|  |
| --- |
| ИБКОРП |
| **Политика информационной безопасности**  ИБКОРП |
|  |
| г. Москва  2025г. |

# СОДЕРЖАНИЕ

1. [ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ](#_TOC_250009)
2. [ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ](#_TOC_250008)
3. [ОБЛАСТЬ ПРИМЕНЕНИЯ](#_TOC_250007)
4. [НОРМАТИВНЫЕ ССЫЛКИ](#_TOC_250006)
5. [ОБЩИЕ ПОЛОЖЕНИЯ](#_TOC_250005)
6. [ПОЛОЖЕНИЯ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ](#_TOC_250004)
7. [ЗАДАЧИ СИСТЕМЫ УПРАВЛЕНИЯ ИБ](#_TOC_250003)
8. [РЕАЛИЗАЦИЯ](#_TOC_250002)
9. [КОНТРОЛЬ](#_TOC_250001)
10. [СОВЕРШЕНСТВОВАНИЕ](#_TOC_250000)

Приложение № 1 ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Приложение № 2 ПОЛОЖЕНИЕ О ДОСТУПЕ К ИНФОРМАЦИОННЫМ РЕСУРСАМ

# ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

В настоящем документе использованы следующие сокращения:

|  |  |  |
| --- | --- | --- |
| **ИБ** | - | Информационная безопасность |
| **ИС** | - | Информационная система |
| **СУИБ** | - | Система управления информационной безопасностью |

# ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Термины и определения, используемые в настоящей Политике и рекомендуемые к использованию в нормативных и организационно- распорядительных документах, созданных на ее основе, приведены в Приложении № 1 «Термины и определения».

# ОБЛАСТЬ ПРИМЕНЕНИЯ

Настоящая Политика информационной безопасности (далее – «Политика») применяется ко всем процессам, связанным с обработкой, хранением, передачей и защитой информации в Организации, независимо от носителя данных и способа обработки.

Политика распространяется на:

* Все структурные подразделения Организации, включая филиалы и дочерние предприятия.
* Всех сотрудников, временных работников, подрядчиков и иных лиц, имеющих доступ к информационным ресурсам Организации.
* Все виды информации, включая конфиденциальные и персональные данные, коммерческую тайну и иную критически важную информацию.
* Все технические и программные средства, используемые для обработки, передачи и хранения информации, включая локальные и облачные информационные системы, серверное и пользовательское оборудование, мобильные устройства и носители данных.
* Все каналы передачи данных, включая внутренние и внешние сети связи, интернет-соединения, а также любые средства удаленного доступа к информационным системам.

Политика обязательна для соблюдения всеми сотрудниками и контрагентами, работающими с информацией Организации. Нарушение требований Политики рассматривается как инцидент информационной безопасности и влечет за собой меры дисциплинарного воздействия в соответствии с внутренними нормативными документами и законодательством Российской Федерации.

* 1. Система обеспечения ИБ представляет собой совокупность …..
  2. Система управления ИБ является составной частью общей системы управления Организации, обеспечивает поддержку и управление процессами обеспечения ИБ на всех этапах деятельности корпоративной информационной системы.
  3. Организация разрабатывает и внедряет систему управления ИБ, отвечающую требованиям и рекомендациям нормативных документов Российской Федерации.
  4. Основные цели внедрения системы управления ИБ Организации:

–

–

…

* 1. Положения настоящей Политики распространяются на все виды информации в Организации, хранящейся либо передающейся любыми способами, в том числе информацию, зафиксированную на материальных носителях.
  2. Положения настоящей Политики также распространяются на средства приема, обработки, передачи, хранения и защиты информации Организации.
  3. Политика применяется к сотрудникам «ИБКОРП», а также к партнерам, имеющим доступ к информации «ИБКОРП».
  4. Область применения настоящей Политики распространяется на все подразделения Организации, в которых обрабатывается информация, не составляющая государственную тайну.

# НОРМАТИВНЫЕ ССЫЛКИ

При разработке настоящей Политики учтены требования и рекомендации следующих документов:

–

–

…

# ОБЩИЕ ПОЛОЖЕНИЯ

5.1. **Необходимость защиты информационных ресурсов**

* сохранность конфиденциальной и коммерчески значимой информации;
* соблюдение требований законодательства в области информационной безопасности (ИБ);
* устойчивость бизнес-процессов и снижение операционных рисков;
* доверие клиентов, партнеров и сотрудников к организации.

5.2. **Цели разработки и реализации Политики информационной безопасности**  
Настоящая Политика разработана для установления единых стандартов и требований в сфере защиты информации. Основными целями Политики являются:

* определение принципов и правил обеспечения информационной безопасности;
* минимизация рисков, связанных с утечками, атаками и несанкционированным доступом к информации;
* защита прав и интересов сотрудников, клиентов и партнеров;
* обеспечение соответствия требованиям нормативно-правовых актов и стандартов в области ИБ;
* создание устойчивой системы управления ИБ, интегрированной в бизнес-процессы организации.

5.3. **Принципы информационной безопасности**

* **Системность** – комплексный подход к управлению информационной безопасностью.
* **Риск-ориентированный подход** – принятие мер защиты на основе оценки актуальных угроз и рисков.
* **Минимизация привилегий** – предоставление пользователям только необходимого уровня доступа.
* **Разграничение ответственности** – четкое определение обязанностей всех участников процессов обеспечения ИБ.
* **Непрерывность процессов ИБ** – постоянный мониторинг и совершенствование системы безопасности.

5.4. **Область применения Политики**  
Настоящая Политика распространяется на всех сотрудников, подрядчиков и партнеров организации, использующих ее информационные ресурсы. Политика применяется ко всем видам информации, включая документы, электронные данные, базы данных, а также к техническим средствам, используемым для обработки и передачи информации.

# ПОЛОЖЕНИЯ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

* + 1. Положения по информационной безопасности Организации (далее –«Положения») разрабатываются на основании Политики информационной безопасности Организации в целях создания, развития и совершенствования общей системы защиты информации Организации.
    2. Положения по ИБ являются приложениями к настоящей Политике.

В рамках настоящей Политики информационной безопасности в Организации разрабатываются и утверждаются следующие частные Положения по ИБ:

* **Положение о доступе к информационным ресурсам** – устанавливает правила и процедуры предоставления, изменения и отзыва прав доступа к информационным системам и данным.
* **Положение о защите персональных данных** – определяет меры по обработке, хранению и передаче персональных данных в соответствии с требованиями законодательства.
* **Положение о защите коммерческой тайны и конфиденциальной информации** – регламентирует порядок работы с информацией, представляющей коммерческую ценность.
* **Положение об управлении инцидентами информационной безопасности** – описывает процессы выявления, регистрации, расследования и реагирования на инциденты ИБ.
* **Положение об использовании средств криптографической защиты информации (СКЗИ)** – определяет порядок применения шифрования и других методов криптографической защиты.
* **Положение о резервном копировании и восстановлении данных** – устанавливает регламент создания резервных копий и процедуры восстановления данных в случае сбоя.
* **Положение об использовании мобильных устройств и удаленного доступа** – регулирует работу сотрудников с корпоративными данными при использовании мобильных устройств и вне офиса.
* **Положение о контроле и мониторинге информационных систем** – определяет механизмы аудита, мониторинга и журналирования событий безопасности.
* **Положение об управлении уязвимостями и обновлениями программного обеспечения** – описывает процедуры своевременного обновления ПО и устранения уязвимостей.
* **Положение об использовании Интернета и электронной почты** – устанавливает ограничения и правила работы с интернет-ресурсами и корпоративной электронной почтой.
* **Положение о физической безопасности информационных ресурсов** – регулирует меры по защите серверных помещений, рабочих мест и других объектов, содержащих критически важные данные.
* **Положение об ответственности за нарушение требований информационной безопасности** – определяет санкции и дисциплинарные меры за несоблюдение требований ИБ.
  + 1. Принятие новых Положений, а также пересмотр или отмена действующих Положений оформляется документально и утверждается приказом директора Организации.
    2. Актуализация Положений осуществляется при изменении законодательной или нормативной базы в области ИБ, а также при изменении внутренней ситуации в Организации.

# ЗАДАЧИ СИСТЕМЫ УПРАВЛЕНИЯ ИБ

* 1. Основной целью управления ИБ является ….
  2. Основными задачами управления ИБ являются:

–  Контроль выполнения правил ИБ;

– Выбор и внедрение мер обеспечения ИБ, адекватных целям и задачам деятельности Организации;

– Анализ состояния ИБ;

– Документирование предупреждающих и корректирующих мер обеспечения ИБ;

* 1. В основе управления ИБ Организации лежит подход, отраженный в модели деятельности в виде циклического процесса «планирование – реализация – контроль – совершенствование» (по ГОСТ Р ИСО/МЭК 27001-2021).
  2. Организация осуществляет деятельность по управлению рисками, повышению осведомленности сотрудников и реагированию на инциденты в области ИБ. Регулярно, не реже одного раза в два года, производится анализ состояния рисков, связанных с ИБ. Защитные меры должны основываться на всесторонней оценке этих рисков и должны быть им соразмерны.
  3. Всю ответственность за защиту своей информации и информационных ресурсов Организация возлагает на:
* Руководство Организации;
* Подразделение информационной безопасности (или ответственное лицо за ИБ);
* Руководители структурных подразделений;
* Администраторы информационных систем;
* Сотрудники Организации;
* Контрагенты и партнеры.

Все участники системы управления ИБ несут ответственность за выполнение своих обязанностей. Нарушение требований информационной безопасности рассматривается как инцидент и может повлечь дисциплинарные, административные или иные меры воздействия в соответствии с законодательством и внутренними документами Организации.

# РЕАЛИЗАЦИЯ

Реализация системы управления ИБ осуществляется на основе четкого распределения ролей и ответственности в области информационной безопасности.

# Структура и ответственность

* + 1. Ответственное лицо, назначенное приказом директора Организации, руководит работами по внедрению и совершенствованию СУИБ, в том числе организует выполнение Положений по ИБ.

# Осведомленность и информирование

**8.2.1. Обучение и повышение квалификации**

* Все сотрудники, имеющие доступ к информационным ресурсам, проходят обязательное ознакомление с Политикой информационной безопасности и связанными нормативными документами.
* Периодически (не реже одного раза в год) организуются тренинги, курсы и семинары по информационной безопасности.
* Для сотрудников, работающих с критически важными данными, предусмотрены дополнительные специализированные курсы по защите информации.
* Прием на работу новых сотрудников сопровождается вводным инструктажем по информационной безопасности.

**8.2.2. Распространение информации по ИБ**

* Внутренние корпоративные каналы связи (интранет, электронная почта, стенды) используются для распространения актуальной информации по вопросам информационной безопасности.
* Организуются тематические рассылки с рекомендациями по защите информации и предотвращению киберугроз.
* Проводятся тестирования и контрольные мероприятия для оценки уровня знаний сотрудников в области ИБ.

**8.2.3. Ответственность за информирование**

* Руководители подразделений несут ответственность за доведение до сотрудников информации о действующих правилах и требованиях в области ИБ.
* Подразделение информационной безопасности разрабатывает методические материалы и организует обучение сотрудников.
* Каждый сотрудник обязан самостоятельно следить за актуальностью своих знаний и консультироваться у ответственных лиц при возникновении вопросов по информационной безопасности.

# Реагирование на инциденты безопасности

* + 1. Для определения возможных сценариев восстановления информационной системы Организации в чрезвычайных ситуациях, конкретизации технических средств и действий работников и структурных подразделений по локализации инцидентов ИБ должны быть разработаны планы восстановительных работ для важных информационных ресурсов.
    2. Реагирование на инциденты ИБ осуществляется в соответствии с «Положением о реагировании на инциденты информационной безопасности» (Приложение № ).

# КОНТРОЛЬ

**9.1. Объекты контроля**

Контроль в области информационной безопасности охватывает следующие аспекты:

* **Соблюдение требований Политики ИБ** – анализ действий сотрудников и подразделений на соответствие установленным правилам.
* **Защищенность информационных систем** – аудит программного обеспечения, оборудования, сетей и баз данных на предмет уязвимостей.
* **Управление доступом** – проверка корректности предоставления, изменения и отзыва прав доступа.
* **Обнаружение и расследование инцидентов** – контроль мер реагирования на инциденты информационной безопасности.
* **Выполнение регламентов резервного копирования и восстановления данных**.
* **Соблюдение требований законодательства и внутренних нормативных актов**.

**9.2. Формы и методы контроля**

Контроль осуществляется с использованием следующих методов:

* **Плановые и внеплановые аудиты информационной безопасности**.
* **Мониторинг событий информационной безопасности** с помощью SIEM-систем и других инструментов.
* **Анализ логов и журналов событий информационных систем**.
* **Проверка соблюдения требований к защите персональных данных**.
* **Оценка осведомленности сотрудников о требованиях ИБ** (проведение тестов, проверочных мероприятий).
* **Пентесты и сканирование уязвимостей** для выявления возможных атак и слабых мест в системе защиты.

**9.3. Ответственные за контроль**

* **Подразделение информационной безопасности** – организует и проводит проверки, анализирует результаты, разрабатывает рекомендации.
* **Руководители подразделений** – контролируют выполнение требований ИБ внутри своих структурных единиц.
* **Системные администраторы** – следят за корректной работой технических средств защиты информации.
* **Внутренний аудит** – проводит независимую оценку состояния информационной безопасности.

**9.4. Периодичность контроля**

* **Плановые проверки** – проводятся не реже одного раза в год.
* **Внеплановые проверки** – инициируются в случае выявления нарушений, инцидентов или изменений в нормативной базе.
* **Аудит системы управления ИБ** – проводится не реже одного раза в два года или в рамках сертификации по стандартам ИБ (например, ГОСТ Р ИСО/МЭК 27001).

**9.5. Документирование и отчетность**

Результаты проверок оформляются в виде отчетов, содержащих:

* выявленные нарушения и несоответствия;
* оценку степени риска;
* рекомендации по устранению недостатков;
* сроки выполнения корректирующих мероприятий;
* перечень ответственных лиц.

Все отчеты передаются на рассмотрение руководству Организации для принятия решений о необходимых мерах.

# СОВЕРШЕНСТВОВАНИЕ

# 10.1. Предпринимаемые действия

# Для повышения эффективности системы информационной безопасности в Организации реализуются следующие меры:

# Регулярный анализ и пересмотр Политики информационной безопасности в соответствии с изменяющейся внешней и внутренней средой.

# Аудиты и оценка соответствия СУИБ требованиям стандартов (например, ГОСТ Р ИСО/МЭК 27001) и законодательным нормам.

# Обновление нормативных документов в области ИБ с учетом новых требований и лучших практик.

# Инвестирование в технологии защиты информации, включая системы предотвращения вторжений, шифрование данных, контроль доступа и мониторинг событий безопасности.

# Развитие культуры информационной безопасности среди сотрудников через регулярное обучение, тестирование знаний и тренинги.

# 10.2. Порядок мониторинга информационной безопасности

# Мониторинг ИБ осуществляется на постоянной основе и включает:

# Автоматизированное отслеживание событий безопасности с использованием SIEM-систем и других инструментов.

# Регулярный анализ уязвимостей и тестирование защиты с применением пентестов и сканеров безопасности.

# Контроль за управлением доступом к информационным системам и критически важным данным.

# Оценку эффективности действующих мер защиты и корректировку стратегии обеспечения ИБ.

# 10.3. Реагирование на инциденты и корректирующие меры

# В случае выявления нарушений или инцидентов информационной безопасности в Организации принимаются меры по их устранению:

# Разрабатываются и внедряются планы корректирующих действий.

# Обеспечивается оперативное реагирование на инциденты в соответствии с утвержденными процедурами.

# Производится анализ причин инцидентов и вырабатываются рекомендации по предотвращению аналогичных случаев в будущем.

# Улучшаются системы обнаружения и реагирования, а также повышается уровень подготовки сотрудников.

# 10.4. Порядок принятия решений по совершенствованию СУИБ

# Изменения и улучшения в СУИБ инициируются по результатам аудитов, анализа инцидентов, тестирования уязвимостей и изменения нормативных требований.

# Предложения по совершенствованию направляются в подразделение информационной безопасности и рассматриваются на заседаниях руководства.

# Решения о внедрении новых мер защиты утверждаются руководством Организации.

# 10.5. Пересмотр, принятие и отмена нормативных документов по ИБ

# Все документы, регулирующие вопросы информационной безопасности, пересматриваются не реже одного раза в два года или при необходимости (например, при изменении законодательства).

# Новые документы принимаются на основании анализа рисков и актуальных угроз.

# Отмена устаревших нормативных актов производится с учетом их актуальности и заменяется новыми версиями.