**Политика ИБ OOO «Радуга»**

1. **Общие положения**
   1. Политика информационной безопасности компании ООО «Радуга» определяет цели и задачи системы обеспечения информационной безопасности и устанавливает совокупность правил, процедур, практических приемов, требований и руководящих принципов в области информационной безопасности которыми руководствуются работники компании при осуществлении своей деятельности.
   2. Под информационной̆ безопасностью понимается состояние защищенности информации, характеризуемое способностью персонала, технических средств и информационных технологий обеспечивать конфиденциальность, целостность и доступность информации при ее обработке техническими средствами.
   3. Настоящая Политика доступна каждому сотруднику и клиенту компании. И представляет собой систему взглядов на проблему информационной защиты, и устанавливает систему принципов по работе с информационной безопасностью.
   4. Руководство компании понимает важность и необходимость мер по обеспечению информационной безопасности для развития компании и ее технологий. Такой подход позволит компании создать конкурентные преимущества, обеспечить финансовую стабильность, рентабельность в соответствии с законами и правовыми документами.
   5. Требования информационной безопасности, предъявляемые компанией, соответствуют их интересам, а также снижают долю рисков защиты информации. Факторы рисков в информационной сфере имеют отношение к ее корпоративному управлению, к работе и взаимодействию с клиентами, заказчиками, а также играют важную роль в организации и реализации бизнес-проектов.
   6. Необходимые требования обеспечения информационной безопасности должны соблюдаться сотрудниками, а также другими сторонами.
   7. Настоящая политика ИБ распространяется на бизнес-процессы предприятия, также ее обязаны соблюдать сотрудники, и пользователи информационных ресурсов
   8. Настоящая Политика в соответствии со всеми правовыми документами и законами является документом по ИБ первого уровня
   9. Документами, детализирующими настоящую политику ИБ, являются частные политики ИБ, которые выступают в роли документов по ИБ второго уровня.
   10. Политика информационной̆ безопасности разработана в соответствии с положениями международного стандарта ISO/IEC 27001:2013.
   11. Политика информационной̆ безопасности утверждается Председателем совета директоров ООО «Радуга».
   12. Пересмотр Политики проводится на регулярной̆ основе не реже одного раз в год.
   13. Ответственность за общий̆ контроль содержания настоящего документа и внесение в него изменений возлагается на Руководителя Департамента безопасности.
2. **Термины и определения**
   1. **Информационные средства** — средства, предназначенные для хранения, обработки и передачи компьютерной информации, а именно: компьютеры и комплексы, терминалы доступа к ним, оборудование локальных вычислительных сетей и узлов связи, специальное оборудование на основе компьютеров, криптографическое оборудование.
   2. **Информационный актив** — различные виды информации (платежной, финансово-аналитической, служебной, управляющей, справочной и пр.) на всех этапах ее жизненного цикла, обеспечивающей деятельность и представляющей ценность с точки зрения достижения поставленных бизнес-целей.
   3. **Компьютерная платформа** — в общем смысле, это любая существующая среда выполнения, в которой должен выполняться вновь разрабатываемый фрагмент программного обеспечения или объектный модуль с учётом накладываемых этой средой ограничений и предоставляемых возможностей.
   4. **Владелец информационного актива** — структурное подразделение, отдел, служба, реализующее полномочия владения, пользования и распоряжения информацией в соответствии со своими функциями и задачами. Владелец информационного актива определяется на этапе его создания.
   5. **Инцидент информационной безопасности** — действительное, предпринимаемое или вероятное нарушение информационной безопасности. Нарушение может быть вызвано ошибками персонала, неправильным функционированием технических средств, природными факторами, преднамеренными злоумышленными действиями, приводящими к нарушению доступности, целостности, конфиденциальности информации.
   6. **ИБ** – Информационная безопасность.
   7. **АРМ** – Автоматизированное рабочее место.
   8. **НГМД** — накопитель на гибких магнитных дисках.
   9. **СУБД** — система управления базами данных.
   10. **Модель** **угроз** (безопасности информации) – физическое, математическое, описательное представление свойств или характеристик **угроз** безопасности информации. Итак, **модель** **угроз** – **это** документ, тем или иным способом описывающий возможные **угрозы** безопасности персональных данных.
   11. **Риск** — возможность возникновения финансовых потерь (убытков), незапланированных расходов или возможность снижения планируемых доходов.
   12. **Операционные риски** — это риски, связанные с финансово-экономической деятельностью (без учета рыночных и кредитных рисков), потери по которым связаны с результатами некомпетентного управления человеческими, технологическими факторами или внешними событиями.
   13. **Служба автоматизаци**и — Департамент ИТ и отдельные сотрудники, ответственные за обеспечение IT-сервиса (в том числе и организации, выполняющие данные работы по договору).
   14. **Автоматизированная система обработки информации (АС)** — организационно-техническая система, представляющая собой совокупность следующих взаимосвязанных компонентов: технических средств обработки и передачи данных (средств вычислительной техники и связи), методов и алгоритмов обработки в виде соответствующего программного обеспечения, массивов (наборов, баз) данных на различных носителях, персонала и пользователей, объединенных по организационно-структурному, тематическому, технологическому или другим признакам для выполнения автоматизированной обработки данных с целью удовлетворения информационных потребностей государственных органов, коммерческих или некоммерческих организаций (юридических лиц), граждан (физических лиц) и иных потребителей информации.
   15. **Бизнес-процесс** — это совокупность взаимосвязанных мероприятий или работ, направленных на создание определённого продукта или услуги для потребителей (под "потребителем" может пониматься в т.ч. внутренний корпоративный субъект, заинтересованный в получении результата процесса, например, бизнес-процесс по формированию и сдаче бухгалтерской отчётности гос.органам.)
   16. **Модель** **нарушителя** (в информатике) — абстрактное (формализованное или неформализованное) описание **нарушителя** правил разграничения доступа.
   17. **ЛВС** — локальная вычислительная сеть.
   18. **Доступ к информации** — ознакомление с информацией, ее обработка, в частности: копирование, модификация или уничтожение информации.
   19. **Санкционированный доступ к информации** — доступ к информации, не нарушающий правила разграничения доступа.
   20. **НСД (Несанкционированный доступ к информации)** — доступ к информации, нарушающий правила разграничения доступа.
   21. **Доступность информации** — свойство системы, в которой циркулирует информация (средств и технологии ее обработки), характеризующееся способностью обеспечивать своевременный беспрепятственный доступ к информации субъектов, имеющих на это надлежащие полномочия.
   22. **Целостность информации** — свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию).
   23. **Конфиденциальность информации** — субъективно определяемая (приписываемая) информации характеристика (свойство), указывающая на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации, и обеспечиваемая способностью системы (среды) сохранять указанную информацию в тайне от субъектов, не имеющих полномочий на право доступа к ней.
   24. **Firewall (межсетевой экран)** — программно-аппаратный комплекс, применяемый для разграничения доступа между сетями.
   25. **Notebook** — переносной персональный компьютер небольших размеров.
   26. **ПРД (Правила разграничения доступа)** — совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.
3. **Описание объекта защиты**
   1. Объектами защиты в контексте данной̆ Политики являются информационные ресурсы ООО «Радуга» , обрабатываемые в информационных системах и ее функциональных подсистемах, содержащие сведения, доступ к которым ограничен, и используемые в процессах сбора, обработки, накопления, хранения и распространения в границах информационных систем ООО «Радуга»

Основными объектами защиты системы информационной безопасности в компании ООО «Радуга» являются:

* + 1. Информационные ресурсы, содержащие коммерческую тайну организации, личные данные сотрудников, базу данных компании, информацию, которая необходима для предоставления ее клиентам
    2. Информационные ресурсы, содержащие личные данные физических и юридических лиц
    3. Сотрудники компании, которые в своей работе взаимодействуют с данными информационной среды компании
    4. Информационная инфраструктура, которая содержит все данные о компании
    5. Информационные ресурсы ограниченного распространения, в том числе содержащие конфиденциальные сведения;
    6. Программные информационные ресурсы, а именно: прикладное программное обеспечение, системное программное обеспечение, инструментальные средства и утилиты;
    7. Физические информационные ресурсы: компьютерное аппаратное обеспечение всех видов;
    8. Носители информации всех видов (электронные, бумажные и прочие);
    9. Все расходные материалы и аксессуары, которые прямо или косвенно взаимодействуют с компьютерным аппаратным и программным обеспечением.
  1. Следует также отметить, что указанные выше основные объекты защиты являются наиболее ценными ресурсами, и, следовательно, по отношению к ним должны применяться самые эффективные правила и методы защиты. И доступность, целостность и конфиденциальность могут иметь особое значение для обеспечения имиджа ООО «Радуга», эффективности его функционирования и т.д.  
     Доступность, целостность и конфиденциальность в обязательном порядке должны учитываться при разработке организационно-распорядительной̆ документации по обеспечению информационной̆ безопасности для системы в целом и для каждого ее ресурса в отдельности.
  2. **Ответственность за ресурсы** 
     1. 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 которой̆ соразмерна ценности и важности ресурсов.
     2. В ИС Учреждения присутствуют следующие типы ресурсов:
* информационные ресурсы, содержащие конфиденциальную информацию, и/или сведения ограниченного доступа, в том числе информацию о финансовой̆ 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.
  + 1. Для каждого ресурса должен быть назначен владелец, который̆ 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.
  1. **Классификация информации** 
     1. Все информационные ресурсы, подлежащие защите, должны быть классифицированы в соответствии с важностью и степенью доступа. Классификация информации должна быть документирована и утверждена руководством Учреждения.
     2. Классификация информации должна проводиться владельцем ресурса, хранящего или обрабатывающего информацию, для определения категории ресурса. Периодически классификация должна пересматриваться для поддержания актуальности её соответствия с категорией̆ ресурса.
     3. Ресурсы, содержащие конфиденциальную или критичную информацию, должны иметь соответствующую пометку.

1. **Цели и задачи деятельности по обеспечению информационной безопасности**
   1. Цель системы обеспечения информационной безопасности — создание и постоянное соблюдение условий, при которых риски, связанные с нарушением безопасности информационных активов, постоянно контролируются и исключаются, либо находятся на допустимом (приемлемом) уровне остаточного риска.
   2. Задачами системы обеспечения информационной безопасности являются:
      1. Снижение операционных рисков, связанных с использованием информационных технологий;
      2. Оптимизация затрат на обеспечение информационной безопасности;
      3. выявление новых угроз;
      4. Контроль информационной безопасности на всех этапах цикла автоматизированных систем;
      5. Минимизация потерь компании при возникновении угроз информационной безопасности;
      6. Обеспечение безопасности его информационных активов в условиях неблагоприятных событий (экономические и политические кризисы, природные и техногенные катастрофы, террористические угрозы и пр.).
   3. Безопасность информационных активов оценивается и обеспечивается по каждому из следующих аспектов:
      1. Доступность;
      2. Целостность;
      3. Конфиденциальность ;
      4. критерием оценки является вероятность, размер и последствия нанесения Организации любого вида ущерба (невыполнение имеющихся перед партнерами обязательств, финансовые потери, потеря репутации и пр.).
   4. Процессы обеспечения информационной безопасности являются составной и неотъемлемой частью процессов управления информационными технологиями и сопутствующими операционными рисками и осуществляются на основе циклической модели: «планирование - реализация - проверка совершенствование - планирование -…».
   5. Состояние информационной безопасности оказывает непосредственное влияние на операционные риски деятельности в связи с чем любой факт (инцидент) нарушения информационной безопасности рассматривается как существенное событие
   6. Положение об обработке персональных данных (далее – Положение) является основополагающим локальным нормативным актом, определяющим позицию Компании в отношении обработки и обеспечения безопасности персональных данных, определяет цели, содержание и порядок обработки персональных данных, меры, направленные на защиту персональных данных, а также процедуры, направленные на выявление и предотвращение нарушений законодательства Российской̆ Федерации в области персональных данных в Компании.
      1. Настоящее Положение определяет политику Компании как оператора, осуществляющего обработку персональных данных, в отношении обработки и защиты персональных данных.
      2. Основной̆ целью настоящего Положения является создание основы для соблюдения прав и свобод человека и гражданина при обработке его персональных данных Компанией̆.
      3. Действие настоящего Положения распространяется на всех руководителей̆ и сотрудников Компании (временных и постоянных), а также руководителей̆ и сотрудников сторонних организаций, связанных договорными отношениями с Компанией̆ и тем или иным образом участвующих в бизнес-процессах Компании, подразумевающих обработку персональных данных.
2. **Угрозы информационной безопасности**
   1. Под угрозами информационной̆ безопасности понимаются потенциально возможные негативные воздействия на защищаемую информацию, к числу которых относятся:
      1. утрата сведений, составляющих банковскую тайну, коммерческую тайну Фонда и иную защищаемую информацию, а также искажение (несанкционированная модификация, подделка) такой̆ информации;
      2. утечка - несанкционированное ознакомление с защищаемой̆ информацией̆ посторонних лиц (несанкционированный̆ доступ, копирование, хищение и т.д.), а также утечка информации по каналам связи и за счет побочных электромагнитных излучений;
      3. недоступность информации в результате ее блокирования, сбоя оборудования или программ, дезорганизации функционирования операционных систем рабочих станций, серверов, маршрутизаторов, систем управления баз данных, распределенных вычислительных сетей̆, воздействия вирусов, стихийных бедствий и иных форс-мажорных обстоятельств;
      4. отсутствие планирования и контроля;
      5. низкая степень надежности программного обеспечения;
      6. недостаточная осведомленность персонала, низкая квалификация персонала и пользователей̆ в области информационных технологий.
   2. В результате воздействия указанных угроз могут возникнуть следующие негативные последствия, влияющие на состояние информационной̆ безопасности Фонда и его нормальное функционирование:
      1. финансовые потери, связанные с утечкой̆ или разглашением защищаемой̆ информации;
      2. финансовые потери, связанные с уничтожением и последующим восстановлением утраченной̆ информации;
      3. ущерб от дезорганизации деятельности Фонда и потери, связанные с невозможностью выполнения им своих обязательств;
      4. моральные потери (ущерб репутации Фонда).
   3. Угрозы конфиденциальности. Подобные угрозы могут возникать вследствие «человеческого фактора», сбоев работе программных и аппаратных средств. К информации ограниченного доступа относится
   4. Угрозы нарушения целостности — это угрозы, связанные с вероятностью модификации той или иной информации, хранящейся в информационной системе. Нарушение целостности может быть вызвано различными факторами — от умышленных действий персонала до выхода из строя оборудования.
   5. Угроза доступности. Нарушение доступности представляет собой создание таких условий, при которых доступ к услуге или информации будет либо заблокирован, либо возможен за время, которое не обеспечит выполнение тех или иных бизнес-целей.
3. **Модель нарушителя ИБ**
   1. Модель нарушителя информационной безопасности – это набор предположений об одном или нескольких возможных нарушителях информационной безопасности, их квалификации, их технических и материальных средствах и т. д. Правильно разработанная модель нарушителя является гарантией построения адекватной системы обеспечения информационной безопасности. Опираясь на построенную модель, уже можно строить адекватную систему информационной защиты.
   2. Среди внутренних нарушителей в первую очередь можно выделить:
      1. Сотрудники, у которых нет доступа к информационным ресурсам
      2. Сотрудники, имеющие доступ к информационным ресурсам
      3. Руководящие должности компании
      4. Непосредственных пользователей и операторов информационной системы, в том числе руководителей различных уровней;
      5. Администраторов вычислительных сетей и информационной безопасности;
      6. Прикладных и системных программистов;
      7. Сотрудников службы безопасности;
      8. Технический персонал по обслуживанию зданий и вычислительной техники, от уборщицы до сервисного инженера;
      9. Вспомогательный персонал и временных работников.
   3. Среди причин, побуждающих сотрудников к неправомерным действиям, можно указать следующие:
      1. Безответственность;
      2. Ошибки пользователей и администраторов;
      3. Демонстрацию своего превосходства (самоутверждение);
      4. «Борьбу с системой»;
      5. Корыстные интересы пользователей системы;
      6. Недостатки используемых информационных технологий.
   4. Группу внешних нарушителей могут составлять:
      1. Бывшие сотрудники банка
      2. Представители компании, взаимодействующие с информационной структурой
      3. Клиенты
      4. Приглашенные посетители;
      5. Представители конкурирующих организаций;
      6. Сотрудники органов ведомственного надзора и управления;
      7. Нарушители пропускного режима;
      8. Наблюдатели за пределами охраняемой территории.
   5. Используемые методы и средства:
      1. Сбор информации и данных;
      2. Пассивные средства перехвата;
      3. Использование средств, входящих в информационную систему или систему ее защиты, и их недостатков;
      4. Активное отслеживание модификаций существующих средств обработки информации, подключение новых средств, использование специализированных утилит, внедрение программных закладок и «черных ходов» в систему, подключение к каналам передачи данных.
   6. Уровень знаний нарушителя относительно организации информационной структуры:
      1. Типовые знания о методах построения вычислительных систем, сетевых протоколов, использование стандартного набора программ;
      2. Высокий уровень знаний сетевых технологий, опыт работы со специализированными программными продуктами и утилитами;
      3. Высокие знания в области программирования, системного проектирования и эксплуатации вычислительных систем;
      4. Обладание сведениями о средствах и механизмах защиты атакуемой системы;
      5. Нарушитель являлся разработчиком или принимал участие в реализации системы обеспечения информационной безопасности.
   7. Время информационного воздействия:
      1. В момент обработки информации;
      2. В момент передачи данных;
      3. В процессе хранения данных (учитывая рабочее и нерабочее состояния системы).
   8. По месту осуществления воздействия:
      1. Удаленно с использованием перехвата информации, передающейся по каналам передачи данных, или без ее использования;
      2. Доступ на охраняемую территорию;
      3. Непосредственный физический контакт с вычислительной техникой, при этом можно выделить: доступ к рабочим станциям, доступ к серверам предприятия, доступ к системам администрирования, контроля и управления информационной системой, доступ к программам управления системы обеспечения информационной безопасности.
4. **Основные положения по обеспечению ИБ**
   1. **Основные принципы обеспечения информационной безопасности**
      1. Осведомленность о риске информационной безопасности
         1. Процессы обеспечения информационной безопасности затрагивают каждого работника, использующего его информационные активы, и накладывают на него соответствующие обязанности и ограничения.
      2. Персональная ответственность
         1. Ответственность за нарушения требований информационной безопасности возлагается непосредственно на работников, допустивших нарушения, и руководителя структурного подразделения, отдела, службы, в котором нарушения допущены.
      3. Ограничение полномочий
         1. Любому сотруднику доступ к информационным активам предоставляется только в том объеме, который необходим ему для выполнения служебных обязанностей. Все операции по предоставлению доступа или назначению полномочий осуществляются строго в соответствии с установленными процедурами (Процедура получения индивидуального доступа).

### Комплексность защиты

### Меры по обеспечению безопасности информационных активов принимаются по всем идентифицированным видам угроз с учетом результатов оценки рисков информационной безопасности.

### Адекватность защиты

### Принимаемые меры обеспечения информационной безопасности эффективны и соразмерны имеющим место рискам информационной безопасности.

### Непрерывность процессов контроля и совершенствования системы обеспечения информационной безопасности

### Постоянный мониторинг и аудит системы обеспечения информационной безопасности, по результатам которых осуществляется анализ эффективности принятых мер обеспечения информационной безопасности с учетом изменений IT-среды, появления новых угроз, инцидентов и проблем, планируются и внедряются дополнительные меры защиты.

### Контроль со стороны руководства

### Руководство на регулярной основе рассматривает отчеты о состоянии информационной безопасности в структурных подразделениях, отделах, службах и фактах нарушений установленных требований, а также общие и частные вопросы информационной безопасности, связанные с использованием технологий повышенного риска или существенно влияющие на бизнес-процессы.

### Целевое финансирование мероприятий по обеспечению информационной безопасности

### Бюджет предусматривает расходы на обеспечение информационной безопасности.

* 1. **Назначение и распределение ролей, и обеспечение доверия к персоналу**
     1. «Ролевое» управление является основным механизмом управления полномочиями пользователей и администраторов в автоматизированных системах.
     2. Роли формируются с учетом принципа минимальности полномочий.
     3. Критичные технологические процессы должны быть защищены от ошибочных и несанкционированных действий администраторов. Штатные процедуры администрирования, диагностики и восстановления должны выполняться через специальные роли в автоматизированных системах без непосредственного доступа к данным.
     4. Должностные обязанности сотрудников и трудовые договоры предусматривают обязанности персонала по выполнению требований по обеспечению информационной безопасности, включая обязательства по неразглашению информации, составляющей коммерческую тайну.
     5. Приказы и распоряжения, актуальная информация по вопросам обеспечения информационной безопасности, в том числе по выявленным нарушениям, доводятся до всех сотрудников под роспись.
     6. Периодически проверяется и оценивается уровень компетентности и информированности работников в вопросах информационной безопасности.
     7. При допуске к работе с критичными АС работники проходят проверку методами, разрешенными законодательством Российской Федерации.
  2. **Управление жизненным циклом автоматизированных систем**
     1. Процедуры по обеспечению информационной безопасности предусматриваются на всех стадиях жизненного цикла автоматизированных систем: при разработке (приобретении), эксплуатации, модернизации, снятии с эксплуатации.
     2. В контрактах со сторонними разработчиками на поставку систем предусматривается их ответственность за наличие в системах скрытых недокументированных возможностей, а также соблюдение условий конфиденциальности,
     3. Системы сторонней разработки проверяются на соответствие требованиям информационной безопасности. При несоответствии текущей версии ПО требованиям информационной безопасности, указанное ПО обновляется или закупается новое.
     4. При выводе АС из эксплуатации или замене входящего в ее состав оборудования осуществляется обязательное гарантированное удаление информации с соответствующих машинных носителей и из памяти компьютеров.
  3. **Антивирусная защита**
     1. Каждый сотрудник обязан выполнять правила эксплуатации антивирусного ПО и требования антивирусной безопасности в отношении внешних источников и носителей информации, а также сети Интернет, немедленно прекращать работу и информировать службы автоматизации и безопасности при подозрениях на вирусное заражение.
     2. Антивирусные средства должны быть установлены на все рабочие места работников и сервера в режиме постоянной защиты.
     3. Запрещается отключать антивирусное ПО, без согласования со службами автоматизации (Департамента ИТ).
     4. Пользователи на рабочих местах не должны иметь административных прав. Наличие административных прав на рабочих местах разрешается только пользователям, выполняющим специальные функции по управлению автоматизированной системой по согласованию ИТ Департаментом.
     5. Все ПО устанавливается на рабочие станции сотрудниками службы автоматизации. Устанавливаемое ПО должно быть лицензионным. Запрещается самостоятельная установка ПО пользователями.
     6. Техническая возможность подключения пользователями к рабочим станциям ЛВС внешних накопителей информации, модемов, мобильных телефонов, беспроводных интерфейсов, использование USB, CD-DVD-дисководов максимально ограничивается. Запрещается подключать любое оборудование без согласования с сотрудниками ИТ Департамента.
     7. Антивирусная защита обеспечивается использованием специализированного лицензионного антивирусного программного обеспечения.
     8. Для снижения влияния человеческого фактора, исключения возможности отключения или не обновления антивирусных средств, контроль и управление антивирусным программным обеспечением, а также устранение выявленных уязвимостей в системном программном обеспечении производится в автоматизированном режиме. При этом обеспечивается минимально возможный период обновления.
  4. **Использование ресурсов Интернет**
     1. Использование ресурсов Интернет разрешается исключительно в производственных целях.
     2. Запрещается использование сети Интернет для информационного взаимодействия между подразделениями Организации без использования средств шифрования.
     3. Использование канальных ресурсов Интернет для построения корпоративных сетей Организации допускается только при использовании средств шифрования (VPN-канал).
     4. Взаимодействие с партнерами по сети Интернет осуществляется с использованием специализированных систем и средств защиты, аттестованных на соответствие требованиям информационной безопасности.
     5. Использование сети Интернет для обработки и хранения информации (в том числе не конфиденциальной) запрещается. Запрещается использование ящиков электронной почты, заведенных не на ресурсах Организации (в частности использование публичных почтовых серверов).
     6. Подключение к рабочим станциям ЛВС мобильных телефонов, беспроводных (радио) интерфейсов, модемов и прочего оборудования, позволяющего выходить в Интернет, запрещается.
     7. Подключение к сети Интернет осуществляется с использованием телефонной сети Организации.
     8. Обсуждение сотрудниками на форумах и в конференциях сети Интернет вопросов, касающихся их служебной деятельности, допускается только при наличии соответствующих указаний руководства.
     9. Доступ сотрудников к ресурсам сети Интернет санкционируется руководством и согласовывается с Департаментом ИТ, которые осуществляют контроль соблюдения сотрудниками требований информационной безопасности, включая контентный анализ сообщений.
     10. Работа сотрудников с web ресурсами Интернет разрешается только в режиме просмотра данных, исключая возможность передачи информации Организации в сеть Интернет.
  5. **Защита информационных и технологических процессов**
     1. Технологические процессы должны быть максимально автоматизированы и обеспечивать возможность выполнения массовых и потенциально опасных операций без участия персонала за счет реализации эффективных процедур контентного контроля и защиты.
     2. Для защиты технологических процессов по результатам анализа рисков информационной безопасности применяются как штатные средства безопасности сетевых операционных систем, СУБД, так и дополнительные программные и программно-аппаратные комплексы и средства криптографической защиты, в совокупности, обеспечивающие достаточный уровень безопасности на всех участках и этапах технологического процесса.
  6. **Доступ к активам (информационным ресурсам)**
     1. Все информационные активы идентифицируются, категорируются и имеют своих владельцев. Доступ к информационным активам всем сотрудникам предоставляется только на основании документально оформленных заявок, согласованных с их владельцами и службой автоматизации (Департамента ИТ). По умолчанию определяется отсутствие доступа.
     2. Доступ к информационным активам не предоставляется (прекращается) в случае отсутствия производственной необходимости, изменения функциональных и должностных обязанностей, увольнения сотрудника.
     3. Департаментом ИТ проводится периодический контроль (не менее одного раза в полугодие) соответствия согласованных и реальных прав доступа к информационным активам, текущему статусу пользователя.
     4. Доступ ко всем информационным активам осуществляется только после авторизации пользователя. В качестве процедуры авторизации используется предъявление уникального имени и пароля. Запрещается передавать свой пароль кому-либо. Запрещается сохранять свой пароль на любых носителях информации.
     5. Журналы аудита действий пользователей и администраторов автоматизированных систем должны быть информативны, защищены от модификации и храниться в течение срока, потенциально необходимого для использования при расследовании возможных инцидентов, связанных с нарушением информационной безопасности.
     6. Наиболее критичные активы могут выделяться в отдельные сегменты сети для ограничения доступа.
  7. **Обеспечение физической безопасности**
     1. Помещения категорируются в зависимости от критичности размещаемых в них информационных активов. В соответствии с категорией обеспечивается техническая укрепленность помещений, оснащение средствами видеоконтроля, контроля доступа, пожаротушения и сигнализации.
     2. Каждый сотрудник, получивший в пользование портативный компьютер (Notebook), обязан принять надлежащие меры по обеспечению его сохранности, как в офисе, так и в иных местах (например, гостинице, конференц-зале, автомобиле или аэропорту). В случае утери (кражи) портативного компьютера ответственность возлагается на данного сотрудника
     3. Портативные компьютеры (Notebooks), должны храниться в физически защищенном месте. Для их сохранности рекомендуется использовать механические замки (например, систему Kensington Lock).
  8. **целями защиты в информационной сфере**:
     1. предотвращение угроз безопасности конфиденциальной информации компании;
     2. предотвращение утечки, разглашения, утечки по техническим каналам, утраты (потери), хищения;
     3. предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации; предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы, обеспечение правового режима документированной информации как объекта собственности;
  9. **Законодательство Российской Федерации в области обработки и обеспечения безопасности персональных данных;** Настоящий документ разработан с учетом Положений следующих нормативных правовых актов Российской Федерации:
     1. Конституция Российской Федерации;
     2. Доктрина информационной безопасности Российской Федерации;
     3. Федеральный закон от 19.12.2005 No160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»;
     4. Федеральный закон от 27.07.2006 No149-ФЗ «Об информации, информационных технологиях и о защите информации»;
     5. Федеральный закон от 27.07.2006 No152-ФЗ «О персональных данных» (далее – ФЗ No152 «О персональных данных»);
     6. Трудовой кодекс Российской Федерации;
     7. Постановление Правительства Российской Федерации от 15.09.2008 No687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
     8. Постановление Правительства Российской Федерации от 01.11.2012 No1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
     9. и других нормативных правовых актов, регулирующие отношения в сфере обеспечения безопасности персональных данных.
  10. **Принципы обработки персональных данных;** В основе обработки персональных данных в Компании лежат следующие принципы:
      1. осуществление обработки персональных данных на законной основе;
      2. ограничение обработки персональных данных достижением конкретных, заранее определенных и законных целей;
      3. соответствие содержания и объема обрабатываемых персональных данных заявленным целям их обработки, отсутствие избыточности обрабатываемых персональных данных по отношению к целям их обработки;
      4. недопустимость объединения баз данных, содержащих персональные данные, обработка которых осуществляется в несовместимых между собой целях;
      5. обеспечение точности персональных данных, их достаточности, а в необходимых случаях и актуальности по отношению к целям обработки персональных данных;
      6. хранение персональных данных в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект персональных данных.
  11. **Основания обработки персональных данных;** Обработка персональных данных Компанией осуществляется в следующих случаях:
      1. с согласия субъекта персональных данных (в том числе, работников) на обработку его персональных данных;
      2. для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на Компанию функций, полномочий и обязанностей;
      3. для исполнения договора, стороной которого, либо выгодоприобретателем или поручителем, по которому является субъект персональных данных, в том числе в случае реализации Оператором своего права на уступку прав (требований) по такому договору, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;
      4. для осуществления прав и законных интересов Компании или третьих лиц, либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;
      5. при необходимости осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве;
      6. в случае, если такая обработка необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;
      7. в случае, когда доступ неограниченного круга лиц к персональным данным субъекта предоставлен самим субъектом персональных данных, либо по его просьбе (далее – персональные данные, сделанные общедоступными субъектом персональных данных);
      8. в случае, когда персональные данные подлежат опубликованию или обязательному раскрытию в соответствии с федеральным законом;
      9. в статистических или иных исследовательских целях, при условии обязательного обезличивания персональных данных.
      10. Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, судимости Компанией не осуществляется. Обработка указанных данных возможна Компанией только на основании согласия субъекта персональных данных в письменной форме.
      11. Компанией с учетом требований действующего законодательства Российской Федерации может осуществляться обработка биометрических персональных данных. Обработка биометрических персональных данных возможна Компанией только на основании согласия субъекта персональных данных в письменной форме.
      12. Персональные данные могут быть получены не от субъекта персональных данных (от третьего лица или из другого источника). При этом, до начала обработки персональных данных, субъекту направляется уведомление об обработке его персональных данных за исключением следующих случаев:
          1. субъект персональных данных уведомлен об осуществлении обработки его персональных данных соответствующим Оператором;
          2. персональные данные получены Компанией на основании федерального законодательства или в связи с исполнением договора, стороной которого, либо выгодоприобретателем или поручителем, по которому является субъект персональных данных;
          3. персональные данные сделаны общедоступными субъектом персональных данных или получены из общедоступного источника;
          4. когда предоставление субъекту персональных данных, содержащихся в уведомлении сведений, нарушает права и законные интересы третьих лиц.
  12. **Обработка персональных данных в целях продвижения товаров, работ, услуг** 
      1. Обработка персональных данных в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи может осуществляться Компанией только при условии предварительного согласия субъекта персональных данных и прекращается по его требованию.
  13. **Конфиденциальность персональных данных**
      1. Компанией не раскрываются третьим лицам и не распространяются персональные данные без согласия субъекта персональных данных, если иное не предусмотрено законодательством Российской Федерации.
  14. **Передача персональных данных третьим лицам**
      1. Компания при осуществлении своей деятельности может передавать персональные данные субъектов государственным органам (Федеральной налоговой службе, Федеральной службе судебных приставов, Министерству внутренних дел Российской Федерации, Прокуратуре и др.) в рамках осуществления последними своих полномочий и функций, а также контрагентам Компании (банкам, страховым компаниям, дилерам, коллекторским агентствам и др.) в строгом соответствии с требованиями законодательства Российской Федерации, локальных актов и при надлежащем обеспечении безопасности этих данных.
  15. **Трансграничная передача персональных данных**
      1. Компанией может с учетом требований действующего законодательства Российской Федерации осуществляться трансграничная передача персональных данных на территории иностранных государств, являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, а также на территории иностранных государств, приведенных в «Перечне иностранных государств, не являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных и обеспечивающих адекватную защиту прав субъектов персональных данных» (утвержден Приказом Роскомнадзора от 15.03.2013 No274).
      2. Трансграничная передача персональных данных на территории иных иностранных государств может осуществляться Компанией с учетом требований действующего законодательства Российской Федерации в случаях:
         1. наличия согласия в письменной форме субъекта персональных данных на трансграничную передачу его персональных данных;
         2. исполнения договора, стороной которого является субъект персональных данных.
  16. **Прекращение обработки и уничтожение персональных данных** 
      1. Обработка персональных данных прекращается или обеспечивается её прекращение, если обработка персональных данных осуществляется другим лицом, действующим по поручению Компании, а собранные персональные данные уничтожаются ( уничтожение персональных данных производится в порядке, установленном отдельными локальными нормативными актами Компании) в сроки, установленные ФЗ No152 «О персональных данных», в следующих случаях, если иное не установлено законодательством Российской Федерации:
         1. по истечению установленного срока обработки персональных данных;
         2. по достижении целей обработки или при утрате необходимости в их достижении;
         3. по требованию субъекта персональных данных или Уполномоченного органа по защите прав субъектов персональных данных — если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки;
         4. при отзыве субъектом персональных данных согласия на обработку своих персональных данных, если такое согласие требуется в соответствии с федеральным законодательством;
         5. при невозможности устранения Компанией допущенных нарушений при обработке персональных данных.
  17. **Взаимодействие с федеральными органами исполнительной власти** 
      1. Взаимодействие с федеральными органами исполнительной власти, в том числе с Уполномоченным органом по защите прав субъектов персональных данных, по вопросам обработки и обеспечения безопасности обрабатываемых Компанией персональных данных осуществляется в соответствии с законодательством Российской Федерации.
  18. **Взаимодействие с субъектами персональных данных** 
      1. Компания способствует реализации законных прав субъектов персональных данных и осуществляет реагирование на запросы и обращения субъектов персональных данных, в том числе предоставление им информации, связанной с обработкой их персональных данных, в соответствии с требованиями законодательства Российской Федерации.
  19. **Организационная основа деятельности по обеспечению ИБ**
  20. Ответственный подразделением – оперативная деятельность и планирование деятельности по обеспечению ИБ компании
  21. В целях выполнения задач по обеспечению ИБ компании, в ней должно быть разделение на:
      1. Руководство – 5
      2. Бухгалтерия – 5
      3. IT-отдел – 5
      4. Менеджеры по работе с клиентами – 30
      5. Отдел безопасности – 5
      6. Куратор
  22. Распределение ролей̆ и ответственности
      1. Для эффективного внедрения процессов управления информационной безопасностью в ООО «Радуга» внедряется система управления информационной безопасностью на основе требований Международного стандарта ISO/IEC 27001:2013. Система управления информационной безопасностью регламентируется отдельными положениями и стандартами, принятыми в ООО «Радуга».
      2. Подразделения информационной безопасности:
         1. совместно с представителями бизнес-подразделений и подразделений Департамента информационных технологий, включая обособленные подразделения Компании, занимающиеся поддержкой̆ и внедрением информационных сервисов (далее ИТ), проводят оценку рисков, связанных с защитой̆ информации, и осуществляют управление этими рисками;
         2. совместно с подразделениями ИТ разрабатывают и внедряют политики и стандарты информационной безопасности, основанные на признанных в мире стандартах информационной безопасности;
         3. разрабатывают планы и технические спецификации для внедрения систем информационной безопасности;
         4. определяют требования по информационной безопасности для существующих и внедряемых информационных систем;
         5. обосновывают и совместно с ИТ защищают общий̆ бюджет ИТ в части, касающейся информационной безопасности ООО «Радуга», с целью выделения достаточных средств для функционирования и развития систем информационной безопасности;
         6. участвуют в разработке стандартов, инструкций и иных нормативных документов в сфере ИТ, выборе контрагентов и утверждении технических решений в части информационной безопасности;
         7. проводят аудит информационных систем с целью выявления потенциальных уязвимостей̆ в корпоративных информационных системах, используют предоставленные ИТ возможности и инструменты, организуют оповещение пользователей̆ о попытках вторжения в информационные системы;
         8. могут привлекать ресурсы сторонних фирм для проведения аудита информационных систем с точки зрения информационной безопасности;
         9. организуют и проводят обучение сотрудников Компании по информационной безопасности, проверяют знания и навыки информационной безопасности сотрудников Компании;
         10. принимают активное участие в процессе изменения информационных систем для обеспечения требуемого уровня информационной безопасности;
         11. согласовывают и контролируют доступ пользователей̆ к информационным ресурсам;
         12. проводят постоянную работу с пользователями информационных ресурсов Компании по разъяснению им основных требований информационной безопасности.
      3. Подразделения Информационных технологий:
         1. внедряют новые информационные системы и инструменты, обеспечивающие реализацию совместно разработанных политик, стандартов информационной безопасности;
         2. обеспечивают работоспособность и доступность информационных систем;
         3. соблюдают все совместно разработанные требования информационной безопасности;
         4. разрабатывают и внедряют планы развития информационных систем, обеспечивают финансирование и осуществляют все виды технической̆ деятельности в корпоративных информационных системах;
         5. следуют совместно принятым корпоративным политикам, стандартам и инструкциям по информационной безопасности, равно как и своим функциональным обязанностям;
         6. следуют совместно разработанным требованиям и рекомендациям подразделений информационной безопасности на всех стадиях реализации новых проектов: от предложения и планирования до осуществления;
         7. управляют процессом изменения информационных систем ООО «Радуга»;
         8. незамедлительно информируют подразделения информационной безопасности о любых нарушениях, уязвимостях, обнаруженных в корпоративных информационных системах и попытках незаконного проникновения в них;
         9. обеспечивают доступ пользователей̆ к компьютерным системам;
         10. являются держателем бюджета ИТ, включая статьи расходов на информационную безопасность, и обеспечивают финансирование утвержденных проектов информационной безопасности;
         11. обеспечивают техническую эксплуатацию систем безопасности.
  23. Ответственность за нарушение Политики информационной безопасности
      1. В случае нарушения установленных правил работы с информационными активами работник может быть ограничен в правах доступа к таким активам, а также привлечен к ответственности в соответствии с Трудовым кодексом, Кодексом об административных правонарушениях и Уголовным кодексом РФ.
      2. За общее руководство по ИБ в компании ООО «Солнышко» отвечает куратор. Ответственность за поддержание политики ИБ лежит на руководстве Ответственного подразделения.
  24. Организация системы обеспечения информационной безопасности
      1. Общее руководство системой обеспечения информационной безопасности осуществляет директор. Он:
         1. утверждает и пересматривает Политику информационной безопасности;
         2. организует процесс управления информационной безопасностью, включая определение подразделений, ответственных за управление отдельными процессами обеспечения информационной безопасности, утверждение положений о них;
         3. обеспечивает условия и утверждает бюджет для эффективной реализации политики информационной безопасности;
         4. рассматривает информацию и отчеты о состоянии информационной безопасности.
      2. Все руководители структурных подразделений, отделов и служб отвечают за реализацию политики информационной безопасности и управление процессами ее обеспечения в рамках своей компетенции:
         1. разрабатывают требования по защите информационных активов в аспектах целостности и конфиденциальности и доступности на основе анализа рисков информационной безопасности;
         2. осуществляют контроль соответствия требованиям по защите информационных активов на всех стадиях жизненного цикла автоматизированных систем, от проектирования до снятия с эксплуатации;
         3. проводят расследования инцидентов и фактов нарушений информационной безопасности и информируют директора о результатах проведенного расследования;
         4. организуют инструктажи работников по вопросам информационной безопасности;
         5. осуществляют инструментальный контроль и мониторинг текущего состояния информационной безопасности;
         6. регулярно (не реже одного раза в полгода) информируют директора о состоянии информационной безопасности.
      3. Отдел безопасности:
         1. обеспечивает выполнение требований информационной безопасности при подключении и администрировании коммуникационного оборудования, операционных систем, СУБД и систем доставки;
         2. проводит обновление системного ПО, связанное с устранением критичных уязвимостей;
         3. обеспечивает доступность информационных активов в условиях отказов и других неблагоприятных событий в части коммуникационного оборудования, операционных систем, СУБД и систем доставки;
         4. обеспечивает выполнение требований информационной безопасности при администрировании автоматизированных систем;
         5. осуществляет регистрацию и направление в службу безопасности информации об инцидентах, имеющих отношение к информационной безопасности;
         6. обеспечивает доступность информационных активов в условиях отказов и других неблагоприятных событий в части автоматизированных систем;
         7. участвует в формировании решений, связанных с организацией технологических процессов, разрабатывает предложения по использованию современных информационных технологий с учетом требований по обеспечению информационной безопасности;
         8. обеспечивает управление ключевыми системами средств криптографической защиты;
         9. эксплуатирует специализированные средства обеспечения безопасности информационных активов и обеспечивает соответствие характеристик данных средств необходимому подразделениям уровню доступности;
         10. организует проведение единой антивирусной политики.
      4. Подразделения:
         1. совместно с Департаментом ИТ, участвуют в оценке рисков реализации угроз их информационным активам;
         2. устанавливают в пределах своей компетенции режим и порядок доступа, правила работы с информационными активами, владельцами которых они являются;
         3. обеспечивают выполнение требований и процедур информационной безопасности при работе сотрудников с информационными активами;
         4. оказывают содействие при проведении проверок и расследований инцидентов безопасности.
  25. **Контроль и Ответственность за соблюдением положений ИБ**
  26. **Контроль**
      1. Общий контроль состояния ИБ лежит на кураторе.
      2. Текущий контроль за соблюдением политики ИБ лежит на Ответственном подразделении.
      3. Контроль осуществляется путем проведения мониторинга и менеджмента инцидентов ИБ Учреждения, по результатам оценки ИБ, а также в рамках иных контрольных мероприятий.
      4. Ежегодно пересматриваются положения настоящей̆ политики. Изменения и дополнения вносятся по инициативе Директора и утверждаются Директором.
      5. Порядок пересмотра документов второго и третьего уровней̆ определяется в данных документах.
      6. Все изменения, внесённые в настоящую Политику ИБ, должны учитываться в листе «История изменений».
      7. Компания осуществляет контроль за выполнением требований по обработке и обеспечению безопасности персональных данных, установленных действующим законодательством Российской Федерации и локальными нормативными актами Компании.
  27. **Ответственность** 
      1. Директор Учреждения определяет приоритетные направления деятельности в области обеспечения ИБ, меры по реализации настоящей̆ Политики, утверждает списки объектов и сведений, подлежащих защите, а также осуществляет общее руководство обеспечением ИБ Учреждения.
      2. Ответственность за поддержание положений настоящей̆ Политики в актуальном состоянии, создание, внедрение, координацию и внесение изменений в процессы Учреждения лежит на начальнике отдела компьютерных и информационных технологий.
      3. Все руководители несут прямую ответственность за реализацию Политики и её соблюдение персоналом в соответствующих подразделениях.
      4. Работники Учреждения несут персональную ответственность за соблюдение требований документов и обязаны сообщать обо всех выявленных нарушениях в области информационной безопасности в Ответственное подразделение.
      5. В трудовых договорах и должностных инструкциях работников устанавливается ответственность за сохранность служебной̆ информации, ставшей̆ известной̆ в силу выполнения своих обязанностей.
      6. 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 административной̆ поддержки инициативам по обеспечению ИБ.
      7. Нарушение требований нормативных актов Учреждения по обеспечению ИБ является чрезвычайным происшествием и будет служить поводом и основанием для проведения служебного расследования.
      8. Ответственность за выполнение правил Политики ИБ несет каждый̆ сотрудник учреждения в рамках своих должностных обязанностей и полномочий.
      9. На основании ст. 192 Трудового кодекса РФ сотрудники, нарушающие требования Политики ИБ Учреждения, могут быть подвергнуты дисциплинарным взысканиям.
      10. Все сотрудники несут персональную (в том числе материальную) ответственность за прямой̆ действительный̆ ущерб, причинённый̆ Учреждению в результате нарушения ими правил политики ИБ (Ст. 238 Трудового кодекса РФ).
      11. За неправомерный̆ доступ к компьютерной̆ информации, создание, использование или распространение вредоносных программ, а также нарушение правил эксплуатации ЭВМ, следствием которых явилось нарушение работы ЭВМ (автоматизированной системы обработки информации), уничтожение, блокирование или модификация защищаемой̆ информации, сотрудники Учреждения несут ответственность в соответствии со статьями 272, 273 и 274 Уголовного кодекса Российской Федерации.
      12. Ответственность за выполнение требований ФЗ от 27.07.2006 No152 «О персональных данных» в Компании и за организацию обработки и обеспечения безопасности персональных данных в соответствии с требованиями вышеуказанного закона и настоящего Положения возложена на структурные подразделения, ответственные за обеспечение безопасности персональных данных.
      13. Персональная ответственность за выполнение требований по обработке и обеспечению безопасности персональных данных возложена на руководителей̆ структурных подразделений и сотрудников Компании, осуществляющих обработку персональных данных.
      14. Сотрудники Компании при нарушении установленного порядка обработки и обеспечения безопасности персональных данных несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством Российской Федерации.
  28. **Заключительные положения**
  29. В случае изменения законов или правовых документов, изменения в политике происходят только в тех аспектах, которые не противоречат новому закону. Ответственным за изменения является Ответственное подразделение.
  30. Порядок пересмотра Политики, документы, регламентирующие Политику
      1. Департаментом безопасности ежегодно пересматриваются основные принципы, направления и требования по защите информации. Пересмотр Политики осуществляется в соответствии с изменениями, влияющими на первоначальную оценку риска, путем выявления существенных инцидентов нарушения информационной безопасности, появления новых уязвимостей̆ или изменения организационной̆, или технологической̆ инфраструктуры.

**Приложение 1**

**Правила использования информационных ресурсов ЛВС (локальная вычислительная сеть)**

1. **Пользователь информационных ресурсов ЛВС обязан:**
   1. Использовать ресурсы ЛВС для служебных целей.
   2. Знать и помнить имя компьютера, персональный логин и пароль (выдается памятка).
   3. По требованию системного администратора производить выход из баз данных вплоть до полного отключения от сети.
   4. При смене должности, рабочего места или уровня доступа к информации немедленно сообщать администратору ЛВС.
   5. Иметь уникальный пароль, соответствующий требованиям информационной безопасности.
      1. Пароль должен иметь длину не менее 5-ми символов и удовлетворять любым 3-м из 4-х условий:
         1. в пароле должны присутствовать цифры;
         2. в пароле должны присутствовать специальные символы (« ?, @ и т.д.);
         3. в пароле должны присутствовать заглавные буквы;
         4. в пароле должны присутствовать строчные буквы.
      2. Пароль не должен повторять пароли других пользователей и предыдущие пароли пользователя (в случае плановой смены пароля).
   6. Сообщать о любых случаях использования другими пользователями ресурсов ЛВС в личных, не связанных с производственной деятельностью, целях.
   7. Сохранять рабочую документацию (письма и т.д.) на сетевом диске.
2. **Пользователю информационных ресурсов ЛВС запрещается:**
   1. Без согласования с системным администратором подключать к ЛВС любые устройства (компьютеры, принтеры, концентраторы и т.д.).
   2. Использовать предоставляемые ресурсы ЛВС для хранения развлекательной информации, такой как: игры, картинки, музыку и др., не связанное с производственной необходимостью.
   3. Самостоятельно изменять настройки компьютера, подключенного к ЛВС (имя компьютера, IP- адрес, сетевые службы и протоколы и др.).
   4. Открывать для общего доступа любые ресурсы закрепленного за пользователем компьютера.
   5. Применять к информации, хранящейся в ЛВС, любые методы шифрования данных.
   6. Хранить персональный пароль на любых материальных носителях и в электронном виде (бумага, диски компьютера и т.д.), сообщать кому-либо свой пароль.
   7. Хранить личную информации (фотографии, видео и т.д.) на ЛВС.
3. **Особые условия**
   1. В случае несоблюдения правил использования информационных ресурсов ЛВС пользователь может быть отключен от ЛВС без предварительного уведомления.
   2. Повторное подключение пользователя к информационным ресурсам ЛВС производится после предварительного предоставления пользователем объяснительной на имя директора компании.

**Приложение 2**

**Процедура получения индивидуального доступа к ресурсам**

1. Оформляется письмо (e-mail) либо служебная записка на имя начальника отдела.
2. После согласования начальником отдела документ передается начальнику Департамента ИТ.
3. Начальником Департамента назначается:
   1. ответственное лицо за проведение анализа о необходимости предоставления индивидуального доступа к ресурсу;
   2. исполнитель.

***Технический регламент***

1. **Технический регламент информационной безопасности**
   1. Регламент информационной безопасности – это совокупность норм, правил и практических рекомендаций, на которых строится управление, защита и распределение информации.
   2. Под Регламентами безопасности понимается совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов.
   3. Регламент информационной безопасности относятся к административным мерам обеспечения информационной безопасности и определяют стратегию Департамента в области ИБ. Регламенты информационной безопасности определяют эффективную работу средств защиты информации.
2. **Регламент предоставления доступа информационному ресурсу**
   1. Назначение:
      1. Настоящий Регламент определяет основные правила предоставления сотрудникам доступа к защищаемым информационным ресурсам Департамента.
   2. Положение Регламента:
      1. К работе с информационным ресурсом допускаются сотрудники, ознакомленные с правилами работы с информационным ресурсом и ответственностью за их нарушение, а также настоящим Регламентом.
      2. Каждому сотруднику Департамента, допущенному к работе с конкретным информационным ресурсом, должно быть сопоставлено персональное уникальное имя (учетная запись), под которым он будет регистрироваться и работать в ИС.
      3. В случае необходимости некоторым сотрудникам могут быть сопоставлены несколько уникальных имен (учетных записей). Использование несколькими сотрудниками при работе в Департаменте одного и того же имени пользователя («группового имени») ЗАПРЕЩЕНО.
   3. **Порядок создания (продления) учетной записи пользователя**
      1. Процедура регистрации (создания учетной записи), так же продления срока действия временной учетной записи пользователя для сотрудника Департамента инициируется заявкой.
      2. В заявке указывается:
         1. должность (с полным наименованием подразделения), фамилия, имя и отчество сотрудника;
         2. основание для регистрации учетной записи (номер приказа о принятии на работу в Департамент или иного договорного документа, определяющего необходимость предоставления сотруднику доступа к информационным ресурсам Департамента).
      3. Заявку подписывает консультант кадровой службы подтверждающий, что указанный сотрудник действительно принят в штат Департамента.
      4. Администратор информационной безопасности рассматривает представленную заявку и совершает необходимые операции по созданию (удалению) учетной записи пользователя, присвоению ему начального значения пароля и минимальных прав доступа к ресурсам Департамента.
      5. По окончании регистрации учетной записи пользователя в заявке делается отметка о выполнении задания за подписями исполнителей.
      6. Минимальные права в ИС, определенные выше, а также присвоение начального пароля производится администратором информационной безопасности, при согласовании заявки на предоставление (изменение) прав доступа пользователя к информационным ресурсам.
   4. **Порядок удаления учетной записи пользователя**
      1. При прекращении срока действия полномочий пользователя (окончание договорных отношений, увольнение сотрудника) учетная запись должна немедленно блокироваться.
      2. В заявке указывается:
         1. должность сотрудника, фамилия, имя и отчество сотрудника;
         2. имя пользователя (учетной записи) данного сотрудника;
         3. дата прекращения полномочий пользователя.
      3. Заявку подписывает консультант кадровой службы, утверждая тем самым факт прекращения срока действия полномочий пользователя.
      4. Администратор информационной безопасности рассматривает представленную заявку и совершает необходимые операции по удалению учетной записи пользователя, По окончании внесения изменений в заявке делается отметка о выполнении задания за подписями исполнителей.
      5. В случае необходимости сохранения персональных документов на АРМ сотрудника, после прекращения срока действия его полномочий, сотрудник (или его непосредственный руководитель) должен своевременно (не позднее, чем за 3 суток до момента прекращения срока действия своих полномочий) подать заявку на блокирование учетной записи пользователя с указанием срока хранения указанной информации.
3. **Регламент защиты АРМ**
   1. **Назначение**
      1. Настоящий Регламент определяет основные правила и требования по защите персональных данных и иной конфиденциальной информации Департамента от неавторизованного доступа, утраты или модификации.
   2. **Положения Регламента**
      1. Во время работы с конфиденциальной информацией должен предотвращаться ее просмотр не допущенными к ней лицами.
      2. При любом оставлении рабочего места, рабочая станция должна быть заблокирована, съемные машинные носители, содержащие конфиденциальную информацию, заперты в помещении, шкафу или ящике стола или в сейфе.
      3. Несанкционированное использование печатающих, факсимильных, копировально-множительных аппаратов и сканеров должно предотвращаться путем их размещения в помещениях с ограниченным доступом, использования паролей или иных доступных механизмов разграничения доступа.
      4. Доступ к компонентам операционной системы и командам системного администрирования на рабочих станциях пользователей ограничен. Право на доступ к подобным компонентам предоставлено только администратору информационной безопасности. Конечным пользователям предоставляется доступ только к тем командам, которые необходимы для выполнения их должностных обязанностей.
      5. Доступ к информации предоставляется только лицам, имеющим обоснованную необходимость в работе с этими данными для выполнения своих должностных обязанностей.
      6. Пользователям запрещается устанавливать неавторизованные программы на компьютеры.
      7. Конфигурация программ на компьютерах должна проверяться ежемесячно на предмет выявления установки неавторизованных программ.
      8. Техническое обслуживание должно осуществляться только на основании обращения пользователя к администратору информационной безопасности.
      9. Локальное техническое обслуживание должно осуществляться только в личном присутствии пользователя.
      10. Дистанционное техническое обслуживание должно осуществляться только со специально выделенных автоматизированных рабочих мест, конфигурация и состав которых должны быть стандартизованы, а процесс эксплуатации регламентирован и контролироваться.
      11. При проведении технического обслуживания должен выполняться минимальный набор действий, необходимых для устранения проблемы, явившейся причиной обращения, и использоваться любые возможности, позволяющие впоследствии установить авторство внесенных изменений.
      12. Копирование конфиденциальной информации и временное изъятие носителей конфиденциальной информации (в том числе в составе АРМ) допускаются только с санкции пользователя. В случае изъятия носителей, содержащих конфиденциальную информацию, пользователь имеет право присутствовать при дальнейшем проведении работ.
      13. Программное обеспечение должно устанавливаться со специальных ресурсов или съемных носителей и в соответствии с лицензионным соглашением с его правообладателем.
      14. Конфигурации устанавливаемых рабочих станций должны быть стандартизованы, а процессы установки, настройки и ввода в эксплуатацию - регламентированы.
      15. АРМ, на которых предполагается обрабатывать конфиденциальную информацию, должны быть закреплены за соответствующими сотрудниками Департамента. Запрещается использование указанных АРМ другими пользователями без согласования с администратором информационной безопасности Департамента. При передаче указанного АРМ другому пользователю, должна производиться гарантированная очистка диска (форматирование).
4. **Регламент учетных записей**
   1. **Назначение**
      1. Настоящий Регламент определяет основные правила присвоения учетных записей пользователям информационных активов Департамента.
   2. **Положение Регламента**
      1. Регистрационные учетные записи подразделяются на:
         1. пользовательские – предназначенные для идентификации/аутентификации пользователей информационных активов Департамента;
         2. системные – используемые для нужд операционной системы;
         3. служебные – предназначенные для обеспечения функционирования отдельных процессов или приложений.
      2. Каждому пользователю информационных активов Департамента назначается уникальная пользовательская регистрационная учетная запись. Допускается привязка более одной пользовательской учетной записи к одному и тому же пользователю (например, имеющих различный уровень полномочий).
      3. В общем случае запрещено создавать и использовать общую пользовательскую учетную запись для группы пользователей. В случаях, когда это необходимо, ввиду особенностей автоматизируемого процесса или организации труда (например, посменное дежурство), использование общей учетной записи должно сопровождаться отметкой в журнале учета машинного времени, которая должна однозначно идентифицировать текущего владельца учетной записи в каждый момент времени. Одновременное использование одной общей пользовательской учетной записи разными пользователями запрещено.
      4. Системные регистрационные учетные записи формируются операционной системой и должны использоваться только в случаях, предписанных документацией на операционную систему.
      5. Служебные регистрационные учетные записи используются только для запуска сервисов или приложений.
      6. Использование системных или служебных учетных записей для регистрации пользователей в системе категорически запрещено.

***Работа Сердюковой Полины БАСО-02-20***