней открытой сети, то ведомственный (защищенный, содержащий конфиденциальную информацию) и внешний (открытый) трафики должны быть физически разделены – не должно быть вычислительных средств (рабочих станций, серверов, межсетевых экранов), концентрирующих на себе одновременно ведомственный и внешний трафик.

При организации сетевого взаимодействия следует использовать средства защиты:

* Выделенные средства межсетевого экранирования (или межсетевые экраны), устанавливаемые на стыке сетей, концентрирующие на себе межсетевой трафик;
* Механизмы контроля доступа к локальным и сетевым ресурсам, входящие в состав системы защиты информации от несанкционированного доступа, устанавливаемой на рабочие станции и серверы, решающие задачи фильтрации внутрисетевого трафика и доступа к локальным ресурсам;
* Антивирусные средства;
* Средства обнаружения компьютерных атак.

Указанными средствами должно обеспечиваться:

* разграничение доступа (по входящему и исходящему трафикам) по адресам (IP адресам) и сетевым протоколам к хостам внешней/внтуренней сети;
* трансляция адресов – во внешней сети должен быть “виден” только адрес крипто маршрутизатора, что позволяет скрывать структуру внутренней сети (адреса рабочих станций и серверов внутренней сети);
* защита от сетевых атак (вирусы, шпионские программы, атаки на отказ в обслуживании);
* аудит доступа к ресурсам внешней сети;
* аутентификация удаленных пользователей

Важнейшим условием обеспечения защищенного доступа к внешним ресурсам является реализация демилитаризованной зоны, с целью физической изоляции внутрисетевого и внешнего трафиков. Данное решение должно позволять взаимодействовать пользователям внешней сети только с серверами внешнего доступа, и делать недоступным для них доступ, прежде всего, к внутренним серверам, а также к рабочим станциям защищаемой корпоративной сети, даже при преодолении защиты, реализуемой средствами межсетевого экранирования.

### Мероприятия по организации криптографической защиты информации

В целях защиты конфиденциальной информации в автоматизированной информационной системы должны применяться средства криптографической защиты информации.

К средствам криптографической защиты информации предъявляются следующие требования:

* средства криптографической защиты информации должны допускать их встраивание в технологическую схему обработки электронных сообщений, обеспечивать взаимодействие с прикладным программным обеспечением на уровне обработки запросов на криптографические преобразования и выдачи результатов;
* средства криптографической защиты информации должны поставляться разработчиками с полным комплектом эксплуатационной документации, включая описание ключевой системы, правила работы с ней, а также обоснование необходимого организационно-штатного обеспечения;
* средства криптографической защиты информации должны быть реализованы на основе криптостойких алгоритмов;
* средства криптографической защиты информации должны иметь строгий регламент использования ключей, предполагающий контроль со стороны администратора безопасности за действиями пользователя на всех этапах работы с ключевой информацией (получение ключевого носителя, ввод ключей, использование ключей и сдача ключевого носителя);
* средства криптографической защиты информации должны обеспечивать реализацию процедур сброса ключей в случаях отсутствия штатной активности пользователей в соответствии с регламентом использования ключей;
* средства криптографической защиты информации не должны предъявлять требований к электронно-вычислительным машинам по специальной проверке на отсутствие закладных устройств, если иное не оговорено в технической документации на конкретное средство защиты;
* средства криптографической защиты информации не должны требовать дополнительной защиты от утечки по побочным каналам электромагнитного излучения.

При применении средств криптографической защиты информации в автоматизированной системе должны поддерживаться непрерывность процессов протоколирования работы средств криптографической защиты информации и обеспечения целостности программного обеспечения для всех элементов автоматизированных информационных систем.

Информационная безопасность процессов изготовления ключевой информации документов средствами криптографической защиты информации должна обеспечиваться комплексом технологических, организационных, технических и программных мер и средств защиты.

Использование средств криптографической защиты информации должно осуществляться в полном соответствии с конструкторской и эксплуатационной документацией, представляемой производителем средств криптографической защиты информации. Внутренний порядок применения средств криптографической защиты информации должен включать:

* порядок ввода в действие;
* порядок эксплуатации;
* порядок восстановления работоспособности в аварийных случаях;
* порядок внесения изменений;
* порядок снятия с эксплуатации;
* порядок управления ключевой системой;
* порядок обращения с носителями ключевой информации.

### Мероприятия по антивирусной защите информационных ресурсов судебной системы

Целью создания системы антивирусной защиты является обеспечение защищенности информационно-коммуникационной системы от воздействия различного рода вредоносных программ и несанкционированных массовых почтовых рассылок, предотвращения их внедрения в информационные системы, выявления и безопасного удаления из систем в случае попадания, а также фильтрации доступа сотрудников судебной системы к непродуктивным Интернет-ресурсам и контроля их электронной переписки.

Основополагающими требованиями к системе антивирусной защиты являются:

* решение задачи антивирусной защиты должно осуществляться в общем виде. Средство защиты не должно оказывать противодействие конкретному вирусу или группе вирусов, противодействие должно оказываться в предположениях, что вирус может быть занесен на компьютер и о вирусе (о его структуре (в частности, сигнатуре) и возможных действиях) ничего не известно;
* решение задачи антивирусной защиты должно осуществляться в реальном времени.

Мероприятия, направленные на решение задач по антивирусной защите:

* необходимо проводить политику, требующую установки только лицензированного программного обеспечения;
* антивирусные программные средства должны регулярно обновляться и использоваться для профилактических проверок (желательно ежедневных);
* непрерывный контроль над всеми возможными путями проникновения вредоносных программ, мониторинг антивирусной безопасности и обнаружение деструктивной активности вредоносных программ на всех объектах;
* ежедневный анализ, ранжирование и предотвращение угроз распространения и воздействия вредоносных программ путем выявления уязвимостей используемом программном обеспечении операционных систем и сетевых устройств и устранения обнаруженных дефектов в соответствии с данными поставщика программного обеспечения и других специализированных экспертных антивирусных служб.
* проведение профилактических мероприятий по предотвращению и ограничению вирусных эпидемий, включающих загрузку и развертывание специальных правил нейтрализации (отражению, изоляции и ликвидации) вредоносных программ на основе рекомендаций по контролю атак, подготавливаемых разработчиком средств защиты от вредоносных программ и другими специализированными экспертными антивирусными службами до того, как будут выпущены файлы исправлений, признаков и антивирусных сигнатур.
* необходимо проводить регулярную проверку целостности критически важных программ и данных. Наличие лишних файлов и следов несанкционированного внесения изменений должно быть зарегистрировано в журнале и расследовано;
* дискеты, диски, дисковые накопители любого типа неизвестного происхождения следует проверять на наличие вирусов до их использования;
* необходимо строго придерживаться установленных процедур по уведомлению о случаях поражения автоматизированной информационной системы компьютерными вирусами и принятию мер по ликвидации последствий от их проникновения;
* следует иметь планы обеспечения бесперебойной работы организации для случаев вирусного заражения, в том числе планы резервного копирования всех необходимых данных и программ и их восстановления. Эти меры особенно важны для сетевых файловых серверов, поддерживающих большое количество рабочих станций.

В рамках создания системы антивирусной защиты информационных ресурсов судебной системы необходимо разработать следующие организационно-распорядительные и нормативно-технические документы:

* Положение об антивирусном контроле, включая определение основных целей и области применения системы антивирусной защиты, требования к персоналу, степень ответственности, структуру и необходимый уровень защищенности от вредоносных программ, статус и должностные обязанности IT консультантов.
* Должностные инструкции IT консультантов и специалистов УИТ “Адилет сот”, которые должны включать:
* Порядок установки и настройки средств антивирусной защиты;
* Порядок эксплуатации средств антивирусной защиты, в т.ч. обновление программного обеспечения, мониторинг и управление;
* Порядок действия в период вирусных эпидемий;
* Порядок действий при возникновении внештатных ситуаций, связанных с работоспособностью средств антивирусной защиты;
* Порядок действия для устранения последствий заражений.
* Технологические инструкции

### Мероприятия по обнаружению компьютерных атак на информационные ресурсы и телекоммуникационные системы

Основополагающими требованиями к системе обнаружения компьютерных атак на информационные ресурсы и телекоммуникационные системы являются:

* система обнаружения компьютерных атак должна быть сертифицирована;
* система обнаружения компьютерных атак должна быть способна выявлять атаки, направленные на нарушение конфиденциальности, целостности и доступности информационных ресурсов.

Система обнаружения компьютерных атак должна обеспечивать возможность выполнения следующих основных функций:

* выявление информационных атак на прикладном уровне стека TCP/IP посредством анализа пакетов данных;
* блокирование пакетов данных, нарушающих заданную политику безопасности;
* мониторинг трафика, циркулирующего на сетевом, транспортном и прикладном уровнях модели взаимодействия открытых систем;
* выявление аномалий сетевого трафика;
* оповещение администратора безопасности об обнаруженных атаках или аномалиях сетевого трафика.

### Мероприятия по совершенствованию организационно-штатной структуры подразделений, отвечающих за обеспечение информационной безопасности

Основные мероприятия по совершенствованию организационно-штатной структуры подразделений защиты информации:

* создание отдела информационной безопасности
* оснащение отдела информационной безопасности программно-техническими средствами для проведения контроля состояния информационной безопасности в судебной системе
* проведение мероприятий по повышению квалификации сотрудников отдела информационной безопасности

### Мероприятия по повышению квалификации специалистов в области защиты информации

Подготовка и переподготовка IT консультантов и специалистов УИТ “Адилет сот” по защите информации требует создание системы повышения уровня технической грамотности и информированности пользователей в области информационной безопасности, а также переподготовки специалистов по защите информации. Для этого необходимо регулярно проводить тренинги для персонала и контроль готовности новых сотрудников по применению правил информационной защиты, а также периодически осуществлять переподготовку специалистов подразделений защиты информации. Особенно важно проводить тренинги при изменении конфигурации информационной системы (внедрении новых технологий и прикладных автоматизированных систем, смены оборудования, операционной системы, ключевых приложений, принятии новых правил или инструкций и т.д.)

### Мероприятия по внутреннему аудиту информационных систем

Внутренний аудит информационных систем производится специалистами УИТ “Адилет сот”, ответственными за информационную безопасность, по распоряжению директора Судебного департамента. Сроки и режим проведения внутреннего аудита устанавливаются директором Судебного департамента.

Целью внутреннего аудита является оценка текущего состояния системы информационной безопасности, разработка или актуализация организационных и технических требований к системе информационной безопасности судебной системы, прогнозирование на основе этого требуемых затрат на ее поддержание и модернизацию.

Требования к системе информационной безопасности разрабатываются на основе анализа существующих угроз информационно-телекоммуникационной системы, идентификации существующих уязвимостей и оценки величины возможного ущерба.

Результаты аудита должны содержать отчёты по обеспечению безопасности информационной системы подразделения в целом или её логических компонентов. Описания, выявленные факты и рекомендации, полученные в ходе проведения аудита, должны быть использованы для дальнейшей оценки защищенности информационной системы.

Комплексные проверки мер по обеспечению информационной безопасности проводятся не реже одного раза в год. Отдельные проверки систем на потенциальные повреждения осуществляются с периодичностью, необходимой для поддержания требуемого уровня оперативности статистических данных.

Приложение № 2

к приказу №\_\_\_\_\_

от «\_\_\_\_» \_\_\_\_\_\_\_\_2018г.

# ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ РЕСУРСОВ

Судебной системы по состоянию на январь 2018 г.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| № | Наименование информационного ресурса | Назначение | Категория конфиденциальности | Размещение ресурса (рабочая машина, устройство, каталог, файл) | Ответственные за: | |
| ведение | администрирование |
| Веб-ресурсы | | | | | | |
| 1 | sot.kg | Система публикации судебных материалов | Рабочая информация |  | Степанов К. А. |  |
| 2 | e-sot.kg | Сайт УИТ "Адилет сот" | Служебная информация |  | Степанов К. А. |  |
| 3 | help.e-sot.kg | “Стол Помощи” специалистов в области IT Судебной системы | Служебная информация |  | Степанов К. А. |  |
| 4 | forum.e-sot.kg | Форум специалистов в области IT Судебной системы | Служебная информация |  | Степанов К. А. |  |
| 5 | АРД | Автоматизированная система распределения судебных дел, проектирования нагрузки на судей |  |  | Степанов К. А. |  |
| 6 | АИС | Автоматизированная система документооброта судов |  |  | Степанов К. А. |  |
| 7 | Реестр должников | Система исполнительного производства ПССИ | Конфиденциальная информация |  | Степанов К. А. |  |
| 8 | Сетевое хранилище документов | Хранение документов УИТ “Адилет сот” для совместной работы сотрудников УИТ “Адилет сот” | Служебная информация | Файловый сервер | Джумакадыров А.Т. | Джумакадыров А.Т.,  Нурмухамедов Д.А. |

Приложение № 3

к приказу №\_\_\_\_\_

от «\_\_\_\_» \_\_\_\_\_\_\_\_2018г.

# План работ по защите информации

1. Вводная часть

Целью работ по защите информации является предотвращение ущерба в результате ее разглашения, утраты, утечки, искажения, уничтожения и незаконного использования.

## Объектами защиты являются:

* информационные ресурсы;
* средства и системы обработки информации;
* средства и системы защиты информации, в т.ч. криптографической защиты информации;
* помещения или объекты, предназначенные для содержания конфиденциальной, служебной и рабочей информации, ведения закрытых переговоров или судебных заседаний.

Основными источниками угроз безопасности информации являются:

* Стихийные – стихийные бедствия, катаклизмы;
* Техногенные: аварии, сбои и отказы оборудования;
* Ошибки эксплуатации;
* Преднамеренные действия нарушителей и злоумышленников.

Все нарушители делятся на две основные группы: внутренние и внешние. Предполагается, что несанкционированный доступ на объекты организации посторонних лиц исключается организационными мерами (охрана территории, организация пропускного режима).

Проведение работ по защите информации без финансовых затрат предполагает выработку организационно-режимных мероприятий, документации, проведение периодических контрольных мероприятий, поддержание системы в работоспособном и актуальном состоянии.

1. Требуемые организационно-методические документы:
2. Концепция информационной безопасности судебной системы
3. Базовая модель угроз информационной безопасности
4. Перечень информационных ресурсов, подлежащих защите, с назначением ответственных за ресурс
5. Перечень защищаемых помещений
6. План защиты автоматизированных систем в судебной системе
7. Положение о разграничении прав доступа к информационным ресурсам
8. Положение об использовании программного обеспечения
9. Положение об использовании сети Internet и электронной почты
10. Положение о парольной защите
11. Положение о резервном копировании
12. Положение об антивирусном контроле
13. Положение об использовании съемных носителях информации
14. Положение об использовании переносных компьютеров
15. Приказы о назначении ответственных лиц за антивирусный контроль, резервное копирование, предоставление доступа
16. Памятка по защите информации для каждого сотрудника
17. Положение о порядке доступа к конфиденциальной информации судебной системы
18. Требуется провести следующие организационно-режимные мероприятия:
19. Изменить принцип организации парольной защиты – изменить тип пароля на сменяемый каждые 30 дней, возложить ответственность за сохранность секретности пароля на пользователя.
20. Использование USB – устройств (USB накопители, сьемные диски, USB-модемы) и записываемых CD, DVD как самого вероятного способа вирусного заражения и хищения конфиденциальной информации следует ограничить до минимально необходимого уровня.
21. Ограничить доступ к сайтам, не имеющим служебный и рабочий контент, сети Internet.
22. Расположить мониторы и печатающие устройства таким образом, чтобы исключить несанкционированный доступ к отображаемой и печатаемой информации.
23. Блокировать рабочую станцию при временном отсутствии на рабочем месте.
24. Должностные инструкции работников организации дополнить пунктом об ответственности за соблюдение правил защиты информации.

По мере составления организационно-методических документов по защите информации потребуется проведение дополнительных организационно-режимных мероприятий.

Приложение № 4

к приказу №\_\_\_\_\_

от «\_\_\_\_» \_\_\_\_\_\_\_\_2018г.

# Порядок доступа к информационным, программным и аппаратным ресурсам Судебной системы

1. Общие положения
   1. Настоящий порядок доступа к информационным, программным и аппаратным ресурсам (далее - Порядок) разработан с учетом сложившейся системы, учитывающей специфику работы, организацию рабочих процессов и утвержденных положений информационной безопасности.
   2. Порядок доступа к информационным, программным и аппаратным ресурсам Судебной системы разработан во исполнение и с учетом требований и положений следующих нормативных документов:

* ”О гарантиях и свободе доступа к информации Кыргызской Республики” от 5 декабря 1997 года № 89 (В редакции Законов КР от [18 октября 2002 года № 147](http://cbd.minjust.gov.kg/act/view/ru-ru/1104?cl=ru-ru), [от 28 декабря 2006 года № 214](http://cbd.minjust.gov.kg/act/view/ru-ru/202011?cl=ru-ru), [29 декабря 2016 года № 224](http://cbd.minjust.gov.kg/act/view/ru-ru/111505?cl=ru-ru), [18 марта 2017 года № 47](http://cbd.minjust.gov.kg/act/view/ru-ru/111554?cl=ru-ru));
* пп. 5.4., 5.5. Концепции информационной безопасности Судебной системы утвержденная приказом Судебным департаментом при ВС КР;
* Закон “О защите государственных секретов Кыргызской Республики” от 14.04.1994 № 1476-XII (В редакции Закона КР от [18 мая 2013 года № 74](http://cbd.minjust.gov.kg/act/view/ru-ru/203882?cl=ru-ru), [21 января 2014 года № 15](http://cbd.minjust.gov.kg/act/view/ru-ru/205236?cl=ru-ru));
  1. Термины и определения, используемые в настоящем Порядке, соответствуют используемым в указанных в п.1.2. нормативных документах. Кроме того, в Порядке используются следующие термины:

Информационный ресурс – сведения (сообщения, данные), входящие в состав отдельных документов, массивов документов, баз данных, представленные в электронно-цифровой форме.

Программный ресурс – системное или прикладное программное обеспечение.

Аппаратный ресурс – внутренние или внешние устройства хранения, обработки или передачи информации.

Внутренний пользователь — работник Судебной системы, пользующийся информационными ресурсами и специализированными программными ресурсами.

Внешний пользователь — государственные органы, сторонние организации и их работники, физические лица.

* 1. Порядок применяется во всех случаях, когда сотрудникам Судебной системы или внешним пользователям, выполняющим работы с использованием информационных ресурсов Судебной системы, предоставляется (впервые или по истечении срока предыдущего получения аналогичных прав доступа) доступ к информационным, программным или аппаратным ресурсам (далее - ресурсы) Судебной системы.
  2. Порядок не применяется в случаях:
* получения материальных ценностей (в том числе аппаратных ресурсов) пользователями;
* восстановления доступа пользователей к ресурсам в случае, если потеря доступа произошла в результате какого-либо инцидента – в таком случае необходимо действовать в установленном в Судебной системе порядке по устранению последствий инцидентов;
* получения доступа к «тестовым» ресурсам;
  1. Положения Порядка должны анализироваться специалистами УИТ “Адилет сот” не реже одного раза в год. В случае если в ходе такого анализа была установлена необходимость внесения изменений в Порядок, новая редакция Порядка должна быть выполнена специалистами УИТ “Адилет сот” и утверждена приказом Судебной системы.

1. **Основные права, обязанности и ответственность**
   1. Обязанности по предоставлению и аннулированию доступа к Ресурсам возлагаются на УИТ “Адилет сот” в соответствии с положениями об отделах и должностными инструкциями сотрудников.
   2. Обязанности по контролю соблюдения Порядка возлагаются на руководителей отделов/подразделений органов судебной системы
   3. Пользователи допускаются к работе с ресурсами только после ознакомления под роспись в соответствующем журнале (приложение 1, далее – Журнал инструктажа пользователей) с положениями Порядка и прохождения инструктажа, проводимого руководителями отделов/подразделений органов судебной системы
   4. Соблюдение требований Порядка обязательно для всех пользователей, допущенных к работе с ресурсами.
   5. Дополнительно к настоящему Порядку допуск специалистов внешних организаций к выполнению работ с информационными ресурсами Судебной системы регламентируется соответствующим нормативным документом Судебной системы.
   6. Деятельность пользователей при работе с ресурсами должна протоколироваться и периодически проверяться на предмет соблюдения установленных правил работы любыми средствами, не противоречащими законодательству Кыргызской Республики.
2. **Учет ресурсов**
   1. Все информационные ресурсы Судебной системы должны быть учтены и систематизированы.
   2. Ведение Реестра возлагается на УИТ “Адилет сот”.
   3. Актуальный Реестр должен быть доступен всем пользователям в произвольный момент времени.
   4. Информация о новом ресурсе (изменениях в имеющемся ресурсе) должна быть доведена до УИТ “Адилет сот” в течение двух рабочих дней с момента появления в виде служебной записки, подписанной руководителем соответствующего подразделения/отдела (приложение 2).
   5. Внесение изменений в Реестр осуществляется в течение одного рабочего дня с момента поступления соответствующей служебной записки.
3. **Предоставление доступа к ресурсам**
   1. Для предоставления доступа пользователю к ресурсу необходимо выполнение одного из следующих условий:

* доступ необходим для выполнения пользователем своих должностных обязанностей;
* доступ необходим для выполнения пользователем обязанностей другого пользователя по поручению (в виде служебной записки) начальника соответствующего отдела;
* доступ необходим для выполнения пользователем обязанностей другого пользователя по указанию (в виде приказа или распоряжения) руководства Судебной системы;
* доступ необходим для выполнения пользователем работ по указанию (в виде приказа или распоряжения) руководства Судебной системы.
  1. Для обеспечения доступа к ресурсам руководитель отдела Судебной системы (лицо, его замещающее) составляет заявку на предоставление доступа (далее – Заявка, приложение 3), руководствуясь Реестром.
  2. УИТ “Адилет сот” в течение одного рабочего дня проверяет наличие у пользователя основания на доступ к ресурсу согласно Заявке. В случае если доступ к ресурсу согласно Заявке по какой-либо причине не может быть предоставлен, Заявка возвращается лицу, инициировавшему Заявку, с подробным описанием данной причины.
  3. Заявка передается на утверждение управляющему УИТ “Адилет сот” (лицу, его замещающему). В случае утверждения в тот же день оригинал утвержденной Заявки передается на постоянное хранение и для выполнения работ по предоставлению доступа согласно Заявке.
  4. Информация об утвержденных Заявках заносится в журнал регистрации и учета заявок на предоставление доступа к ресурсам (далее – Журнал регистрации заявок, приложение 4), который ведется в электронном виде специалистами УИТ “Адилет сот”.

1. **Использование ресурсов**
   1. Использование ресурсов осуществляется в соответствии с  
      инструкциями и руководствами по эксплуатации программного и аппаратного обеспечения.
   2. Запрещается умышленное выведение ресурсов из строя, блокировка доступа к ним и любые иные действия, препятствующие штатному режиму эксплуатации ресурсов.
   3. В случае обнаружения сбоя в работе ресурса пользователь обязан сообщить об инциденте в УИТ “Адилет сот”.
2. **Изменение прав доступа к ресурсам**
   1. В случае необходимости предоставления пользователю дополнительных полномочий (ролей) по доступу к уже используемому им ресурсу следует действовать в соответствии с разделом 4 Порядка.
   2. В случае необходимости замены (полной или частичной) полномочий пользователя по доступу к уже используемому им ресурсу следует действовать в соответствии с п.7.1. Порядка.
3. **Аннулирование доступа к ресурсам**
   1. Аннулирование доступа к ресурсам происходит в случаях:

* изменения должностных обязанностей пользователя;
* истечения периода действия Заявки;
* изменения технологических процессов обработки информации таким образом, что доступ пользователю более не требуется;
* нарушения пользователем правил доступа к ресурсу;
* ухода сотрудника в декретный отпуск (отпуск по уходу за ребенком);
* увольнение пользователя;
* по иным требованиям руководства Судебной системы или УИТ “Адилет сот”.

Аннулирование доступа должно быть инициировано в течение одного рабочего дня с момента возникновения соответствующего события.

* 1. Обязанности по инициированию аннулирования доступа пользователя к ресурсам возлагаются:
* в случае изменения должностных обязанностей пользователя или его увольнения, изменения технологических процессов обработки информации таким образом, что доступ пользователю более не требуется - на управляющего УИТ “Адилет сот”;
* в случае истечения периода действия Заявки, нарушения пользователем правил доступа к ресурсу – на управляющего УИТ “Адилет сот”.
  1. Информация об инициировании аннулировании доступа (с указанием причины) доводится в произвольной форме в письменном виде начальником соответствующего подразделения/отдела Судебной системы до УИТ “Адилет сот”.
  2. Аннулирование доступа осуществляется специалистами УИТ “Адилет сот”.
  3. Информация об аннулировании доступа заносится специалистами УИТ “Адилет сот” в течение одного рабочего дня в Журнал регистрации заявок.

Приложение № 5

к приказу №\_\_\_\_\_

от «\_\_\_\_» \_\_\_\_\_\_\_\_2018г.

# Положение об использовании программного обеспечения в Судебной системе

1. Общие положения
   1. Настоящее Положение устанавливает правила использования программного обеспечения вычислительной техники в Судебной системе, а также определяет права и обязанности сотрудников Судебной системы в процессе эксплуатации всех видов программного обеспечения.
2. Основные термины, сокращения и определения

АРМ – автоматизированное рабочее место пользователя (персональный компьютер с прикладным ПО) для выполнения определенной производственной задачи.

АС – автоматизированная система Организации – система, обеспечивающая хранение, обработку, преобразование и передачу информации Организации с использованием компьютерной и другой техники.

ИТ – информационные технологии – совокупность методов и процессов, обеспечивающих хранение, обработку, преобразование и передачу информации Организации с использованием средств компьютерной и другой техники.

Лицензионное Соглашение – документ, регламентирующий передаваемые конечному пользователю права на использование ПО; формулируется правообладателем.

Паспорт ПК (паспорт АРМ) – документ, содержащий полный перечень оборудования и программного обеспечения АРМ.

ПК – персональный компьютер – комплекс вычислительной техники с установленным системным ПО; используется одним или несколькими пользователями АС в производственных целях.

Пользователь ИС – работник Организации, использующий ПО (в составе АРМ) для выполнения своих трудовых обязанностей.

ПО – программное обеспечение вычислительной техники, базы данных.

ПО бесплатное – ПО сторонних производителей/разработчиков, свободно распространяемое на безвозмездной основе.

ПО коммерческое – ПО сторонних производителей (правообладателей). Предоставляется в пользование на возмездной (платной) основе.

ПО прикладное – офисное программное обеспечение (в том числе, разработанное специалистами Организации); информационно-справочные системы; АС для решения производственных, хозяйственных и управленческих задач Организации; системы проектирования и управления.

ПО системное – операционные системы, средства антивирусной защиты, средства создания резервных копий, драйверы устройств, административные утилиты, средства организации сетевых сервисов.

ПО специализированное – ПО систем управления технологическими процессами на производстве, ПО системного администрирования/управления ресурсами вычислительных сетей.

Правообладатель – автор, его наследник, а также любое физическое или юридическое лицо, которое обладает исключительным правом на программу для ЭВМ или базу данных в силу закона или договора.

Перечень – документ "Перечень программного обеспечения, разрешенного для использования на компьютерах ЗАО «ХХХ»». Содержит перечень коммерческого ПО, разрешенного к использованию в Организации в текущем году. Утверждается один раз в год приказом Руководителя Организации.

1. Порядок эксплуатации программного обеспечения
   1. В целях автоматизации производственной, управленческой, вспомогательной деятельности в Судебной системе разрешено применение ограниченного перечня коммерческого и бесплатного программного обеспечения, необходимого для выполнения производственных задач (Приложение 5) и указанного в Паспорте ПК (Приложение 6).
   2. В состав каждого автоматизированного рабочего места входит набор программного обеспечения для выполнения определенного вида деятельности. Первоначальная комплектация автоматизированного рабочего места определяется УИТ “Адилет сот”. Программное обеспечение, не входящее в состав автоматизированного рабочего места, не может быть установлено и использовано сотрудниками Судебной системы без процедуры согласования.
   3. Конкретный состав установленного программного обеспечения на каждом автоматизированном рабочем месте определяется на основании перечня коммерческого и бесплатного программного обеспечения и перечня информационных ресурсов Судебной системы.
   4. Описание конфигурации персонального компьютера и перечень установленного программного обеспечения фиксируется в Паспорте ПК, подписывается специалистами УИТ “Адилет сот”, начальником структурного подразделения и пользователем автоматизированной системы.
   5. Все операции по установке, сопровождению и поддержке, удалению программного обеспечения выполняются непосредственно или при участии специалистов УИТ “Адилет сот”.
   6. Изменение конфигурации аппаратно-программных средств защищенных рабочих станций и серверов без согласования со специалистами УИТ “Адилет сот” категорически запрещается. Работы по изменению конфигурации защищенных рабочих станций и серверов производятся в присутствии специалистов УИТ “Адилет сот” и пользователя данной автоматизированной рабочей станции.

При эксплуатации программного обеспечения необходимо:

* + 1. Соблюдать требования настоящего Положения.
    2. Использовать имеющееся в распоряжении программное обеспечение исключительно для выполнения своих служебных обязанностей.
    3. Обеспечивать сохранность переданных в составе автоматизированного рабочего места носителей с ключевой информацией, сертификатов подлинности коммерческого программного обеспечения, наклеенных на корпус системного блока автоматизированного рабочего места.
    4. Содействовать специалистам УИТ “Адилет сот” в выполнении работ по установке, настройке, устранению неисправностей и аудита установленного программного обеспечения.
    5. Ставить в известность специалистов УИТ “Адилет сот” о любых фактах нарушения требований настоящего Положения.
  1. При эксплуатации программного обеспечения запрещено:
     1. Использовать автоматизированное рабочее место не по назначению.
     2. Самостоятельно вносить изменения в конструкцию или конфигурацию автоматизированного рабочего места и другого оборудования автоматизированных систем.
     3. Изменять состав установленного на автоматизированное рабочее место программного обеспечения (устанавливать новое программное обеспечение, изменять состав компонент пакетов программного обеспечения и удалять программное обеспечение).
     4. Приносить на внешних носителях, загружать и не санкционированно запускать на своем или другом автоматизированном рабочем месте любые системные или прикладные программы, не указанные в Паспорте ПК.

1. Порядок установки программного обеспечения
   1. Запрос на установку программного обеспечения может быть инициирован по следующим основаниям:

* необходимости организации автоматизированного рабочего места для нового работника;
* необходимости выполнения работниками новых (дополнительных) обязанностей, для которых требуется дополнительное программное обеспечение или полная замена автоматизированного рабочего места;
* появления качественно нового (альтернативного) программного обеспечения, взамен используемого в составе автоматизированного рабочего места.
  1. Специалисты УИТ “Адилет сот” производит установку программного обеспечения в случаях:
* устранения уязвимостей систем обеспечения информационной безопасности Судебной системы;
* необходимости установки программного обеспечения для защиты информации.
  1. При отсутствии в Судебной системе вакантных лицензий на коммерческое программное обеспечение из перечня либо при отсутствии в перечне запрашиваемого программного обеспечения, специалисты УИТ “Адилет сот” готовят заявку на приобретение дополнительных лицензий, либо на приобретение требуемого программного обеспечения согласно принятым в Судебной системе правилам документооборота.
  2. До начала установки программного обеспечения, оно должно быть предварительно проверено на работоспособность, а также отсутствие опасных функций и недокументированных возможностей специалистами УИТ “Адилет сот”.
  3. После приобретения и установки дополнительного программного обеспечения специалисты УИТ “Адилет сот” вносят сведения о новом коммерческом программном обеспечении в Паспорт ПК и в Перечень.

1. Порядок поддержки и сопровождения программного обеспечения.
   1. Поддержка и сопровождение программного обеспечения выполняется специалистами УИТ “Адилет сот”.
   2. Поддержка и сопровождение программного обеспечения заключается в выполнении следующих видов работ:

* настройка и адаптация установленного программного обеспечения;
* установка обновлений программного обеспечения;
* регламентированное создание резервных копий (архивирование) программного обеспечения и пользовательских данных (электронных документов, баз данных);
* устранение неисправностей, связанных с использованием установленного программного обеспечения;
* консультирование пользователей информационных систем.
  1. Работа по сопровождению программного обеспечения может быть инициирована пользователем автоматизированной станции либо непосредственно специалистами УИТ “Адилет сот”.
  2. Любое изменение перечня установленного программного обеспечения, возникшее в ходе выполнения работ, должно быть отражено в Паспорте ПК.

1. Порядок удаления (вывода из эксплуатации) программного обеспечения
   1. Программное обеспечение выводится из эксплуатации в следующих случаях:

* окончание лицензионного срока использования программного обеспечения;
* замена используемого программного обеспечения на альтернативное;
* прекращение использования программного обеспечения в следствии отсутствия надобности, морального старения или выхода из строя.
  1. Вывод из эксплуатации выполняется специалистами УИТ “Адилет сот”.
  2. Выполняются необходимые обновления Паспортов ПК;
  3. При удалении (выводе из эксплуатации) коммерческого программного обеспечения в УИТ “Адилет сот” в целях дальнейшего хранения передаются (при необходимости оформляются акты возврата): оригиналы носителей с дистрибутивом программного обеспечения, документация к программному обеспечению, лицензионные договора (соглашения), копии договоров поставки, а также документов, подтверждающих факт купли-продажи. Так же в УИТ “Адилет сот” передаются аппаратные ключи, ключевые носители, находившиеся у пользователя информационной системы.
  4. УИТ “Адилет сот” в случае необходимости путем резервного копирования обеспечивает сохранность пользовательских данных, настроек, баз и банков данных, содержащихся в удаляемом программном обеспечении.

1. Аудит использования программного обеспечения
   1. Аудит использования программного обеспечения (далее – Аудит) проводится с целью выявления несоответствия перечней фактически установленного программного обеспечения перечням, зафиксированным в Паспортах ПК, а также нарушения исполнения сотрудниками Судебной системы других требований данного Положения.
   2. Аудит проводится специалистами УИТ “Адилет сот”.
   3. Для проведения аудита может применяться специализированное программное обеспечение.
   4. В случае несанкционированной установки программного обеспечения, данный факт рассматривается как нарушение действующей в Судебной системе Концепции информационной безопасности и настоящего Положения.
   5. Несанкционированно установленное программное обеспечение подлежит немедленному удалению, перечень установленного программного обеспечения приводится в соответствие текущей редакции Паспорта ПК данного автоматизированного рабочего места.
   6. Расследование допущенных нарушений производится на основании Регламента реагирования на инциденты информационной безопасности, утвержденного в Судебной системе.
   7. Если программное обеспечение установлено санкционировано, но не указано в Паспорте ПК, ИТ-консультант либо начальник структурного подразделения/отдела направляет поручение УИТ “Адилет сот” о внесении соответствующих изменений в Паспорт ПК.
   8. Плановый аудит проводится по всему парку вычислительной техники, использующейся в автоматизированных системах Судебной системы, не реже, чем один раз в год.
   9. Внеплановый аудит (полный или выборочный) проводится по мере необходимости. Необходимость, время и область проведения внеочередных аудитов определяются УИТ “Адилет сот” в соответствии с настоящим Положением.
2. Ответственность
   1. Работники, нарушившие требования настоящего Положения, несут ответственность в соответствии с действующим законодательством и локальными нормативными актами Судебной системы.

Приложение № 6

к приказу №\_\_\_\_\_

от «\_\_\_\_» \_\_\_\_\_\_\_\_2018г.

# Модель угроз и нарушителя безопасности персональных данных, обрабатываемых в информационных системах персональных данных Судебной системы

# Общие положения

Настоящая модель угроз безопасности персональных данных (далее – Модель) содержит систематизированный перечень угроз безопасности персональных данных при их обработке в информационной системе персональных данных Судебной системы. Указанные угрозы могут исходить от источников, имеющих антропогенный, техногенный и стихийный характер и воздействующих на уязвимости информационной системы персональных данных, характерные для данной информационной системы персональных данных, реализуя тем самым угрозы информационной безопасности.

В Модели дается обобщенное описание информационной системы персональных данных, состав, категории и предполагаемый объем обрабатываемых персональных данных с последующей классификацией информационных систем персональных данных.

Модель описывает потенциального нарушителя безопасности персональных данных и подходы по определению актуальности угроз с учетом возможностей нарушителя и особенностей конкретной информационной системы персональных данных.

**2. Характеристика объекта информатизации**

В Судебной системе предполагаются следующие типы информационных систем персональных данных:

1. Информационная система персональных данных ведения бухгалтерского учета, управления персоналом, расчета заработной платы Судебной системы.

2. Информационная система персональных данных передачи информации, в том числе персональные данные, в целях исполнения законов КР.

В качестве объектов информатизации выступают:

1. Автономные автоматизированные рабочие места.

2. Локальные вычислительные сети.

В зависимости от характеристик и особенностей отдельных объектов часть вычислительных средств данных подключена к сетям связи общего пользования и (или) сетям международного информационного обмена.

Ввод персональных данных осуществляется как с бумажных носителей (например, документов, удостоверяющих личность субъекта персональных данных), так и с электронных носителей информации.

Информационные системы персональных данных предполагают как распределенную (на автономное автоматизированное рабочее место), так и централизованную (на выделенных файловых серверах сети) обработку и хранение персональных данных.

Персональные данные субъектов могут выводиться из информационных систем персональных данных с целью передачи персональных данных сотрудников Судебной системы, как в электронном, так и в бумажном виде.

Контролируемой зоной информационных систем персональных данных являются здания и отдельные помещения. В пределах контролируемой зоны находятся рабочие места пользователей и места хранения архивных копий данных, серверы системы, сетевое и телекоммуникационное оборудование информационных систем персональных данных. Вне контролируемой зоны находятся линии передачи данных и телекоммуникационное оборудование, используемое для информационного обмена по сетям связи общего пользования и (или) сетям международного информационного обмена.

**3. Состав, категории и объем персональных данных, определение уровня защищенности персональных данных**

На основе характеристик и особенностей используемых информационных систем персональных данных и обрабатываемых в них персональных данных, можно констатировать, что персональные данные субъектов, обрабатываются в Судебной системе информационной системой, обрабатывающей общедоступные персональные данные, а также системой, обрабатывающей иные категории персональных данных. Специальные категории персональных данных и биометрические персональные данные в информационной системе персональных данных Судебной системы не обрабатываются.

**4. Способы нарушения характеристик безопасности персональных данных**

Исходя из перечня персональных данных, обрабатываемых в информационной системе персональных данных, существуют следующие способы нарушения характеристик безопасности персональных данных:

* хищение персональных данных сотрудниками Судебной системы для использования в корыстных целях;
* передача финансовой, адресной, юридической и прочей информации о субъекте персональных данных третьим лицам;
* несанкционированное публичное разглашение персональных данных, ставших известными сотрудникам Судебной системы;
* несанкционированное получение персональных данных третьими лицами;
* уничтожение финансовой, адресной, юридической и прочей информации о субъекте персональных данных;
* модификация финансовой, адресной, юридической и прочей информации о субъекте персональных данных;
* блокирование финансовой, адресной, юридической и прочей информации о субъекте персональных данных;
* ввод некорректной финансовой, адресной, юридической и прочей информации о субъекте персональных данных;
* передача некорректной финансовой, адресной, юридической и прочей информации о субъекте персональных данных;
* искажение архивной информации по субъекту персональных данных.
* уничтожение архивной информации по субъекту персональных данных.

**5. Угрозы безопасности персональных данных, при их обработке в информационных системах персональных данных**

Под угрозами безопасности персональных данных при их обработке в информационной системе персональных данных понимается совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и (или) несанкционированными и (или) непреднамеренными воздействиями на нее. Таким образом, угрозы безопасности персональным данным при их обработке в информационной системе персональных данных могут быть связаны как с непреднамеренными действиями персонала информационных систем персональных данных, так и со специально осуществляемыми неправомерными действиями сотрудниками Судебной системы и граждан, а также иными источниками угроз.

В целях формирования систематизированного перечня угроз безопасности персональным данным при их обработке в информационной системе персональных данных и разработке на их основе частных (детализированных) моделей применительно к конкретному виду информационной системе персональных данных, угрозы безопасности персональным данным в информационной системе персональных данных можно классифицировать в соответствии со следующими признаками:

* по видам возможных источников угроз;
* по типу информационных систем персональных данных, на которые направлена реализация угроз;
* по виду нарушаемого свойства информации (виду несанкционированных действий, осуществляемых с персональными данными);
* по способам реализации угроз;
* по используемой уязвимости;
* по объекту воздействия.

Для информационной системы персональных данных существуют следующие классы угроз безопасности персональных данных:

1. По видам возможных источников угроз безопасности персональных данных:

* угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, имеющими доступ к информационному ресурсу информационной системы персональных данных, включая пользователей, реализующие угрозы непосредственно в информационной системе персональных данных;
* угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, не имеющих доступа к информационным системам персональных данных, реализующие угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена;
* угрозы, возникновение которых напрямую зависит от свойств техники, используемой в информационных системах персональных данных;
* угрозы, связанные со стихийными природными явлениями.

Кроме этого, угрозы могут возникать в результате внедрения аппаратных закладок и вредоносных программ.

1. По типу информационных систем персональных данных, на которые направлена угроза:

По структуре информационных систем персональных данных, на которые направлена угроза, необходимо рассматривать следующие классы угроз:

* угрозы безопасности данных, обрабатываемых в информационных системах персональных данных на базе автоматизированных рабочих мест;
* угрозы безопасности данных, обрабатываемых в информационных системах персональных данных на базе локальных информационных систем.

1. По способам реализации угроз:

По способам реализации угроз выделяют следующие классы угроз:

* угрозы, связанные с несанкционированным доступом к персональным данным (в том числе угрозы внедрения вредоносных программ);
* угрозы утечки персональных данных по техническим каналам утечки информации;
* угрозы специальных воздействий на информационные системы персональных данных.

1. По виду нарушаемого свойства информации (несанкционированных действий, осуществляемых с персональными данными):

* угрозы, приводящие к нарушению конфиденциальности персональных данных (копированию или несанкционированному распространению), при реализации которых не осуществляется непосредственного воздействия на содержание информации;
* угрозы, приводящие к несанкционированному воздействию на содержание информации, в результате которого происходит изменение данных или их уничтожение;
* угрозы, приводящие к несанкционированному воздействию на программные или программно-аппаратные элементы информационных систем персональных данных, в результате которых осуществляется блокирование данных.

1. По используемой уязвимости выделяются следующие классы угроз:

* угрозы, реализуемые с использованием уязвимости системного программного обеспечения;
* угрозы, реализуемые с использованием уязвимости прикладного программного обеспечения; - угрозы, возникающие в результате использования уязвимости, вызванной наличием в информационной системе персональных данных аппаратной закладки;
* угрозы, реализуемые с использованием уязвимостей протоколов сетевого взаимодействия и каналов передачи данных;
* угрозы, возникающие в результате использования уязвимости, вызванной недостатками технической защиты информации от несанкционированного доступа;
* угрозы, реализуемые с использованием уязвимостей, обусловливающих наличие технических каналов утечки информации;
* угрозы, реализуемые с использованием уязвимостей средств защиты информации.

1. По объекту воздействия выделяются следующие классы угроз:

* угрозы безопасности персональных данных, обрабатываемых на автономном автоматизированном рабочем месте;
* угрозы безопасности персональных данных, обрабатываемых в выделенных средствах обработки (принтерах, вынесенных мониторах, видеопроекторах, средствах звуковоспроизведения и т.п.); угрозы безопасности персональных данных, передаваемых по сетям связи;
* угрозы прикладным программам, с помощью которых обрабатываются персональные данные;
* угрозы системному программному обеспечению, обеспечивающему функционирование информационной системе персональных данных.

**6. Характеристика источников угроз безопасности персональных данных в информационной системе персональных данных**

В отношении информационной системе персональных данных могут существовать три типа источников угроз безопасности персональных данных:

1. Антропогенные источники угроз безопасности персональных данных.

2. Техногенные источники угроз безопасности персональных данных.

3. Стихийные источники угроз безопасности персональных данных.

**Антропогенные источники угроз безопасности персональных данных**

В качестве антропогенного источника угроз для информационной системы персональных данных необходимо рассматривать субъекта (личность), имеющего санкционированный или несанкционированный доступ к работе со штатными средствами информационной системы персональных данных, действия которого могут привести к нарушению безопасности персональных данных. Антропогенные источники угроз по отношению к информационным систем персональных данных могут быть как внешними, так и внутренними

Среди внешних антропогенных источников можно выделить случайные и преднамеренные источники.

Случайные (непреднамеренные) источники могут использовать такие уязвимости, как ошибки, совершенные при проектировании информационной системы персональных данных и ее элементов, ошибки в программном обеспечении; различного рода сбои и отказы, повреждения, проявляемые в информационной системе персональных данных. К таким источникам можно отнести персонал поставщиков различного рода услуг, персонал надзорных и аварийных служб и т.п. Действия (угрозы), исходящие от данных источников, совершаются по незнанию, невнимательности или халатности, из любопытства, но без злого умысла.

Преднамеренные источники проявляются в корыстных устремлениях нарушителей. Основная цель таких источников – умышленная дезорганизацияя работы, вывод систем Судебной системы из строя, искажение информации за счет проникновения в информационные системы персональных данных путем несанкционированного доступа.

Внутренними источниками, как правило, являются специалисты в области программного обеспечения и технических средств, в том числе средств защиты информации, имеющие возможность использования штатного оборудования и программно-технических средств информационных систем персональных данных. К таким источникам можно отнести основной персонал, представителей служб безопасности, вспомогательный и технический персонал.

Для внутренних источников угроз особое место занимают угрозы в виде ошибочных действия и (или) нарушений требований эксплуатационной и иной документации сотрудниками Судебной системы, имеющих доступ к информационным ресурсам информационных систем персональных данных. К подобным угрозам, в частности, относятся:

* непредумышленное искажение или удаление программных компонентов;
* внедрение и использование неучтенных программ;
* игнорирование организационных ограничений (установленных правил) при работе с ресурсами информационных систем персональных данных, включая средства защиты информации. В частности:
  + нарушение правил хранения информации ограниченного доступа, используемой при эксплуатации средств защиты информации (ключевой, парольной и аутентифицирующей информации);
  + предоставление посторонним лицам возможности доступа к средствам защиты информации, а также к техническим и программным средствам, способным повлиять на выполнение предъявляемых к средствам защиты информации требований;
  + настройка и конфигурирование средств защиты информации, а также технических и программных средств, способных повлиять на выполнение предъявляемых к средствам защиты информации требований, в нарушение нормативных и технических документов;
  + несообщение о фактах утраты, компрометации ключевой, парольной и аутентифицирующей информации, а также любой другой информации ограниченного доступа.

Наибольшую опасность представляют преднамеренные угрозы, исходящие как от внешних, так и от внутренних антропогенных источников.

Необходимо рассматривать следующие классы таких угроз:

* угрозы, связанные с преднамеренными действиями лиц, имеющими доступ к информационным системам персональных данных, включая пользователей информационных систем персональных данных и иных сотрудников Судебной системы, реализующими угрозы непосредственно в информационной системе персональных данных (внутренний нарушитель);
* угрозы, связанные с преднамеренными действиями лиц, не имеющими доступа к информационным системам персональных данных и реализующими угрозы из внешних сетей связи общего пользования или сетей международного информационного обмена (внешний нарушитель);
* угрозы, связанные с преднамеренными действиями лиц, не имеющими доступа к информационным системам персональных данных и реализующими угрозы по техническим каналам утечки информации.

**Техногенные источники угроз безопасности персональных данных**

Техногенные источники угроз напрямую зависят от свойств техники. Данные источники также могут быть как внешними, так и внутренними.

К внешним источникам относятся инфраструктурные элементы информационной системы персональных данных: средства связи (телефонные линии, линии передачи данных и т.п.), сети инженерных коммуникаций (водоснабжение, канализация, отопление и пр.).

К внутренним источникам относятся некачественные технические и программные средства обработки информации, вспомогательные средства (охраны, сигнализации, телефонии), другие технические средства, применяемые в информационных системах персональных данных, а также вредоносное программное обеспечение и аппаратные закладки.

**Аппаратная закладка**

Аппаратные закладки могут быть конструктивно встроенными и автономными. Аппаратные закладки могут реализовать угрозы:

* сбора и накопления персональных данных, обрабатываемых и хранимых в информационных системах персональных данных;
* формирования технических каналов утечки информации.

В силу отмеченных свойств аппаратных закладок эффективная защита от них может быть обеспечена только за счет тщательного учета их специфики и соответствующей организации технической защиты информации на всех стадиях жизненного цикла информационной системы персональных данных.

**Носитель вредоносной программы**

В качестве носителя вредоносной программы в информационной системе персональных данных может выступать аппаратный элемент средств вычислительной техники из состава информационных система персональных данных или программоное обеспечение, выполняющее роль программного контейнера.

Если вредоносная программа не ассоциируется с какой-либо прикладной программой из состава системного или общего программного обеспечения информационной системы персональных данных, в качестве ее носителя выступают:

* внешний машинный (отчуждаемый) носитель, т.е. дискета, оптический диск, лазерный диск, флэш-память, внешний жесткий диск и т.п.;
* встроенные носители информации (жесткие диски, микросхемы оперативной памяти, процессор, микросхемы системной платы, микросхемы устройств, встраиваемых в системный блок устройства – видеоадаптера, сетевой платы, устройств ввода/вывода и т.д.)
* микросхемы внешних устройств (монитора, клавиатуры, принтера, плоттера, сканера и т.п.).

В том случае, если вредоносная программа может быть проассоциирована с системным или общим программным обеспечением, с файлами различной структуры или с сообщениями, передаваемыми по сети, то ее носителем являются:

* пакеты передаваемых по сети информационной системы персональных данных сообщений;
* файлы (исполняемые, текстовые, графические и т.д.).

При возникновении угроз из данной группы появляется потенциальная возможность нарушения конфиденциальности, целостности, доступности и других характеристик безопасности персональных данных.

**Стихийные источники угроз безопасности персональных данных**

Стихийные источники угроз отличается большим разнообразием и непредсказуемостью и являются, как правило, внешними. Под ними, прежде всего, рассматриваются различные природные катаклизмы: пожары, землетрясения, ураганы, наводнения. Возникновение этих источников трудно спрогнозировать и им тяжело противодействовать, но при наступлении подобных событий нарушается штатное функционирование самой информационной системы персональных данных и ее средств защиты, что потенциально может привести к нарушению конфиденциальности, целостности, доступности и других характеристик безопасности персональных данных.

Защита от угроз, исходящих от техногенных и стихийных источников угроз безопасности персональных данных, регламентируется инструкциями, разработанными и утвержденными оператором с учетом особенностей эксплуатации информационных систем персональных данных.

**7. Модель нарушителя безопасности персональных данных**

Анализ возможностей, которыми может обладать нарушитель, проводится в рамках модели нарушителя.

При разработке модели нарушителя зафиксированы следующие положения:

1. Безопасность персональных данных в информационной системе персональных данных обеспечивается средствами защиты информации информационными системами персональных данных, а также используемыми в них информационными технологиями, техническими и программными средствами, удовлетворяющими требованиям по защите информации;

2. Средства защиты информации штатно функционируют совместно с техническими и программными средствами, которые способны повлиять на выполнение предъявляемых к средствам защиты информации требований;

3. Средства защиты информации не могут обеспечить защиту персональных данных от действий, выполняемых в рамках предоставленных субъекту действий полномочий (например, средство защиты информации не может обеспечить защиту персональных данных от раскрытия лицами, которым предоставлено право на доступ к этим данным).

**8. Описание нарушителей**

С точки зрения наличия права постоянного или разового доступа в контролируемую зону объектов размещения информационных систем персональных данных все физические лица могут быть отнесены к следующим двум категориям:

* категория I – лица, не имеющие права доступа в контролируемую зону информационных систем персональных данных;
* категория II – лица, имеющие право доступа в контролируемую зону информационных систем персональных данных.

Все потенциальные нарушители подразделяются на:

* внешних нарушителей, осуществляющих атаки из-за пределов контролируемой зоны информационных систем персональных данных;
* внутренних нарушителей, осуществляющих атаки, находясь в пределах контролируемой зоны информационных систем персональных данных.

В качестве внешнего нарушителя кроме лиц категории I должны рассматриваться также лица категории II, находящиеся за пределами контролируемой зоны.

В отношении информационной системы персональных данных в качестве внешнего нарушителями из числа лиц категории I могут выступать:

* бывшие сотрудники Судебной системы;
* посторонние лица, пытающиеся получить доступ к персональным данным в инициативном порядке;
* представители преступных организаций.

Внешний нарушитель может осуществлять:

* перехват обрабатываемых техническими средствами информационные системы персональных данных за счет их утечки по техническим каналам утечки информации с использованием портативных, возимых, носимых, а также автономных автоматических средств разведки серийной разработки;
* деструктивные воздействия через элементы информационной инфраструктуры информационных систем персональных данных, которые в процессе своего жизненного цикла (модернизация, сопровождение, ремонт, утилизация) оказываются за пределами контролируемой зоны;
* несанкционированный доступ к информации с использованием специальных программных воздействий посредством программы вирусов, вредоносных программ, алгоритмических или программных закладок;
* перехват информации, передаваемой по сетям связи общего пользования или каналам связи, не защищенным от несанкционированного доступа к информации организационно- техническими мерами;
* атаки на информационные системы персональных данных путем реализации угроз удаленного доступа.

Внутренний нарушитель (лица категории II) подразделяется на восемь групп в зависимости от способа и полномочий доступа к информационным ресурсам информационных систем персональных данных.

К первой группеотносятся сотрудники Судебной системы, не являющиеся зарегистрированными пользователями и не допущенные к информационным ресурсам информационных систем персональных данных, но имеющие санкционированный доступ в контролируемые зоны. К этой категории нарушителей относятся сотрудники различных структурных подразделений предприятий: энергетики, сантехники, уборщицы, сотрудники охраны и другие лица, обеспечивающие нормальное функционирование объекта информатизации.

Лицо данной группы может:

* располагать именами и вести выявление паролей зарегистрированных пользователей информационных систем персональных данных;
* изменять конфигурацию технических средств обработки персональных данных, вносить программно-аппаратные закладки в программно-технические средства информационных систем персональных данных и обеспечивать съем информации, используя непосредственное подключение к техническим средствам обработки информации.

Ко второй группеотносятся зарегистрированные пользователи информационных систем персональных данных, осуществляющие ограниченный доступ к информационным ресурсам информационных систем персональных данных с рабочего места. К этой категории относятся сотрудники предприятий, имеющие право доступа к локальным информационным ресурсам информационных систем персональных данных для выполнения своих должностных обязанностей.

Лицо данной группы:

* обладает всеми возможностями лиц первой категории;
* знает, по меньшей мере, одно легальное имя доступа;
* обладает всеми необходимыми атрибутами (например, паролем), обеспечивающим доступ к информационным ресурсам информационных систем персональных данных;
* располагает персональными данными, к которым имеет доступ.

К третьей группеотносятся зарегистрированные пользователи подсистем информационных ресурсов, осуществляющие удаленный доступ к персональным данным по локальной сети Судебной системы.

Лицо данной группы:

* обладает всеми возможностями лиц второй категории;
* располагает информацией о топологии сети информационных систем персональных данных и составе технических средств информационных систем персональных данных;
* имеет возможность прямого (физического) доступа к отдельным техническим средствам информационных систем персональных данных.

К четвертой группеотносятся зарегистрированные пользователи информационных систем персональных данных с полномочиями администратора безопасности сегмента (фрагмента) информационной системы персональных данных.

Лицо данной группы:

* обладает полной информацией о системном и прикладном программном обеспечении, используемом в сегменте информационной системы персональных данных;
* обладает полной информацией о технических средствах и конфигурации сегмента информационной системы персональных данных;
* имеет доступ к средствам защиты информации и протоколирования, а также к отдельным элементам, используемым в сегменте информационной системы персональных данных;
* имеет доступ ко всем техническим средствам сегмента информационной системы персональных данных;
* обладает правами конфигурирования и административной настройки некоторого подмножества технических средств сегмента информационной системы персональных данных.

К пятой группеотносятся зарегистрированные пользователи с полномочиями системного администратора, выполняющего конфигурирование и управление программным обеспечением и оборудованием, включая оборудование, отвечающее за безопасность защищаемого объекта: средства мониторинга, резервного копирования, антивирусного контроля, защиты от несанкционированного доступа.

Лицо данной группы:

* обладает полной информацией о системном, специальном и прикладном программном обеспечении, используемом в информационной системе персональных данных;
* обладает полной информацией о технических средствах и конфигурации информационной системы персональных данных
* имеет доступ ко всем техническим средствам информационной системы персональных данных;
* обладает правами конфигурирования и административной настройки технических средств информационной системы персональных данных.

К шестой группеотносятся зарегистрированные пользователи информационных систем персональных данных с полномочиями администратора безопасности Судебной системы, отвечающего за соблюдение правил разграничения доступа, за генерацию ключевых элементов, смену паролей, криптографическую защиту информации. Администратор безопасности осуществляет аудит тех же средств защиты объекта, что и системный администратор.

Лицо данной группы:

* обладает полной информацией об информационных системах персональных данных;
* имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов информационных систем персональных данных;
* не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).

К седьмой группеотносятся лица из числа программистов - разработчиков сторонних организаций, являющихся поставщиками программного обеспечения и лица, обеспечивающие его сопровождение на объекте размещения информационной системы персональных данных.

Лицо данной группы:

* обладает информацией об алгоритмах и программах обработки информации в информационной системе персональных данных;
* обладает возможностями внесения ошибок, недекларированных возможностей, программных закладок, вредоносных программ в программное обеспечение информационной системы персональных данных на стадии его разработки, внедрения и сопровождения;
* может располагать любыми фрагментами информации о технических средствах обработки и защиты информации в информационной системе персональных данных.

К восьмой группеотносятся персонал, обслуживающий технические средства информационных систем персональных данных, а также лица, обеспечивающие поставку, сопровождение и ремонт технических средств информационных систем персональных данных.

Лицо данной группы:

* обладает возможностями внесения закладок в технические средства информационных систем персональных данных на стадии их разработки, внедрения и сопровождения;
* может располагать фрагментами информации о топологии информационных систем персональных данных, автоматизированных рабочих местах, серверах и коммуникационном оборудовании, а также о технических средствах защиты информации в информационных системах персональных данных.

**9. Предположения о возможностях нарушителя**

Для получения исходных данных о информационной системе персональных данных нарушитель (как I категории, так и II категории) может осуществлять перехват зашифрованной информации и иных данных, передаваемых по каналам связи сетям общего пользования и (или) сетям международного информационного обмена, а также по локальным сетям информационных систем персональных данных.

Любой внутренний нарушитель может иметь физический доступ к линиям связи, системам электропитания и заземления.

Предполагается, что возможности внутреннего нарушителя существенным образом зависят от действующих в пределах контролируемой зоны объектов размещения информационных систем персональных данных ограничительных факторов, из которых основными являются режимные мероприятия и организационно-технические меры, направленные на:

* предотвращение и пресечение несанкционированных действий;
* подбор и расстановку кадров;
* допуск физических лиц в контролируемую зону и к средства вычислительной техники;
* контроль за порядком проведения работ.

В силу этого внутренний нарушитель не имеет возможности получения специальных знаний о информационных системах персональных данных в объеме, необходимом для решения вопросов создания и преодоления средств защиты персональных данных, и исключается его возможность по созданию и применению специальных программно-технических средств реализации целенаправленных воздействий данного нарушителя на подлежащие защите объекты и он может осуществлять попытки несанкционированного доступа к информационным ресурсам с использованием только штатных программно-технических средств информационной системы персональных данных без нарушения их целостности.

Возможность сговора внутренних нарушителей между собой, сговора внутреннего нарушителя с персоналом организаций-разработчиков подсистем информационной системы персональных данных, а также сговора внутреннего и внешнего нарушителей должна быть исключена применением организационно-технических и кадрово-режимных мер, действующих на объектах размещения информационных систем персональных данных.

**10. Предположения об имеющихся у нарушителя средствах атак**

Предполагается, что нарушитель имеет все необходимые для проведения атак по доступным ему каналам атак средства.

Внешний нарушитель (лица категории I, а также лица категории II при нахождении за пределами контролируемой зоны) может использовать следующие средства доступа к защищаемой информации:

* доступные в свободной продаже аппаратные средства и программное обеспечение, в том числе программные и аппаратные компоненты криптосредств;
* специально разработанные технические средства и программное обеспечение;
* средства перехвата и анализа информационных потоков в каналах связи;
* специальные технические средства перехвата информации по техническим каналам утечки информации;
* штатные средства информационной системы персональных данных (только в случае их расположения за пределами контролируемой зоны).

Внутренний нарушитель для доступа к защищаемой информации, содержащей персональные данные, может использовать только штатные средства информационной системы персональных данных. При этом его возможности по использованию штатных средств зависят от реализованных в информационной системе персональных данных организационно-технических и режимных мер.

**11. Описание каналов атак**

Возможными каналами атак, которые может использовать нарушитель для доступа к защищаемой информации в информационной системе персональных данных, являются:

* каналы непосредственного доступа к объекту (визуально-оптический, акустический, физический);
* электронные носители информации, в том числе съемные, сданные в ремонт и вышедшие из употребления;
* бумажные носители информации;
* штатные программно-аппаратные средства информационной системы персональных данных;
* кабельные системы и коммутационное оборудование, расположенные в пределах контролируемой зоны и не защищенные от несанкционированного доступа к информации организационно-техническими мерами;
* незащищенные каналы связи; техническим каналам утечки информации.

Приложение № 7

к приказу №\_\_\_\_\_

от «\_\_\_\_» \_\_\_\_\_\_\_\_2018г.

# Положение об использовании сети Интернет и электронной почты в Судебной системе

2. **Общие положения**
   1. Настоящее Положение разработано во исполнение Концепции информационной безопасности Судебной системы и устанавливает порядок использования сети Интернет и электронной почты сотрудниками Судебной системы.
   2. Действие настоящего Положения распространяется на сотрудников Судебной системы, подключенных к сети Интернет.
3. **Основные термины, сокращения и определения**
4. Адрес IP – уникальный идентификатор АРМ, подключенного к информационной системе, а также сети Интернет.
5. АРМ – автоматизированное рабочее место пользователя (персональный компьютер с прикладным ПО) для выполнения определенной производственной задачи.
6. Интернет – глобальная ИС, обеспечивающая удаленный доступ к ресурсам различного содержания и направленности.
7. АС – автоматизированная система – система, обеспечивающая хранение, обработку, преобразование и передачу информации с использованием компьютерной и другой техники.
8. ИТ – информационные технологии – совокупность методов и процессов, обеспечивающих хранение, обработку, преобразование и передачу информации с использованием средств компьютерной и другой техники.
9. Паспорт ПК – документ, содержащий полный перечень оборудования и программного обеспечения АРМ.
10. ПК – персональный компьютер.
11. ПО – программное обеспечение вычислительной техники, базы данных.
12. ПО вредоносное – ПО или изменения в ПО, приводящие к нарушению конфиденциальности, целостности и доступности информации.
13. ПО коммерческое – ПО сторонних производителей (правообладателей). Предоставляется в пользование на возмездной (платной) основе.
14. Пользователь – работник, использующий ресурсы Интернет для выполнения своих должностных обязанностей.
15. Реестр – документ «Реестр разрешенного к использованию ПО». Содержит перечень коммерческого ПО, разрешенного к использованию.
16. Электронная почта – сервис обмена электронными сообщениями в рамках АС (внутренняя электронная почта) и общедоступных сетей Интернет (внешняя электронная почта).
17. Электронное почтовое сообщение – сообщение, формируемое отправителем с помощью почтового клиента и предназначенное для передачи получателю посредством электронной почты.
18. Электронный документ – документ, в котором информация представлена в электронно-цифровой форме.
19. Электронный почтовый ящик – персональное пространство на почтовом сервере, в котором хранятся электронные сообщения.

**3. Порядок использования сети Интернет и электронной почты**

3.1. Доступ в сеть Интернет и к электронной почте (далее – к Сервисам) в Судебной системе осуществляется централизованно с применением специальных программно-технических средств защиты (межсетевых экранов).

3.2. Доступ к Сервисам с использованием мобильных устройств (мобильного интернета) не допускается.

3.3. На автоматизированном рабочем месте, подключенном к сети Internet, в обязательном порядке должно быть установлено антивирусное программное обеспечение с актуальной антивирусной базой.

3.4. Доступ к Сервисам предоставляется пользователям в целях выполнения ими своих служебных обязанностей, требующих непосредственного подключения к внешним информационным ресурсам, для обмена служебной информацией в виде электронных сообщений и документов в электронном виде в интересах Судебной системы после ознакомления с настоящим Положением и Приложениями к нему.

3.5. Для доступа сотрудников Судебной системы к Сервисам допускается применение коммерческого или бесплатного программного обеспечения, входящего в Реестр разрешенного к использованию программного обеспечения и указанного в Паспорте ПК.

3.6. Доступ сотруднику Судебной системы к Сервисам может быть инициирован Руководителем структурного подразделения в случаях:

* необходимости организации автоматизированного рабочего места (для нового работника);
* необходимости выполнения сотрудником новых (дополнительных) обязанностей, для которых требуется доступ к внешним ресурсам.

3.7. Предоставление доступа сотрудников Судебной системы к Сервисам и их техническому обеспечению выполняется в соответствии с Порядком доступа к информационным, программным и аппаратным ресурсам Судебной системы сотрудниками УИТ “Адилет сот” через заявку на имя управляющего УИТ “Адилет сот”.

3.8. При использовании Сервисов необходимо:

3.8.1. Соблюдать требования настоящего Положения.

3.8.2. Использовать сеть Интернет исключительно для выполнения своих служебных обязанностей.

3.8.3. Ставить в известность УИТ “Адилет сот” о любых фактах нарушения требований настоящего Положения.

Типичные угрозы при работе с Сервисами и рекомендации по их предотвращению приведены в Приложении №7.

Общие меры предосторожности при работе с Сервисами приведены в Приложении №8.

3.9. При использовании Сервисов запрещено:

3.9.1. Использовать предоставленный Судебной системой доступ к Сервисам в личных целях.

3.9.2. Использовать специализированные аппаратные и программные средства, позволяющие сотрудникам Судебной системы для получения несанкционированного доступа к Сервисам.

3.9.3. Публиковать, загружать и распространять материалы содержащие:

* конфиденциальную информацию, а также информацию, составляющую коммерческую тайну, персональные данные, за исключением случаев, когда это входит в служебные обязанности и способ передачи является безопасным, согласованным с УИТ “Адилет сот” заранее;
* информацию, полностью или частично, защищенную авторскими или другим правами, без разрешения владельца;
* вредоносное программное обеспечение, предназначенное для нарушения, уничтожения либо ограничения функциональности любых аппаратных и программных средств, для осуществления несанкционированного доступа, а также серийные номера к коммерческому программному обеспечению и программное обеспечение для их генерации, пароли и прочие средства для получения несанкционированного доступа к платным Интернет-ресурсам, а также ссылки на вышеуказанную информацию;
* угрожающую, клеветническую, непристойную информацию, а также информацию, оскорбляющую честь и достоинство других лиц, материалы, способствующие разжиганию национальной розни, подстрекающие к насилию, призывающие к совершению противоправной деятельности и т.д.

3.9.4. Фальсифицировать свой IP-адрес, а также прочую служебную информацию.

3.9.5. Распространять и устанавливать на других автоматизированных системах любое программное обеспечение и данные, полученные с использованием Сервисов.

3.9.6. Осуществлять попытки несанкционированного доступа к ресурсам Сети, проведение сетевых атак и сетевого взлома и участие в них.

3.9.7. Переходить по ссылкам и открывать вложенные файлы входящих электронных сообщений, полученных от неизвестных отправителей.

3.9.8. По собственной инициативе осуществлять рассылку (в том числе и массовую) электронных сообщений, если рассылка не связана с выполнением служебных обязанностей.

3.9.10. Использовать адрес электронной почты для оформления подписки на периодическую рассылку материалов из сети Интернет, не связанных с исполнением служебных обязанностей.

3.9.11. Публиковать свой электронный адрес, либо электронный адрес других сотрудников Судебной системы на общедоступных Интернет-ресурсах (форумы, конференции и т.п.).

3.9.12. Предоставлять сотрудникам Судебной системы (за исключением специалистов УИТ “Адилет сот”) и третьим лицам доступ к своему электронному почтовому ящику.

3.9.13. Перенаправлять электронные сообщения с личных почтовых ящиков на корпоративный.

3.9.14. Запрещается использование в качестве паролей для доступа к ресурсам Сервисов паролей, аналогичных паролям, используемым для доступа к ресурсам Судебной системы.

3.9.15. Запрещается отключать установленное на автоматизированном рабочем месте антивирусное программное обеспечение.

3.10. Содержание Интернет-ресурсов, а также файлы, загружаемые из Сервисов, подлежат обязательной проверке на отсутствие вредоносного программного обеспечения.

3.12. Информация о посещаемых сотрудниками Судебной системы Интернет-ресурсах протоколируется для последующего анализа и, при необходимости, может быть предоставлена Руководителям структурных подразделений, а также директору Судебного департамента для контроля.

3.13. УИТ “Адилет сот” по согласованию с руководством Судебного департамента имеет право блокировать или ограничивать доступ пользователей к Интернет-ресурсам, содержание которых не имеет отношения к исполнению служебных обязанностей, а также к ресурсам, содержание и направленность которых запрещены международным законодательством.

3.14. УИТ “Адилет сот” имеет право доступа к электронным сообщениям работников с целью их архивирования и централизованного хранения, а также мониторинга выполнения требований настоящего Положения.

3.15. В случае нарушения пунктов Положения УИТ “Адилет сот” вправе отключить автоматизированное рабочее место от Сервисов, уведомив об этом руководство структурного подразделения.

3.16. Расследование допущенных нарушений Положения производится на основании Регламента реагирования на инциденты информационной безопасности, утвержденного в Судебной системе.

**4. Ответственность**

4.1. Сотрудники, нарушившие требования настоящего Положения, несут ответственность в соответствии с действующим законодательством и локальными нормативными актами Судебной системы.

**5. Заключительные положения**

5.1. Анализ актуальности данного Положения должен проводиться УИТ “Адилет сот” не реже одного раза в год, а также в каждом случае внедрения новых сервисов в дополнение к имеющимся. В случае если в ходе такого анализа была установлена необходимость внесения изменений в Положение, новая редакция Положения должна быть утверждена приказом директора Судебного департамента.

5.2. Контроль над соблюдением требований данного Положения проводится УИТ “Адилет сот”.

# 

Приложение № 8

к приказу №\_\_\_\_\_

от «\_\_\_\_» \_\_\_\_\_\_\_\_2018г.

# Положение по организации парольной защиты

# в Судебной системе

1. **ОБЩИЕ ПОЛОЖЕНИЯ**
   1. Данное положение регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в автоматизированных системах Судебной системы, меры обеспечения безопасности при использовании паролей, а также контроль за действиями пользователей и обслуживающего персонала систем при работе с паролями.
   2. Требования настоящего Положения являются неотъемлемой частью комплекса мер безопасности и защиты информации в Судебной системе.
   3. Требования настоящего Положения распространяются на всех сотрудников судебной системы, использующих в работе средства вычислительной техники (включая работу в локальной вычислительной сети) и должны применяться для всех средств вычислительной техники, эксплуатируемой в судебной системе.
   4. Организационное обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах автоматизированных системах судебной системы и контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями возлагается на УИТ “Адилет сот”. Техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей возлагается на ответственного сотрудника УИТ “Адилет сот”.
   5. Ознакомление всех сотрудников Судебной системы, использующих средства вычислительной техники, с требованиями положения проводит ответственный сотрудник местных судов, либо ответственный сотрудник подразделений Судебного департамента при ВС КР. При ознакомлении с Положением внимание сотрудников акцентируется на предупреждении их о персональной ответственности за разглашение парольной информации.
   6. Термины и определения:

Автоматизированная система (АС) - совокупность программных и аппаратных средств, предназначенных для хранения, передачи и обработки данных и информации и производства вычислений.

Информационная безопасность (ИБ) – обеспечение защищенности информации (ее конфиденциальности, целостности, доступности) от широкого спектра угроз с целью обеспечения непрерывности бизнеса, минимизации рисков бизнеса и максимального увеличения возможностей бизнеса.

Несанкционированный доступ (НСД) - доступ субъекта к объекту в нарушение установленных в системе правил разграничения доступа.

Учетная запись - информация о сетевом пользователе: имя пользователя, его пароль, права доступа к ресурсам и привилегии при работе в системе. Учетная запись может содержать дополнительную информацию (адрес электронной почты, телефон и т.п.).

Принцип минимальных привилегий - принцип, согласно которому «каждому субъекту системы предоставляется минимальный набор полномочий (или минимальный допуск), необходимый для выполнения вверенных задач. Применение этого принципа ограничивает ущерб, наносимый в случае случайного, ошибочного или несанкционированного использования.

Компрометация – утрата доверия к тому, что информация недоступна посторонним лицам.

Ключевой носитель – электронный носитель (дискета, флэш-накопитель, компакт-диск и т.п.), на котором находится ключевая информация (сертификаты и т.п.).

1. **ОБЩИЕ ТРЕБОВАНИЯ К ПАРОЛЯМ**
2. Пароли доступа ко всем подсистемам автоматизированных систем и информационным ресурсам первоначально формируются ответственным сотрудником УИТ “Адилет сот”, а в дальнейшем выбираются пользователями самостоятельно, но с учетом требований, изложенных ниже.
3. Личные пароли пользователей автоматизированных систем должны выбираться с учетом следующих требований:

* длина пароля должна быть не менее 8 символов;
* в числе символов пароля обязательно должны присутствовать буквы, цифры и (или) специальные символы (@, #, $, &, \*, % и т.п.). Исключение составляют подсистемы автоматизированных систем, в которых использование подобных спецсимволов недопустимо;
* пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования рабочих станций и т.д.), а также общепринятые сокращения и термины (qwerty, pa$$w0rd, и т.п.);
* при смене пароля новый пароль должен отличаться от старого не менее, чем двумя символами;

1. Пароли служебных и привилегированных учетных записей автоматизированной системы должны выбираться с учетом следующих требований:

* длина пароля должна быть не менее 12 символов;
* в числе символов пароля обязательно должны присутствовать, цифры и (или) специальные символы (@, #, $, &, \*, % и т.п.). Исключение составляют подсистемы автоматизированных систем, в которых использование подобных спецсимволов недопустимо;
* пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования рабочих станций и т.д.), а также общепринятые сокращения и термины (qwerty, pa$$w0rd, и т.п.), пароль не должен быть словом русского либо английского языка, в котором заменены некоторые символы (o->0,s->$, a->@ и т.п.).
* при смене пароля новый пароль должен отличаться от старого не менее, чем четырьмя символами, расположенными не подряд;
* при создании паролей служебных учетных записей возможно использование специализированного программного обеспечения для генерации сложных для подбора легко запоминаемых паролей.

1. **БЕЗОПАСНОСТЬ ЛОКАЛЬНЫХ УЧЕТНЫХ ЗАПИСЕЙ**
   1. Локальные учетные записи компьютеров (Administrator, Guest) предназначены для служебного использования специалистами УИТ “Адилет сот” при настройке систем и не предназначены для повседневной работы.
   2. Создание и использование локальных учетных записей на рабочих станциях, подключенных к автоматизированным системам и входящих в состав домена, либо в состав какого-либо из его поддоменов пользователям **ЗАПРЕЩЕНО**.
   3. Встроенная учетная запись Guest (Гость) должна быть заблокирована на всех рабочих станциях в составе автоматизированных систем при первоначальном конфигурировании операционной системы.
   4. Встроенная учетная запись Administrator (Администратор) должна быть защищена паролем согласно п. 2.3. настоящей инструкции.
   5. BIOS рабочих станций в составе автоматизированных систем должна быть защищена паролем согласно п. 2.3. настоящей инструкции.
2. **БЕЗОПАСНОСТЬ ДОМЕННЫХ УЧЕТНЫХ ЗАПИСЕЙ**
3. Создание, изменение, удаление доменных учетных записей, а также учетных записей сервисов автоматизированных систем (корпоративная электронная почта и др.) необходимо производить в соответствии с положением «о порядке доступа к информационным, программным и аппаратным ресурсам Судебной системы».
4. Пользователь несет персональную ответственность за сохранение в тайне личного пароля. Запрещается сообщать пароль другим лицам, а также хранить записанный пароль в общедоступных местах.
5. В случае производственной необходимости (командировка, отпуск и т.п.), при проведении проверочных мероприятий, выполняемых УИТ “Адилет сот” и требующих знания пароля пользователя, допускается раскрытие значений своего пароля специалистам УИТ “Адилет сот”. По окончанию производственных, или проверочных работ работники самостоятельно производят немедленную смену значений "раскрытых" паролей.
6. В случае возникновении нештатных ситуаций, форс-мажорных обстоятельств, а также технологической необходимости использования имен и паролей работников (в их отсутствие) допускается изменение паролей. В подобных случаях, сотрудники, чьи пароли были изменены, обязаны сразу же после выяснения факта смены своих паролей, создать их новые значения.
7. Пароли учетных записей пользователей автоматизированных систем должны соответствовать требованиям п. 2.2. Настоящего Положения.
8. К управлению доменными учетными записями пользователей необходимо подходить исходя из принципа «минимальных привилегий», т.е. пользователь не должен иметь прав доступа как к локальной системе, так и к ресурсам автоматизированной системы больше, чем это необходимо ему для выполнения своих должностных обязанностей.
9. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в 2 месяца. Плановая смена должна предусматривать информирование пользователя о необходимости сменить пароль и возможность смены пароля без обращения к специалистам УИТ “Адилет сот”.
10. Внеплановая смена личного пароля или удаление учетной записи пользователя автоматизированной системы в случае прекращения его полномочий (увольнение и т.п.) должна производиться ответственным сотрудником УИТ “Адилет сот” немедленно после окончания последнего сеанса работы данного пользователя с системой.
11. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на работу в другое подразделение или отдел внутри Судебной системы и другие обстоятельства) сотрудников, которым по роду работы были предоставлены полномочия по управлению парольной защитой подсистем.
12. В случае длительного отсутствия пользователя (командировка, болезнь и т.п.) его учетная запись блокируется, и, в случае необходимости, изменяются права доступа других пользователей в отношении ресурсов данного пользователя в соответствии с положением «о порядке доступа к информационным, программным и аппаратным ресурсам Судебной системы».
13. В случае компрометации личного пароля пользователя должны быть немедленно предприняты меры по внеплановой смене личного пароля самим пользователем с немедленным информированием специалистов УИТ “Адилет сот”.
14. Смена забытого пользовательского пароля производится ответственным сотрудником УИТ “Адилет сот” на основании сообщения пользователя с обязательной установкой параметра «Требовать смену пароля при следующем входе в систему».
15. Для предотвращения угадывания паролей ответственным сотрудником УИТ “Адилет сот” обязан настроить механизм блокировки учетной записи на 20 минут при пятикратном неправильном вводе пароля.
16. При временном оставлении рабочего места в течение рабочего дня рабочая станция в обязательном порядке блокируется нажатием комбинации клавиш «Win + L».
17. При возникновении вопросов, связанных с использованием доменных учетных записей пользователь автоматизированной системы обязан обратиться к специалистам УИТ “Адилет сот”.
18. **ВРЕМЕННЫЕ УЧЕТНЫЕ ЗАПИСИ**
    1. Для предоставления временного доступа к ресурсам Судебной системы (для лиц, не являющихся сотрудниками Судебной системы, для сотрудников, которым необходимо получить временный доступ к ресурсам автоматизированных систем, и т.п.) необходимо использовать процедуру временных учетных записей.
    2. Временная учетная запись – учетная запись, имеющая ограничение по времени действия, имеющая ограниченные права по доступу. Для временных учетных записей проводится подробное протоколирование их использования. Процедура получения временных учетных записей состоит в следующем:

# сотрудник подразделения/отдела Судебной системы через своего руководителя оформляет соответствующим образом Заявку «на предоставление доступа к информационным, программным и аппаратным ресурсам Судебной системы», указав в заявке, что требуемая учетная запись временная и определив временные рамки ее использования;

* заявка направляется управляющему УИТ “Адилет сот” для рассмотрения;
* временная учетная запись создается ответственным сотрудником УИТ “Адилет сот”;
* пользователь, получивший временную учетную запись, информируется об ограничениях, связанных с ее использованием.

1. **БЕЗОПАСНОСТЬ СЛУЖЕБНЫХ И ПРИВИЛЕГИРОВАННЫХ УЧЕТНЫХ ЗАПИСЕЙ**
   1. К служебным учетным записям относятся учетные записи, используемые отделами либо техническим персоналом автоматизированных систем для доступа к ресурсам, необходимым для выполнения их функций. К привилегированным учетным записям относятся учетные записи, используемые для управления работой автоматизированных систем.
   2. При использовании привилегированных учетных записей (администратора) необходимо руководствоваться принципом «минимальных привилегий», т.е. привилегии администратора должны использоваться только администратором и только если выполняемая задача требует наличия таких привилегий.
   3. Использование привилегированных учетных записей в повседневной работе, не связанной с необходимостью их использования (установка, конфигурирование, восстановление и т.п. операционной системы и сервисов) недопустимо, в случае необходимости запуска программы с правами Администратора пользователь обязан использовать команду «Run As..» либо «вторичный вход в систему».
   4. Учетная запись администратора домена должна использоваться только при установке, конфигурировании, восстановлении контроллера домена и иных действиях, при которых использование других учетных записей невозможно. Для этой учетной записи необходимо подробное протоколирование всех событий ее использования, а также немедленное расследование любого нецелевого ее использования;
   5. Использование принципа «минимальных привилегий» необходимо для служб и сервисов, выполняющихся на серверах, т.е. службы и сервисы должны работать с минимально возможными для их корректной работы привилегиями исходя из следующей иерархии:

* Локальная служба.
* сетевая служба.
* уникальная учетная запись локального пользователя.
* уникальная учетная запись пользователя домена.
* локальная система
* учетная запись локального администратора.
* учетная запись администратора домена.
  1. К серверам высокой степени безопасности (контроллеры домена, серверы баз данных, иные серверы, от которых зависит бесперебойная работа автоматизированных систем) необходимо предъявлять повышенные требования к минимизации привилегий доступа со стороны как удаленных, так и локальных пользователей и служб.
  2. В случае компрометации, либо подозрении на компрометацию привилегированной учетной записи необходима внеплановая смена паролей всех зависящих от нее учетных записей.

1. **АППАРАТНЫЕ СРЕДСТВА АУТЕНТИФИКАЦИИ**
   1. Для повышения степени защиты критически важных объектов (рабочие станции и мобильные компьютеры с информацией высокой степени конфиденциальности, иные объекты) от несанкционированного доступа необходимо использование двухфакторной аутентификации (по паролю и предмету – далее ключевой носитель информации).
   2. Каждому пользователю, для которого предусмотрена двухфакторная аутентификация, выдается персональный ключевой носитель информации, который учитывается УИТ “Адилет сот” установленным образом (однозначное сопоставление ключевого носителя и его владельца).
   3. Ключевые носители информации маркируются УИТ “Адилет сот” установленным образом (уникальный номер ключевого носителя).
   4. В случае прекращения необходимости использования персонального ключевого носителя (увольнение пользователя, прекращение функционирования объекта, для аутентификации на котором носитель использовался и т.п.) информация с данного носителя стирается установленным образом, либо уничтожается сам носитель в случае невозможности его очистки.
   5. Пользователям категорически запрещается оставлять без личного присмотра, а также передавать другим лицам персональные ключевые носители, сообщать коды от персонального ключевого носителя, если таковые имеются.
   6. В случае утраты персонального ключевого носителя пользователь обязан немедленно сообщить об инциденте руководителю своего подразделения/отдела и управляющему УИТ “Адилет сот”. При возникновении подобного инцидента необходимо незамедлительно принять меры для недопущения несанкционированного использования утраченного персонального ключевого носителя.
2. **КОНТРОЛЬ**
   1. Повседневный контроль над соблюдением требований данного Положения заключается в контроле процессов использования и изменения учетных записей, процессов доступа к ресурсам, процессов изменения учетных записей и предоставления доступа к ресурсам автоматизированных систем УИТ “Адилет сот”.
   2. УИТ “Адилет сот” проводит ежеквартальный выборочный контроль выполнения сотрудниками Судебной системы требований Положения. О фактах несоответствия качества паролей или условий обеспечения их сохранности специалисты УИТ “Адилет сот” сообщают управляющему УИТ “Адилет сот” в форме служебной записки.
   3. Контроль за выполнением требований данного Положения возлагается на УИТ “Адилет сот”.
3. **ОТВЕТСТВЕННОСТЬ**
   1. Пользователи автоматизированных систем несут персональную ответственность за несоблюдение требований по парольной защите;
   2. Специалисты УИТ “Адилет сот” несут ответственность за компрометацию и нецелевое использование привилегированных учетных записей.

Форма ответственности определяются в соответствии с нормативно-законодательными актами КР.

Приложение № 9

к приказу №\_\_\_\_\_

от «\_\_\_\_» \_\_\_\_\_\_\_\_2018г.

**Положение** **о резервном копировании в Судебной системе**

1. **Общие положения**
   1. Настоящее Положение разработано во исполнение Концепции информационной безопасности Судебной системы и другими нормативными правовыми актами и устанавливает порядок проведения резервного копирования данных в Судебной системе.
   2. Целью резервного копирования является предотвращение потери информации при сбоях оборудования, программного обеспечения, в критических и кризисных ситуациях и т.д.
   3. Резервному копированию подлежит информация следующих основных категорий:

* Персональная информация пользователей (личные каталоги на файловых серверах);
* Групповая информация пользователей (общие каталоги подразделений/отделов);
* Информация, необходимая для восстановления серверов и систем управления базами данных (далее – СУБД);
* Персональные профили пользователей сети;
* Информация автоматизированных систем, в т.ч. баз данных;
* Данные справочно-информационных систем общего использования;
* Рабочие копии установочных компонент программного обеспечения рабочих станций;
* Данные с рабочих станций, содержащих критически важную информацию.

1. **Основные термины, сокращения и определения**

АС – автоматизированная система Организации – система, обеспечивающая хранение, обработку, преобразование и передачу информации Организации с использованием компьютерной и другой техники.

Резервное копирование – это сохранение очередного текущего состояния информации (системы) без обязательного сохранения предыдущего.

Полное копирование - создание полной копии (одна копия);

Инкрементальное копирование - создание копий измененных данных, которые были изменены после последнего полного, инкрементального или дифференциального копирования (несколько копий, первая запись – это полная копия, вторая запись – копия только тех данных, которые были изменены со времени первой записи, а на третьем этапе копируются данные модифицированные со времени второго этапа и т.д.);

Дифференциальное копирование - создание последней копии измененных данных со времени проведения полного копирования (две копии, первая запись – это полная копия, а на последующих этапах копируются только данные, которые изменились со времени проведения полного копирования).

Архивирование – долгосрочное хранение информации, либо состояния системы.

Система резервного копирования – подсистема АС Организации, которая предназначена для создания резервных копий и восстановления данных.

Ресурс сервера (далее Ресурс) – это каталог, файл с данными, программное обеспечение или сервис на сервере.

1. **Организация резервного копирования**
   1. Для обеспечения резервного копирования, восстановления и архивного хранения электронных данных приказом назначается ответственный за резервное копирование. Ответственный за резервное копирование в своей работе руководствуются настоящим Положением, нормативными актами по защите информации, техническими инструкциями на серверное оборудование, систему хранения данных и другими документами.
   2. Инструктивно-методическое руководство деятельностью ответственного за резервное копирование осуществляется УИТ “Адилет сот”.
   3. Основными задачами ответственного за резервное копирование являются:

* Планирование резервного копирования и восстановления;
* Установление жизненного цикла и календаря операций;
* Ежедневный обзор логов процесса резервного копирования;
* Защита данных резервного копирования от повреждения, модификации и несанкционированного доступа;
* Развитие системы резервного копирования;

К ежедневным задачам ответственного за резервное копирование относятся:

* мониторинг заданий;
* отчеты о сбоях и успешном выполнении;
* анализ и разрешение проблем;
* манипуляции с резервными копиями;
* расписание выполнения заданий.

К еженедельным, ежемесячным и другим задачам ответственного за резервное копирование относятся:

* анализ производительности;
* тенденции изменения объемов и планирование этих изменений;
* рассмотрение и анализ методики резервного копирования;
* проверку возможности восстановления;
* планирование развития архитектуры, определение ежедневных, еженедельных и ежемесячных заданий.

3.4. Основные обязанности ответственного за резервное копирование:

* Обеспечить функционирование и поддержание работоспособности средств системы резервного копирования информации;
* Немедленно докладывать управляющему УИТ “Адилет сот” о выявленных ошибках и сбоях при резервном копировании информации, а также принимать необходимые меры по их устранению;
* Обеспечить целостность и сохранность резервных копий информации.

3.5. Права ответственного за резервное копирование:

* Требовать от пользователей автоматизированных систем Судебной системы безусловного соблюдения установленной технологии и выполнения инструкций по обеспечению резервного копирования и восстановления информации;
* Вносить предложения и требовать прекращения обработки информации в случаях нарушения установленной технологии резервного копирования информации или нарушения функционирования средств системы резервного копирования;

3.6. На ответственного за резервное копирование возлагается персональная ответственность за качество проводимых им работ по обеспечению резервного копирования и восстановления информации в соответствии с функциональными обязанностями, определенными в настоящем Положении.

**4. Порядок резервного копирования**

4.1. В Судебной системе должна быть реализована централизованная система резервного копирования, что позволит сократить совокупную стоимость владения ИТ-инфраструктурой за счет оптимального использования устройств резервного копирования и сокращения расходов на администрирование по сравнению с децентрализованной системой.

4.2. Ответственный за организацию резервного копирования в организации на основании п. 1.3. настоящего Положения и Перечня информационных ресурсов Судебной системы готовит Перечень данных¸ подлежащих резервному копированию и хранению (далее – перечень) по установленной форме (Приложение 9).

4.3. Система резервного копирования должна обеспечивать производительность, достаточную для сохранения информации, указанной в Перечне, в установленные сроки и с заданной периодичностью. Расписание проведения резервного копирования описано в Приложении 10.

4.4. О выявленных попытках несанкционированного доступа к резервируемой информации, а также иных нарушениях информационной безопасности, произошедших в процессе резервного копирования, сообщается управляющему УИТ “Адилет сот”.

**5. Контроль результатов**

5.1. Контроль результатов всех процедур резервного копирования осуществляется ответственным за резервное копирование в срок до 17 часов рабочего дня, следующего за установленной датой выполнения этих процедур.

5.2. В случае обнаружения ошибки резервного копирования ответственный за резервное копирование выполняет повторное копирование информации вручную в максимально сжатые сроки, не нарушая технологические процессы обработки информации пользователями автоматизированных систем Судебной системы.

**6. Хранение резервных копий**

6.1 Хранение резервных копий данных осуществляется на сменных носителях информации (CD/DVD, внешние жесткие диски и т.п.), промаркированных ответственным за резервное копирование в соответствие с расписанием резервного копирования. Маркировка должна содержать номер копии, дату ее создания, наименование информационной системы данных.

6.2 Использование носителей информации при резервном хранении должно подчиняться принципу ротации носителей, при котором для записи текущей копии используется носитель с самой ранней датой создания предыдущей копии.

6.3. Срок хранения резервных копий определяется в соответствии с нормативно-правовыми актами Судебной системы.

6.4. Хранение резервных копий осуществляется в соответствии с правилами работы с документами, содержащими информацию ограниченного доступа вместе, отличном от места их изготовления.

6.5 Удаление резервных копий для повторного использования носителя информации либо окончательное удаление производится специалистами УИТ “Адилет сот” по согласованию с лицом, ответственным за ведение соответствующего информационного ресурса.

**7. Восстановление данных с резервных копий**

7.1. Восстановление данных с резервных копий производится в соответствие с планом обеспечения непрерывной работы и восстановления работоспособности.

7.2 Основанием для инициирования процедуры восстановления служит полная или частичная утрата информации вследствие сбоев оборудования, программного обеспечения, в критических и кризисных ситуациях. Восстановление данных производится специалистами УИТ “Адилет сот” по заявке руководителя структурного подразделения, утвержденной управляющим УИТ “Адилет сот”.

7.3. Восстановление утраченных данных производится из резервной копии, обеспечивающей минимальную потерю данных, содержащихся в информационном ресурсе.

# 

Приложение № 10

к приказу №\_\_\_\_\_

от «\_\_\_\_» \_\_\_\_\_\_\_\_2018г.

# Положение об антивирусном контроле в Судебной системе

1. **Общие положения**
   1. Настоящее Положение разработано во исполнение Концепции информационной безопасности Судебной системы и устанавливает порядок проведения антивирусного контроля в Судебной системе.
   2. Требования настоящего Положения являются неотъемлемой частью комплекса мер безопасности и защиты информации в Судебной системе.
   3. Требования настоящего Положения распространяются на всех сотрудников Судебной системы, использующих в работе средства вычислительной техники (включая работу в локальной вычислительной сети Судебной системы) и должны применяться для всех средств вычислительной техники, эксплуатируемой в Судебной системе.
   4. Организационное обеспечение мероприятий антивирусного контроля и контроль за действиями пользователей возлагается на УИТ “Адилет сот”.
2. **Основные термины, сокращения и определения**

АС – автоматизированная система Судебной системы – система, обеспечивающая хранение, обработку, преобразование и передачу информации Судебной системы с использованием компьютерной и другой техники.

Компьютерный вирус - это код-сценарий или код-скрипт, способный создавать свои копии (не обязательно полностью совпадающие с оригиналом программы-цели) и внедрять их в различные объекты или ресурсы компьютерных систем, сетей и так далее без ведома пользователя. При этом копии сохраняют способность дальнейшего распространения.

Зараженная программа - это программа, содержащая внедренный в нее вредоносный код.

1. **Организация системы антивирусного контроля**
   1. Целью мероприятий по антивирусному контролю является предотвращение потерь информации в АС.
   2. Задачами антивирусной защиты являются:

* определение состава и регламента запуска антивирусных диагностических средств, регламента их ревизии и обновления;
* проведение профилактических работ с применением антивирусных диагностических средств;
* непрерывное обеспечение защиты информации от действия вредоносных программ на всех этапах эксплуатации АС.
  1. Проведение анализа вирусных угроз, поведения компьютерных вирусов, а также проведение разработки инструкций и методов борьбы осуществляется УИТ “Адилет сот”. Ответственность за антивирусный контроль, как и проведение мероприятий по предотвращению вирусного заражения и борьбы с зараженными программами осуществляется сотрудниками УИТ “Адилет сот”.
  2. К использованию в Судебной системе допускаются только лицензионные антивирусные средства, централизованно закупленные Судебным департаментом у разработчиков (поставщиков) указанных средств.
  3. Установка средств антивирусной защиты и настройка их параметров в соответствии с руководствами по применению конкретных антивирусных средств на компьютерах в Судебной системе осуществляется сотрудниками УИТ “Адилет сот”.
  4. Проверка наличия обновлений антивирусных баз должно производиться не реже 1 раза в сутки автоматически, согласно возможностям программного обеспечения. В случае сбоя автоматического обновления обновление баз производится вручную с той же периодичностью.
  5. Обязательному входному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам связи, а также информация на съемных носителях и мобильных устройствах.
  6. Файлы резервных копий, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в месяц.
  7. Мероприятия по антивирусной защите на компьютерах в Судебной системе включают в себя:
* профилактика вирусного заражения;
* анализ ситуаций;
* применение средств антивирусной защиты;
* проведение расследований инцидентов связанных с вирусами.

1. **Профилактика вирусного заражения**
   1. В целях исключения появления и распространения вирусов на рабочих станциях АС должны регулярно проводится профилактические мероприятия. К основным профилактическим работам и мероприятиям относятся:

* ежедневная автоматическая проверка наличия вирусов по расписанию;
* регулярная (не реже одного раза в квартал) выборочная проверка рабочих станций и серверов на наличие вирусов, даже при отсутствии внешних проявлений вирусов;
* проверка наличия вирусов на рабочих станциях, вернувшихся с ремонта (в том числе гарантийного) в сторонних организациях;
* создание резервной копии программного продукта сразу же после приобретения;
* установка защиты от записи на съемные носители информации, где это возможно;
* тщательная проверка всех поступающих и купленных программ и баз данных;
* ограничение доступа к компьютеру посторонних лиц.
  1. Создание резервной копии программного продукта, профилактические работы и мероприятия выполняются специалистами УИТ “Адилет сот”.
  2. При обнаружении вирусов на компьютере, работающем в локальной сети, проверке подлежат все компьютеры, включенные в эту сеть и работающие с общими данными и программным обеспечением.

1. **Анализ ситуаций**
   1. При сообщении антивирусных программы о подозрении на наличие вирусов на рабочей станции, необходимо приостановить работу и немедленно известить об этом IT-консультанта при наличии данного сотрудника в штате субъекта Судебной системы, либо к специалисту УИТ “Адилет сот”, а также других пользователей и подразделения, использующие эти файлы в работе, если зараженные файлы являются совместно используемыми.
   2. Анализ ситуации наличия вирусов выполняется сотрудниками УИТ “Адилет сот”. При анализе могут дополнительно использоваться специальное программное обеспечение для обнаружения вирусов.
   3. В ходе анализа ситуации обязательно требуется определить источник заражения. Если источником заражения является съемный носитель либо другая рабочая станция Судебной системы, то необходимо проверить на наличие вирусов рабочую станцию - источник заражения. В случае заражения через глобальную сеть Интернет или по электронной почте следует немедленно заблокировать ресурс или адрес электронной почты – источник заражения.
   4. В случае обнаружения вирусного заражения расследование допущенных нарушений производится специалистами УИТ “Адилет сот” на основании Регламента реагирования на инциденты информационной безопасности, утвержденного в Судебной системе.
2. **Применение средств антивирусной защиты**
   1. Уничтожение вирусов выполняется сотрудниками УИТ “Адилет сот”.
   2. После уничтожения вирусов и восстановления зараженных программ и файлов с данными необходимо еще раз выполнить проверку наличия вирусов, используя антивирусные программы.
   3. В случае обнаружения, не поддающегося лечению применяемыми антивирусными средствами, ответственный за антивирусный контроль должен направить зараженный вирусом файл в организацию, с которой заключен договор на антивирусную поддержку.
3. **Ответственность**
   1. Ответственность за выполнение мероприятий по антивирусной защите информации на средствах вычислительной техники, эксплуатируемых сотрудниками Судебной системе в соответствии с требованиями настоящего Положения, возлагается на УИТ “Адилет сот”.
   2. Ответственность за выполнение мероприятий по антивирусной защите информации на средствах вычислительной техники на рабочем месте в соответствии с требованиями настоящего Положения, возлагается на пользователя средств вычислительной техники.
   3. Ответственность за проведение профилактических мероприятий по обеспечению антивирусной защиты в АС, а также уничтожение выявленных вирусов возлагается на УИТ “Адилет сот”.
   4. Периодический контроль за состоянием антивирусной защиты в АС, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящего Положения сотрудниками подразделений Судебной системы осуществляется УИТ “Адилет сот”.
   5. Сотрудники Судебной системы, нарушившие требования настоящего документа, привлекаются к ответственности в соответствии с действующим законодательством Кыргызской Республики.

**Инструкция пользователя по антивирусной защите**

Характерные проявления вирусов

При заражении компьютера вирусом важно его обнаружить. Для этого следует знать об основных признаках проявления вирусов. К ним можно отнести следующие:

* прекращение работы или неправильная работа ранее успешно функционировавших программ;
* медленная работа компьютера;
* невозможность загрузки операционной системы;
* исчезновение файлов и каталогов или искажение их содержимого;
* изменение даты и времени модификации файлов;
* изменение размеров файлов;
* неожиданное значительное увеличение количества файлов на диске;
* существенное уменьшение размера свободной оперативной памяти;
* вывод на экран непредусмотренных сообщений или изображений;
* подача непредусмотренных звуковых сигналов;
* частые зависания и сбои в работе компьютера.

Основные источники вирусов:

* съемный носитель (дискета, флеш-карта, CD-ROM, DVD-ROM, мобильное дисковое устройство) на котором находятся зараженные вирусом файлы;
* компьютерная сеть, особенно беспроводная сеть, в том числе система электронной почты и Интернет;
* жесткий диск, на который попал вирус в результате работы с зараженными программами.

Пользователь обязан:

* ежедневно при начальной загрузке рабочей станции убедиться в загрузке антивирусного программного обеспечения и в случае его отсутствия уведомить штатного сотрудника ответственного за сопровождение АС, либо сотрудников УИТ “Адилет сот”;
* Сотрудник обязан проводить антивирусный контроль всех внешних носителей информации (дискет, компакт-дисков, магнитооптических дисков и т.п.), поступающих со стороны (из внешних организаций, других субъектов Судебной системы и т.п.) или полученных по компьютерным сетям (скопированных на общедоступный ресурс локального компьютера другими пользователями). Если антивирусная программа не работает в фоновом режиме, самому проводить проверку всех этих файлов или обращаться для этого к специалистам УИТ “Адилет сот”;
* Во всех случаях возможного проявления действия вирусов, обнаружения файлов, пораженных вирусом или подозрении на наличие вируса сотрудник должен:
* без попытки какого-либо лечения незамедлительно сообщить об этом штатному сотруднику ответственного за сопровождение АС, либо сотрудников УИТ “Адилет сот” и вместе оценить возможные пути заражения и распространения данного вируса;
* совместно провести лечебно-восстановительные мероприятия.
* Сотрудник обязан делать резервные копии файлов, содержащих ценную служебную информацию, если эти файлы не размещены в сетевых папках на серверах Судебной системы;
* Сотрудник не должен самостоятельно устанавливать программное обеспечение, если это не входит в его обязанности. Запрещается устанавливать и запускать нелицензионное или не относящееся к выполнению им своих должностных обязанностей программное обеспечение;
* КАТЕГОРИЧЕСКИ ЗАПРЕЩЕНО использование съёмных носителей, принадлежащих лицам, временно допущенным к работе на компьютере в Судебной системе (студенты-практиканты, временно замещающие, сотрудники сторонних организаций и т.п.).

Пользователю запрещается:

* изменять настройки и конфигурацию средств антивирусной защиты;
* удалять или добавлять в систему какие-либо другие средства антивирусной защиты.

# 

Приложение № 11

к приказу №\_\_\_\_\_

от «\_\_\_\_» \_\_\_\_\_\_\_\_2018г.

# Положение об использовании мобильных устройств и носителей конфиденциальной информации (персональных данных) Судебной системы

1. **Общие положения**
   1. Настоящее Положение разработано во исполнение Концепции информационной безопасности Судебной системы и устанавливает порядок использования мобильных устройств и носителей информации, предоставляемых Судебной системой для использования в автоматизированных системах Судебной системы.
   2. Требования настоящего Положения являются неотъемлемой частью комплекса мер безопасности и защиты информации в Судебной системе.
   3. Требования настоящего Положения распространяются на всех работников подразделений, использующих в работе средства вычислительной техники и должны применяться для всех средств вычислительной техники, эксплуатируемой в Судебной системе.
2. **Основные термины, сокращения и определения**

АС – автоматизированная система Судебной системы – система, обеспечивающая хранение, обработку, преобразование и передачу информации с использованием компьютерной и другой техники.

АРМ – автоматизированное рабочее место пользователя (персональный компьютер с прикладным программным обеспечением) для выполнения определенной производственной задачи.

Администратор ИБ – должностное лицо Судебной системы, осуществляющее комплекс организационно-технических мероприятий, обеспечивающих конфиденциальность, целостность и доступность информации.

Мобильное устройство – переносное электронно-вычислительное устройство, способное принимать, отображать, хранить, обрабатывать и передавать информацию.

Носитель информации – любой материальный объект, используемый для хранения и передачи электронной информации.

Паспорт ПК – документ, содержащий полный перечень оборудования и программного обеспечения АРМ.

ПК – персональный компьютер.

ПО – Программное обеспечение вычислительной техники.

ПО вредоносное – ПО или изменения в ПО, приводящие к нарушению конфиденциальности, целостности и доступности критичной информации.

ПО коммерческое – ПО сторонних производителей (правообладателей). Предоставляется в пользование на возмездной (платной) основе.

Пользователь – сотрудник Судебной системы, использующий мобильные устройства и носители информации для выполнения своих служебных обязанностей.

Перечень – документ «Перечень разрешенного к использованию ПО». Содержит перечень коммерческого свободно распространяемого ПО, разрешенного к использованию в Судебной системе.

**3. Порядок использования мобильных устройств и носителей информации**

3.1. Под использованием мобильных устройств и носителей информации в АС Судебной системе понимается их подключение к инфраструктуре АС с целью обработки, приема/передачи информации между АС и мобильными устройствами, а также носителями информации.

3.2. В АС допускается использование только учтенных мобильных устройств и носителей информации, которые являются собственностью Судебной системы и подвергаются регулярной ревизии и контролю.

3.3. На предоставленных мобильных устройствах допускается использование коммерческого и свободно распространяемого ПО, по согласования с УИТ “Адилет сот”.

3.4. К предоставленным мобильным устройствам и носителям информации предъявляются те же требования по защите информации, что и для стационарных АРМ

3.5. Мобильные устройства и носители информации предоставляются сотрудникам Судебной системы по инициативе руководителей структурных подразделений или отделов в случаях:

* необходимости выполнения работником своих должностных обязанностей;
* возникновения у сотрудника Судебной системы производственной необходимости.

3.6. Процесс предоставления сотруднику Судебной системы мобильных устройств и носителей информации состоит из следующих этапов:

3.6.1. Подготовка заявки (Приложение 11) в утвержденной форме, осуществляется Руководителем структурного подразделения или отдела на имя директора Судебного департамента при ВС КР.

3.6.2. Согласование подготовленной заявки (для получения заключения о возможности предоставления сотруднику Судебной системы заявленного мобильного устройства или носителя информации) со специалистами УИТ “Адилет сот”.

3.6.3. Передача заявки в УИТ “Адилет сот” для учета предоставленного мобильного устройства или носителя информации и внесения изменений в «Список сотрудников Судебной системы, имеющих право работы с мобильными устройствами вне территории объектов Судебной системы, а также выполнения технических настроек по регистрации мобильного устройства в АС или предоставлению права использования носителей информации на АРМах Судебной системы.

3.8. При использовании предоставленных сотрудникам Судебной системы мобильных устройств и носителей информации необходимо:

3.8.1. Соблюдать требования настоящего Положения.

3.8.2. Использовать мобильные устройства и носители информации исключительно для выполнения своих служебных обязанностей.

3.8.3. Ставить в известность специалиста информационной безопасности о любых фактах нарушения требований настоящего Положения.

3.8.4. Эксплуатировать и транспортировать мобильные устройства и носители информации в соответствии с требованиями производителей.

3.8.5. Обеспечивать физическую безопасность мобильных устройств и носителей информации всеми разумными способами.

3.8.7. Извещать УИТ “Адилет сот” о фактах утраты (кражи) мобильных устройств и носителей информации.

3.9. При использовании предоставленных сотрудникам Судебной системы мобильных устройств и носителей информации запрещено:

3.9.1. Использовать мобильные устройства и носители информации в личных целях.

3.9.2. Передавать мобильные устройства и носители информации другим лицам (за исключением сотрудников УИТ “Адилет сот”).

3.9.3. Оставлять мобильные устройства и носители информации без присмотра, если не предприняты действия по обеспечению их физической безопасности.

3.10. Любое взаимодействие (обработка, прием/передача информации) инициированное сотрудником Судебной системы между АС и неучтенными (личными) мобильными устройствами, а также носителями информации, рассматривается как несанкционированное (за исключением случаев, оговоренных со специалистом УИТ “Адилет сот” заранее). Специалисты УИТ “Адилет сот” оставляют за собой право блокировать или ограничивать использование таких устройств и носителей информации в случаях возникновения угроз информационной безопасности.

3.11. Информация об использовании сотрудниками Судебной системы мобильных устройств и носителей информации в АС протоколируется и, при необходимости, может быть предоставлена Руководителям структурных подразделений, отделов, а также директору Судебного департамента при ВС КР (Приложение 12).

3.12. При подозрении сотрудника Судебной системы в несанкционированном или нецелевом использовании мобильных устройств и носителей информации инициализируется расследование допущенных нарушений, производимое УИТ “Адилет сот” на основании Регламента реагирования на инциденты информационной безопасности.

3.13. Информация, хранящаяся на предоставляемых мобильных устройствах и носителях информации, подлежит обязательной проверке на отсутствие вредоносного ПО.

3.14. Съемные носители конфиденциальной информации (персональных данных), пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению. По результатам уничтожения носителей составляется акт по прилагаемой форме

3.15. В случае увольнения или перевода сотрудника в другое структурное подразделение Судебной системы, предоставленные ему мобильные устройства и носители информации изымаются.

**4. Ответственность**

4.1. Сотрудники, нарушившие требования настоящего Положения, несут ответственность в соответствии с действующим законодательством и локальными нормативными актами Судебной системы.

# 

Приложение № 12

к приказу №\_\_\_\_\_

от «\_\_\_\_» \_\_\_\_\_\_\_\_2018г.

# Обязанности сотрудников Судебной системы по защите информации

**Председатель суда КР**

Составлять заявки для предоставления доступа к ресурсам сотрудников суда, руководствуясь Перечнем информационных ресурсов.

Инициировать аннулирование доступа пользователя к ресурсам в случае изменения должностных обязанностей пользователя или его увольнения, изменения технологических процессов обработки информации таким образом, что доступ пользователю более не требуется.

Формировать заявки на установку дополнительного программного обеспечения на имя директора Судебного департамента.

Подавать заявки на восстановление данных из резервных копий вследствие полной или частичной утраты информации вследствие сбоев оборудования, программного обеспечения, в критических и кризисных ситуациях.

Согласовывать заявки в утвержденной форме на предоставление мобильных устройств и носителей информации работникам с Судебным департаментом.

Сообщать в УИТ “Адилет сот”, ставшие известными случаи нарушения принятых в Судебной системе нормативных и распорядительных документов по информационной безопасности, критических и кризисных ситуациях, инцидентах информационной безопасности.

Согласовывать с УИТ “Адилет сот” отключение от информационных ресурсов сотрудников на время расследования инцидентов информационной безопасности.

Требовать предоставления объяснительной записки от нарушителя информационной безопасности из числа подчиненных.

Предоставлять по запросам специалистов УИТ “Адилет сот” устные и письменные разъяснения и иную информацию, необходимую для проведения разбирательства инцидента информационной безопасности.

**Сотрудники и специалисты Судебной системы**

Подавать заявки на восстановление данных из резервных копий вследствие полной или частичной утраты информации вследствие сбоев оборудования, программного обеспечения, в критических и кризисных ситуациях.

Согласовывать заявки в утвержденной форме на предоставление мобильных устройств и носителей информации работникам с Судебным департаментом.

**Начальники отделов Судебного департамента КР**

Составлять заявки для предоставления доступа к ресурсам сотрудникам отдела, руководствуясь перечнем информационных ресурсов.

Инициировать аннулирование доступа пользователя к ресурсам в случае изменения должностных обязанностей пользователя или его увольнения, изменения технологических процессов обработки информации таким образом, что доступ пользователю более не требуется.

Формировать заявки на установку дополнительного программного обеспечения на имя управляющего УИТ “Адилет сот”.

Определять срок хранения резервных копий данных, возможность их удаления в пределах своей компетенции.

Подавать заявки на восстановление данных из резервных копий вследствие полной или частичной утраты информации вследствие сбоев оборудования, программного обеспечения, в критических и кризисных ситуациях.

Согласовывать заявки в утвержденной форме на предоставление мобильных устройств и носителей информации работникам Судебной системы.

Сообщать в УИТ “Адилет сот”, ставшие известными случаи нарушения принятых в Судебной системе нормативных и распорядительных документов по информационной безопасности, критических и кризисных ситуациях, инцидентах информационной безопасности.

Требовать предоставления объяснительной записки от нарушителя информационной безопасности из числа подчиненных.

Предоставлять по запросам специалистов УИТ “Адилет сот” устные и письменные разъяснения и иную информацию в рамках своей компетенции, необходимую для проведения разбирательства инцидента информационной безопасности.

**Сотрудники и специалисты Судебного департамента КР**

Подавать заявки на восстановление данных из резервных копий вследствие полной или частичной утраты информации вследствие сбоев оборудования, программного обеспечения, в критических и кризисных ситуациях.

**Руководители подразделений Судебной системы**

Составлять заявки для предоставления доступа к ресурсам сотрудникам подразделения, руководствуясь перечнем информационных ресурсов.

Инициировать аннулирование доступа пользователя к ресурсам в случае изменения должностных обязанностей пользователя или его увольнения, изменения технологических процессов обработки информации таким образом, что доступ пользователю более не требуется.

Формировать заявки на установку дополнительного программного обеспечения на имя управляющего УИТ “Адилет сот”.

Подавать заявки на восстановление данных из резервных копий вследствие полной или частичной утраты информации вследствие сбоев оборудования, программного обеспечения, в критических и кризисных ситуациях.

Согласовывать заявки в утвержденной форме на предоставление мобильных устройств и носителей информации работникам с Судебным департаментом.

Сообщать в Судебный департамент, ставшие известными случаи нарушения принятых в Судебной системе нормативных и распорядительных документов по информационной безопасности, критических и кризисных ситуациях, инцидентах информационной безопасности.

Согласовывать с УИТ “Адилет сот” отключение от информационных ресурсов сотрудников на время расследования инцидентов информационной безопасности.

Требовать предоставления объяснительной записки от нарушителя информационной безопасности из числа подчиненных.

Предоставлять по запросам специалистов УИТ “Адилет сот” устные и письменные разъяснения и иную информацию в рамках своей компетенции, необходимую для проведения разбирательства инцидента информационной безопасности.

Приложение № 13

к приказу №\_\_\_\_\_

от «\_\_\_\_» \_\_\_\_\_\_\_\_2018г.

# Регламент «Иформационной безопасности в Судебной системе»

**Общие положения**

Регламент по обеспечению информационной безопасности (далее – регламент) разработан в соответствии с Государственной целевой программой «Развитие судебной системы КР на 2014-2017 годы», а также в соответствии с постановлением Правительства КР “О проекте Концепции информационной безопасности Кыргызской Республики”.

Регламент устанавливает основные требования для обеспечения конфиденциальности персональных судебных данных в процессах электронного судопроизводства, разграничению прав доступа к электронным информационным ресурсам, содержащим персональные данные, а также порядок работы и взаимодействия ответственных лиц по защите информации.

Настоящий регламент определяет требования к предоставлению доступа к информационным системам электронного судопроизводства, устанавливает ответственность пользователей, системных администраторов и лиц, ответственных за информационную безопасность, по исполнению и контролю указанных мероприятий.

Настоящий регламент определяет требования для выполнения процедур по предоставлению и прекращению доступа к информационным системам электронного судопроизводства.

**Разграничение полномочий в сети**

Пользователи сети Судебной системы в соответствии со своими полномочиями разделяются на 3 группы.

Внешние пользователи – пользователи, не зарегистрированные ни на одном сетевом узле и имеющие доступ только к открытой информации, либо пользователи имеющие временный доступ к сетевым ресурсам с ограниченной функциональностью.

Пользователи-специалисты судебного департамента – пользователи, зарегистрированные на одном или нескольких сетевых узлах и имеющие доступ к ключевой информации сетевого узла.

Пользователи-специалисты УИТ “Адилет сот” – пользователи, имеющие ограниченный доступ к программному или функциональному обеспечению серверов или специализированных сетевых узлов.

Пользователи-специалисты УИТ “Адилет сот” – пользователи сети, обладающие неограниченным доступом к серверам или специализированным сетевым узлам. Для обеспечения безопасной эксплуатации сети данные пользователи должны выполнять следующие функции:

* осуществлять контроль и нести ответственность за соблюдение правил безопасной эксплуатации сети или группы подчиненных ему сетевых узлах;
* осуществлять настройку сети и прикладного программного обеспечения;
* осуществлять контроль за попытками несанкционированного изменения режима безопасности;
* осуществлять контроль за соблюдением правил эксплуатации и соблюдением мер защиты от несанкционированного доступа;
* контролировать попытки несанкционированного доступа к программному обеспечению, попытки сетевых атак и проявления сетевой активности приложений.

Для обеспечения своих функций специалист УИТ “Адилет сот” должен:

* иметь связь со всеми подконтрольными ему сетвыми узлами сети;
* иметь возможность входа в сеть Судебной системы с правами администратора.

**Регистрация пользователей в сетевых узлах**

Регистрацию пользователей и сетевых узлов в сети осуществляют специалисты УИТ “Адилет сот”, с использованием специализированных инструментов в операционных системах.

При регистрации сетевых узлов администратор руководствуется следующими правилами:

* сетевые узлы регистрируется только в тех прикладных задачах, которые необходимы пользователям данных сетевых узлов для выполнения своих задач;
* связи сетевых узлов задаются согласно требованиям прикладной задачи;

**Режимы безопасности в сети**

Для безопасной работы Судебной системы существуют следующие режимы безопасности обработки трафика:

1. блокировать IP-пакеты всех внешних соединений;
2. блокировать все соединения, кроме разрешенных;
3. пропускать все исходящие соединения, кроме запрещенных;
4. пропускать все соединения;
5. пропускать IP-пакеты без обработки.

Режимы работы 1, 2 предусмотрены при возникновении угроз целостности персональных данных Судебной системы для определенных на момент времени ресурсов.

При выборе 2 режима безопасности перечень открытых адресов, направлений соединений, допустимых протоколов и портов в фильтрах открытой сети, регистрируемый для конкретных групп сетевых узлов, определяется по согласованию с управляющим УИТ ”Адилет сот”.

Режимы 3, 4 предусмотрены для работы сетевых узлов Судебной системы, при которых целостность рабочих моментов не нарушается.

При необходимости использования 3 режима безопасности специалисты УИТ ”Адилет сот” обязаны:

* определить, при необходимости, перечень открытых адресов, протоколов и портов, запрещенных к использованию при инициативных соединениях для конкретных групп сетевых узлов;
* обеспечить соответствующие настройки фильтров открытой сети, блокирующие открытые инициативные соединения с запрещенными адресами;
* осуществлять периодический контроль IP-трафика сетевых узлов.

Режим 5 предназначен для проведения тестирования и настроек [локальной вычислительной сет](https://ru.wikipedia.org/wiki/%D0%9B%D0%BE%D0%BA%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D0%B2%D1%8B%D1%87%D0%B8%D1%81%D0%BB%D0%B8%D1%82%D0%B5%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D1%81%D0%B5%D1%82%D1%8C)и, требующий исключение влияния на рабочие процессы сотрудников Судебной системы.

Контроль трафика осуществляется специалистами УИТ ”Адилет сот” путем удаленного запроса журналов IP-пакетов. При выявлении установленных соединений с потенциально опасными открытыми сетевыми ресурсами или изменении списка запрещенных адресов и протоколов, специалисты осуществляют дополнительную настройку фильтров открытой

сети или принимают решение об изменении режима безопасности для сетевых узлов.

**Установка и ввод в эксплуатацию сетевых узлов**

При размещении технических средств следует руководствоваться следующими рекомендациями.

1. Размещение, охрана и специальное оборудование помещений, в которых установлены технические средства и ведется работа с носителями персональной ключевой информации, должны исключать возможность бесконтрольного проникновения в них посторонних лиц, прослушивания ведущихся там переговоров и просмотра помещений посторонними лицами, а также гарантировать сохранность находящихся в этих помещениях конфиденциальных документов.
2. Оборудование помещений средствами вентиляции и кондиционирования

воздуха должно соответствовать санитарно-гигиеническими нормам СНиП.

1. При подключении средств криптографической защиты информации к каналам передачи данных, выходящих за пределы контролируемой зоны, необходимо выполнение мероприятияй по защите информации от утечки по техническим каналам, в том числе по каналу связи.
2. Помещения, в которых устанавливаются компоненты аппаратная часть сетевых узлов относится к защищаемым помещениям, обеспечивающим конфиденциальность проводимых работ и исключающим возможность бесконтрольного нахождения в нем посторонних лиц.
3. Входные двери помещений должны быть оборудованы внутренними замками, гарантирующими надежное закрытие дверей при выходе из помещения и в нерабочее время. Окна (при необходимости) и двери должны быть оборудованы охранной сигнализацией, связанной с центральным пультом наблюдения за сигнализацией поста охраны.
4. В помещение допускаются только сотрудники, имеющие непосредственное отношение к организации эксплуатации сетевого оборудования.
5. Уборка помещения, обслуживание оборудования систем жизнеобеспечения осуществляется назначенным персоналом при выключенных мониторах в присутствии администратора.
6. Должны быть приняты меры по надежному сохранению в тайне паролей доступа, ключевых дистрибутивов и другой ключевой информации, размещенной на съемных носителях. Для хранения съемных носителей помещение должно быть оборудовано сейфом.
7. По окончании рабочего дня, помещения закрываются. Порядок сдачи помещений определяется ответственным подразделением/отделом Судебной системы.

При эксплуатации оборудования следует руководствоваться следующими рекомендациями.

* исключить из состава системы все оборудование, которое может создавать угрозу безопасности;
* каждый пользователь должен иметь для входа в ОС свою учетную запись;
* длина пароля учетной записи должна быть не менее 10 символов;
* запретить пользователям, не входящим в группу администраторов, осуществлять установку и модификацию прикладного и системного программного обеспечения;
* установить права доступа к каталогам установки программного обеспечения и другим каталогам компьютера для каждой учетной записи в соответствии с полномочиями пользователя в объеме, необходимом для выполнения его обязанностей;
* отключить учетную запись для гостевого входа (Guest);

***OC Windows***

* удалить у группы Everyone все привилегии;
* ограничить права пользователей, не входящих в группу администраторов безопасности, на запись в системный реестр, что реализуется при помощи ACL или установкой прав доступа;
* ограничить использование Scheduler;
* устанавливать атрибуты SECURITY\_ATTRIBUTES процессов и потоков в соответствии с требованиями безопасности всей системы в целом;
* для предотвращения стороннего анализа остаточной информации желательно использовать дополнительные ограничения по доступу к временным файлам;
* отказаться от использования режима автоматического входа пользователя при ее загрузке;
* исключить возможность удаленного редактирования системного реестра;
* включать фильтры паролей, устанавливаемые вместе с пакетами обновлений операционной системы;
* ограничить доступ пользователей в каталог %SystemRoot%;
* установить права доступа к каталогам %Systemroot%\System32\Config, %Systemroot%\System32\SPOOL, %Systemroot%\Repair, %Systemroot%\COOKIES, %Systemroot%\FORMS, %Systemroot%\HISTORY, %Systemroot%\SENDTO, %Systemroot%\PROFILES, %Systemroot%\OCCACHE, \TEMP, а также файлам boot.ini, autoexec.bat, config.sys, ntdetect.com и ntldr в соответствии с политикой безопасности;
* после установки операционной системы удалить изкаталога %Systemroot%\System32\Config файл sam.sav;
* использовать систему аудита в соответствии с политикой безопасности;
* в ключе HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\Lsa установить параметр RestrictAnonymous (REG\_DWORD) со значением 1 для исключения доступа анонимного пользователя к списку разделяемых ресурсов, а также для исключения доступа к содержимому системного реестра;
* удалить имя SPOOLSS из ключа HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\NullSessionPipes для исключения утечки информации при передаче данных по именованному каналу [\\server\PIPE\SPOOLSS;](file:///\\server\PIPE\SPOOLSS;)
* в ключе HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters установить параметры AutoShareWks (для Windows NT Workstation) и AutoShareServer (для Windows NT Server), имеющие тип REG\_DWORD, со значением 0 для запрета автоматического создания скрытых совместных ресурсов;
* в ключе HKEY\_LOCAL\_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon установить параметр CachedLogonsCount (REG\_DWORD) со значением 0 для отключения кэширования паролей последних десяти пользователей, вошедших в систему;
* в ключе HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\Eventlog\<LogName> (LogName – имя журнала, для которого следует ограничить доступ пользователям группы Everyone) установить параметр RestrictedGuestAccess (REG\_DWORD) со значением 1 для исключения доступа группы Everyone к системному журналу и журналу приложений;
* в ключе HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\ установить SessionManager\MemoryManagement параметр ClearPageFileAtShutDown (REG\_DWORD) со значением 1 для включения механизма затирания файла подкачки при перезагрузке;
* в ключе HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\SecurePipeServers установить параметр winreg(REG\_DWORD) со значением 1 для ограничения удаленного доступа к реестру;
* в ключе HKEY\_LOCAL\_MACHINE\Software\Microsoft\WindowsNT\СurrentVersion\Winlogon установить параметр AllocateFloppies (REG\_SZ) со значением 1 для исключения параллельного использования дисковода для гибких дисков;
* в ключе HKEY\_LOCAL\_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon установить параметр DontDisplayLastUserName (REG\_SZ) со значением 1 для отключения отображения имени последнего зарегистрированного пользователя;
* в ключе HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\Lsa установить параметр AuditBaseObjects (REG\_DWORD) со значением 1 для включения аудита базовых объектов системы;
* в ключе HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\Lsa установить параметр FullPrivilegeAuditing (REG\_BINARY) со значением 1 для включения аудита привилегий;
* в ключе HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\Rdr\Parameters установить параметр EnablePlainTextPassword (REG\_DWORD) со значением 0 для исключения передачи пароля пользователей по сети в открытом виде.

***ОС Linux:***

* на все директории, содержащие системные файлы операционной системы Linux и каталоги программного обеспечения устанавливают права доступа, запрещающие всем пользователям, кроме Владельца (Owner), запись;
* установить право доступа к файлам конфигурации только пользователю root;
* ограничить доступ пользователей к файлам и каталогам, находящимся на жестком диске рабочей станции;
* разрешить пользователям только запуск исполняемых файлов необходимых им для работы;

**Установка и эксплуатация программного обеспечения**

Установка вэб-ресурсов, специализированного программного обеспечения и контроль целостности исходных файлов и файлов журналов в операционных системах осуществляется ведущим разработчиком или сотрудником ответственным за работоспособность этих ресурсов.

В случае нарушения целостности исходных файлов и файлов журналов событий в прикладном программном обеспечении специалист, при необходимости, может ограничить доступ к сетевому узлу для дальнейшей работы по выявлению причины и восстановлению. При наличии искажений в работе программного обеспечения пользователь обязан уведомить УИТ “Адилет сот” для дальнейшей работы по исправлению программного обеспечения.

Специалист УИТ ”Адилет сот” обязан осуществлять периодический контроль работоспособности и соблюдения правил эксплуатации сетевых узлов.

Контроль осуществляется как непосредственно на проверяемом сетевом узле, так и удаленно.

Контрольная проверка на сетевом узле осуществляется в следующих случаях:

* при вводе сетевого узла в эксплуатацию;
* при изменении лица, ответственного за эксплуатацию;
* при изменении состава аппаратных средств сетевых узлов;
* при установке пакетов обновлений операционной системы, изменении версии операционной системы или состава дополнительного программного обеспечения, установленного на сетевой узел;

**Ключевая информация в информационной безопасности**

В состав ключевой информации сетевых узлов входят следующие составляющие:

* личные ключи пользователя - ключи защиты пользователя, необходимые для его аутентификации на сетевом узле, и может содержать ключи подписи пользователя. Личные ключи пользователя могут передаваться пользователю вместе с дистрибутивом для первичной инициализации или переноситься на ключевой носитель в процессе первичной инициализации сетевого узла. Ответственность за сохранность личных ключей пользователя несет сам пользователь;
* ключевой набор сетевого узла – набор ключей и справочной информации, общий для всех пользователей данного сетевого узла;
* резервный набор персональных ключей пользователя, предназначенный для получения дистанционного обновления ключевой информации при изменении исходной ключевой информации. Резервные наборы персональных ключей должны храниться на съемных носителях. Помещение для хранения должно быть оборудовано сейфом для хранения ключевых документов и охранной сигнализацией. Хранение наборов на жестком диске сетевого узла допускается в специально оборудованных помещениях при обеспечении дополнительных организационных и технических мер по защите от несанкционированного доступа к сетевому узлу. Жесткий диск такого сетевого узла подлежит учету наравне с ключевыми носителями. Запрещается хранение наборов на мобильных персональных компьютерах и на сетевых узлах в помещениях, в которые могут иметь доступ посторонние лица. Актуальная копия набора персональных ключей должен находиться в защищенном хранилище УИТ “Адилет сот”.

# 

Приложение № 14

к приказу №\_\_\_\_\_

от «\_\_\_\_» \_\_\_\_\_\_\_\_2018г.

# Регламент «О реагировании на инциденты информационной безопасности в Судебной системе»

**1.Общие положения**

1.1. Настоящий Регламент устанавливает порядок разбирательства и подготовки заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений, а так же выявления, разбирательства и предотвращения иных инцидентов связанных с информационной безопасностью (далее - инцинденты) в Судебной системе.

1.2. Регламент разработан в соответствии с Концепцией информационной безопасности, постановлением Правительства КР от 11 июля 2008 года № 373 "О проекте Концепции информационной безопасности Кыргызской Республики" и иными нормативными правовыми актами, а также в соответствии с локальными нормативными актами Судебной системы.

1.3. Настоящий Регламент обязателен к соблюдению всеми сотрудниками Судебной системы, участвующими в выявлении, разбирательстве и предотвращении инцидентов.

1.4. Разбирательство по всем подозрениям нарушения информационной безопасности проводится специалистами УИТ “Адилет сот”с привлечением в необходимых случаях руководителей и сотрудников других отделов.

1.5. Разбирательство по подозрениям нарушения информационной безопасности, затрагивающих два или более подразделений/отделов Судебной системы, проводится специалистами УИТ “Адилет сот” с привлечением руководителей соответствующих подразделений/отделов.

**2. Выявление инцидента**

2.1. Основными источниками информации о нарушении информационной безопасности являются:

* факты, выявленные начальниками подразделений/отделов или иные руководители подразделений Судебной системы, специалистами УИТ “Адилет сот”, а также другими сотрудниками Судебной системы.
* результаты работы средств мониторинга информационной безопасности, результаты проверок и аудита (внутреннего или внешнего);
* журналы и оповещения операционных систем серверов и рабочих станций, антивирусной системы, системы резервного копирования и других систем;
* обращения субъектов персональных данных с указанием инцидента, связанного с информационной безопасностью;
* запросы и предписания органов надзора за соблюдением прав субъектов персональных данных;
* другие источники информации.

2.2. Основными видами инцидентов, связанных с информационной безопасность в Судебной системе, являются:

* разглашение конфиденциальной или внутренней информации, либо угроза такого разглашения;
* несанкционированный доступ - доступ к информации лиц, которые не имеют никакого легального доступа к ресурсам или помещениям организации;
* превышение полномочий - несанкционированный доступ к каким-либо ресурсам и помещениям сотрудников Судебной системы;
* компрометация учетных записей или паролей;
* вирусная атака или вирусное заражение;
* нарушение или сбои в работе системы резервного копирования;
* нарушение правил использования персональных данных.
  1. Сотрудник Судебной системы может выявить признаки наличия инцидента путем анализа текущей ситуации на предмет ее соответствия требованиям защиты информации, утвержденными в Судебной системе. Выявленные несоответствия дают основания предполагать факт возникновения инцидента. Любые сведения о происшествиях или инцидентах должны быть незамедлительно переданы выявившим их сотрудником своему руководству или управляющему УИТ “Адилет сот”.

**3. Анализ исходной информации и принятие решения о проведении разбирательства**

3.1. Специалисты УИТ “Адилет сот” после получения информации о предполагаемом инциденте незамедлительно проводят первоначальный анализ полученных данных. В процессе анализа проводится проверка наличия в выявленном факте нарушений.

3.2. По усмотрению специалистов УИТ “Адилет сот” единичный инцидент, не приведший к негативным последствиям и совершенный сотрудником Судебной системы впервые, фиксируется в карточке данных «Инциденты ИБ» *(*приложение №13*)* с присвоением статуса «Разбирательство не требуется».

3.4. В случае наличия в инценденте признаков, приведших к негативным последствиям, специалист УИТ “Адилет сот” классифицирует инцидент, определяет предварительную степень важности инцидента и принимает решение о необходимости проведения разбирательства, информирует управляющего УИТ “Адилет сот” об инциденте, инициирует формирование регистрационной карточки инцидента с присвоением ему статуса «В процессе разбирательства».

3.5. В срок не более 3 (трех) рабочих дней с момента поступления информации об инциденте, специалист УИТ “Адилет сот” по согласованию с управляющим УИТ “Адилет сот” определяет и инициирует первоочередные меры, направленные на локализацию инцидента и на минимизацию его последствий.

**4. Разбирательство инцидента связанного с информационной безопасностью**

4.1.Цели и этапы разбирательства инцидента:

4.1.1. Целями разбирательства инцидентов являются:

* выработка организационных и технических решений, направленных на снижение рисков нарушения информационной безопасности, предотвращение и минимизацию подобных нарушений в будущем;
* защита репутации Судебной системы и ее информационных ресурсов;
* обеспечение безопасности персональных данных;
* обеспечение прав субъектов персональных данных на обеспечение безопасности и конфиденциальности их персональных данных, обрабатываемых Судебной системой;
* предотвращение несанкционированного доступа к конфиденциальной информации, информации, содержащей коммерческую и государственную тайну, персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации.

4.1.2. Разбирательство в инциденте, состоит из следующих этапов:

* подтверждение/опровержение факта возникновения инцидента;
* классификация инцидента;
* подтверждение/корректировка уровня значимости инцидента;
* уточнение дополнительных обстоятельств (деталей) инцидента;
* получение (сбор) доказательств возникновения инцидента, обеспечение их сохранности и целостности;
* минимизация последствий инцидента;
* информирование и консультирование сотрудников Судебной системы по действиям обнаружения, устранения последствий и предотвращения инцидентов;
* переоценка рисков, повлекших возникновение инцидента, актуализация необходимых положений, регламентов, правил.

4.2. Порядок проведения разбирательства инцидента:

4.2.1. В процессе проведения разбирательства инцидента обязательными для установления являются:

* дата и время фиксации инцидента;
* ФИО, должность, отдел или подразделение судебной системы нарушителя информационной безопасности;
* классификация инцидента;
* уровень критичности инцидента;
* обстоятельства и мотивы совершения инцидента;
* информационные ресурсы, затронутые инцидентом информационной безопасности;
* характер и размер реального и потенциального ущерба;
* обстоятельства способствовавшие совершению инцидента.

4.2.2. При инциденте, затрагивающем не более одного структурного подразделения, сотрудник Судебной системы информирует о факте инцидента руководителя соответствующего структурного подразделения.

4.2.3. При инциденте, затрагивающим более одного структурного подразделения, управляющий УИТ “Адилет сот” информирует руководителей соответствующих подразделений и инициирует проведение разбирательства.

4.2.4. В случае проведения временного отключения прав доступа у предполагаемого нарушителя информационной безопасности, информация об отключении прав доступа управляющим УИТ “Адилет сот” направляется руководителю предполагаемого нарушителя информационной безопасности.

4.2.5. Осуществляющий разбирательство специалист УИТ ”Адилет сот” в процессе проведения расследования инцидента при необходимости запрашивает информацию в структурных подразделениях, запрос направляется на имя руководителя подразделения с обязательным указанием сроков предоставления информации (с учетом необходимости ее анализа, сбора и подготовки).

4.2.6. После получения необходимой информации по инциденту осуществляющий разбирательство специалист УИТ “Адилет сот” проводит анализ полученных данных.

4.2.7. В течение 5 (пяти) рабочих дней с момента выявления инцидента специалист УИТ “Адилет сот” запрашивает у руководителя структурного подразделения объяснительную записку нарушителя информационной безопасности. Объяснительная записка должна быть составлена, подписана нарушителем информационной безопасности в течение (двух) рабочих дней и представлена его непосредственным руководителем специалисту УИТ “Адилет сот” в течение 3 (трех) рабочих дней с момента поступления запроса. В случае отказа нарушителя информационной безопасности предоставить объяснительную записку, специалист УИТ “Адилет сот” составляет акт, составленный в соответствии с установленным порядком.

4.2.8. специалист УИТ “Адилет сот” проводит оценку негативных последствий от реализации инцидента. В ходе данной оценки учитываются;

* репутационный ущерб;
* потенциальный ущерб;
* косвенные потери, связанные с недоступностью сервисов, потерей информации;
* другие виды ущерба или аспекты негативных последствий для Судебной системы или субъектов персональных данных.

4.2.9. С целью минимизации последствий инцидента возможно временное отключение прав доступа сотрудника к информационным ресурсам на время проведения расследования. Подобное отключение инициируется специалистом УИТ “Адилет сот” с обязательным предварительным устным согласованием с руководителем сотрудника.

4.2.10. В случае, если у нарушителя информационной безопасности были отключены права доступа к информационным ресурсам на время проведения разбирательства, то по его результатам специалист УИТ “Адилет сот” по согласованию с руководителем нарушителя информационной безопасности принимает решение и инициирует возвращение в полном или ограниченном объеме ранее имеющихся у нарушителя информационной безопасности прав доступа к информационным ресурсам либо инициирует официальную процедуру отмены (изменения) прав доступа к информационным ресурсам в соответствии с установленным порядком доступа к информационным, программным и аппаратным ресурсам Судебной системы. Если нарушение информационной безопасности было вызвано незнанием нарушителем правил (технологии) работы с информационными ресурсами, то основанием для возврата прав доступа является успешное прохождение инструктажа по информационной безопасности, ознакомлением с положениями должностной инструкции, иными локальными нормативными актами Судебной системы.

4.2.11.Восстановление временно отключенных у нарушителя информационной безопасности прав доступа к информационным ресурсам (разблокировка пользователя) может производиться только специалистом УИТ “Адилет сот”.

**5. Оформление результатов проведенного разбирательства**

5.1. Собранная в процессе разбирательства инцидента информация фиксируется специалистом УИТ “Адилет сот” в картотеке данных «Инциденты ИБ» и учитывается при подготовке итогового заключения по инциденту *(*Приложение №13*)*.

5.2. Специалисты УИТ “Адилет сот” формируют, согласовывают со всеми участниками разбирательства и подписывают итоговое заключение по расследованию инцидента.

5.3. Итоговое заключение по инциденту управляющий УИТ “Адилет сот” направляет руководителям структурных подразделений, затронутых инцидентом.

5.4. Специалист УИТ “Адилет сот” фиксирует завершение разбирательства в карточке «Инциденты ИБ» и присваивает инциденту статус «Разбирательство завершено».

5.5. Специалист УИТ “Адилет сот”, при необходимости определения правовой оценки инцидента, может обратиться за консультациями в правовое подразделение Судебной системы.

5.6. В случае выявления в инциденте признаков административного правонарушения или уголовного преступления, относящихся к сфере информационных технологий, специалист УИТ “Адилет сот” передает все материалы по инциденту директору Судебного департамента для принятия решения о подаче заявления в правоохранительные органы Кыргызской Республики.

**6. Завершение разбирательства, превентивные мероприятия**

6.1. По завершению разбирательства инцидента, управляющий УИТ “Адилет сот” передает имеющиеся материалы (в объеме, достаточном для принятия решения) директору Судебного департамента для решения вопроса о целесообразности привлечения нарушителя информационной безопасности к дисциплинарной ответственности.

6.2. На основании полученных результатов разбирательства руководитель структурного подразделения совместно со специалистами УИТ “Адилет сот” в срок не более 3 (трех) рабочих дней организовывают проведение одного или нескольких мероприятий, направленных на снижение рисков информационной безопасности в будущем:

* анализ и пересмотр имеющихся прав доступа к информационным ресурсам у нарушителя информационной безопасности;
* доведение до всех сотрудников структурного подразделения требований внутренних нормативных документов Судебной системы;
* обсуждение инцидента на совещании руководителей или собрании коллектива;
* отмена неактуальных прав доступа к информационным ресурсам;
* проведение мероприятий, направленных на предотвращение несанкционированного доступа к конфиденциальной информации, информации, содержащей коммерческую тайну, персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;

6.3. О результатах проведенного разбирательства инцидента специалист УИТ “Адилет сот” инициирует подготовку сообщения об инциденте в адрес управляющего УИТ “Адилет сот” для предоставления информации директору Судебного департамента.

**7. Права, обязанности и ответственность участников разбирательства**

7.1. Специалист УИТ “Адилет сот” имеет право:

* По согласованию с непосредственным руководителем нарушителя информационной безопасности требовать предоставлений письменных объяснений по обстоятельствам инцидента информационной безопасности у нарушителя информационной безопасности.
* Запрашивать и получать от руководителей и сотрудников Судебной системы, в рамках их компетенций, устные и письменные разъяснения и иную информацию, необходимую для проведения разбирательства инцидента информационной безопасности.
* Инициировать отключение от информационных ресурсов сотрудников Судебной системы, нарушивших правила или требования информационной безопасности, на период проведений расследования инцидента информационной безопасности в случае если имеется существенный риск того, что продолжение работы сотрудника с информационным ресурсом может повлечь значительное увеличение ущерба или новые инциденты информационной безопасности.
* По результатам расследования инцидента информационной безопасности инициировать изменения в бизнес-процессах и информационных ресурсах Судебной системы с целью повышения их защищенности и снижения рисков инцидентов информационной безопасности.
* Инициировать процедуры привлечения нарушителя информационной безопасности к дисциплинарной и (или) материальной ответственность согласно внутренним нормативным документам Судебной системы.

7.2. Специалист УИТ “Адилет сот” обязан:

* Объективно проводить разбирательство каждого инцидента информационной безопасности.
* Определять первоочередные меры, направленные на локализацию инцидента информационной безопасности и минимизацию негативных последствий.
* Фиксировать в карточке данных «Инциденты ИБ» всю исходную информацию об инциденте информационной безопасности и результаты его расследования.
* Предоставлять отчеты и рекомендации по проведенным разбирательствам руководству УИТ “Адилет сот”
* Проводить анализ обстоятельств, способствовавших совершению каждого инцидента информационной безопасности, и на его основе разрабатывать рекомендации и предложения по оптимизации бизнес-процессов и снижения ущерба от подобных инцидентов информационной безопасности и минимизации возможности их повторения в будущем.

7.3. Руководители структурных подразделений и сотрудники Судебной системы обязаны:

* предоставлять по запросам специалистов УИТ “Адилет сот” устные и письменные разъяснения и иную информацию в рамках своей компетенции, необходимую для проведения разбирательства инцидента информационной безопасности;
* информировать управляющего УИТ “Адилет сот” о выявленных инцидентах информационной безопасности и об имеющихся запросах и обращениях субъектов персональных данных;

7.4. Управляющий УИТ “Адилет сот” обязан лично информировать директора судебного департамента о всех инцендентах и результатах разбирательств по этим инцидентам.

Приложение № 15

к приказу №\_\_\_\_\_

от «\_\_\_\_» \_\_\_\_\_\_\_\_2018г.

# Регламент «Проведения мероприятий по контролю (надзору) выполнения требований, установленных Судебным департаментом при ВС КР, по обеспечению безопасности персональных данных при их обработке в информационных системах»

**I. Общие положения.**

**1.1.         Порядок организации и проведения проверки**

Мероприятие по контролю (надзору) за выполнением требований, установленных Судебным департаментом при ВС КР, по обеспечению безопасности персональных данных при их обработке в информационных системах (далее – проверка) проводится на основании распоряжения или приказа директора Судебного департамента при ВС КР либо лица его замещающего. Проверка может проводиться только должностным лицом УИТ “Адилет сот”.

**1.2. Ограничения при проведении проверки**

1.2.1. При проведении проверки должностные лица не вправе:

* проверять выполнение требований, не относящихся к их компетенции;
* требовать представления документов, информации, если они не являются объектами проверки и не относятся к предмету проверки, а также изымать оригиналы документов, относящихся к предмету проверки;
* распространять информацию, имеющию гриф секретности и полученную в результате проведения проверок, за исключением случаев, предусмотренных законодательством Кыргызской Республики.

При проведении проверки должностные лица должны допускаться к средствам криптографической защиты информации, техническим средствам, на которых они реализованы, оборудованию комплексов, в помещения, в которых установлены средства криптографической защиты информации, к средствам технической защиты, предназначенным для хранения, обработки и передачи персональных, и ключевых документов.

**III.Порядок оформления результатов проверки**

3.1. По результатам проверки должностными лицами, проводящими проверку, составляется акт в двух экземплярах.

3.2. В акте проверки указываются:

* + дата и номер распоряжения или приказа, на основании которого проведена проверка;
  + фамилия, имя, отчество и должности должностного лица или должностных лиц, проводивших проверку;
  + объект проверки, а также фамилии, имена, отчества операторов (ответственных пользователей криптосредств), осуществляющих обработку персональных данных, в отношении которых проводится проверка;
  + сведения о результатах проверки, в том числе о выявленных нарушениях обязательных требований, об их характере, о лицах, на которых возлагается ответственность за совершение этих нарушений;
  + сведения об ознакомлении или об отказе в ознакомлении с актом оператора, осуществляющего обработку персональных данных, а также лиц, присутствовавших при проведении проверки;
  + дата, время и место проведения проверки;
  + подписи должностного лица или должностных лиц, проводивших проверку.

3.3. К акту проверки могут прилагаться протоколы (заключения) проведённых экспертиз, объяснения должностных лиц, работников, на которых возлагается ответственность за нарушения обязательных требований, и другие документы или их копии, связанные с результатами проверки.

3.4. Акт оформляется непосредственно после завершения проверки в двух экземплярах, один из которых с копиями приложений, вручается оператору, осуществляющему обработку персональных данных, или уполномоченному им лицу под расписку об ознакомлении или отказе в ознакомлении с актом проверки.

3.5. В журнале учёта проверок должностными лицами осуществляется запись о проведённой проверке, содержащая сведения о датах начала и окончания проведения проверки, времени её проведения, правовых основаниях, целях, задачах и предмете проверки, выявленных нарушениях и выданных предписаниях, а также указываются фамилии, имена, отчества и должности должностного лица или должностных лиц, проводящих проверку, его или их подписи (При отсутствии журнала учёта проверок в акте проверки делается соответствующая запись).

Приложение № 16

к приказу №\_\_\_\_\_

от «\_\_\_\_» \_\_\_\_\_\_\_\_2018г.

# Модель угроз и нарушителя безопасности персональных данных, обрабатываемых в информационных системах персональных данных Судебной системы

# 

# Общие положения

Настоящая модель угроз безопасности персональных данных (далее – Модель) содержит систематизированный перечень угроз безопасности персональных данных при их обработке в информационной системе персональных данных Судебной системы. Указанные угрозы могут исходить от источников, имеющих антропогенный, техногенный и стихийный характер и воздействующих на уязвимости информационной системы персональных данных, характерные для данной информационной системы персональных данных, реализуя тем самым угрозы информационной безопасности.

В Модели дается обобщенное описание информационной системы персональных данных, состав, категории и предполагаемый объем обрабатываемых персональных данных с последующей классификацией информационных систем персональных данных.

Модель описывает потенциального нарушителя безопасности персональных данных и подходы по определению актуальности угроз с учетом возможностей нарушителя и особенностей конкретной информационной системы персональных данных.

**2. Характеристика объекта информатизации**

В Судебной системе предполагаются следующие типы информационных систем персональных данных:

1. Информационная система персональных данных ведения бухгалтерского учета, управления персоналом, расчета заработной платы Судебной системы.

2. Информационная система персональных данных передачи информации, в том числе персональные данные, в целях исполнения законов КР.

Состав информационной системы персональных данных и обрабатываемых в них персональных данных приведен в Приложении №1 к настоящему документу

В качестве объектов информатизации выступают:

1. Автономные автоматизированные рабочие места.

2. Локальные вычислительные сети.

В зависимости от характеристик и особенностей отдельных объектов часть вычислительных средств данных подключена к сетям связи общего пользования и (или) сетям международного информационного обмена.

Ввод персональных данных осуществляется как с бумажных носителей (например, документов, удостоверяющих личность субъекта персональных данных), так и с электронных носителей информации.

Информационные системы персональных данных предполагают как распределенную (на автономное автоматизированное рабочее место), так и централизованную (на выделенных файловых серверах сети) обработку и хранение персональных данных.

Персональные данные субъектов могут выводиться из информационных систем персональных данных с целью передачи персональных данных сотрудников Судебной системы, как в электронном, так и в бумажном виде.

Контролируемой зоной информационных систем персональных данных являются здания и отдельные помещения. В пределах контролируемой зоны находятся рабочие места пользователей и места хранения архивных копий данных, серверы системы, сетевое и телекоммуникационное оборудование информационных систем персональных данных. Вне контролируемой зоны находятся линии передачи данных и телекоммуникационное оборудование, используемое для информационного обмена по сетям связи общего пользования и (или) сетям международного информационного обмена.

**3. Состав, категории и объем персональных данных, определение уровня защищенности персональных данных**

На основе характеристик и особенностей используемых информационных систем персональных данных и обрабатываемых в них персональных данных, можно констатировать, что персональные данные субъектов, обрабатываются в Судебной системе информационной системой, обрабатывающей общедоступные персональные данные, а также системой, обрабатывающей иные категории персональных данных. Специальные категории персональных данных и биометрические персональные данные в информационной системе персональных данных Судебной системы не обрабатываются.

**4. Способы нарушения характеристик безопасности персональных данных**

Исходя из перечня персональных данных, обрабатываемых в информационной системе персональных данных, существуют следующие способы нарушения характеристик безопасности персональных данных:

* хищение персональных данных сотрудниками Судебной системы для использования в корыстных целях;
* передача финансовой, адресной, юридической и прочей информации о субъекте персональных данных третьим лицам;
* несанкционированное публичное разглашение персональных данных, ставших известными сотрудникам Судебной системы;
* несанкционированное получение персональных данных третьими лицами;
* уничтожение финансовой, адресной, юридической и прочей информации о субъекте персональных данных;
* модификация финансовой, адресной, юридической и прочей информации о субъекте персональных данных;
* блокирование финансовой, адресной, юридической и прочей информации о субъекте персональных данных;
* ввод некорректной финансовой, адресной, юридической и прочей информации о субъекте персональных данных;
* передача некорректной финансовой, адресной, юридической и прочей информации о субъекте персональных данных;
* искажение архивной информации по субъекту персональных данных.
* уничтожение архивной информации по субъекту персональных данных.

**5. Угрозы безопасности персональных данных, при их обработке в информационных системах персональных данных**

Под угрозами безопасности персональных данных при их обработке в информационной системе персональных данных понимается совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и (или) несанкционированными и (или) непреднамеренными воздействиями на нее. Таким образом, угрозы безопасности персональным данным при их обработке в информационной системе персональных данных могут быть связаны как с непреднамеренными действиями персонала информационных систем персональных данных, так и со специально осуществляемыми неправомерными действиями сотрудниками Судебной системы и граждан, а также иными источниками угроз.

В целях формирования систематизированного перечня угроз безопасности персональным данным при их обработке в информационной системе персональных данных и разработке на их основе частных (детализированных) моделей применительно к конкретному виду информационной системе персональных данных, угрозы безопасности персональным данным в информационной системе персональных данных можно классифицировать в соответствии со следующими признаками:

* по видам возможных источников угроз;
* по типу информационных систем персональных данных, на которые направлена реализация угроз;
* по виду нарушаемого свойства информации (виду несанкционированных действий, осуществляемых с персональными данными);
* по способам реализации угроз;
* по используемой уязвимости;
* по объекту воздействия.

Для информационной системы персональных данных существуют следующие классы угроз безопасности персональных данных:

* **По видам возможных источников угроз безопасности персональных данных:**
  + угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, имеющими доступ к информационному ресурсу информационной системы персональных данных, включая пользователей, реализующие угрозы непосредственно в информационной системе персональных данных;
  + угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, не имеющих доступа к информационным системам персональных данных, реализующие угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена;
  + угрозы, возникновение которых напрямую зависит от свойств техники, используемой в информационных системах персональных данных;
  + угрозы, связанные со стихийными природными явлениями.

Кроме этого, угрозы могут возникать в результате внедрения аппаратных закладок и вредоносных программ.

* **По типу информационных систем персональных данных, на которые направлена угроза:**

По структуре информационных систем персональных данных, на которые направлена угроза, необходимо рассматривать следующие классы угроз:

* + угрозы безопасности данных, обрабатываемых в информационных системах персональных данных на базе автоматизированных рабочих мест;
  + угрозы безопасности данных, обрабатываемых в информационных системах персональных данных на базе локальных информационных систем.
* **По способам реализации угроз:**

По способам реализации угроз выделяют следующие классы угроз:

* + угрозы, связанные с несанкционированным доступом к персональным данным (в том числе угрозы внедрения вредоносных программ);
  + угрозы утечки персональных данных по техническим каналам утечки информации;
  + угрозы специальных воздействий на информационные системы персональных данных.
* **По виду нарушаемого свойства информации (несанкционированных действий, осуществляемых с персональными данными):**

По виду несанкционированных действий, осуществляемых с персональными данными, можно выделить следующий класс угроз:

* + угрозы, приводящие к нарушению конфиденциальности персональных данных (копированию или несанкционированному распространению), при реализации которых не осуществляется непосредственного воздействия на содержание информации;
  + угрозы, приводящие к несанкционированному воздействию на содержание информации, в результате которого происходит изменение данных или их уничтожение;
  + угрозы, приводящие к несанкционированному воздействию на программные или программно-аппаратные элементы информационных систем персональных данных, в результате которых осуществляется блокирование данных.
* **По используемой уязвимости выделяются следующие классы угроз:**
  + угрозы, реализуемые с использованием уязвимости системного программного обеспечения;
  + угрозы, реализуемые с использованием уязвимости прикладного программного обеспечения; - угрозы, возникающие в результате использования уязвимости, вызванной наличием в информационной системе персональных данных аппаратной закладки;
  + угрозы, реализуемые с использованием уязвимостей протоколов сетевого взаимодействия и каналов передачи данных;
  + угрозы, возникающие в результате использования уязвимости, вызванной недостатками технической защиты информации от несанкционированного доступа;
  + угрозы, реализуемые с использованием уязвимостей, обусловливающих наличие технических каналов утечки информации;
  + угрозы, реализуемые с использованием уязвимостей средств защиты информации.
* **По объекту воздействия выделяются следующие классы угроз:**
  + угрозы безопасности персональных данных, обрабатываемых на автономном автоматизированном рабочем месте;
  + угрозы безопасности персональных данных, обрабатываемых в выделенных средствах обработки (принтерах, вынесенных мониторах, видеопроекторах, средствах звуковоспроизведения и т.п.); угрозы безопасности персональных данных, передаваемых по сетям связи;
  + угрозы прикладным программам, с помощью которых обрабатываются персональные данные;
  + угрозы системному программному обеспечению, обеспечивающему функционирование информационной системе персональных данных.

**6. Характеристика источников угроз безопасности персональных данных в информационной системе персональных данных**

В отношении информационной системе персональных данных могут существовать три типа источников угроз безопасности персональных данных:

1. Антропогенные источники угроз безопасности персональных данных.

2. Техногенные источники угроз безопасности персональных данных.

3. Стихийные источники угроз безопасности персональных данных.

**Антропогенные источники угроз безопасности персональных данных**

В качестве антропогенного источника угроз для информационной системы персональных данных необходимо рассматривать субъекта (личность), имеющего санкционированный или несанкционированный доступ к работе со штатными средствами информационной системы персональных данных, действия которого могут привести к нарушению безопасности персональных данных. Антропогенные источники угроз по отношению к информационным систем персональных данных могут быть как внешними, так и внутренними.

Среди внешних антропогенных источников можно выделить случайные и преднамеренные источники.

Случайные (непреднамеренные) источники могут использовать такие уязвимости, как ошибки, совершенные при проектировании информационной системы персональных данных и ее элементов, ошибки в программном обеспечении; различного рода сбои и отказы, повреждения, проявляемые в информационной системе персональных данных. К таким источникам можно отнести персонал поставщиков различного рода услуг, персонал надзорных и аварийных служб и т.п. Действия (угрозы), исходящие от данных источников, совершаются по незнанию, невнимательности или халатности, из любопытства, но без злого умысла.

Преднамеренные источники проявляются в корыстных устремлениях нарушителей. Основная цель таких источников – умышленная дезорганизацияя работы, вывод систем Судебной системы из строя, искажение информации за счет проникновения в информационные системы персональных данных путем несанкционированного доступа.

Внутренними источниками, как правило, являются специалисты в области программного обеспечения и технических средств, в том числе средств защиты информации, имеющие возможность использования штатного оборудования и программно-технических средств информационных систем персональных данных. К таким источникам можно отнести основной персонал, представителей служб безопасности, вспомогательный и технический персонал.

Для внутренних источников угроз особое место занимают угрозы в виде ошибочных действия и (или) нарушений требований эксплуатационной и иной документации сотрудниками Судебной системы, имеющих доступ к информационным ресурсам информационных систем персональных данных. К подобным угрозам, в частности, относятся:

* непредумышленное искажение или удаление программных компонентов;
* внедрение и использование неучтенных программ;
* игнорирование организационных ограничений (установленных правил) при работе с ресурсами информационных систем персональных данных, включая средства защиты информации. В частности:
* нарушение правил хранения информации ограниченного доступа, используемой при эксплуатации средств защиты информации (ключевой, парольной и аутентифицирующей информации);
* предоставление посторонним лицам возможности доступа к средствам защиты информации, а также к техническим и программным средствам, способным повлиять на выполнение предъявляемых к средствам защиты информации требований;
* настройка и конфигурирование средств защиты информации, а также технических и программных средств, способных повлиять на выполнение предъявляемых к средствам защиты информации требований, в нарушение нормативных и технических документов;
* несообщение о фактах утраты, компрометации ключевой, парольной и аутентифицирующей информации, а также любой другой информации ограниченного доступа.

Наибольшую опасность представляют преднамеренные угрозы, исходящие как от внешних, так и от внутренних антропогенных источников.

Необходимо рассматривать следующие классы таких угроз:

* угрозы, связанные с преднамеренными действиями лиц, имеющими доступ к информационным системам персональных данных, включая пользователей информационных систем персональных данных и иных сотрудников Судебной системы, реализующими угрозы непосредственно в информационной системе персональных данных (внутренний нарушитель);
* угрозы, связанные с преднамеренными действиями лиц, не имеющими доступа к информационным системам персональных данных и реализующими угрозы из внешних сетей связи общего пользования или сетей международного информационного обмена (внешний нарушитель);
* угрозы, связанные с преднамеренными действиями лиц, не имеющими доступа к информационным системам персональных данных и реализующими угрозы по техническим каналам утечки информации.

**Техногенные источники угроз безопасности персональных данных**

Техногенные источники угроз напрямую зависят от свойств техники. Данные источники также могут быть как внешними, так и внутренними.

К внешним источникам относятся инфраструктурные элементы информационной системы персональных данных: средства связи (телефонные линии, линии передачи данных и т.п.), сети инженерных коммуникаций (водоснабжение, канализация, отопление и пр.).

К внутренним источникам относятся некачественные технические и программные средства обработки информации, вспомогательные средства (охраны, сигнализации, телефонии), другие технические средства, применяемые в информационных системах персональных данных, а также вредоносное программное обеспечение и аппаратные закладки.

**Аппаратная закладка**

Аппаратные закладки могут быть конструктивно встроенными и автономными. Аппаратные закладки могут реализовать угрозы:

* сбора и накопления персональных данных, обрабатываемых и хранимых в информационных системах персональных данных;
* формирования технических каналов утечки информации.

В силу отмеченных свойств аппаратных закладок эффективная защита от них может быть обеспечена только за счет тщательного учета их специфики и соответствующей организации технической защиты информации на всех стадиях жизненного цикла информационной системы персональных данных.

**Носитель вредоносной программы**

В качестве носителя вредоносной программы в информационной системе персональных данных может выступать аппаратный элемент средств вычислительной техники из состава информационных система персональных данных или программоное обеспечение, выполняющее роль программного контейнера.

Если вредоносная программа не ассоциируется с какой-либо прикладной программой из состава системного или общего программного обеспечения информационной системы персональных данных, в качестве ее носителя выступают:

* внешний машинный (отчуждаемый) носитель, т.е. дискета, оптический диск, лазерный диск, флэш-память, внешний жесткий диск и т.п.;
* встроенные носители информации (жесткие диски, микросхемы оперативной памяти, процессор, микросхемы системной платы, микросхемы устройств, встраиваемых в системный блок устройства – видеоадаптера, сетевой платы, устройств ввода/вывода и т.д.)
* микросхемы внешних устройств (монитора, клавиатуры, принтера, плоттера, сканера и т.п.).

В том случае, если вредоносная программа может быть проассоциирована с системным или общим программным обеспечением, с файлами различной структуры или с сообщениями, передаваемыми по сети, то ее носителем являются:

* пакеты передаваемых по сети информационной системы персональных данных сообщений;
* файлы (исполняемые, текстовые, графические и т.д.).

При возникновении угроз из данной группы появляется потенциальная возможность нарушения конфиденциальности, целостности, доступности и других характеристик безопасности персональных данных.

**Стихийные источники угроз безопасности персональных данных**

Стихийные источники угроз отличается большим разнообразием и непредсказуемостью и являются, как правило, внешними. Под ними, прежде всего, рассматриваются различные природные катаклизмы: пожары, землетрясения, ураганы, наводнения. Возникновение этих источников трудно спрогнозировать и им тяжело противодействовать, но при наступлении подобных событий нарушается штатное функционирование самой информационной системы персональных данных и ее средств защиты, что потенциально может привести к нарушению конфиденциальности, целостности, доступности и других характеристик безопасности персональных данных.

Защита от угроз, исходящих от техногенных и стихийных источников угроз безопасности персональных данных, регламентируется инструкциями, разработанными и утвержденными оператором с учетом особенностей эксплуатации информационных систем персональных данных.

**7. Модель нарушителя безопасности персональных данных**

Анализ возможностей, которыми может обладать нарушитель, проводится в рамках модели нарушителя.

При разработке модели нарушителя зафиксированы следующие положения:

1. Безопасность персональных данных в информационной системе персональных данных обеспечивается средствами защиты информации информационными системами персональных данных, а также используемыми в них информационными технологиями, техническими и программными средствами, удовлетворяющими требованиям по защите информации;

2. Средства защиты информации штатно функционируют совместно с техническими и программными средствами, которые способны повлиять на выполнение предъявляемых к средствам защиты информации требований;

3. Средства защиты информации не могут обеспечить защиту персональных данных от действий, выполняемых в рамках предоставленных субъекту действий полномочий (например, средство защиты информации не может обеспечить защиту персональных данных от раскрытия лицами, которым предоставлено право на доступ к этим данным).

**Описание нарушителей**

С точки зрения наличия права постоянного или разового доступа в контролируемую зону объектов размещения информационных систем персональных данных все физические лица могут быть отнесены к следующим двум категориям:

* категория I – лица, не имеющие права доступа в контролируемую зону информационных систем персональных данных;
* категория II – лица, имеющие право доступа в контролируемую зону информационных систем персональных данных.

Все потенциальные нарушители подразделяются на:

* внешних нарушителей, осуществляющих атаки из-за пределов контролируемой зоны информационных систем персональных данных;
* внутренних нарушителей, осуществляющих атаки, находясь в пределах контролируемой зоны информационных систем персональных данных.

В качестве внешнего нарушителя кроме лиц категории I должны рассматриваться также лица категории II, находящиеся за пределами контролируемой зоны.

В отношении информационной системы персональных данных в качестве внешнего нарушителями из числа лиц категории I могут выступать:

* бывшие сотрудники Судебной системы;
* посторонние лица, пытающиеся получить доступ к персональным данным в инициативном порядке;
* представители преступных организаций.

Внешний нарушитель может осуществлять:

* перехват обрабатываемых техническими средствами информационные системы персональных данных за счет их утечки по техническим каналам утечки информации с использованием портативных, возимых, носимых, а также автономных автоматических средств разведки серийной разработки;
* деструктивные воздействия через элементы информационной инфраструктуры информационных систем персональных данных, которые в процессе своего жизненного цикла (модернизация, сопровождение, ремонт, утилизация) оказываются за пределами контролируемой зоны;
* несанкционированный доступ к информации с использованием специальных программных воздействий посредством программы вирусов, вредоносных программ, алгоритмических или программных закладок;
* перехват информации, передаваемой по сетям связи общего пользования или каналам связи, не защищенным от несанкционированного доступа к информации организационно- техническими мерами;
* атаки на информационные системы персональных данных путем реализации угроз удаленного доступа.

Внутренний нарушитель (лица категории II) подразделяется на восемь групп в зависимости от способа и полномочий доступа к информационным ресурсам информационных систем персональных данных.

К первой группеотносятся сотрудники Судебной системы, не являющиеся зарегистрированными пользователями и не допущенные к информационным ресурсам информационных систем персональных данных, но имеющие санкционированный доступ в контролируемые зоны. К этой категории нарушителей относятся сотрудники различных структурных подразделений предприятий: энергетики, сантехники, уборщицы, сотрудники охраны и другие лица, обеспечивающие нормальное функционирование объекта информатизации.

Лицо данной группы может:

* располагать именами и вести выявление паролей зарегистрированных пользователей информационных систем персональных данных;
* изменять конфигурацию технических средств обработки персональных данных, вносить программно-аппаратные закладки в программно-технические средства информационных систем персональных данных и обеспечивать съем информации, используя непосредственное подключение к техническим средствам обработки информации.

Ко второй группеотносятся зарегистрированные пользователи информационных систем персональных данных, осуществляющие ограниченный доступ к информационным ресурсам информационных систем персональных данных с рабочего места. К этой категории относятся сотрудники предприятий, имеющие право доступа к локальным информационным ресурсам информационных систем персональных данных для выполнения своих должностных обязанностей.

Лицо данной группы:

* обладает всеми возможностями лиц первой категории;
* знает, по меньшей мере, одно легальное имя доступа;
* обладает всеми необходимыми атрибутами (например, паролем), обеспечивающим доступ к информационным ресурсам информационных систем персональных данных;
* располагает персональными данными, к которым имеет доступ.

К третьей группеотносятся зарегистрированные пользователи подсистем информационных ресурсов, осуществляющие удаленный доступ к персональным данным по локальной сети Судебной системы.

Лицо данной группы:

* обладает всеми возможностями лиц второй категории;
* располагает информацией о топологии сети информационных систем персональных данных и составе технических средств информационных систем персональных данных;
* имеет возможность прямого (физического) доступа к отдельным техническим средствам информационных систем персональных данных.

К четвертой группеотносятся зарегистрированные пользователи информационных систем персональных данных с полномочиями администратора безопасности сегмента (фрагмента) информационной системы персональных данных.

Лицо данной группы:

* обладает полной информацией о системном и прикладном программном обеспечении, используемом в сегменте информационной системы персональных данных;
* обладает полной информацией о технических средствах и конфигурации сегмента информационной системы персональных данных;
* имеет доступ к средствам защиты информации и протоколирования, а также к отдельным элементам, используемым в сегменте информационной системы персональных данных;
* имеет доступ ко всем техническим средствам сегмента информационной системы персональных данных;
* обладает правами конфигурирования и административной настройки некоторого подмножества технических средств сегмента информационной системы персональных данных.

К пятой группеотносятся зарегистрированные пользователи с полномочиями системного администратора, выполняющего конфигурирование и управление программным обеспечением и оборудованием, включая оборудование, отвечающее за безопасность защищаемого объекта: средства мониторинга, резервного копирования, антивирусного контроля, защиты от несанкционированного доступа.

Лицо данной группы:

* обладает полной информацией о системном, специальном и прикладном программном обеспечении, используемом в информационной системе персональных данных;
* обладает полной информацией о технических средствах и конфигурации информационной системы персональных данных
* имеет доступ ко всем техническим средствам информационной системы персональных данных;
* обладает правами конфигурирования и административной настройки технических средств информационной системы персональных данных.

К шестой группеотносятся зарегистрированные пользователи информационных систем персональных данных с полномочиями администратора безопасности Судебной системы, отвечающего за соблюдение правил разграничения доступа, за генерацию ключевых элементов, смену паролей, криптографическую защиту информации. Администратор безопасности осуществляет аудит тех же средств защиты объекта, что и системный администратор.

Лицо данной группы:

* обладает полной информацией об информационных системах персональных данных;
* имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов информационных систем персональных данных;
* не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).

К седьмой группеотносятся лица из числа программистов - разработчиков сторонних организаций, являющихся поставщиками программного обеспечения и лица, обеспечивающие его сопровождение на объекте размещения информационной системы персональных данных.

Лицо данной группы:

* обладает информацией об алгоритмах и программах обработки информации в информационной системе персональных данных;
* обладает возможностями внесения ошибок, недекларированных возможностей, программных закладок, вредоносных программ в программное обеспечение информационной системы персональных данных на стадии его разработки, внедрения и сопровождения;
* может располагать любыми фрагментами информации о технических средствах обработки и защиты информации в информационной системе персональных данных.

К восьмой группеотносятся персонал, обслуживающий технические средства информационных систем персональных данных, а также лица, обеспечивающие поставку, сопровождение и ремонт технических средств информационных систем персональных данных.

Лицо данной группы:

* обладает возможностями внесения закладок в технические средства информационных систем персональных данных на стадии их разработки, внедрения и сопровождения;
* может располагать фрагментами информации о топологии информационных систем персональных данных, автоматизированных рабочих местах, серверах и коммуникационном оборудовании, а также о технических средствах защиты информации в информационных системах персональных данных.

**Предположения о возможностях нарушителя**

Для получения исходных данных о информационной системе персональных данных нарушитель (как I категории, так и II категории) может осуществлять перехват зашифрованной информации и иных данных, передаваемых по каналам связи сетям общего пользования и (или) сетям международного информационного обмена, а также по локальным сетям информационных систем персональных данных.

Любой внутренний нарушитель может иметь физический доступ к линиям связи, системам электропитания и заземления.

Предполагается, что возможности внутреннего нарушителя существенным образом зависят от действующих в пределах контролируемой зоны объектов размещения информационных систем персональных данных ограничительных факторов, из которых основными являются режимные мероприятия и организационно-технические меры, направленные на:

* предотвращение и пресечение несанкционированных действий;
* подбор и расстановку кадров;
* допуск физических лиц в контролируемую зону и к средства вычислительной техники;
* контроль за порядком проведения работ.

В силу этого внутренний нарушитель не имеет возможности получения специальных знаний о информационных системах персональных данных в объеме, необходимом для решения вопросов создания и преодоления средств защиты персональных данных, и исключается его возможность по созданию и применению специальных программно-технических средств реализации целенаправленных воздействий данного нарушителя на подлежащие защите объекты и он может осуществлять попытки несанкционированного доступа к информационным ресурсам с использованием только штатных программно-технических средств информационной системы персональных данных без нарушения их целостности.

Возможность сговора внутренних нарушителей между собой, сговора внутреннего нарушителя с персоналом организацийй-разработчиков подсистем информационной системы персональных данных, а также сговора внутреннего и внешнего нарушителей должна быть исключена применением организационно-технических и кадрово-режимных мер, действующих на объектах размещения информационных систем персональных данных.

**Предположения об имеющихся у нарушителя средствах атак**

Предполагается, что нарушитель имеет все необходимые для проведения атак по доступным ему каналам атак средства.

Внешний нарушитель (лица категории I, а также лица категории II при нахождении за пределами контролируемой зоны) может использовать следующие средства доступа к защищаемой информации:

* доступные в свободной продаже аппаратные средства и программное обеспечение, в том числе программные и аппаратные компоненты криптосредств;
* специально разработанные технические средства и программное обеспечение;
* средства перехвата и анализа информационных потоков в каналах связи;
* специальные технические средства перехвата информации по техническим каналам утечки информации;
* штатные средства информационной системы персональных данных (только в случае их расположения за пределами контролируемой зоны).

Внутренний нарушитель для доступа к защищаемой информации, содержащей персональные данные, может использовать только штатные средства информационной системы персональных данных. При этом его возможности по использованию штатных средств зависят от реализованных в информационной системе персональных данных организационно-технических и режимных мер.

**Описание каналов атак**

Возможными каналами атак, которые может использовать нарушитель для доступа к защищаемой информации в информационной системе персональных данных, являются:

* каналы непосредственного доступа к объекту (визуально-оптический, акустический, физический);
* электронные носители информации, в том числе съемные, сданные в ремонт и вышедшие из употребления;
* бумажные носители информации;
* штатные программно-аппаратные средства информационной системы персональных данных;
* кабельные системы и коммутационное оборудование, расположенные в пределах контролируемой зоны и не защищенные от несанкционированного доступа к информации организационно-техническими мерами;
* незащищенные каналы связи; техническим каналам утечки информации.

Приложение № 17

к приказу №\_\_\_\_\_

от «\_\_\_\_» \_\_\_\_\_\_\_\_2018г.

# Памятка пользователю по информационной безопасности

*Парольная защита*

* Никогда не сохраняйте ваши пароли в программах. Большинство программ хранят их в открытом виде и тот, кто получит доступ к вашему компьютеру, получит доступ и к ним.
* Сохраняйте в тайне личный пароль. Никогда не сообщайте пароль другим лицам, и не храните записанный пароль в общедоступных местах.
* В случае производственной необходимости (командировка, отпуск и т.п.), при проведении проверочных мероприятий, выполняемых специалистами УИТ “Адилет сот”, требующих знания пароля пользователя, допускается раскрытие значений своего пароля. По окончанию производственных, или проверочных работ сотрудники должны самостоятельно сменить "раскрытых" пароли.
* Не используйте пароль доступа в локальную сеть Судебной системы в других программах и на сайтах, где требуется регистрация;
* Следует помнить, что для печати документов на принтере, подключенном к другому компьютеру, не требуется знать пароль от этого компьютера. Достаточно включить компьютер, к которому присоединен нужный принтер, дождаться приглашения. После появления приглашения можно осуществлять печать. Для выключения компьютера нужно нажать кнопку «Завершить работу» не вводя пароль.

*Антивирусная защита*

* Никогда не отключайте установленное на автоматизированном рабочем месте антивирусное программное обеспечение.
* Обязательно проверяйте на наличие вирусов все внешние носители информации (дискеты, диски, флешки и т.п.), поступающие со стороны (из внешних организаций, других подразделений Судебной системы и т.п.)
* Во всех случаях возможного проявления действия вирусов или подозрении на наличие вируса не пытайтесь удалить вирус самостоятельно, незамедлительно сообщите об этом ответственному за антивирусный контроль и оцените с ним возможные пути заражения и распространения данного вируса.

*Интернет и электронная почта*

* Содержание Интернет-ресурсов, а также файлы, загружаемые из Интернета, обязательно проверяйте на отсутствие вредоносных программ и вирусов.
* Не переходите по ссылкам, не запускайте программы и не открывайте файлы, полученные по электронной почте от неизвестного Вам отправителя.
* Не передавать по электронной почте Ваши пароли.
* Не принимайте никаких соглашений при посещении сайтов, смысла которых Вы не понимаете.

*Прочее*

* Не устанавливайте самостоятельно программное обеспечение, если это не входит в Ваши обязанности. Запрещается устанавливать и запускать нелицензионное или не относящееся к выполнению Ваших должностных обязанностей программное обеспечение;
* Располагайте мониторы и печатающие устройства таким образом, чтобы исключить несанкционированный доступ к отображаемой и печатаемой информации.
* При временном оставлении рабочего места в течение рабочего дня в обязательным порядке блокируйте компьютер нажатием комбинации клавиш «Win + L».

Приложение № 18

к приказу №\_\_\_\_\_

от «\_\_\_\_» \_\_\_\_\_\_\_\_2018г.

# ПОЛИТИКА

# Судебной системы в области обработки и защиты персональных данных

1. **Общие положения**

1.1. В целях поддержания деловой репутации и гарантирования выполнения норм государственного законодательства в полном объеме Судебная система считает важнейшими своими задачами соблюдение принципов законности, справедливости и конфиденциальности при обработке персональных данных, а также обеспечение безопасности процессов их обработки.

1.2. Настоящая политика в области обработки и защиты персональных данных в Судебной системе (далее – Политика) характеризуется следующими признаками:

1.2.1. Разработана в целях обеспечения реализации требований законодательства КР в области обработки персональных данных субъектов.

1.2.2. Раскрывает основные категории персональных данных, обрабатываемых в Судебной системе, цели, способы и принципы обработки персональных данных, права и обязанности при обработке персональных данных, права субъектов персональных данных, а также включает перечень мер, обеспечивающих безопасность персональных данных при их обработке.

1.2.3. Является общедоступным документом, декларирующим концептуальные основы деятельности Судебной системы при обработке персональных данных.

1. **Правовые основания обработки персональных данных**
   1. Политика в области обработки персональных данных определяется в соответствии со следующими нормативными правовыми актами КР:
      1. Конституцией Кыргызской Республики;
      2. Гражданским кодексом Кыргызской Республики;
      3. Законом Кыргызской Республики от 14 апреля 2008 №58 “Об информации персонального характера” (В редакции Закона КР от [20 июля 2017 года № 129](http://cbd.minjust.gov.kg/act/view/ru-ru/111636?cl=ru-ru));
      4. Закон Кыргызской Республики от 5 декабря 1997 года № 89 ”О гарантиях и свободе доступа к информации Кыргызской Республики” (В редакции Законов КР от [18 октября 2002 года № 147](http://cbd.minjust.gov.kg/act/view/ru-ru/1104?cl=ru-ru), [от 28 декабря 2006 года № 214](http://cbd.minjust.gov.kg/act/view/ru-ru/202011?cl=ru-ru), [29 декабря 2016 года № 224](http://cbd.minjust.gov.kg/act/view/ru-ru/111505?cl=ru-ru), [18 марта 2017 года № 47](http://cbd.minjust.gov.kg/act/view/ru-ru/111554?cl=ru-ru));
      5. Закон Кыргызской Республики от 14.04.1994 № 1476-XII “О защите государственных секретов Кыргызской Республики” (В редакции Закона КР от [18 мая 2013 года № 74](http://cbd.minjust.gov.kg/act/view/ru-ru/203882?cl=ru-ru), [21 января 2014 года № 15](http://cbd.minjust.gov.kg/act/view/ru-ru/205236?cl=ru-ru));
      6. Постановление Правительства КР от 11 июля 2008 года № 373 "О проекте Концепции информационной безопасности Кыргызской Республики".
   2. Во исполнение настоящей Политики директором Судебного департамента утверждены следующие локальные нормативные правовые акты:
      1. Положение об обработке персональных данных;
      2. Перечень обрабатываемых персональных данных;
      3. Перечень информационных систем персональных данных;
      4. Перечень лиц, осуществляющих обработку персональных данных;
      5. Модель угроз и нарушителя безопасности персональных данных, обрабатываемых в информационных системах персональных данных;
      6. Инструкция о порядке обработки персональных данных без использования средств автоматизации.
2. **Цели обработки персональных данных**
   1. Обработка персональных данных в Судебной системе происходит исключительно в следующих целях:
      1. Осуществление правосудия.
      2. Исполнение судебных решений.
      3. Выполнение должностных обязанностей.
      4. Исполнения положений нормативных актов, указанных в п. 2.1.
      5. Осуществления пропускного и внутриобъектового режима.
3. **Категории обрабатываемых персональных данных, источники их получения, сроки обработки и хранения**
   1. В информационных системах персональных данных Судебной системы обрабатываются следующие категории персональных данных:
      1. Персональные данные судей и сотрудников судов. Источники получения: субъекты персональных данных Судебной системы;
      2. Персональные данные граждан принимающие участие в судебных разбирательствах. Источиники: Система межведомственного взаимодействия “Тундук”, граждане КР;
      3. Персональные данные посетителей. Источники получения: субъекты персональных данных-посетители;
      4. Персональные данные кандидатов. Источники получения: субъекты персональных данных кандидаты на должность сотрудника Судебной системы и на должность судьи КР.
   2. Сроки обработки и хранения персональных данных:
      1. Персональные данные обрабатываются сотрудниками Судебной системы в течении 1 рабочего дня и хранятся бессрочно. Право доступа к персональным данным имеют сотрудники Судебной системы, работающие непосредстведственно с персональными данными.
4. **Основные принципы обработки, передачи и хранения персональных данных**
   1. Судебная система в своей деятельности обеспечивает соблюдение принципов хранения и защиты персональных данных, основанных на законодательной базе КР, и обеспечивает необходимые условия для обработки персональных данных сотрудниками Судебной системы;
   2. Передача персональных данных производится на основании законодательной базы КР;
5. **Меры по обеспечению безопасности персональных данных при их обработке**
   1. Ответственные сотрудники судебной системы при обработке персональных данных принимают все необходимые правовые, организационные и технические меры для их защиты от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении них. Обеспечение безопасности персональных данных достигается, в частности, следующими способами:
      1. Определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных.
      2. Применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных.
      3. Оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных.
      4. Учетом электронных носителей персональных данных.
      5. Выявлением фактов несанкционированного доступа к персональным данным и принятием соответствующих мер.
      6. Восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.
      7. Установлением правил доступа к персональным данным, обрабатываемым в информационных системах, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационных системах.
      8. Контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровнем защищенности информационных систем.
6. **Права субъектов персональных данных**
   1. Субъект персональных данных имеет право на получение сведений об обработке его персональных данных Судебной системой.
   2. Субъект персональных данных не вправе требовать от Судебной системы уточнения этих персональных данных, их блокирования или уничтожения.
   3. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с законадательством КР, в том числе в следующих случаях:
      1. Если обработка персональных данных, включая те, что получены в результате оперативно-розыскной, контрразведывательной и разведывательной деятельности, выполняется в целях укрепления обороны страны, обеспечения безопасности государства и охраны правопорядка.
      2. При условии, что обработка персональных данных производится органами, осуществившими задержание субъекта персональных данных по подозрению в совершении преступления, либо предъявившими субъекту персональных данных обвинение по уголовному делу, либо применившими к субъекту персональных данных меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным кодексом КР случаев, когда допускается ознакомление подозреваемого или обвиняемого с такими персональными данными.

Если обработка персональных данных выполняется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма.

Приложение № 19

к приказу №\_\_\_\_\_

от «\_\_\_\_» \_\_\_\_\_\_\_\_2018г.

# Положение

# об обработке персональных данных в Судебной системе

1. **Общие положения**
   1. Настоящее Положение разработано во исполнение Концепции информационной безопасности Судебной системы в соответствии с [Трудовым кодексом К](http://www.securitypolicy.ru/index.php/%D0%92%D1%8B%D0%B4%D0%B5%D1%80%D0%B6%D0%BA%D0%B8_%D0%B8%D0%B7_%D0%A2%D1%80%D1%83%D0%B4%D0%BE%D0%B2%D0%BE%D0%B3%D0%BE_%D0%9A%D0%BE%D0%B4%D0%B5%D0%BA%D1%81%D0%B0_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B9%D1%81%D0%BA%D0%BE%D0%B9_%D0%A4%D0%B5%D0%B4%D0%B5%D1%80%D0%B0%D1%86%D0%B8%D0%B8)ыргызской Республики, [Конституцией К](http://www.securitypolicy.ru/index.php/%D0%9A%D0%BE%D0%BD%D1%81%D1%82%D0%B8%D1%82%D1%83%D1%86%D0%B8%D1%8F_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B9%D1%81%D0%BA%D0%BE%D0%B9_%D0%A4%D0%B5%D0%B4%D0%B5%D1%80%D0%B0%D1%86%D0%B8%D0%B8)ыргызской Республики, [Гражданским кодексом К](http://www.securitypolicy.ru/index.php/%D0%92%D1%8B%D0%B4%D0%B5%D1%80%D0%B6%D0%BA%D0%B8_%D0%B8%D0%B7_%D0%93%D1%80%D0%B0%D0%B6%D0%B4%D0%B0%D0%BD%D1%81%D0%BA%D0%BE%D0%B3%D0%BE_%D0%9A%D0%BE%D0%B4%D0%B5%D0%BA%D1%81%D0%B0_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B9%D1%81%D0%BA%D0%BE%D0%B9_%D0%A4%D0%B5%D0%B4%D0%B5%D1%80%D0%B0%D1%86%D0%B8%D0%B8)ыргызской Республики и другими нормативными правовыми актами и определяет порядок обработки персональных данных всех субъектов персональных данных, данные которых подлежат обработке в Судебной системе.
   2. Требования настоящего Положения являются неотъемлемой частью комплекса мер безопасности и информационной защиты в Судебной системе.
   3. Требования настоящего Положения распространяются на всех сотрудников Судебной системы, осуществляющих обработку персональных данных в Судебной системе.
2. **Основные термины, сокращения и определения**

2.1. Персональные данные — любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

2.2. Обработка персональных данных — действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

2.3. Конфиденциальность персональных данных — обязательное для соблюдения назначенного ответственного лица, получившего доступ к персональным данным, требование не допускать их распространения без согласия субъекта или иного законного основания.

2.4. Распространение персональных данных — действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

2.5. Использование персональных данных — действия (операции) с персональными данными, совершаемые должностным лицом Судебной системы в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъектов либо иным образом затрагивающих их права и свободы или права и свободы других лиц.

2.6. Блокирование персональных данных — временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи.

2.7. Уничтожение персональных данных — действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

2.8. Обезличивание персональных данных — действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту.

2.9. Общедоступные персональные данные — персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта или на которые в соответствии с законами не распространяется требование соблюдения конфиденциальности.

2.10. Информация — сведения (сообщения, данные) независимо от формы их представления.

**3. Состав персональных данных**

3.1. В состав персональных данных входят:

3.1.1. Фамилия, имя, отчество.

3.1.2. Дата рождения

3.1.3. Место рождения

3.1.4. Адрес.

3.1.5. Семейное, социальное и имущественное положение.

3.1.6. Образование и специальность.

3.1.7. Профессия.

3.1.8. Должность.

3.1.9. Заработная плата (оклад, премии, надбавки).

3.1.10. Номера банковских расчетных счетов.

3.1.11. Сведения о социальных льготах.

3.1.12. Судимости и/или наличие обязательств по исполнительным листам.

3.1.13. Паспортные данные.

3.1.14. ИНН.

3.1.15. Информация о воинской обязанности.

3.1.16. Данные страхового полиса обязательного медицинского страхования.

3.1.17. Данные страхового полиса обязательного пенсионного страхования.

3.1.18. Трудовой и общий стаж.

3.1.19. Данные о предыдущих местах работы.

3.1.20. Фотография.

3.1.21. Адрес электронной почты.

3.1.22. Телефон (домашний, сотовый).

3.1.23. Фамилия, имя отчество, дата рождения детей.

**4. Цель обработки персональных данных**

4.1. Целью обработки персональных данных является соблюдение [трудового законодательств](consultantplus://offline/ref=BDA114E1AC23957EA1860DC1DF83593437700436B8B557AC6EFD59CB14E364571F3BD3412F88A329GF21L)а КР, законодательства КР об охране труда и техники безопасности, законодательства КР об охране здоровья, законодательства КР о судопроизводстве, заключение и исполнение договоров, стороной которых являются субъекты персональных данных, организация однократного пропуска субъекта персональных данных на территорию объектов Судебной системы, зачисление заработной платы сотрудников.

**5. Сбор, обработка и защита персональных данных**

5.1. Порядок получения (сбора) персональных данных:

5.1.1. Все персональные данные субъекта следует получать у него лично с его письменного согласия, кроме случаев, определенных в п. 5.1.4 и 5.1.6 настоящего Положения и иных случаях, предусмотренных законами.

5.1.2. Форма заявления-согласия субъекта, являющегося сотрудником Судебной системы, на обработку персональных данных представлена в приложении №14 к настоящему положению. Форма заявления-согласия субъекта, не являющегося работником Судебной системы, на обработку персональных данных представлена в приложении №15 к настоящему положению.

5.1.3. Согласие субъекта на обработку персональных данных действует в течение неопределенного срока.

5.1.4. Если персональные данные возможно получить только у третьей стороны, субъект должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие (Приложение №17 к настоящему положению).

5.1.6. Обработка персональных данных субъектов без их согласия осуществляется в следующих случаях:

5.1.6.1. Персональные данные являются общедоступными.

5.1.6.2. По требованию полномочных государственных органов в случаях, предусмотренных законом КР.

5.1.6.3. Обработка персональных данных осуществляется на основании закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке.

5.1.6.4. Обработка персональных данных осуществляется для статистических целей при условии обязательного обезличивания персональных данных.

5.1.6.6. В иных случаях, предусмотренных законом.

5.2. Порядок обработки персональных данных:

5.2.1. На основании полученной информации сотрудник Судебной системы проверяет наличие данного субъекта, зарегистрированного в информационной системе. Если субъект отсутствует в информационной системе, то операционный сотрудник заносит полную информацию о субъекте. В случае наличия информации о субъекте в информационной системе – сверяет данные с ранее предоставленными (при необходимости вносит соответствующие изменения).

5.2.3. Своевременно, в срок не превышающий пяти рабочих дней, субъект персональных данных обязан лично или через своего законного представителя сообщать работнику, ответственному за сбор информации, об изменениях своих персональных данных с предоставлением соответствующих документов.

5.3. Защита персональных данных:

5.3.1. Под защитой персональных данных субъекта понимается комплекс мер (организационно-распорядительных, технических, юридических), направленных на предотвращение неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных субъектов, а также от иных неправомерных действий.

5.3.2. Защита персональных данных субъекта осуществляется за счёт Судебной системы в порядке, установленном соответствующими государственными законами и внутренними организационными документами Судебной системы.

5.3.3. Судебная система при защите персональных данных субъектов принимает все необходимые организационно-распорядительные, юридические и технические меры, в том числе:

5.3.3.1. Шифровальные (криптографические) средства при передаче персональных данных.

5.3.3.2. Антивирусная защита.

5.3.3.3. Организация режима обеспечения безопасности помещений, в которых размещена информационная система и обрабатываются персональные данные, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения, а именно:

* Запрещение нахождение сотрудников в таких помещениях, в целях, не связанных со служебной деятельностью;
* Нахождение лиц, не участвующих в обработке персональных данных в таких помещениях возможно только в присутствии лиц, осуществляющих обработку персональных данных;
* После исполнения своих обязанностей в таких помещениях сотруднику необходимо убрать все документы ограниченного пользования в специально отведенное для этого место, выключить всю аппаратуру, если это не препятствует технологическому процессу обработки информации, запереть помещение и произвести его опечатывание.
* При начале работы, а также после продолжительного отсутствия на рабочем месте следует проверить отсутствие несанкционированного доступа в такое помещение, а при его обнаружении немедленно сообщить об этом факте начальнику службы охраны и управляющему УИТ “Адилет сот”.

Перечень помещений, в которых обрабатываются персональные данные субъектов, приведен в Приложении №18 к настоящему положению.

5.3.3.4. Обеспечение сохранности и учета носителей персональных данных.

5.3.3.5. Утверждение руководителем оператора перечня лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных обязанностей.

5.3.3.6. Создание резервных копий персональных данных.

5.3.3.8. Издание нормативно-методических локальных актов, регулирующих защиту персональных данных.

**6. Блокировка, обезличивание, уничтожение персональных данных**

6.1. Порядок блокировки и разблокировки персональных данных:

6.1.1. Блокировка персональных данных подразумевает:

6.1.2.1. Запрет редактирования персональных данных.

6.1.2.2. Запрет распространения персональных данных любыми средствами (e-mail, сотовая связь, материальные носители).

6.1.2.3. Запрет использования персональных данных в массовых рассылках (sms, e-mail, почта).

6.1.2.4. Запрет открытия банковских счетов.

6.1.2.5. Изъятие бумажных документов, относящихся к субъекту персональных данных и содержащих его персональные данные из внутреннего документооборота Судебной системы и запрет их использования.

6.1.3. Блокировка персональных данных субъекта может быть временно снята, если это требуется для соблюдения законодательства.

6.1.4. Разблокировка персональных данных субъекта осуществляется с его письменного согласия или заявления.

6.2. Порядок обезличивания и уничтожения персональных данных:

6.2.1. Обезличивание персональных данных субъекта происходит по письменному заявлению субъекта персональных данных, при условии, что все договорные отношения завершены и от даты окончания последнего договора прошло не менее 5 лет.

6.2.2. При обезличивании персональные данные в информационных системах заменяются набором символов, по которому невозможно определить принадлежность персональных данных к конкретному субъекту.

6.2.3. Бумажные носители документов при обезличивании персональных данных уничтожаются. В случае невозможности уничтожения бумажных носителей, содержащих персональные данные как обезличиваемого субъекта, так и других субъектов персональных данных, персональные данные уничтожаются путем стирания или замазывания.

6.2.4. Операция обезличивания персональных данных субъекта необратима.

6.2.5. УИТ “Адилет сот” обязано обеспечить конфиденциальность в отношении персональных данных при необходимости проведения испытаний информационных систем на территории разработчика и произвести обезличивание персональных данных в передаваемых разработчику информационных системах.

6.2.6. Уничтожение персональных данных субъекта подразумевает прекращение какого-либо доступа к персональным данным субъекта.

6.2.7. При уничтожении персональных данных субъекта сотрудники Судебной системы не могут получить доступ к персональным данным субъекта в информационных системах.

6.2.8. Бумажные носители документов при уничтожении персональных данных уничтожаются, персональные данные в информационных системах обезличиваются. Персональные данные восстановлению не подлежат.

6.2.9. Операция уничтожения персональных данных необратима.

**7. Передача и хранение персональных данных**

7.1. Передача персональных данных:

7.1.1. Под передачей персональных данных субъекта понимается распространение информации по каналам связи и на материальных носителях.

7.1.2. При передаче персональных данных сотрудники Судебной системы должны соблюдать следующие требования:

7.1.2.1. Не сообщать персональные данные субъекта в коммерческих целях. Обработка персональных данных субъектов в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи не допускается.

7.1.2.2. Осуществлять передачу персональных данных субъектов в пределах Судебной системы в соответствии с настоящим Положением, нормативно-технологической документацией и должностными инструкциями.

7.1.2.3. Разрешать доступ к персональным данным только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения должностных обязанностей.

7.1.2.4. Передавать персональные данные субъекта представителям субъекта в порядке, установленном законодательством и нормативно-технологической документацией и ограничивать эту информацию только теми персональными данными субъекта, которые необходимы для выполнения указанными представителями их функции.

7.2. Хранение и использование персональных данных:

7.2.1. Под хранением персональных данных понимается существование записей в информационных системах и на материальных носителях.

7.2.2. Персональные данные субъектов обрабатываются и хранятся в информационных системах, а также на бумажных носителях.

7.2.3. Хранение персональных данных субъектов осуществляется (уточнить у СД и ВС КР) кадровой службой, бухгалтерией, сметно-договорным отделом, отделом по охране труда и технике безопасности, профкомом, службой охраны на бумажных и электронных носителях с ограниченным доступом.

7.2.4 Личные дела хранятся в бумажном виде в папках, прошитые и пронумерованные по страницам. Личные дела хранятся в специально отведенной секции сейфа, обеспечивающего защиту от несанкционированного доступа.

7.2.5. Подразделения, хранящие персональные данные на бумажных носителях, обеспечивают их защиту от несанкционированного доступа и копирования.

7.2.6. Срок хранения персональных данных субъекта определяется на основе соответствующих государственных законов и внутренних нормативных документов Судебной системы.

**8. Доступ к персональным данным**

8.1. Право доступа к персональным данным субъектов имеют сотрудники Судебной системы, входящие в перечень лиц, осуществляющих обработку персональных данных.

8.2. Сотрудники Судебной системы, получившие доступ к персональным данным субъекта, обязаны использовать их лишь в целях, для которых сообщены персональные данные и обязаны соблюдать режим секретности (конфиденциальности) обработки и использования полученной информации (персональных данных субъектов).

8.3. К числу массовых потребителей персональных данных вне Судебной системы относятся иные государственные и негосударственные функциональные структуры: налоговые инспекции; правоохранительные органы; органы статистики; страховые агентства; военкоматы; органы социального страхования; пенсионные фонды; подразделения органов управления. Надзорно-контрольные органы имеют доступ к информации только в сфере своей компетенции.

8.4. Организации, в которые субъект может осуществлять перечисления денежных средств (страховые Общества, негосударственные пенсионные фонды, благотворительные организации, кредитные учреждения) могут получить доступ к персональным данным субъекта только в случае его письменного разрешения.

8.3. Субъект может получить доступ к своим персональным данным на основании письменного запроса или при обращении, включая право на безвозмездное получение копий любой записи, содержащей персональные данные субъекта.

8.4. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Кыргызской Республики.

8.5. Обращение субъекта или поступивший запрос рассматривается должностным лицом Судебной системы, ответственным за обеспечение безопасности персональных данных в информационной системе.

8.6. В случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя ответственный за обеспечение безопасности персональных данных в информационной системе готовит в письменной форме мотивированный ответ, содержащий ссылку на положение государственного закона, являющееся основанием для такого отказа, в срок, не превышающий тридцати дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя.

8.7. Организация предоставляет безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных.

8.8. В срок, не более семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, Судебная система вносит в них необходимые изменения.

С этой целью ответственный за обеспечение безопасности персональных данных дает поручение должностному лицу Судебной системы, входящему в Перечень лиц, осуществляющих обработку персональных данных, внести изменения в персональные данные субъекта.

8.9. В срок, не более семи рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, Судебная система уничтожает такие персональные данные и уведомляет субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах.

8.10. Организация сообщает в уполномоченный [орган](consultantplus://offline/ref=22DE3A3EA6CBBA2BFA0E2F0FD5A2FEB0F682C413AD6464FD2C033DA79E987594D34320D85082727EL2n0J) по защите прав субъектов персональных данных по запросу этого органа необходимую информацию в течение тридцати дней с даты получения такого запроса.

**9. Права субъекта персональных данных**

Субъект персональных данных имеет право:

10.1. Требовать уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;

10.2. Требовать перечень обрабатываемых персональных данных, имеющихся в Судебной системе и источник их получения.

10.3. Получать информацию о сроках обработки персональных данных, в том числе о сроках их хранения.

10.4. Требовать извещения всех лиц, которым ранее были сообщены неверные или неполные его персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях.

10.5. Обжаловать в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке неправомерные действия или бездействия при обработке его персональных данных.

**10. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных**

11.1. Сотрудники Судебной системы, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с государственными законами.

11.2. Сотрудники Судебной системы, осуществляющие обработку персональных данных, обязаны заполнить заявку на предоставление доступа внутренних пользователей к информационным, программным и аппаратным ресурсам Судебной системы Форма заявки представлена в приложении №19 настоящего положения.

Приложение № 20

к приказу №\_\_\_\_\_

от «\_\_\_\_» \_\_\_\_\_\_\_\_2018г.

# Перечень персональных данных, обрабатываемых в Судебной системе

1. Фамилия, имя, отчество.

2. Дата рождения

3. Место рождения

4. Адрес.

5. Семейное, социальное и имущественное положение.

6. Образование и специальность.

7. Профессия.

8. Должность.

9. Заработная плата (оклад, премии, надбавки).

10. Номера банковских расчетных счетов.

11. Сведения о социальных льготах.

12. Судимости и/или наличие обязательств по исполнительным листам.

13. Паспортные данные.

14. ИНН.

15. Информация о воинской обязанности.

16. Данные страхового полиса обязательного медицинского страхования.

17. Данные страхового полиса обязательного пенсионного страхования.

18. Трудовой и общий стаж.

19. Данные о предыдущих местах работы.

20. Фотография.

21. Адрес электронной почты.

22. Телефон (домашний, сотовый).

23. Фамилия, имя отчество, дата рождения детей.

Приложение № 21

к приказу №\_\_\_\_\_

от «\_\_\_\_» \_\_\_\_\_\_\_\_2018г.

# Инструкция о порядке обработки персональных данных без использования средств автоматизации в Судебной системе

* 1. Обработка персональных данных без использования средств автоматизации (далее – неавтоматизированная обработка персональных данных) может осуществляться в виде документов на бумажных носителях и в электронном виде (файлы, базы банных) на электронных носителях информации.
  2. При неавтоматизированной обработке различных категорий персональных данных должен использоваться отдельный материальный носитель для каждой категории персональных данных.
  3. При неавтоматизированной обработке персональных данных на бумажных носителях:

- не допускается фиксация на одном бумажном носителе персональных данных, цели обработки которых заведомо не совместимы;

- персональные данные должны обособляться от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков);

- документы, содержащие персональные данные, формируются в дела в зависимости от цели обработки персональных данных;

- дела с документами, содержащими персональные данные, должны иметь внутренние описи документов с указанием цели обработки и категории персональных данных.

* 1. Неавтоматизированная обработка персональных данных в электронном виде осуществляется на внешних электронных носителях информации.
  2. При отсутствии технологической возможности осуществления неавтоматизированной обработки персональных данных в электронном виде на внешних носителях информации необходимо принимать организационные (охрана помещений) и технические меры (установка сертифицированных средств защиты информации), исключающие возможность несанкционированного доступа к персональным данным лиц, не допущенных к их обработке.
  3. При несовместимости целей неавтоматизированной обработки персональных данных, зафиксированных на одном электронном носителе, если электронный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

а) при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;

б) при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

* 1. Документы и внешние электронные носители информации, содержащие персональные данные, должны храниться в служебных помещениях в надежно запираемых и опечатываемых шкафах (сейфах). При этом должны быть созданы надлежащие условия, обеспечивающие их сохранность.
  2. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

Уточнение персональных данных производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

Приложение № 22

к приказу №\_\_\_\_\_

от «\_\_\_\_» \_\_\_\_\_\_\_\_2018г.

# Перечень неавтоматизированных систем, в которых обрабатываются персональные данные в Судебной системе (пример)

|  |  |  |
| --- | --- | --- |
| № | Система | Виды персональных данных |
| 1 | Пропуск посетителей на территорию предприятия | ФИО, паспортные данные |
| 2 | Кадровый учет | ФИО, дата и место рождения, адрес, семейное, социальное и имущественное положение, образование и специальность,  профессия, должность, заработная плата (оклад, премии, надбавки), судимости и/или наличие обязательств по исполнительным листам, паспортные данные, ИНН, информация о воинской обязанности, данные страхового полиса обязательного медицинского страхования, данные страхового полиса обязательного пенсионного страхования, личные дела, трудовой и общий стаж. |
|  |  |  |

Приложение № 23

к приказу №\_\_\_\_\_

от «\_\_\_\_» \_\_\_\_\_\_\_\_2018г.

# Перечень лиц, осуществляющих обработку персональных данных в Судебной системе

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № | Структурное подразделение | Занимаемая должность | Цели обработки персональных данных | Перечень информационных и неавтоматизированных систем персональных данных | Перечень персональных данных, подлежащих обработке |
| 1 |  |  |  |  |  |

Приложение № 24

к приказу №\_\_\_\_\_

от «\_\_\_\_» \_\_\_\_\_\_\_\_2018г.

Перечень сотрудников, имеющих доступ в помещения с ограниченным доступом

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № | Наименование помещения | Расположение помещения | Сотрудники, имеющие доступ | |
| Должность | ФИО |
| 1 |  |  |  |  |
|  |  |
| 2 |  |  |  |  |
|  |  |

Приложение № 25

к приказу №\_\_\_\_\_

от «\_\_\_\_» \_\_\_\_\_\_\_\_2018г.

ТЕХНИЧЕСКИЙ ПАСПОРТ

**на защищаемое помещение №\_\_\_\_\_\_\_\_\_\_\_\_**

СОСТАВИЛ: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(должность, инициалы, фамилия специалиста по защите информации)

«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 201\_\_

ОЗНАКОМЛЕН: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(должность, инициалы, фамилия ответственного за помещение)

«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 201\_\_

**1. Памятка**

по обеспечению режима безопасности и эксплуатации

оборудования, установленного в защищаемом

помещении №

1. Ответственность за режим безопасности в защищаемом помещении и правильность использования установленных в нем технических средств несет лицо, которое постоянно в нем работает, или лицо, специально на то уполномоченное.

1. Установка нового оборудования, мебели и т.п. или замена их, а также ремонт помещения должны проводиться только по согласованию со специалистами УИТ “Адилет сот”.
2. В нерабочее время помещение должно закрываться на ключ.
3. В рабочее время, в случае ухода, помещение должно быть закрыто на ключ или оставлено под ответственность лиц, назначенных руководителем.
4. При проведении конфиденциальных мероприятий бытовая радиоаппаратура, установленная в помещении (телевизоры, радиоприемники и т.п.), должна отключаться от сети электропитания.
5. Для исключения просмотра текстовой и графической конфиденциальной информации через окна помещения рекомендуется оборудовать их шторами (жалюзи).
6. Должны выполняться предписания на эксплуатацию средств связи, вычислительной техники, оргтехники, бытовых приборов и другого оборудования, установленного в помещении.

8. Запрещается использование в защищаемом помещении радиотелефонов, оконечных устройств сотовой, пейджинговой и транкинговой связи. При установке в защищаемое помещение, имеющих выход в городскую АТС, телефонных и факсимильных аппаратов с автоответчиком и (или) спикерфоном следует отключать эти аппараты на время проведения конфиденциальных мероприятий.

9. Повседневный контроль за выполнением требований по защите помещения осуществляют лица, ответственные за помещение, и служба безопасности Судебной системы.

10. Периодический контроль эффективности мер защиты помещения осуществляется специалистами УИТ “Адилет сот”.

**2. Перечень оборудования, установленного в помещении**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Вид оборудования | Тип | Учетный (зав.) номер | Дата установки | Класс  ТС (ОТСС или  ВТСС) | Сведения по сертификации, спец. исследованиям  и спец. проверкам |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**4. Отметка о проверке средств защиты**

|  |  |  |  |
| --- | --- | --- | --- |
| Вид оборудования | Учетный номер | Дата проверки | Результаты проверки и № отчетного документа |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**5. Результаты аттестационного и периодического контроля помещения**

|  |  |  |
| --- | --- | --- |
| Дата проведения | Результаты аттестации или периодического контроля, № отчетного документа | Подпись проверяющего |
|  |  |  |
|  |  |  |
|  |  |  |

Приложение № 26

к приказу №\_\_\_\_\_

от «\_\_\_\_» \_\_\_\_\_\_\_\_2018г.

# Перечень помещений с ограниченным доступом Судебной системы (пример)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № | Название помещения | Причина отнесения к защищаемым | Расположение помещения | Ответственный за помещение | |
| Должность | ФИО |
| 1 | Помещение серверной | Критически важное оборудование информационных систем | Административное здание, \_ этаж, кабинет №\_\_ |  |  |
| 2 | Помещение с терминальным сервером и коммутатором \_ этажа | Критически важное оборудование информационных систем | Административное здание, \_ этаж, кабинет №\_\_ |  |  |
| 3 | Помещение кассы и отправки платежных поручений | Работа с денежными средствами, обработка информации с использованием средств криптозащиты информации | Административное здание, \_ этаж, кабинет №\_\_ | Главный бухгалтер |  |
| 4 | Помещение архива бухгалтерии | Хранение документов ограниченного доступа бухгалтерии | Административное здание, \_ этаж, кабинет №\_\_ | Главный бухгалтер |  |
| 5 | Помещение отдела кадров | Хранение личных дел сотрудников | Административное здание, \_ этаж, кабинет №\_\_ | Начальник отдела кадров |  |
| 6 | Комната архива суда | Ведение конфиденциальных переговоров, хранение информации ограниченного доступа | Административное здание, \_ этаж, кабинет №\_\_ | Архивариус |  |
|  |  |  |  |  |  |

Приложение № 27

к приказу №\_\_\_\_\_

от «\_\_\_\_» \_\_\_\_\_\_\_\_2018г.

# Перечень защищаемых помещений Судебной системы (пример)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № | Название помещения | Причина отнесения к защищаемым | Расположение помещения | Ответственный за помещение | |
| Должность | ФИО |
| 1 | Кабинет директора | Ведение конфиденциальных переговоров, хранение информации ограниченного доступа | Административное здание, \_ этаж, кабинет №1\_\_, правое помещение |  |  |
| 2 | Кабинет \_ заместителя директора | Ведение конфиденциальных переговоров, хранение информации ограниченного доступа | Административное здание, \_ этаж, кабинет №\_\_ |  |  |
| 3 | Кабинет статс-секретаря | Ведение конфиденциальных переговоров, хранение информации ограниченного доступа | Административное здание, \_ этаж, кабинет №\_\_, левое помещение |  |  |
| 4 | Кабинет главного бухгалтера | Ведение конфиденциальных переговоров, хранение информации ограниченного доступа | Административное здание, \_ этаж, кабинет №\_\_ |  |  |
| 5 | Кабинет председателя суда | Ведение конфиденциальных переговоров, хранение информации ограниченного доступа | Административное здание, \_ этаж, кабинет №\_\_ |  |  |

Приложение № 28

к приказу №\_\_\_\_\_

от «\_\_\_\_» \_\_\_\_\_\_\_\_2018г.

# Лист ознакомления с документами по защите персональных данных

Ознакомлены: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(Сотрудники субъекта Судебной системы, подразделения или отдела)

|  |  |  |
| --- | --- | --- |
| Ф.И.О. | Подпись | Дата ознакомления |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Приложение № 29

к приказу №\_\_\_\_\_

от «\_\_\_\_» \_\_\_\_\_\_\_\_2018г.

# Журнал

# регистрации и учета заявок на предоставление доступа к информационным,

# программным и аппаратным ресурсам Судебной системы

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| №  заявки | ФИО, должность | Отдел | Информационный ресурс по заявке | Дата согласования заявки | Период доступа |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Приложение № 30

к приказу №\_\_\_\_\_

от «\_\_\_\_» \_\_\_\_\_\_\_\_2018г.

# ЖУРНАЛ

# УЧЕТА ДОПУСКА К ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Начат: «\_\_\_» \_\_\_\_\_\_\_\_\_ 20\_\_г.

Окончен: «\_\_\_» \_\_\_\_\_\_\_\_\_ 20\_\_г.

На \_\_\_\_\_\_\_\_\_\_ листах

| № п.п. | Ф.И.О. | Должность | Сведения о допуске к персональным данным | | | Сведения о прекращении допуска к персональным данным | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Вид обработки: А - автоматизированная, Н - неавтоматизированная | Дата обучения Правилам работы с персональными данными | Подпись лица ответственного за защиту персональных данных | Дата исключения из списка должностей в функциональные обязанности которых входит обработка персональных данных или доступ к ним / дата увольнения/перевода на иную работу | Номер приказа об увольнении | Подпись лица ответственного за защиту персональных данных |
| 1 | 2 | 3 | 4 | 6 | 7 | 8 | 9 | 10 |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

Приложение № 31

к приказу №\_\_\_\_\_

от «\_\_\_\_» \_\_\_\_\_\_\_\_2018г.

**Приложение 1**

Порядка доступа к информационным,

программным и аппаратным ресурсам

Судебной системы

**Журнал**

инструктажа пользователей с правилами доступа к ресурсам

Судебной системы

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **№**  **п/п** | **Инструктаж получил:** | | | **Инструктаж провел:** | | |
| **Фамилия И.О.** | **Занимаемая должность** | **Подпись** | **Фамилия И.О.** | **Подпись** | **Дата** |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

Приложение № 31

к приказу №\_\_\_\_\_

от «\_\_\_\_» \_\_\_\_\_\_\_\_2018г.

**Приложение 2**

Порядка доступа к информационным,

программным и аппаратным ресурсам

Судебной системы

Управляющему

УИТ “Адилет сот”

Юрьеву А. А.

# СЛУЖЕБНАЯ ЗАПИСКА

**на изменение состава информационных ресурсов**

В соответствии с Порядком доступа к информационным, программным и аппаратным ресурсам, утвержденным приказом от \_\_\_.201\_г. № \_\_\_\_\_\_, прошу включить (аннулировать) в (из) реестр(а) новый информационный ресурс.

|  |  |  |
| --- | --- | --- |
| Наименование информационного (программного) ресурса | Основание для включения нового ресурса в реестр Судебной системы | Период действия (постоянно или указать интервал) |
| 1 | 3 | 6 |
|  |  |  |

Начальник \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(*наименование отдела)*

«\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_201\_г \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_

Фамилия, инициалы подпись

Приложение № 31

к приказу №\_\_\_\_\_

от «\_\_\_\_» \_\_\_\_\_\_\_\_2018г.

**Приложение 3**

Порядка доступа к информационным,

программным и аппаратным ресурсам

Судебной системы

**Заявка № \_\_\_\_\_\_**

**на предоставление доступа к информационным, программным и аппаратным ресурсам**

**Судебной системы**

**В соответствии с Порядком доступа к информационным, программным и аппаратным ресурсам, утвержденным приказом от .\_\_\_.201\_г. №  \_\_\_\_\_\_, прошу выдать (аннулировать) доступ к нижеперечисленным информационный ресурс следующим сотрудникам.**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Фамилия И.О. сотрудника,,  должность | Объект судебной системы, № каб.,  Телефон | Обоснование необходимости предоставления/ аннулирования доступа при проведении указанного вида работ | Ресурс  (согласно Перечню) | Режим доступа  (**открыть/закрыть**) | Период действия (постоянно или указать интервал дат) |
| 1 | 2 | 3 | 4 | 5 | 6 |
|  |  |  |  |  |  |

Начальник \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(*Наименование отдела)*

«\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_201\_г \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_

Фамилия, инициалы подпись

**Согласовано:**

Управляющий УИТ “Адилет сот”:

«\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_201\_г \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Фамилия, инициалы подпись

Приложение № 31

к приказу №\_\_\_\_\_

от «\_\_\_\_» \_\_\_\_\_\_\_\_2018г.

**Приложение 4**

Порядка доступа к информационным,

программным и аппаратным ресурсам

Судебной системы

**Журнал**

**регистрации и учета заявок на предоставление доступа к информационным, программным и аппаратным ресурсам**

**Судебной системы**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Заявка № | ФИО, должность | Объект Суд. системы, отдел | Информационный ресурс по заявке | Дата согласования заявки | Период доступа |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Приложение № 32

к приказу №\_\_\_\_\_

от «\_\_\_\_» \_\_\_\_\_\_\_\_2018г.

**Приложение 5**

к Положению об использовании

программного обеспечения

в Судебной системе

**ПЕРЕЧЕНЬ**

**Программного обеспечения, разрешенного для использования**

**на компьютерах Судебной системы (пример)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № | Описание ПО | Наименование ПО | Используемое кол-во программ | Вид лицензирования |
| ПО, устанавливаемое на каждый компьютер | | | | |
| 1 | Операционная система | Windows XP Pro |  | Лицензия |
| Windows Vista |  | Лицензия |
| Windows 7 |  | Лицензия |
| Ubuntu Linux |  | Открытая лицензия GNU GPL |
| 2 | Антивирусная защита | ESET NOD32 Antivirus Business Edition |  | Лицензия |
| 3 | Офисные пакеты | Open Office |  | Открытая лицензия GNU LGPL |
| Microsoft Office |  | Лицензия |
| 4 | Архиваторы | 7-Zip |  | Открытая лицензия GNU GPL |
| 5 | Интернет браузер | Mozilla Firefox |  | Открытая лицензия MPL |
| Chromium Browser |  | Открытая лицензия MPL |
| 6 | Почтовый клиент | Mozilla Thunderbird |  | Открытая лицензия MPL |
| 7 | Программа для просмотра файлов PDF | Adobe Acrobat reader |  | Открытая лицензия GNU GPL |
| 8 | Программа для просмотра файлов DJVU | DjVu viewer |  | Открытая лицензия GNU GPL |
| 9 | Программа для просмотра графических файлов (jpg, gif, png, bmp) | FastStone Image Viewer |  | Открытая лицензия GNU GPL |
| 10 | Пакет кодеков | K-Lite Codec Pack |  | Открытая лицензия GNU LGPL |
| 11 | Видеоплеер | Windows Media Player |  | В комплекте с ОС |
| Серверное ПО | | | | |
| 12 | Серверная ОС | Windows Server 2003 SP2 R2 |  | Лицензия |
| Ubuntu Servser |  | Открытая лицензия GNU GPL |
| 13 | ПО для распределения интернет траффика (Прокси-сервер) | User Gate |  | Лицензия |
| 14 | СУБД сервера | PostgreSQL |  | Лицензия |
| Специализированное ПО | | | | |
| 15 |  |  |  |  |

Приложение № 32

к приказу №\_\_\_\_\_

от «\_\_\_\_» \_\_\_\_\_\_\_\_2018г.

**Приложение 6**

к Положению об использовании

программного обеспечения

в Судебной системе

**Паспорт автоматизированного рабочего места**

|  |  |
| --- | --- |
| Материально-ответственное лицо: |  |
| Подразделение/отдел: |  |
| Ответственный пользователь: |  |
| Расположение автоматизированного рабочего места: |  |
| Имя компьютера: |  |
| Домен/Рабочая группа: |  |

Состав АРМ:

|  |  |  |
| --- | --- | --- |
| Наименование | | Марка/модель |
| *Системный блок* | |  |
|  | Материнская плата |  |
|  | Процессор |  |
|  | ОЗУ |  |
|  | Диск |  |
|  | Видеоадаптер |  |
|  | Сетевой адаптер |  |
|  | Оптический дисковод |  |
|  | Картридер |  |
| *Монитор* | |  |
| *Клавиатура* | |  |
| *Мышь* | |  |
| *Принтер* | |  |
| *Прочее (указать что именно)* | |  |
|  | |  |

* 1. Программное обеспечение

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № | Наименование ПО, издатель | Версия | Дата установки | ФИО установившего |
| 1 | Установлено антивирусное ПО: |  |  |  |
| 2 | Установлено средство защиты от НСД: |  |  |  |
| 3 | Установлено средство криптозащиты: |  |  |  |
| 4 | Операционная система |  |  |  |
| 5 |  |  |  |  |
| 6 |  |  |  |  |

* 1. Сведения об удалении программного обеспечения

|  |  |  |  |
| --- | --- | --- | --- |
| № | Номер удаляемой позиции | Дата удаления | ФИО удалившего |
| 1 |  |  |  |
| 2 |  |  |  |

* 1. Сведения о проведенных ремонтно-профилактических работах

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № | Оборудование, неисправность | проведенные работы | дата ремонта | ФИО ремонтировавшего |
| 1 |  |  |  |  |
| 2 |  |  |  |  |

Ответственный пользователь: Ф.И.О. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Подпись \_\_\_\_\_\_\_\_\_\_\_\_\_

IT-консультант: Ф.И.О. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Подпись \_\_\_\_\_\_\_\_\_\_\_\_\_

Специалист УИТ “Адилет сот”: Ф.И.О. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Подпись \_\_\_\_\_\_\_\_\_\_\_\_\_

Управляющий УИТ “Адилет сот”: Юрьев А.А. Подпись \_\_\_\_\_\_\_\_\_\_\_\_\_

Приложение № 33

к приказу №\_\_\_\_\_

от «\_\_\_\_» \_\_\_\_\_\_\_\_2018г.

**Приложение 7**

к Положению об использования

сети Интернет и электронной почты

в Судебной системе

**Типичные угрозы**

**при работе с сетью Интернет и электронной почтой**

|  |  |  |  |
| --- | --- | --- | --- |
| № | Угроза | Примечание | Рекомендуемые меры предосторожности |
|  | Заражение компьютера вирусом. | Чаще всего заражение вирусами происходит при посещении специально созданных «вредоносных» веб-страниц, «хакерских» сайтов, сайтов «для взрослых». | - не посещать перечисленные сайты;  - установить, своевременно обновлять и не отключать антивирусное программное обеспечение. |
|  | Заражения компьютера вирусом при просмотре почтовых сообщений. | Обычно происходит при открытии прикрепленного к письму файла. | - не открывать письма, если электронный адрес отправителя вам не знаком или выглядит «странно»;  - не открывать прикрепленные файлы, если отправитель письма вам неизвестен;  - установить, своевременно обновлять и не отключать антивирусное программное обеспечение. |
|  | Утечка информации с рабочей станции. | Уязвимым может оказаться программное обеспечение (чаще всего таковым является свободно распространяемое ПО, а также ПО от неизвестных или малоизвестных производителей).  Также причиной утечки может оказаться заражение компьютера вирусом. | - использовать только принятое к использованию в Судебной системе программное обеспечение;  - установить, своевременно обновлять и не отключать антивирусное программное обеспечение. |
|  | Предоставление возможности удаленного управления компьютером. | Такая возможность может быть получена как с ведома пользователя (при использовании им ПО, выполняющего данную функцию), так и без его ведома (при заражении компьютера вирусом). | - использовать только принятое к использованию в Судебной системе программное обеспечение;  - установить, своевременно обновлять и не отключать антивирусное программное обеспечение. |
|  | Потеря функциональности (полной или частичной) рабочей станцией. | Чаще всего это происходит вследствие использования уязвимостей программного обеспечения злоумышленником или из-за заражения вирусом. | - использовать только принятое к использованию в Судебной системе программное обеспечение;  - установить, своевременно обновлять и не отключать антивирусное программное обеспечение. |
|  | Кража личной информации. | Чаще всего к этому приводит ввод такой информации на веб-страницах, в том числе сайтах-двойниках, которые внешне идентичны настоящим сайтам (например, сайту банка), но на самом деле являются подделкой. | - не открывать письма (и особенно вложения) от незнакомых адресатов;  - внимательно проверять адрес страницы, на которой вы собираетесь оставить личную информацию;  - не сохранять пароли в формах веб-страниц. |
|  | Захват адресов электронной почты, веб-страниц и т.п. | Чаще всего к этому приводит использование «слабого» пароля для доступа к ресурсу, а также подбор ответа на контрольной вопрос, используемый для восстановления пароля в случае его возможной утери. | - использовать «стойкие» пароли (от 7 символов, с использованием букв различного регистра и цифр);  - не использовать в качестве ответов на контрольные вопросы (и, конечно, в качестве самих паролей) информацию, которую достаточно легко узнать: дату рождения, имя, фамилию (ваши или близких родственников), кличку собаки, девичью фамилию;  - никогда не раскрывать перечисленную выше информацию (если она используется для описанных целей) незнакомым людям;  - не сохранять пароли в формах веб-страниц. |

Приложение № 31

к приказу №\_\_\_\_\_

от «\_\_\_\_» \_\_\_\_\_\_\_\_2018г.

**Приложение 8**

к Положению об использования сети

Интернет и электронной почты

в Судебной системе

**Общие меры предосторожности**

**при работе с сетью Интернет и электронной почтой**

|  |  |  |
| --- | --- | --- |
| № | Мера предосторожности | Примечание |
|  | Использование только разрешенногоУИТ “Адилет сот” программного обеспечения. | Использование нерегламентированного ПО может привести к утечке информации, заражению компьютера вирусом, выходу компьютера из строя из-за ошибок в написании ПО.  Ответственность возлагается на пользователя. |
|  | Отслеживание появления обновлений ПО, используемого на компонентах автоматизированных систем Судебной системы, взаимодействующих с сетью Интернет. | ПО может содержать уязвимости, использование которых злоумышленником может привести к утере информации, выходу компонента из строя.  Ответственность возлагается на администраторов соответствующих компонентов. |
|  | В случае обнаружения в используемом ПО критических с точки зрения безопасности уязвимостей и невозможности их устранения – приостановить эксплуатацию такого ПО. | Используемое ПО может содержать уязвимости, использование которых злоумышленником может привести к утере информации, выходу компонента из строя.  Ответственность возлагается на пользователей и администраторов соответствующих компонентов автоматизированных систем Судебной системы. |
|  | Обязательное использование и своевременное обновление антивирусного ПО на компонентах автоматизированных систем Судебной системы, взаимодействующих с сетью Интернет, в режиме мониторинга событий. | Заражение вирусами может произойти и без «интерактивного» участия пользователя – достаточно связи с сетью Интернет.  Ответственность возлагается на администраторов соответствующих компонентов. |
|  | При работе с электронной почтой – не открывать письма с вложенными файлами от неизвестных авторов, перед запуском/открытием любых файлов производить их антивирусную проверку. | В последнее время наиболее распространенный канал распространения вирусов, а также кражи личной информации – электронная почта.  В случае возникновения вопросов необходимо обратиться в УИТ “Адилет сот” до принятия решения о дальнейших действиях.  Ответственность возлагается на пользователей. |
|  | Запретить автоматическое сохранение и/или запуск файлов и элементов ActiveX, скриптов из сети Интернет на рабочей станции пользователя. | Большинство уязвимостей в программном обеспечении используются через файлы, загружаемые с веб-страниц, или через сами веб-страницы, которые содержат вредоносный/опасный код.  Для опытных пользователей с разрешения УИТ “Адилет сот” допускается возможность предоставления выбора о необходимости загрузки/запуска таких элементов.  Ответственность возлагается на пользователей. |
|  | Не рекомендуется сохранять пароли в формах при посещении веб-страниц. | Это может привести к тому, что кто-то иной воспользуется (в то числе – изменит пароль на новый) ресурсом, защищенным паролем.  Ответственность возлагается на пользователей. |

Приложение № 34

к приказу №\_\_\_\_\_

от «\_\_\_\_» \_\_\_\_\_\_\_\_2018г.

**Приложение 9**

к Положению о резервном копировании

в Судебной системе

**Перечень данных¸ подлежащих резервному копированию и хранению (пример)**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № | Наименование данных | Расположение | Периодичность копирования | Тип копирования | Объем данных, Мбайт |
| 1 | Состояние системы | \\server\SystemState | ежедневно | полное | 200 |
| 2 | Системный диск контроллера домена | \\server\c$ | ежедневно | полное | 300 |
| 3 |  |  |  |  |  |

Приложение № 34

к приказу №\_\_\_\_\_

от «\_\_\_\_» \_\_\_\_\_\_\_\_2018г.

**Приложение 10**

к Положению о резервном копировании

в Судебной системе

**Расписание резервного копирования**

СЕРВЕРА

Еженедельное копирование

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| № | Ресурс | Понедельник | Вторник | Среда | Четверг | Пятница |
| 1 | Файловый сервер | Инкр.копия 1 (23.00) | Инкр.копия 2 (23.00) | Инкр.копия 3 (23.00) | Инкр.копия 4 (23.00) | Полная копия (23.00) |
| 2 |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |

Ежемесячное копирование

|  |  |  |
| --- | --- | --- |
| № | Ресурс | Пятница первой недели нового месяца |
| 1 | Файловый сервер | Полная копия последней недели прошедшего месяца (23.00) |
| 2 |  |  |
| 3 |  |  |

Годовое копирование

|  |  |  |
| --- | --- | --- |
| № | Ресурс | Пятница первой недели первого месяца нового года |
| 1 | Файловый сервер | Полная копия последней недели прошедшего месяца (23.00) |
| 2 |  |  |
| 3 |  |  |

БАЗЫ ДАННЫХ

Еженедельное копирование

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| № | Ресурс | Понедельник | Вторник | Среда | Четверг | Пятница |
| 1 | База данных | Инкр.копия 1 (01.00) | Инкр.копия 2 (01.00) | Инкр.копия 3 (01.00) | Инкр.копия 4 (01.00) | Полная копия (01.00) |
| 2 |  |  |  |  |  |  |

Ежемесячное копирование

|  |  |  |
| --- | --- | --- |
| № | Ресурс | Пятница первой недели нового месяца |
| 1 | База данных | Полная копия последней недели прошедшего месяца (01.00) |
| 2 |  |  |

Годовое копирование

|  |  |  |
| --- | --- | --- |
| № | Ресурс | Пятница первой недели первого месяца нового года |
| 1 | База данных | Полная копия последней недели прошедшего месяца (01.00) |
| 2 |  |  |

РАБОЧИЕ СТАНЦИИ, CОДЕРЖАЩИЕ ОСОБО ВАЖНУЮ ИНФОРМАЦИЮ

I. Категории А - Еженедельное копирование

|  |  |  |
| --- | --- | --- |
| № | Ресурс | Пятница |
| 1 | Рабочая станция | Полная копия (13.00) |
| 2 |  |  |

I. Категории Б - Еженедельное копирование

|  |  |  |
| --- | --- | --- |
| № | Ресурс | 15-е число нового месяца |
| 1 | Рабочая станция | Полная копия (13.00) |
| 2 |  |  |
| 3 |  |  |

Приложение № 35

к приказу № \_\_\_\_\_

от «\_\_\_\_»\_\_\_\_\_\_\_\_2018г.

**Приложение 11**

к Положению об использовании

мобильных устройств и

носителей информации

в Судебной системе

Директору Судебного департамента при ВС КР Ибраимову Р. И.

**ЗАЯВКА  
на предоставление сотруднику Судебной системы**

**мобильного устройства/носителя информации**

"\_\_\_"\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 201\_\_ года

В связи с возникшей производственной необходимостью, прошу предоставить следующему сотруднику:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(Ф.И.О.)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(должность)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(структурное подразделение)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(номер служебного телефона)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(наименование мобильного устройства/носителя информации)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(перечень задач, решаемых с использованием мобильного устройства/носителя информации)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Руководитель: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(наименование структурного подразделения)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(подпись) (фамилия и инициалы)

Согласовано:

Управляющий УИТ “Адилет сот”

Юрьев А. А. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Приложение № 35

к приказу № \_\_\_\_\_

от «\_\_\_\_»\_\_\_\_\_\_\_\_2018г.

**Приложение 12**

к Положению об использовании

мобильных устройств и

носителей информации

в Судебной системе

Директору Судебного департамента при ВС КР Ибраимову Р. И.

**Список работников, имеющих право работы с мобильными устройствами вне территории объектов Судебной системы**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № | Ф.И.О. | Должность | Структурное подразделение  / отдел | Наименование мобильного устройства | Инвентарный номер мобильного устройства |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Управляющий УИТ “Адилет сот” Юрьев А. А.

"\_\_\_" \_\_\_\_\_\_\_\_\_\_\_\_\_ 201\_\_ г. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Приложение № 36

к приказу № \_\_\_\_\_

от «\_\_\_\_»\_\_\_\_\_\_\_\_2018г.

**Приложение 13**

к Регламенту о реагировании на

инциденты информационной

безопасности в Судебной

системе

**Карточка данных о инциденте ИБ.**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Дата события | | | |  | | |  | | | |  | | | | |
| Номер события | | | |  | | |  | | | |  | | | | |
| Информация о сообщающем лице  Фамилия и имя \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Подразделение/отдел \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Рабочий телефон \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Электронная почта \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | | | | | | | | | | | | | |
| Описание события ИБ | | | | | | | | | | | | | | | |
| Описание события: | | | | | | | | | | | | | | | |
|  Что произошло | | | | | | |  | | | | | | | | |
|  Как произошло | | | | | | |  | | | | | | | | |
|  Почему произошло | | | | | | |  | | | | | | | | |
|  Пораженные компоненты | | | | | | |  | | | | | | | | |
|  | | | | | | |  | | | | | | | | |
|  Любые идентифицированные уязвимости | | | | | | |  | | | | | | | | |
| Детали события ИБ | | | | | | | | | | | | | | | |
| Дата и время возникновения события | | | | | | |  | | | | | | | | |
| Дата и время обнаружения события | | | | | | |  | | | | | | | | |
| Дата и время сообщения о событии  Классификация события | | | | | | |  | | | | | | | | |
| Закончилось ли событие? (отметить квадрат) | | | | | | | Да  Нет  | | | | | | | | |
| Если «да», то уточнить, как долго длилось событие в днях/часах/минутах | | | | | | |  | | | | | | | | |
|  | | | |  | | | | |  | | | |  | | |
| Тип инцидента ИБ | | | | | | | | | | | | | | | |
|  | | | Действительный  | | | | | | | Попытка  | Подозрение  | | | | |
|  | | | | | | | | | | | | | | | |
| (Один из) | | Намеренная  | | | | | (указать типы угрозы) | | | |  | | | | |
|  | | | | | | | | | | | | | | | |
| Копирование информации | | | | | |  | | | Хакерство/Логическое проникновение | | | | | |  |
| Изменение информации | | | | | |  | | | Неправильное использование ресурсов | | | | | |  |
| Саботаж/физический ущерб | | | | | |  | | | Другой ущерб | | | | | |  |
| Вредоносная программа | | | | | |  | | |  | | | | | |  |
|  | | | | | |  | | | Определить: | | | | | |  |
|  | | | | | | | | | | | | | | | |
| (Один из) | | Случайная  | | | | | (указать типы угрозы) | | | | | | | | |
|  | | | | | | | | | | | | | | | |
| Отказ аппаратуры | | | | | |  | | |  | | | | | |  |
| Отказ ПО | | | | | |  | | | Определить: | | | | | |  |
| Отказ связи | | | | | |  | | | Потеря существенных сервисов | | | | | |  |
| Отказ электропитания | | | | | |  | | | Недостаточное кадровое обеспечение | | | | | |  |
| Природные явления | | | | | |  | | | Другие случаи | | | | | |  |
|  | | | | | | | | | Определить: | | | | | | |
|  | | | | | | | | | | | | | | | |
| (Один из) | | Ошибка  | | | | | (указать типы угрозы) | | | | | | | | |
|  | | | | | | | | | | | | | | | |
| Операционная ошибка | | | | | |  | | | Ошибка пользователя | | | | |  | |
| Ошибка аппаратной поддержки | | | | | |  | | | Ошибка конструкции | | | | |  | |
| Ошибка поддержки ПО | | | | | |  | | | Другие случаи (включая истинные заблуждения) | | | | |  | |
|  | | | | | | | | | Определить: | | | | | | |
|  | | | | | | | | | | | | | | | |
| Неизвестно  | | | | | |  | | | (Если еще не установлен тип инцидента (намеренный, случайный, ошибка), то следует отметить квадрат «неизвестно» и, по возможности, указать тип угрозы, используя сокращения, приведенные выше) | | | | | | |
|  | | | | | | | | | Определить: | | | | | | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | |  | | | |  | | | | | |  |
| Пораженные активы | | | | | | | | | | | | | |
| Пораженные активы (если есть) | | (Дать описания активов, пораженных инцидентом, или связанных с ним, включая серийные, лицензионные номера и номера версий, по возможности) | | | | | | | | | | | |
|  | | | | | | | | | | | | | |
|  | Информация/Данные | | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | | | | | |
|  | Аппаратура | | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | | | | | |
|  | Программное обеспечение | | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | | | | | |
|  | Средства связи | | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | | | | | |
|  | Документация | | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | | | | | |
|  | | | | | | | | | | | | | |
| Негативное воздействие/влияние инцидента на бизнес | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | |
| Отметить соответствующие квадраты для указанных ниже нарушений, затем в колонке «значимость» указать уровень негативного воздействия на бизнес по шкале 110, используя сокращения (указатели категорий): (КИ) - коммерческие и экономические интересы, (ПД) – информация, содержащая персональные данные, (ПО) – правовые и нормативные обязательства, (БО) – менеджмент и бизнес-операции, (ПП) – потеря престижа Запишите кодовые буквы в колонке «указатели», а если известны действительные стоимости, то указать их в колонке «стоимость» | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | |
|  | | | | | Значимость | | | | Указатели | | | Стоимость | |
|  | | | | |  | | | |  | | |  | |
| Нарушение конфиденциальности  (т. е., несанкционированное раскрытие) | | | |  |  | | | | |  | |  | |
| Нарушение целостности  (т. е., несанкционированная модификация) | | | |  |  | | | | |  | |  | |
| Нарушение доступности  (т. е., недоступность) | | | |  |  | | | | |  | |  | |
| Нарушение отказоустойчивости | | | |  |  | | | |  | | |  | |
| Уничтожение | | | |  |  | | | |  | | |  | |
|  | | | | | | | | | | | | | |
| Полные стоимости восстановления после инцидента | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | |
| (Где возможно, необходимо указать общие расходы на восстановление после инцидента в целом по шкале 110 для «значимости» и в деньгах для «стоимости») | | | | | Значимость | | | | | Указатели | | Стоимость | |
|  | | |  | | | | |  | | |  | | | |
|  | | |  | | | | |  | | |  | | | |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | |  | | | |  | |  | | |
| Устранение последствий инцидента | | | | | | | | | | |
| Дата начала расследования инцидента | | | | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | |
| Фамилия лица (лиц), проводившего (их) расследование инцидента | | | | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | |
| Дата окончания инцидента | | | | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | |
| Дата окончания воздействия | | | | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | |
| Дата завершения расследования инцидента | | | | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | |
| Ссылка и место хранения отчета о расследовании | | | | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | |
|  | | | | | | | | | | |
| Причастные лица | | | | | | | | | | |
|  | | | | | | | | | | |
| (Один из) | Лицо | | |  | | Легально учрежденная организация/учреждение | | | |  |
| Организованная группа | | | |  | | Случайность | | | |  |
|  | | | |  | | Нет виновного  Например, природные факторы, отказ оборудования, ошибка человека | | | |  |
|  | | | | | | | | | | |
| Описание нарушителя | | | | | | | | | | |
|  | | | | | | | | | | |
| Действительная или предполагаемая мотивация | | | | | | | | | | |
|  | | | | | | | | | | |
| (Один из) | Криминальная/финансовая выгода | |  | | | Развлечение/хакерство | | |  | |
| Политика/Терроризм | | |  | | | Реванш | | |  | |
|  | | |  | | | Другие мотивы | | |  | |
|  | | |  | | | Определить: | | |  | |
|  | | | | | | | | | | |
| Действия, предпринятые для разрешения инцидента | | | | | | | | | | |
|  | | | | | | | | | | |
| (например, «никаких действий», «подручными средствами», «внутреннее расследование», «внешнее расследование с привлечением…») | | |  | | | | | | | |
|  | | | | | | | | | | |
| Действия, запланированные для разрешения инцидента | | | | | | | | | | |
|  | | | | | | | | | | |
| (например, см. выше) | | | | |  | | | | | |
|  | | | | | | | | | | |
| Прочие действия | | | | | | | | | | |
|  | | | | | | | | | | |
| (например, по-прежнему требуется проведение расследования для другого персонала) | | | | |  | | | | | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Заключение | | | | | | | | | | | | | | |
| (Отметить один из квадратов, является ли инцидент значительным или нет и добавить в краткое объяснение для обоснования этого заключения) | | | | | | | Значительный  | | | | | Незначительный  | | |
|  | | | | | | | | | | | | | | |
| (Укажите любые другие заключения) | | | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | | | | | | |
|  | | | | | | | | | | | | | | |
| Ознакомленные лица/субъекты | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | |
| (Эта часть отчета заполняется соответствующим лицом, на которое возложены обязанности в области ИБ и которое формулирует требуемые действия | | Администратор ИБ | | | | | |  | Руководитель организации | | | | |  |
| Руководитель подразделения (уточнить какого) | | | | | |  | Специалист УИТ “Адилет сот” | | | | |  |
| Автор отчета | | | | | |  | Начальник отдела кадров | | | | |  |
| Полиция | | | | | |  | Другое лица | | | | |  |
|  | | | | | | | | | (например, служба охраны, регулятивного органа, сторонняя организация) | | | | | |
|  | | | | | | | | | Определить: | | | | | |
|  | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | |
| Привлеченные лица | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | |
| Инициатор | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | | | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | |
|  | | | | | | | | | | | | | | |
| Подпись | \_\_\_\_\_\_\_\_\_\_\_\_\_ | | | Подпись | \_\_\_\_\_\_\_\_\_\_\_\_ | | | | | Подпись | | | \_\_\_\_\_\_\_\_\_\_\_\_\_ | |
| Фамилия | \_\_\_\_\_\_\_\_\_\_\_\_\_ | | | Фамилия | \_\_\_\_\_\_\_\_\_\_\_\_ | | | | | Фамилия | | | \_\_\_\_\_\_\_\_\_\_\_\_\_ | |
| Роль | \_\_\_\_\_\_\_\_\_\_\_\_\_ | | | Роль | \_\_\_\_\_\_\_\_\_\_\_\_ | | | | | Роль | | | \_\_\_\_\_\_\_\_\_\_\_\_\_ | |
| Дата | \_\_\_\_\_\_\_\_\_\_\_\_\_ | | | Дата | \_\_\_\_\_\_\_\_\_\_\_\_ | | | | | Дата | | | \_\_\_\_\_\_\_\_\_\_\_\_\_ | |
|  | | | | | | | | | | | | | | |

Приложение № 37

к приказу № \_\_\_\_\_

от «\_\_\_\_»\_\_\_\_\_\_\_\_2018г.

**Приложение 14**

к положению об обработке

персональных данных

в Судебной системе

Директору Судебного департамента при ВС КР

Ибраимову Р. И.

**Заявление-согласие**

**субъекта на обработку его персональных данных**

Я, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

(Ф.И.О. полностью)

паспорт серии \_\_\_\_\_\_\_\_, номер \_\_\_\_\_\_\_\_\_\_\_\_, выданный \_\_\_\_\_\_ «\_\_\_» \_\_\_\_\_\_\_\_ \_\_\_\_ г.,

зарегистрированный (ая) по адресу: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

даю согласие на автоматизированную, а также без использования средств автоматизации обработку моих персональных данных, а именно:

фамилия, имя, отчество; дата рождения; место рождения; адрес; семейное, социальное и имущественное положение; образование и специальность; профессия; должность; заработная плата (оклад, премии, надбавки); номера банковских расчетных счетов; сведения о социальных льготах; судимости и/или наличие обязательств по исполнительным листам; паспортные данные; ИНН; информация о воинской обязанности; данные страхового полиса обязательного медицинского страхования; данные страхового полиса обязательного пенсионного страхования; трудовой и общий стаж; данные о предыдущих местах работы; фотография; адрес электронной почты; телефон (домашний, сотовый); фамилия, имя отчество, дата рождения детей; для обработки с целью: соблюдения [трудового законодательств](consultantplus://offline/ref=BDA114E1AC23957EA1860DC1DF83593437700436B8B557AC6EFD59CB14E364571F3BD3412F88A329GF21L)а КР, законодательства КР об охране труда и техники безопасности, законодательства КР об охране здоровья.

Перечень действий с персональными данными, на совершение которых дается согласие: сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение.

Я утверждаю, что ознакомлен с документами, устанавливающими порядок обработки персональных данных, а также с моими правами и обязанностями в этой области.

Согласие вступает в силу со дня его подписания и действует в течение неопределенного срока. Согласие может быть отозвано мною в любое время на основании моего письменного заявления.

Об ответственности за достоверность представленных сведений предупрежден(а).

«\_\_\_» \_\_\_\_\_\_\_\_\_\_ 201\_\_ г. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(подпись)

Приложение № 37

к приказу № \_\_\_\_\_

от «\_\_\_\_»\_\_\_\_\_\_\_\_2018г.

**Приложение 15**

к положению об обработке

персональных данных

в Судебной системе

Директору Судебного департамента при ВС КР

Ибраимову Р. И.

**Заявление-согласие**

**субъекта на обработку его персональных данных**

Я, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

(Ф.И.О. полностью)

паспорт серии \_\_\_\_\_\_\_\_, номер \_\_\_\_\_\_\_\_\_\_\_\_, выданный \_\_\_\_\_\_ «\_\_\_» \_\_\_\_\_\_\_\_ \_\_\_\_ г.,

зарегистрированный (ая) по адресу: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

даю согласие на автоматизированную, а также без использования средств автоматизации обработку моих персональных данных, а именно: фамилия, имя, отчество; адрес; имущественное положение; номера банковских расчетных счетов; паспортные данные; ИНН; номер страхового полиса обязательного медицинского страхования; номер страхового полиса обязательного пенсионного страхования; для обработки с целью: заключения и исполнение договоров.

Перечень действий с персональными данными, на совершение которых дается согласие: сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение.

Я утверждаю, что ознакомлен с документами, устанавливающими порядок обработки персональных данных, а также с моими правами и обязанностями в этой области.

Согласие вступает в силу со дня его подписания и действует в течение неопределенного срока. Согласие может быть отозвано мною в любое время на основании моего письменного заявления.

Об ответственности за достоверность представленных сведений предупрежден(а).

«\_\_\_» \_\_\_\_\_\_\_\_\_\_ 201\_\_ г. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(подпись)

Приложение № 37

к приказу № \_\_\_\_\_

от «\_\_\_\_»\_\_\_\_\_\_\_\_2018г.

**Приложение 16**

к положению об обработке

персональных данных

в Судебной системе

Директору Судебного департамента при ВС КР

Ибраимову Р. И.

**Отзыв согласия на обработку персональных данных**

Я, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

(Ф.И.О. полностью)

паспорт серии \_\_\_\_\_\_\_\_, номер \_\_\_\_\_\_\_\_\_\_\_\_, выданный \_\_\_\_\_\_ «\_\_\_» \_\_\_\_\_\_\_\_ \_\_\_\_ г.,

зарегистрированный (ая) по адресу: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

Прошу Вас прекратить обработку моих персональных данных в связи с

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(указать причину)

начиная с «\_\_\_» \_\_\_\_\_\_\_\_\_\_ 201\_\_ г.

«\_\_\_» \_\_\_\_\_\_\_\_\_\_ 201\_\_ г. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(подпись)

Приложение № 37

к приказу № \_\_\_\_\_

от «\_\_\_\_»\_\_\_\_\_\_\_\_2018г.

**Приложение 17**

к положению об обработке

персональных данных

в Судебной системе

Директору Судебного департамента при ВС КР

Ибраимову Р. И.

**Заявление-согласие**

**субъекта на получение его персональных данных у третьей стороны**

Я, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

(Ф.И.О. полностью)

паспорт серии \_\_\_\_\_\_\_\_, номер \_\_\_\_\_\_\_\_\_\_\_\_, выданный \_\_\_\_\_\_ «\_\_\_» \_\_\_\_\_\_\_\_ \_\_\_\_ г.,

согласен/не согласен на получение моих персональных данных, а именно:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(указать состав персональных данных (Ф.И.О, паспортные данные, адрес и т.д.)

для обработки в целях \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ ,

(указать цели обработки)

у следующих лиц \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(указать Ф.И.О. физического лица или наименование организации, которым сообщаются данные)

Я также утверждаю, что ознакомлен с возможными последствиями моего отказа дать письменное согласие на их получение.

«\_\_\_» \_\_\_\_\_\_\_\_\_\_ 201\_\_ г. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(подпись)

Приложение № 35

к приказу № \_\_\_\_\_

от «\_\_\_\_»\_\_\_\_\_\_\_\_2018г.

**Приложение 18**

к положению об обработке

персональных данных

в Судебной системе

**Перечень помещений, в которых обрабатываются персональные данные в Судебной системе**

|  |  |  |
| --- | --- | --- |
| № | Название помещения | Расположение помещения |
|
| 1 |  |  |
| 2 |  |  |
| 3 |  |  |

Приложение № 37

к приказу № \_\_\_\_\_

от «\_\_\_\_»\_\_\_\_\_\_\_\_2018г.

**Приложение 19**

к положению об обработке

персональных данных

в Судебной системе

**Заявка №**\_\_\_\_\_\_\_\_\_

**на предоставление доступа внутренних пользователей к информационным, программным и аппаратным ресурсам Судебной системы**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Фамилия И.О. сотрудника,  (таб. номер),  должность | № каб.,  Телефон (вн.) | Обоснование необходимости проведения указанного вида работ в соответствии с должностными обязанностями сотрудника | Ресурс  (согласно Перечню) | Режим доступа  (открыть/закрыть: чт/зап; просмотр, ввод, корр., распеч.) | Период действия (постоянно или указать интервал дат) |
| 1 | 2 | 3 | 4 | 5 | 6 |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Начальник \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(Наименование подразделения/отдела)

«\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_\_г \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_

Фамилия, инициалы подпись

Согласовано:

Управляющий УИТ “Адилет сот”:

«\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_\_г \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_

Фамилия, инициалы подпись