|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  | УТВЕРЖДАЮ | |
| Руководитель | | | | | |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ ФИО | | | | | |
| **№** | **от** | **«** | **»** | **20** | **г.** |

Политика информационной безопасности

Город, 20\_\_ г.

1. **Оглавление**
2. Общее положение [4](#_bookmark0)
3. [Обозначения и сокращения 5](#_bookmark1)
4. [Термины и определения 6](#_bookmark2)
5. [Цель 9](#_bookmark3)
6. [Основания для разработки 10](#_bookmark4)
7. [Область действия 11](#_bookmark5)
8. [Содержание политики 12](#_bookmark6)
   1. [Система управления информационной безопасностью 12](#_bookmark7)
      1. [Структура документов 12](#_bookmark8)
      2. [Ответственность за обеспечение ИБ 1](#_bookmark9)2
   2. [Объект защиты 14](#_bookmark10)
      1. [Ответственность за ресурсы 14](#_bookmark11)
      2. [Классификация информации 14](#_bookmark12)
   3. [Оценка и обработка рисков 15](#_bookmark13)
   4. [Безопасность персонала 16](#_bookmark14)
      1. [Условия найма 16](#_bookmark15)
      2. [Ответственность руководства 16](#_bookmark16)
      3. [Обучение ИБ 16](#_bookmark17)
      4. [Завершение или изменения трудовых отношений 16](#_bookmark18)
   5. [Физическая безопасность 17](#_bookmark19)
      1. [Защищённые области 17](#_bookmark20)
      2. [Области общего доступа 17](#_bookmark21)
      3. [Вспомогательные службы 17](#_bookmark22)
      4. [Утилизация или повторное использование оборудования 17](#_bookmark23)
      5. [Перемещение имущества 17](#_bookmark24)
   6. [Контроль доступа 18](#_bookmark25)
      1. [Управление привилегиями 19](#_bookmark26)
      2. [Управление паролями](#_bookmark27) 19
      3. [Контроль прав доступа 20](#_bookmark28)
      4. [Использование паролей 21](#_bookmark29)
      5. [Пользовательское оборудование, оставляемое без присмотра 2](#_bookmark30)1
      6. [Политика чистого стола 2](#_bookmark31)1
   7. [Политика допустимого использования информационных ресурсов 2](#_bookmark33)2
      1. [Использование АРМ и ИС 2](#_bookmark34)2
      2. [Использование ресурсов локальной сети 2](#_bookmark35)2
      3. [Обработка конфиденциальной информации 2](#_bookmark36)3
      4. [Использование электронной почты 2](#_bookmark37)3
      5. [Работа в сети](#_bookmark38) 24
      6. [Защита от вредоносного ПО](#_bookmark40) 25
   8. [Приобретение, Разработка и обслуживание систем](#_bookmark41) 26
      1. [Требования безопасности для информационных систем](#_bookmark42) 26
      2. [Корректная обработка информации](#_bookmark43) 26
      3. [Криптографические средства](#_bookmark44) 26
      4. [Безопасность системных файлов](#_bookmark45) 27
      5. [Безопасность процесса разработки и обслуживания систем](#_bookmark46) 27
   9. [Управление инцидентами информационной безопасности](#_bookmark47) 28
   10. [Управление непрерывностью и восстановлением](#_bookmark48) 29
   11. [Соблюдение требований законодательства](#_bookmark49) 30
   12. [Аудит информационной безопасности](#_bookmark50) 31
   13. [Предоставление услуг сторонним организациям](#_bookmark51) 32
       1. [Соглашения о предоставлении услуг](#_bookmark52) 32
       2. [Анализ предоставления услуг](#_bookmark53) 32
       3. [Приёмка систем](#_bookmark54) 32
9. [Ответственность](#_bookmark55) 33
10. [Контроль и пересмотр](#_bookmark56) 34
11. [История изменений](#_bookmark57) 35

# Общее положение

Настоящая Политика информационной безопасности (далее – Политика) является основополагающим документом, предназначенным для выражения позиции ОРГАНИЗАЦИИ (далее – Сокращение) в области информационной безопасности и определяет систему взглядов на проблему обеспечения информационной (далее – ИБ). Представляет собой систематизированное изложение высокоуровневых целей и задач защиты, которыми необходимо руководствоваться в своей деятельности.

Обеспечение информационной безопасности включает в себя любую деятельность, направленную на защиту информационных ресурсов и/или поддерживающей инфраструктуры. Политика охватывает все автоматизированные и телекоммуникационные системы, владельцем и пользователем которых является Учреждение.

Настоящая Политика разработата в соответствии с требованиями законодательства Российской федерации в области информационной безопасности, с учетом применимых международных стандартов, передового опыта и лучших практик.

Реализация Политики должна исходить из предпосылки, что невозможно обеспечить требуемый уровень защищённости информационных ресурсов не только с помощью отдельного средства, но и с помощью их простой совокупности. Необходимо их системное, согласованное между собой применение, а отдельные разрабатываемые элементы информационной системы должны рассматриваться как часть единой информационной системы в защищённом исполнении при оптимальном соотношении технических и организационных мероприятий.

Настоящая Политика обязательна для исполнения всеми сотрудниками и руководством Учреждения, а также пользователями его информационных ресурсов. и является локальным нормативным документом постоянного действия первого уровня. Регламенты и дополнительные политики направленные на обеспечение информационной безопасности не должны противоречить документу первого уровня, обязательны для исполнения всеми сотрудниками и руководством Учреждения, а также пользователями его информационных ресурсов. и являются локальным нормативным документом постоянного действия второго уровня.

Настоящая Политика утверждается, изменяется и признается утратившей силу в соотвествиии с приказом Директора.

# Обозначения и сокращения

|  |  |
| --- | --- |
| АРМ | Автоматизированное рабочее место |
| АС | Автоматизированная система |
| ИБ | Информационная безопасность |
| ИР | Информационный ресурс |
| ИС | Информационная система |
| ИТ | Информационные технологии |
| НСД | Несанкционированный доступ |
| ОКЗ | Орган криптографической защиты |
| ПО | Программное обеспечение |
| СКЗИ | Средство криптографической защиты информации |
| СУИБ | Система управления информационной безопасностью |

# Термины и определения

**Автоматизированная система** – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

**Авторизация** – предоставление субъекту прав на доступ, а также предоставление доступа в соответствии с установленными правами на доступ.

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

**Безопасность информации** – защищённость информации от её нежелательного разглашения (нарушения конфиденциальности), искажения (нарушения целостности), утраты или снижения степени доступности, а также незаконного её тиражирования.

**Бизнес-процесс** – последовательность технологически связанных операций по предоставлению продуктов, услуг и/или осуществлению конкретного вида деятельности Учреждения.

**Владелец актива** – физическое или юридическое лицо, которое наделено административной ответственностью за руководство изготовлением, разработкой, хранением, использованием и безопасностью актива. Термин «владелец» не означает, что этот человек фактически имеет право собственности на этот актив.

**Владелец информационных ресурсов, информационных систем, технологий и средств их обеспечения** – субъект, осуществляющий владение и пользование указанными объектами и реализующий полномочия распоряжения в пределах, установленных законом.

**Документ** – зафиксированная на материальном носителе информация с реквизитами, позволяющими её идентифицировать.

**Доступность информации** – состояние, характеризуемое способностью ИС обеспечивать беспрепятственный доступ к информации субъектов, имеющих на это полномочия.

**Защита информации** – деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию и средства доступа к ней.

**Идентификация –** присвоение субъектам доступа, объектам доступа идентификаторов (уникальных имен) и (или) сравнение предъявленного идентификатора с перечнем присвоенных идентификаторов.

**Информация** – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

**Информационная безопасность (ИБ)** – состояние защищённости интересов Учреждения.

**Информационная система** – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

**Информационный процесс** – процессы сбора, обработки, накопления, хранения, поиска и распространения информации.

**Информационный ресурс (актив)** – всё, что имеет ценность и находится в распоряжении Учреждения.

**Инцидент** – непредвиденное или нежелательное событие (группа событий) безопасности, которое привело (могут привести) к нарушению функционирования информационной системы или возникновению угроз безопасности информации (нарушению конфиденциальности, целостности, доступности).

**Инцидент информационной безопасности** – одно или серия нежелательных или неожиданных событий ИБ, имеющих значительную вероятность нарушения бизнес-процессов или представляющих угрозу ИБ.

**Контролируемая зона** – пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание лиц, а также транспортных, технических или иных средств.

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

**Конфиденциальность информации** – состояние защищённости информации, характеризуемое способностью ИС обеспечивать сохранение в тайне информации от субъектов, не имеющих полномочий на ознакомление с ней.

**Несанкционированный доступ** – доступ к информации иди действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

**Обработка риска** – процесс выбора и реализации мер по модификации (снижению) риска.

**Политика** – общие цели и указания, формально выраженные руководством.

**Привилегии** – это права доверенного объекта на совершение каких-либо действий по отношению к объектам системы.

**Риск** – сочетание вероятности события и его последствий.

**Система управления информационной безопасностью (СУИБ)** – часть системы управления, основанная на оценке рисков, предназначенная для создания, внедрения, эксплуатации, мониторинга, анализа, сопровождения и совершенствования ИБ.

**Собственник информационных ресурсов, информационных систем, технологий и средств их обеспечения** – субъект, в полном объёме реализующий полномочия владения, пользования, распоряжения указанными объектами.

**События информационной безопасности** – идентифицированное состояние системы, сервиса или сети, свидетельствующее о возможном нарушении политики безопасности или отсутствии механизмов защиты, либо прежде неизвестная ситуация, которая может иметь отношение к безопасности.

**Угроза** – Опасность, предполагающая возможность потерь (ущерба).

**Целостность информации** – устойчивость информации к несанкционированному доступу или случайному воздействию на неё в процессе обработки техническими средствами, результатом которого может быть уничтожение и искажение информации.

# Цель

Основной целью, на достижение которой направлены все положения настоящей Политики, является защита информационных ресурсов от возможного нанесения им материального, физического, морального или иного ущерба, посредством случайного или преднамеренного воздействия на информацию, её носители, процессы обработки и передачи, а также минимизация рисков ИБ.

Для достижения основной цели необходимо обеспечивать эффективное решение следующих задач:

* своевременное выявление, оценка и прогнозирование источников угроз ИБ;
* создание механизма оперативного реагирования на угрозы ИБ;
* предотвращение и/или снижение ущерба от реализации угроз ИБ;
* защита от вмешательства в процесс функционирования ИС посторонних лиц;
* соответствие требованиям Федерального законодательства, нормативно- методических документов ФСБ России, ФСТЭК России и договорным обязательствам в части ИБ;
* обеспечение непрерывности критических бизнес-процессов;
* достижение адекватности мер по защите от угроз ИБ;
* выявление, предупреждение и пресечение возможной противоправной и иной негативной деятельности сотрудников;
* повышение деловой репутации и корпоративной культуры.

# Основания для разработки

Настоящая политика разработана на основе требований законодательства Российской Федерации, накопленного в Учреждении опыта в области обеспечения ИБ, интересов и целей Учреждения.

При написании отдельных положений настоящей политики использовались следующие нормативные документы:

* ГОСТ Р ИСО/МЭК 27001 «Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности»;
* РС БР ИББС-2.0-2007 «Методические рекомендации по документации в области обеспечения информационной безопасности…»;
* РС БР ИББС-2.2-2009 «Методика оценки рисков нарушения информационной безопасности»;
* РС БР ИББС-2.5-2014 «Менеджмент инцидентов информационной безопасности»;
* Федеральный закон «Об информации, информационных технологиях и защите информации» от 27.07.2006 № 149-ФЗ;
* Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ;
* Федеральный закон «О коммерческой тайне» от 29.07.2004 № 98-ФЗ.

# Область действия

Настоящая Политика распространяется на все бизнес-процессы Учреждения и обязательна для применения всеми сотрудниками и руководством Учреждения, а также пользователями его информационных ресурсов.

Настоящая политика распространяется на информационные системы учреждения.

Лица, осуществляющие разработку внутренних документов Учреждения, регламентирующих вопросы информационной безопасности, обязаны руководствоваться настоящей Политикой.

# Содержание политики

## Система управления информационной безопасностью

Для достижения указанных целей и задач в Учреждении внедряется система управления информационной безопасностью. Документированные требования СУИБ доводятся до сведения работников Учреждения.

Средства управления информационной безопасностью внедряются по результатам проведения оценки рисков информационной безопасности. Стоимость внедряемых средств управления информационной безопасностью не должна превышать возможный ущерб, возникающий при реализации угроз.

### Структура документов

В целях создания взаимосвязанной структуры нормативных документов Учреждения в области обеспечения информационной безопасности, разрабатываемые и обновляемые нормативные документы должны соответствовать следующей иерархии:

1. Настоящая Политика является внутренним нормативным документом по ИБ **первого уровня**.
2. Документы **второго уровня** – инструкции, порядки, регламенты и прочие документы, описывающие действия сотрудников Учреждения по реализации документов первого и второго уровня.
3. Документы **третьего уровня** – отчётные документы о выполнении требований документов верхних уровней.

### Ответственность за обеспечение ИБ

Для непосредственной организации и эффективного функционирования системы обеспечения информационной безопасности в Учреждении функции обеспечения ИБ возложены на отдел информационной безопасности. На это подразделение возлагается решение следующих основных задач:

* проведение в жизнь Политики ИБ;
* определение требований к защите информации;
* организация мероприятий и координация работ всех подразделений по вопросам комплексной защиты информации;
* контроль и оценка эффективности принятых мер и применяемых средств защиты;
* оказание методической помощи сотрудникам в вопросах обеспечения информационной безопасности;
* регулярная оценка и управление рисками информационной безопасности в соответствии с установленными процедурами в области управления рисками;
* выбор и внедрение средств защиты информации, включая организационные, физические, технические, программные и программно-аппаратные средства обеспечения СУИБ;
* обеспечение минимально-необходимого доступа к информационным ресурсам, основываясь на требованиях бизнес-процессов;
* информирование, обучение и повышение квалификации работников Учреждения в сфере информационной безопасности;
* расследования инцидентов информационной безопасности;
* сбор, накопление, систематизация и обработка информации по вопросам информационной безопасности;

Для решения задач, возложенных на отдел информационной безопасности, его сотрудники имеют следующие права:

* определять необходимость и разрабатывать нормативные документы, касающиеся вопросов обеспечения безопасности информации, включая документы, регламентирующие деятельность пользователей информационной системы в указанной области;
* получать информацию от пользователей информационных систем Учреждения по любым аспектам применения информационных технологий в Учреждении;
* участвовать в проработке технических решений по вопросам обеспечения безопасности информации при проектировании и разработке новых информационных технологий;
* участвовать в испытаниях разработанных информационных технологий по вопросам оценки качества реализации требований по обеспечению безопасности информации;
* контролировать деятельность пользователей по вопросам обеспечения ИБ;
* готовить предложения руководству по обеспечению требований ИБ.

## Объект защиты

### Ответственность за ресурсы

В учреждении должны быть выявлены и оценены с точки зрения их важности все ресурсы. Для всех ценных ресурсов должен быть составлен реестр (перечень). Благодаря информации о ресурсах Учреждения реализуется защита информации, степень которой соразмерна ценности и важности ресурсов.

В ИС Учреждения присутствуют следующие типы ресурсов:

* информационные ресурсы, содержащие конфиденциальную информацию, и/или сведения ограниченного доступа, в том числе информацию о финансовой деятельности Учреждения;
* открыто распространяемая информация, необходимая для работы Учреждения, независимо от формы и вида её представления;
* информационная инфраструктура, включая системы обработки и анализа информации, технические и программные средства её обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены такие системы.

Для каждого ресурса должен быть назначен владелец, который отвечает за соответствующую классификацию информации и ресурсов, связанных со средствами обработки информации, а также за назначение и периодическую проверку прав доступа и категорий, определённых политиками управления доступа.

### Классификация информации

Все информационные ресурсы, подлежащие защите, должны быть классифицированы в соответствии с важностью и степенью доступа. Классификация информации должна быть документирована и утверждена отделом информационной безопасности. Классификация информации должна проводиться владельцем ресурса, хранящего или обрабатывающего информацию, для определения категории ресурса. Периодически классификация должна пересматриваться для поддержания актуальности её соответствия с категорией ресурса. Ресурсы, содержащие конфиденциальную или критичную информацию, должны иметь соответствующую пометку (гриф).

## Оценка и обработка рисков

В учреждении должны быть определены требования к безопасности путём методической оценки рисков. Оценки рисков должны выявить, определить количество и расположить по приоритетам риски в соответствии с критериями принятия рисков и бизнес-целями учреждения. Результаты оценки должны определять соответствующую реакцию руководства, приоритеты управления рисками ИБ и набор механизмов контроля для защиты от этих рисков.

Оценка рисков и выбор механизмов контроля должны производиться периодически, чтобы:

* учесть изменения бизнес-требований и приоритетов;
* принять во внимание новые угрозы и уязвимости;
* убедиться в том, что реализованные средства сохранили свою эффективность.

Перед обработкой каждого риска Учреждение должно выбрать критерии для определения возможности принятия этого риска. Риск может быть принят, если его величина достаточно мала и стоимость обработки нерентабельна для Учреждения. Такие решения должны регистрироваться.

Для каждого из оцененных рисков должно приниматься одно из решений по его обработке:

* применение соответствующих механизмов контроля для уменьшения величины риска до приемлемого уровня;
* сознательное и объективное принятие риска, если он точно удовлетворяет Политике Учреждения и критериям принятия рисков;
* уклонение от риска путём недопущения действий, могущих быть его причиной;
* передача рисков другой стороне (аутсорсинг, страхование и т.п.).

## Безопасность персонала

Роли и обязанности по обеспечению безопасности информационных ресурсов, описанные в соответствии с Политикой ИБ Учреждения, должны быть доведены до сотрудника при трудоустройстве и внесены в его должностные обязанности. Сюда должны входить как общие обязанности по реализации и поддержке политики безопасности, так и конкретные обязанности по защите ресурсов и по выполнению конкретных операций, связанных с безопасностью.

### Условия найма

В договор должно быть включено согласие сотрудника на проведение контрольных мероприятий со стороны Учреждения по проверке выполнения требований ИБ, а также обязательства по неразглашению конфиденциальной информации. В договоре должны быть описаны меры, которые будут приняты в случае несоблюдения сотрудником требований ИБ.

При предоставлении сотруднику доступа к ИС Учреждения он должен ознакомиться под роспись с инструкцией пользователя ИС.

### Ответственность руководства

Руководство Учреждения должно требовать от всех сотрудников, подрядчиков и пользователей сторонних организаций принятия мер безопасности в соответствии с установленными в Учреждении политиками и процедурами.

Сотрудники отдела информационной безопасности имеют право в установленном порядке, без уведомления пользователей, производить проверки:

* Выполнения действующих инструкций по вопросам ИБ;
* Данных, находящихся на носителях информации;
* Порядка использования сотрудниками информационных ресурсов;
* Содержания служебной переписки.

### Обучение ИБ

Все сотрудники должны проходить периодическую подготовку в области политики и процедур ИБ, принятых в Учреждении.

### Завершение или изменения трудовых отношений

При увольнении все предоставленные сотруднику права доступа к ресурсам ИС должны быть удалены. При изменении трудовых отношений удаляются только те права, необходимость в которых отсутствует в новых отношениях.

## Физическая безопасность

### Защищённые области

Средства обработки информации, поддерживающие критически важные и уязвимые ресурсы Учреждения, должны быть размещены в защищённых областях. Защищённые области должны обеспечиваться соответствующими средствами контроля доступа, обеспечивающим возможность доступа только авторизованного персонала.

Для хранения служебных документов и машинных носителей с защищаемой информацией помещения должны снабжаться сейфами, металлическими шкафами или шкафами, оборудованными замком.

### Вспомогательные службы

Все вспомогательные службы, такие как электропитание, водоснабжение, канализация, отопление, вентиляция и кондиционирование воздуха должны обеспечивать гарантированную и устойчивую работоспособность компонентов ИС Учреждения.

### Утилизация или повторное использование оборудования

Со всех носителей информации, должны гарантированно удаляться все конфиденциальные данные и лицензионное ПО. Отсутствие защищаемой информации на носителях должно быть проверено отделом информационной безопасности, о чём должна быть сделана отметка в акте списания.

### Перемещение имущества

Оборудование, информация или ПО должны перемещаться за пределы Учреждения только при наличии письменного разрешения руководства. Сотрудники, имеющие право перемещать оборудование и носители информации за пределы Учреждения должны быть чётко определены. Время перемещения оборудования за пределы Учреждения и время его возврата должны регистрироваться.

## Контроль доступа

Основными пользователями информации в информационной системе Учреждения являются сотрудники структурных подразделений. Уровень полномочий каждого пользователя минимальны и определяются индивидуально. Каждый сотрудник пользуется только предписанными ему правами по отношению к информации, с которой ему необходимо работать в соответствии с должностными обязанностями.

Допуск пользователей к работе с информационными ресурсами должен быть строго регламентирован. Любые изменения состава и полномочий пользователей подсистем должны производиться в установленном порядке, согласно регламента предоставления доступа пользователей.

Временная учетная запись может быть заведена для пользователя на ограниченный срок для выполнения задач, требующих расширенных полномочий, или для проведения настройки, тестирования информационной системы, для организации гостевого доступа (посетителям, сотрудникам сторонних организаций, стажерам и иным пользователям с временным доступом к информационной системе).

В общем случае запрещено создавать и использовать общую пользовательскую учётную запись для группы пользователей.

Регистрируемые учётные записи подразделяются на:

* Пользовательские – предназначенные для аутентификации пользователей ИР Учреждения;
* Администраторские – используемые для администрирования инфраструктуры Учреждения;
* Служебные – предназначенные для функционирования отдельных процессов или приложений.

Администраторские учётные записи используются только для администраторов Учреждения.

Служебные учётные записи используются только для запуска и работы сервисов или приложений.

Использование администраторских или служебных учётных записей для регистрации пользователей в системе категорически запрещено.

Процедуры регистрации и блокирования учётных записей пользователей должны применяться с соблюдением следующих правил:

* использование уникальных идентификаторов (ID) пользователей для однозначного определения и сопоставления личности с совершёнными ей действиями;
* предоставление и блокирование прав должны быть санкционированы и документированы;
* предоставление прав доступа к ИР, только после согласования с владельцем данного ИР;
* уровень предоставленных полномочий должен соответствовать производственной необходимости и настоящей Политике и не ставить под угрозу разграничение режимов работы;
* согласование изменения прав доступа с отделом информационной безопасности;
* ознакомление пользователей под подпись с письменными документами, в которых регламентируются их права доступа;
* обеспечение создания и поддержания формального списка всех пользователей, зарегистрированных для работы с ИР или сервисом;
* немедленное удаление или блокирование прав доступа пользователей, сменивших должность, форму занятости или уволившихся из Учреждения;
* аудит ID и учетных записей пользователей на наличие неиспользуемых, их удаление и блокировка;
* обеспечить возможность предоставления пользователям доступа в соответствии с их должностями, основанными на производственных требованиях, путем суммирования некоторого числа прав доступа в типовые профили доступа пользователей.

### Управление привилегиями

Доступ сотрудника к информационным ресурсам Учреждения должен быть санкционирован руководителем структурного подразделения, в котором числится согласно штатному расписанию данный сотрудник, и владельцами соответствующих информационных ресурсов. Управление доступом осуществляется в соответствии с установленными процедурами.

Наделение привилегиями и их использование должно быть строго ограниченным и управляемым. Распределение привилегий должно управляться с помощью процесса регистрации этих привилегий.

Контроль и периодический пересмотр прав доступа пользователей к информационным ресурсам Учреждения осуществляется в процессе аудита ИБ в соответствии с Правилами аудита ИБ и установленными процедурами.

### Управление паролями

Пароли – средство проверки личности пользователя для доступа к ИС или сервису, обеспечивающее идентификацию и аутентификацию на основе сведений, известных только пользователю.

Предоставление паролей должно контролироваться посредством официальной процедуры, отвечающей следующим требованиям:

* при наличии возможности, необходимо настроить систему таким образом, чтобы при первом входе пользователя с назначенным ему временным паролем система сразу же требовала его сменить;
* временные пароли должны назначаться пользователю только после его идентификации;
* необходимо избегать передачи паролей с использованием третьих лиц или незашифрованной электронной почтой;
* временные пароли не должны быть угадываемыми и повторяющимися от пользователя к пользователю;
* пользователь должен подтвердить получение пароля;
* пароли должны храниться в электронном виде только в защищенной форме;
* назначенные производителем ПО пароли должны быть изменены сразу после завершения инсталляции;

### Использование паролей

Идентификатор и пароль пользователя в ИС являются учётными данными, на основании которых сотруднику Учреждения предоставляются права доступа, протоколируются производимые им в системе действия и обеспечивается режим конфиденциальности, обрабатываемой (создаваемой, передаваемой и хранимой) сотрудником информации. Не допускается использование различными пользователями одних и тех же учётных данных.

Первоначальное значение пароля учетной записи пользователя устанавливает Администратор безопасности.

Сотруднику запрещается:

* сообщать свой пароль кому-либо;
* указывать пароль в сообщениях электронной почты;
* хранить пароли, записанные на бумаге, в легко доступном месте;
* использовать тот же самый пароль, что и для других систем (например, домашний интернет провайдер, бесплатная электронная почта, форумы и т.п.);

Вход пользователя в систему не должен выполняться автоматически. Покидая рабочее место пользователь обязан заблокировать компьютер (используя комбинации Win + «L» или Ctrl + Alt + Delete → «Блокировать компьютер»).

Сотрудник обязан:

* в случае подозрения на то, что пароль стал кому-либо известен, поменять пароль и сообщить о факте компрометации сотруднику отдела информационной безопасности;
* немедленно сообщить сотруднику отдела информационной безопасности в случае получения от кого-либо просьбы сообщить пароль;
* менять пароль по требованию Администратора ИБ.

После 20 неудачных попыток ввода пароля учётная запись блокируется на 10 минут. При систематической блокировке учётной записи работником (более 3 раз) оповещается Администратор ИБ. Учреждение оставляет за собой право осуществлять периодическую проверку стойкости паролей пользователей, используемых сотрудниками для доступа к ИС

### Пользовательское оборудование, оставляемое без присмотра

Пользователи должны обеспечивать необходимую защиту оборудования, остающегося без присмотра. Все пользователи должны быть осведомлены о требованиях ИБ и правилах защиты остающегося без присмотра оборудования, а также о своих обязанностях по обеспечению этой защиты.

### Политика чистого стола

Сотрудники Учреждения обязаны:

* сохранять известные им пароли в тайне;
* закрывать активные сеансы по завершении работы, если только их нельзя защитить подходящим блокирующим механизмом, например, защищённый паролем хранитель экрана;
* по завершении сеанса выходить из системы у универсальных ЭВМ, серверов и офисных ПК.

Документы и носители с конфиденциальной информацией должны убираться в запираемые места (сейфы, шкафы и т.п.), особенно при уходе с рабочего места.

Компьютеры и терминалы должны быть оставлены в состоянии выполненного выхода из системы, когда они находятся без присмотра.

Вход пользователя в систему не должен выполняться автоматически. Покидая рабочее место пользователь обязан заблокировать компьютер (используя комбинации Win + «L» или Ctrl + Alt + Delete → «Блокировать компьютер»).

Документы, содержащие конфиденциальную информацию, должны изыматься из печатающих устройств немедленно.

По окончании рабочего дня и в случае длительного отсутствия на рабочем месте необходимо запирать на замок все шкафы и сейфы.

## Политика допустимого использования информационных ресурсов

Общие обязанности пользователя:

* при работе с ПО руководствоваться нормативной документацией (руководством пользователя);
* обращаться в службу поддержки пользователей или к специалистам, назначенными ответственными за системное администрирование и информационную безопасность, по всем техническим вопросам, связанным с работой в корпоративной ИС (подключение к корпоративной ИС/домену, инсталляция и настройка ПО, удаление вирусов, предоставление доступа в сеть Интернет и к внутренним сетевым ресурсам, ремонт и техническое обслуживание и т.п.), а также за необходимой методологической/консультационной помощью по вопросам применения технических и программных средств корпоративной ИС;
* знать признаки правильного функционирования установленных программных продуктов и средств защиты информации;
* минимизировать вывод на печать обрабатываемой информации.

Пользователю запрещено производить несанкционированное распространение справочной информации, которая становится доступна при подключении к корпоративной ИС Учреждения.

* + 1. **Использование ПО**

На АРМ Учреждения допускается использование только лицензионного программного обеспечения, утверждённого в перечне разрешённого программного обеспечения.

Запрещено незаконное хранение на жестких дисках АРМ Учреждения информации, являющейся объектом авторского права (ПО, фотографии, музыкальные файлы, игры, и т.д.).

Документы, подтверждающие покупку программного обеспечения, хранятся на протяжении всего времени использования лицензии, копии указанных документов вместе с лицензионными соглашениями на ПО, ключами защиты ПО и дистрибутивами хранятся в <название ответственного отдела>.

Пользователи АРМ не имеют права удалять, изменять, дополнять, обновлять программную конфигурацию на АРМ. Указанные работы, а так же работы по установке, регистрации и активации приобретённого лицензионного ПО могут быть выполнены только сотрудниками <название ответственного отдела>.

Сведения о вновь приобретённом программном обеспечении должны быть внесены в перечень разрешённого программного обеспечения.

* + 1. **Использование ресурсов локальной сети**

Для выполнения своих служебных обязанностей каждый сотрудник обеспечивается доступом к соответствующим информационным ресурсам. Информационными ресурсами являются каталоги и файлы, хранящиеся на дисках серверов Учреждения, базы данных, электронная почта. Основными рабочими каталогами являются личные каталоги сотрудников и каталоги подразделений, созданные в соответствии с особенностями их работы. Доступ сотрудников к ресурсам сети осуществляется согласно матрицы доступа.

* + 1. **Обработка конфиденциальной информации**

При обработке конфиденциальной информации сотрудники обязаны:

* знать и выполнять требования Инструкции по работе с конфиденциальной информацией;
* размещать экран монитора таким образом, чтобы исключить просмотр обрабатываемой информации посторонними лицами;
* не отправлять на печать конфиденциальные документы, если отсутствует возможность контроля вывода на печать и изъятия отпечатанных документов из принтера сразу по окончании печати;
* обязательно проверять адреса получателей электронной почты на предмет правильности их выбора;
* не запускать исполняемые файлы на съемных накопителях, полученные не из доверенного источника;
* не передавать конфиденциальную информацию по открытым каналам связи, кроме сетей корпоративной ИС;

не оставлять без личного присмотра на рабочем месте или где бы то ни было электронные носители информации (CD/DVD – диски, Flash – устройства и пр.), а также распечатки из принтера или бумажные копии документов, содержащие конфиденциальную информацию.

* + 1. **Использование электронной почты**

Электронная почта используется для обмена в рамках ИС Учреждения и общедоступных сетей информацией в виде электронных сообщений и документов в электронном виде. Для обеспечения функционирования электронной почты допускается применение ПО, входящего в реестр разрешённого к использованию ПО.

Каждый сотрудник Учреждения получает почтовый адрес вида [name@](mailto:name@er76.ru)stu.lipetsk.ru в домене Учреждения. Адрес электронной почты выдаётся сотрудником отдела ИБ при начальной регистрации пользователя в домене Учреждения.

Корпоративная электронная почта Учреждения предназначена исключительно для использования в служебных целях.

Функционирование электронной почты обеспечивается оборудованием, каналами связи и иными ресурсами, принадлежащими Учреждению. Все почтовые сообщения, переданные или принятые с использованием корпоративной электронной почты принадлежат Учреждению и являются неотъемлемой частью его производственного процесса.

Любые сообщения корпоративной электронной почты могут быть прочитаны, использованы в интересах Учреждения либо удалены уполномоченными сотрудниками Учреждения.

Пользователям корпоративной электронной почты Учреждения запрещено вести частную переписку с использованием средств корпоративной электронной почты Учреждения. К частной переписке относится переписка, не связанная с исполнением сотрудником своих должностных обязанностей.

Каждый сотрудник Учреждения имеет право на просмотр либо иное использование в интересах Учреждения сообщений корпоративной электронной почты, которые направлены или получены им, соответственно, с его или на его корпоративный электронный адрес.

Использование сообщений корпоративной электронной почты в интересах Учреждения, в том числе ознакомление с содержанием сообщений, осуществляется в соответствии с правами доступа к информации, установленными внутренними Положениями о конфиденциальной информации и иными правовыми актами, регламентирующими порядок обращения с информацией ограниченного доступа.

Исходящие электронные сообщения сотрудников Учреждения должны содержать следующие поля:

* адрес получателя;
* тема электронного сообщения;
* текст электронного сообщения (вложенные файлы);
* подпись отправителя;

Формат подписи отправителя:

*С уважением,*

*<Фамилия имя>*

*<Должность>*

*<Структурное подразделение>*

*<Наименование Учреждения>*

*<Адрес>*

*<номера контактов: телефон, мессенджеры, адреса электронной почты>*

*<сайт>*

При формировании ответов на полученные электронные сообщения можно использовать следующую упрощённую подпись:

*С уважением,*

*<Фамилия имя>*

*<Номера телефонов, мессенджеры, адреса электронной почты>*

Прекращение предоставления сотруднику Учреждения услуг электронной почты наступает при прекращении действия трудового договора (контракта) сотрудника.

* + 1. **Работа в сети**

Доступ к сети Интернет предоставляется сотрудникам Учреждения в целях выполнения ими своих служебных обязанностей, требующих непосредственного подключения к внешним информационным ресурсам.

Для доступа сотрудников Учреждения к сети Интернет допускается применение ПО, входящего в Реестр разрешённого к использованию ПО.

При использовании сети Интернет необходимо:

* соблюдать требования настоящей Политики;
* использовать сеть Интернет исключительно для выполнения своих служебных обязанностей;
* ставить в известность о любых фактах нарушения требований настоящей Политики;

При использовании сети Интернет запрещено:

* использовать предоставленный Учреждением доступ в сеть Интернет в личных целях;
* использовать несанкционированные аппаратные и программные средства, позволяющие получить несанкционированный доступ к сети Интернет;
* Совершать любые действия, направленные на нарушение нормального функционирования элементов ИС Учреждения.

Учреждение оставляет за собой 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 законодательством.

Блокирование и ограничение доступа пользователей к Интернет-ресурсам осуществляется на основе Регламента применения категорий Интернет-ресурсов.

Информация о посещаемых сотрудниками Учреждения Интернет-ресурсах протоколируется для последующего анализа и, при необходимости, может быть представлена Руководителям структурных подразделений, а также Руководству Учреждения для контроля.

Содержание Интернет-ресурсов, а также файлы, загружаемые из сети Интернет, подлежат обязательной проверке на отсутствие вредоносного ПО.

* + 1. **Защита от вредоносного ПО**

Отдел ИБ регулярно проверяет сетевые ресурсы Учреждения антивирусным программным обеспечением и обеспечивает защиту входящей электронной почты от проникновения вирусов и другого вредоносного ПО.

При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление о системных ошибках, увеличение исходящего/входящего трафика и т.п.) сотрудник Учреждения должен незамедлительно оповестить об этом отдел ИБ. После чего администратор ИБ должен провести внеочередную полную проверку на вирусы рабочей станции пользователя, проверив, в первую очередь, работоспособность антивирусного ПО.

В случае обнаружения при проведении антивирусной проверки заражённых компьютерными вирусами файлов сотрудники подразделений обязаны:

* приостановить работу;
* немедленно поставить в известность о факте обнаружения заражения своего руководителя и отдел ИБ, а также владельца файла и смежные подразделения, использующие эти файлы в работе.
* Совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования.

## Приобретение, Разработка и обслуживание систем

### Требования безопасности для информационных систем

При описании требований к созданию новых систем или к усовершенствованию существующих необходимо учитывать потребность в средствах обеспечения безопасности.

Требования к безопасности и средства защиты должны соответствовать ценности используемых ИР и потенциальному ущербу для Учреждения в случае сбоя или нарушения безопасности. Основой для анализа требований к безопасности и выбору мер для поддержки безопасности является оценка рисков и управление рисками.

Системные требования к ИБ и процессам, обеспечивающим защиту информации, должны быть включены на ранних стадиях проектирования ИС.

### Корректная обработка информации

Данные, вводимые в прикладные системы, необходимо проверять, чтобы гарантировать их правильность и соответствие поставленной задаче.

### Криптографические средства

Все, поступающие в Учреждение, СКЗИ должны быть учтены в соответствующем журнале поэкземплярного учёта СКЗИ.

В Учреждении должно осуществляться управление ключами для эффективного применения криптографических методов. Компрометация или потеря криптографических ключей может привести к нарушению конфиденциальности, подлинности и/или целостности информации.

Криптографические системы и методы следует использовать для защиты конфиденциальной информации, когда другие средства контроля не обеспечивают адекватной защиты.

Для критической информации должно использоваться шифрование при их хранении в базах данных или передаче по коммерческим или открытым сетям, таким как Интернет. Шифрование любой другой информации в ИС Учреждения должно осуществляться только после получения письменного разрешения на это.

#### Требований по обеспечению ИБ при использовании СКЗИ

Шифрование – это криптографический метод, который может использоваться для обеспечения защиты конфиденциальной, важной или критичной информации.

СКЗИ должны поставляться разработчиками с полным комплектом эксплуатационной документации, включающей описание ключевой системы, правила работы с ней и обоснование необходимого организационно-штатного обеспечения.

Для шифрования конфиденциальной информации минимально допустимой длинной ключа является 128 бит.

При использовании шифрования в ИС Учреждения должны применяться только утверждённые стандартные алгоритмы и сертифицированные ФСБ России продукты, их реализующие.

#### Электронные цифровые подписи

ЭЦП обеспечивают защиту аутентификации и целостности электронных документов.

ЭЦП могут применяться для любой формы документа, обрабатываемого электронным способом. ЭЦП должны быть реализованы при использовании криптографического метода, основывающегося на однозначно связанной паре ключей, где один ключ используется для создания подписи (секретный/личный ключ), а другой – для проверки подписи (открытый ключ).

Необходимо с особой тщательностью обеспечивать конфиденциальность личного ключа, который следует хранить в секрете, так как любой, имеющий к нему доступ, может подписывать документы (платежи, контракты), тем самым фальсифицируя подпись владельца ключа. Защиты целостности открытого ключа должна обеспечиваться при использовании сертификата открытого ключа.

Криптографические ключи, используемые для цифровых подписей, должны отличаться от тех, которые используются для шифрования.

При использовании ЭЦП, необходимо учитывать требования действующего законодательства Российской Федерации, определяющего условия, при которых цифровая подпись имеет юридическую силу.

### Безопасность системных файлов

Чтобы свести к минимуму риск повреждения ИС, в учреждении необходимо обеспечить контроль над внедрением ПО в рабочих системах.

Тестовые данные должны находиться под контролем и защитой. Для испытаний обычно требуются значительные объёмы тестовых данных, максимально близко соответствующие рабочим данным. Необходимо избегать использования рабочих баз данных, содержащих конфиденциальную информацию. Если эти базы всё же будут использоваться, то конфиденциальные данные должны быть удалены или изменены.

### Безопасность процесса разработки и обслуживания систем

Чтобы свести к минимуму вероятность повреждения ИС Учреждения, следует ввести строгий контроль над внесением изменений. Необходимо установить официальные правила внесения изменений. Эти правила должны гарантировать, что процедуры, связанные с безопасностью и контролем, не будут нарушены, что программисты, занимающиеся поддержкой, получат доступ только к тем частям системы, которые необходимы для их работы, и что для выполнения любого изменения требуется получить официальное разрешение и подтверждение.

После внесения изменений в ИС критичные для бизнес-процессов Учреждения приложения должны анализироваться и тестироваться, чтобы гарантировать отсутствие вредных последствий для безопасности Учреждения.

Следует препятствовать внесению изменений в пакеты ПО, за исключением необходимых изменений. Все изменения должны строго контролироваться.

## Управление инцидентами информационной безопасности

В Учреждении должна быть разработана и утверждена формальная процедура уведомления о происшествиях в области ИБ, а также процедура реагирования на такие происшествия, включающая в себя действия, которые должны выполняться при поступлении сообщений о происшествии.

Все сотрудники должны быть ознакомлены с процедурой уведомления, а в их обязанности должна входить максимально быстрая передача информации о происшествиях.

В дополнение к уведомлению о происшествиях ИБ и недостатках безопасности должен использоваться мониторинг систем, сообщений и уязвимостей для обнаружения инцидентов ИБ.

Цели управления инцидентами ИБ должны быть согласованы с руководством для учёта приоритетов Учреждения при обращении с инцидентами.

Необходимо создать механизмы, позволяющие оценивать и отслеживать типы инцидентов, их масштаб и связанные с ними затраты.

## Управление непрерывностью и восстановлением

Необходимо разработать контролируемый процесс для обеспечения и поддержки непрерывности бизнес-процессов Учреждения. Данный процесс должен объединять в себе основные элементы поддержки непрерывности бизнес-процессов.

В Учреждении должны быть разработаны и реализованы планы, которые позволят продолжить или восстановить операции и обеспечить требуемый уровень доступности информации в установленные сроки после прерывания или сбоя критически важных бизнес- процессов.

В каждом плане поддержки непрерывности бизнеса должны быть чётко указаны условия начала его исполнения и сотрудники, ответственные за выполнение каждого фрагмента плана. При появлении новых требований необходимо внести поправки в принятые планы действия в нештатных ситуациях.

Для каждого плана должен быть назначен определённый владелец. Правила действия в нештатных ситуациях, планы ручного аварийного восстановления и планы возобновления деятельности должны находиться в ведении владельцев соответствующих ресурсов или процессов, к которым они имеют отношение.

## Соблюдение требований законодательства

Все значимые требования, установленные действующим законодательством, подзаконными актами и договорными отношениями, а также подход Учреждения к обеспечению соответствия этим требованиям должны быть явным образом определены, документированы и поддерживаться в актуальном состоянии.

Необходимо соблюдение регламентированного процесса, предупреждающего нарушение целостности, достоверности и конфиденциальности ИР, содержащих персональные данные, начиная от стадии сбора и ввода данных до их хранения. Персональные данные конкретного сотрудника и процесс их обработки должен быть открытым для этого сотрудника.

В Учреждении должны быть внедрены соответствующие процедуры для обеспечения соблюдения законодательных ограничений, подзаконных актов и контрактных обязательств по использованию материалов, охраняемых авторским правом, а также по использованию лицензионного ПО.

Важная документация Учреждения должна быть защищена от утери, уничтожения и фальсификации в соответствии с требованиями законодательства, подзаконных актов, контрактных обязательств и бизнес-требований.

Система хранения и обработки должна обеспечивать чёткую идентификацию записей и их периода хранения в соответствии с требованиями законов и нормативных актов. Эта система должна иметь возможность уничтожения записей по истечении периода хранения, если эти записи больше не требуются Учреждению.

Криптографические средства должны использоваться в соответствии со всеми имеющимися соглашениями, законодательными и нормативными актами.

## Аудит информационной безопасности

Учреждение должно проводить внутренние проверки СУИБ через запланированные интервалы времени.

Основные цели проведения таких проверок:

* оценка текущего уровня защищённости ИС;
* выявление и локализация уязвимостей в системе защиты ИС;
* анализ рисков, связанных с возможностью осуществления угроз безопасности в отношении ИР;
* оценка соответствия ИС требованиям настоящей Политики;
* выработка рекомендаций по совершенствованию СУИБ за счёт внедрения новых и повышения эффективности существующих мер защиты информации.

В число задач, решаемых при проведении проверок и аудитов СУИБ, входят:

* сбор и анализ исходных данных об организационной и функциональной структуре ИС, необходимых для оценки состояния ИБ;
* анализ существующей политики безопасности и других организационно- распорядительных документов по защите информации на предмет их полноты и эффективности, а также формирование рекомендаций по их разработке (или доработке);
* технико-экономическое обоснование механизмов безопасности;
* проверка правильности подбора и настройки средств защиты информации, формирование предложений по использованию существующих и установке дополнительных средств защиты для повышения уровня надёжности и безопасности ИС;
* разбор инцидентов ИБ и минимизация возможного ущерба от их проявления.

Руководство и сотрудники Учреждения при проведении у них аудита СУИБ обязаны оказывать содействие аудиторам и предоставлять всю необходимую для проведения аудита информацию.

## Предоставление услуг сторонним организациям

### Соглашения о предоставлении услуг

В соглашения о предоставлении услуг сторонним организациям должны быть включены требования безопасности, описание, объёмы и характеристики качества предоставляемых услуг.

### Анализ предоставления услуг

Услуги, отчёты и записи, предоставляемые сторонним организациям, должны постоянно проверяться и анализироваться. В отношениях со сторонней организацией должны присутствовать следующие процессы:

* контроль объёма и качества услуг, оговоренных в соглашениях;
* предоставление сторонней организации информации об инцидентах ИБ, связанных с предоставляемыми услугами, и совместное изучение этой информации;
* анализ предоставленных сторонними организациями отчётов о предоставленных услугах;
* управление любыми обнаруженными проблемами.

### Приёмка систем

В учреждении должен быть разработан и утверждён порядок приёмки новых ИС, обновления и новых версий ПО.

# Ответственность

Директор Учреждения определяет приоритетные направления деятельности в области обеспечения ИБ, меры по реализации настоящей Политики, утверждает списки объектов и сведений, подлежащих защите, а также осуществляет общее руководство обеспечением ИБ Учреждения.

Ответственность за поддержание положений настоящей Политики в актуальном состоянии, создание, внедрение, координацию и внесение изменений в процессы СУИБ Учреждения лежит на руководстве отдела ИБ.

Все руководители несут прямую ответственность за реализацию Политики и её соблюдение персоналом в соответствующих подразделениях.

Работники Учреждения несут персональную ответственность за соблюдение требований документов СУИБ и обязаны сообщать обо всех выявленных нарушениях в области информационной безопасности в отдел ИБ.

В трудовых договорах и должностных инструкциях работников устанавливается ответственность за сохранность служебной информации, ставшей известной в силу выполнения своих обязанностей.

Руководство Учреждения регулярно проводит совещания, посвящённые проблемам обеспечения информационной безопасности с целью формирования чётких указаний по этому вопросу, осуществления контроля их выполнения, а также оказания административной поддержки инициативам по обеспечению ИБ.

Нарушение требований нормативных актов Учреждения по обеспечению ИБ является чрезвычайным происшествием и будет служить поводом и основанием для проведения служебного расследования.

# Контроль и пересмотр

Общий контроль состояния ИБ Учреждения осуществляется Директором.

Текущий контроль соблюдения настоящей Политики осуществляет отдел ИБ. Контроль осуществляется путем проведения мониторинга и менеджмента инцидентов ИБ Учреждения, по результатам оценки ИБ, а также в рамках иных контрольных мероприятий.

Отдел ИБ ежегодно пересматривает положения настоящей политики. Изменения и дополнения вносятся по инициативе отдела ИБ или Директора и утверждаются Директором.

Порядок пересмотра документов второго и третьего уровней определяется в данных документах.

Все изменения, внесённые в настоящую Политику ИБ должны учитываться в листе «История изменений».

# История изменений

|  |  |  |  |
| --- | --- | --- | --- |
| Версия | Дата  утверждения | Изменения | Кто внёс изменения |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |