**ПРИМЕР СТРУКТУРЫ И ОФОРМЛЕНИЯ ПРИЛОЖЕНИЯ № 2**

Приложение № 2 к Политике информационной безопасности «ИБКОРП»

# ПОЛОЖЕНИЕ

**О ДОСТУПЕ К ИНФОРМАЦИОННЫМ РЕСУРСАМ**

# Назначение и область действия

* 1. Настоящее Положение о доступе к информационным ресурсам (далее – «Положение») определяет основные правила и требования по обеспечению информационной безопасности информационных ресурсов «ИБКОРП» (далее – «Организация») от любых форм неавторизованного доступа, использования и раскрытия информации.
  2. Соответствует требованиям Политики информационной безопасности Организации.
  3. Распространяется на всех работников Организации и третьих лиц, использующих информационные ресурсы и системы Организации. Является обязательным для исполнения.

# Основные требования

* 1. Получение пользователями доступа к информационным ресурсам основывается на аутентификации этих пользователей и разграничении доступа.
  2. В качестве объектов доступа рассматриваются информационные ресурсы Организации, в отношении которых Организация имеет права владения, распоряжения, пользования: данные (информация), технические средства, программные средства, услуги (сервисы) информационных систем.
  3. Каждому пользователю сопоставляется учетная запись пользователя, присваиваются, по возможности, единые для различных объектов доступа Организации атрибуты информационной безопасности: уникальный идентификатор, «секрет» аутентификации, права доступа – с учетом их важности и ценности для деятельности Организации.
  4. В Организации могут применяться виды аутентификации, основанные на знании пользователем пароля (базовый вид аутентификации), на владении физическим носителем «секрета» (смарт-карты, устройства контактной памяти, USB-ключи, криптографические токены), на уникальных данных пользователя (биометрические параметры). При необходимости может использоваться комбинация двух или более видов.
  5. Пользователи уведомляются об обязанностях по обращению с «секретами» аутентификации и сроках истечения их действия. «Секреты», в свою очередь передаются пользователям способом, исключающим несанкционированное ознакомление с ними. Передача пользователем личного «секрета» другому лицу запрещена.
  6. Назначение прав доступа соответствует принципу «Запрещено все, что явно не разрешено» и определяется, исходя из служебных обязанностей пользователя.
  7. Категорически запрещен доступ к ресурсам по принципу «Всем – Полный доступ». Запрещен также неавторизованный (анонимный, гостевой) доступ к любым ресурсам, кроме общедоступных страниц веб-сайтов Организации.
  8. Пересмотр прав доступа осуществляется при возникновении производственной необходимости и документируется.
  9. Управление доступом к сетевым информационным ресурсам и услугам производится, в том числе, путем разделения информационной телекоммуникационной системы Организации на отдельные логические и физические сетевые сегменты.
  10. В Организации должны использоваться средства контроля над соблюдением правил доступа к объектам доступа.
  11. Служебный доступ к объектам доступа Организации, осуществляемый по внешним каналам связи, должен защищаться с применением механизмов аутентификации и криптографической защиты информации.
  12. Доступ к общедоступным страницам веб-сайтов Организации не требует соблюдения требований раздела 2.11, достаточно обеспечить шифрование трафика.
  13. Для снижения вероятности угроз несанкционированного доступа, необходимо минимизировать число устройств, имеющих легальные внешние IP-адреса сети Интернет. Оборудование, имеющее легальные внешние IP-адреса сети Организации, должно проверяться на наличие уязвимостей и автоматически получать обновления безопасности.
  14. Объекты доступа Организации должны быть защищены от внешних угроз из сети Интернет и из локальной сети сетевыми брандмауэрами и штатными средствами защиты, входящими в состав операционной системы и приложений. Число открытых для доступа сервисов и ресурсов на этих объектах должно быть минимально необходимым.
  15. В договорах с поставщиками информационно-технических услуг определяются требования по управлению доступом к этим услугам.
  16. При увольнении работника обеспечивается невозможность его доступа к объектам доступа Организации.
  17. При нарушении требований данного Положения доступ пользователя к информационным ресурсам может быть временно заблокирован ответственными лицами (см. раздел 3.2) до устранения нарушения.
  18. Порядок работы с информационными ресурсами, содержащими сведения, отнесенные к государственной тайне либо к персональным данным, защита которых организуется в соответствии с требованиями законодательства РФ, определяется соответствующими внутренними документами Организации. Разработка и утверждение этих документов производится вне настоящего Положения.

# Роли и ответственность

* 1. Ответственность за соблюдение данного Положения возлагается на всех работников Организации и третьих лиц, использующих информационные ресурсы и системы Организации.
  2. Ответственность за реализацию данного Положения возлагается на: руководителей подразделений Организации; работников, ответственных за администрирование сегментов информационной телекоммуникационной системы Организации; работников, выполняющих следующие функции: администраторов информационных систем, администраторов локальной вычислительной сети, администраторов по обеспечению безопасности информации.

**Частные ПИБ (положений)**

**(дополнительно к ГОСТ 27002-2021)**

**1. Положение о защите конфиденциальной информации и коммерческой тайны**

* Определяет перечень защищаемой информации.
* Устанавливает порядок маркировки, хранения и передачи конфиденциальных данных.
* Регламентирует ответственность сотрудников за разглашение информации.

**2. Положение об управлении доступом к информационным ресурсам**

* Определяет уровни доступа сотрудников к системам и данным.
* Регламентирует процессы предоставления, изменения и отзыва прав доступа.
* Включает принципы минимально необходимого доступа и разделения полномочий.

**3. Положение об использовании мобильных устройств и BYOD**

* Регламентирует использование личных устройств сотрудников в корпоративной сети (Bring Your Own Device, BYOD).
* Определяет требования к защите данных на мобильных устройствах.
* Включает меры по удаленному управлению и блокировке устройств при утрате.

**4. Положение об использовании облачных сервисов и удаленного доступа**

* Определяет правила работы с корпоративными данными в облачных сервисах.
* Устанавливает требования к VPN, двухфакторной аутентификации и безопасному удаленному подключению.
* Регламентирует контроль над доступом к облачным хранилищам.

**5. Положение о безопасной разработке программного обеспечения (DevSecOps)**

* Включает рекомендации по безопасному кодированию и тестированию.
* Определяет процедуры анализа кода на уязвимости.
* Регламентирует управление обновлениями и исправлениями уязвимостей.

**6. Положение о резервном копировании и восстановлении данных**

* Определяет критически важные данные для резервного копирования.
* Устанавливает частоту и методы резервирования.
* Включает порядок восстановления данных в случае аварий.

**7. Положение о реагировании на инциденты информационной безопасности**

* Определяет классификацию инцидентов.
* Устанавливает порядок их выявления, фиксации, расследования и устранения последствий.
* Регламентирует процедуру оповещения руководства и ответственных лиц.

**8. Положение о мониторинге информационных систем и событий безопасности**

* Описывает принципы сбора и анализа логов.
* Определяет порядок выявления аномалий и угроз.
* Регламентирует работу SIEM-систем и других инструментов мониторинга.

**9. Положение о защите персональных данных (в соответствии с 152-ФЗ)**

* Устанавливает требования к сбору, обработке и хранению персональных данных.
* Определяет меры защиты персональных данных в ИС.
* Включает порядок уничтожения персональных данных по истечении срока хранения.

**10. Положение об использовании электронной почты и корпоративных мессенджеров**

* Определяет правила пересылки конфиденциальной информации по почте.
* Устанавливает запреты на использование несанкционированных мессенджеров.
* Регламентирует меры защиты от фишинга и спама.

**11. Положение об управлении уязвимостями и обновлениями ПО**

* Определяет процедуры анализа уязвимостей в системах.
* Регламентирует установку обновлений безопасности и патчей.
* Устанавливает требования к тестированию обновлений перед развертыванием.

**12. Положение о физической безопасности информационных ресурсов**

* Определяет требования к защите серверных помещений и центров обработки данных (ЦОД).
* Регламентирует использование видеонаблюдения, контроля доступа и сигнализации.
* Устанавливает порядок работы с носителями информации (уничтожение, архивирование).

**13. Положение о политике паролей и аутентификации**

* Определяет требования к длине и сложности паролей.
* Регламентирует сроки смены паролей и использование многофакторной аутентификации (MFA).
* Включает запрет на использование одинаковых паролей в разных системах.

**14. Положение об аудитах и проверках информационной безопасности**

* Определяет периодичность и процедуры внутренних аудитов ИБ.
* Устанавливает порядок взаимодействия с внешними аудиторами.
* Регламентирует обработку и внедрение результатов аудита.

**15. Положение о контроле действий сотрудников в информационных системах**

* Определяет допустимый уровень мониторинга действий пользователей.
* Устанавливает порядок расследования подозрительных действий.
* Включает меры предотвращения инсайдерских угроз.

**16. Положение о защите веб-ресурсов и корпоративных сайтов**

* Устанавливает требования к безопасности веб-приложений.
* Регламентирует проведение тестов на проникновение (pentesting).
* Определяет защитные механизмы от DDoS-атак и веб-уязвимостей.

**17. Положение о лицензировании и управлении программным обеспечением**

* Определяет порядок использования и закупки ПО.
* Включает меры предотвращения установки нелицензионного ПО.
* Регламентирует контроль версий и обновлений ПО.

**18. Положение о защите данных при увольнении и смене должности сотрудников**

* Определяет порядок отзыва прав доступа при увольнении.
* Включает процедуры передачи учетных записей и оборудования.
* Регламентирует проверку наличия копий конфиденциальных данных у увольняемых сотрудников.

**19. Положение о взаимодействии с подрядчиками и третьими лицами**

* Устанавливает требования к информационной безопасности при работе с внешними организациями.
* Регламентирует аудит ИБ подрядчиков.
* Определяет ответственность за нарушение условий защиты информации.

**20. Положение о защите критической инфраструктуры**

* Определяет меры защиты для промышленных и стратегически важных объектов.
* Включает требования к SCADA-системам и IoT-устройствам.
* Регламентирует защиту от атак на объекты критической инфраструктуры.