

# ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

## 1. Цель

1.1. Общество с ограниченной ответственностью ПРОИЗВОДСТВЕННАЯ КОМПАНИЯ «СЕВАСТОПОЛЬ» (далее по тексту – ООО ПК «СЕВАСТОПОЛЬ») для целей осуществления своих основных видов деятельности и поддержания своих бизнес-процессов на регулярной основе обрабатывает информацию ограниченного доступа, содержащую сведения, относящиеся к коммерческой тайне, персональным данным и банковской тайне.

1.2. ООО ПК «СЕВАСТОПОЛЬ» обязуется сохранять конфиденциальность, целостность и доступность обрабатываемой информации.

1.3. Настоящая Политика информационной безопасности (далее по тексту – Политика) является документом, который отражает систему взглядов на цели, задачи, принципы и основные механизмы обеспечения информационной безопасности в ООО ПК «СЕВАСТОПОЛЬ».

1.4. Политика является общедоступным документом и размещена в открытом доступе на веб-сайте ООО ПК «СЕВАСТОПОЛЬ».

## 2. Область применения

2.1. Политика применяется при использовании информации, информационных систем, электронно-вычислительных устройств, приложений и сетевых сервисов (далее по тексту – информационные активы), используемых для ведения бизнеса.

2.2. Действие настоящей Политики распространяется на деятельность всех сотрудников ООО ПК «СЕВАСТОПОЛЬ».

## 3. Ответственность

3.1. Подразделение информационной безопасности отвечает за разработку и поддержание Политики в актуальном состоянии.

3.2. Подразделение информационной безопасности несет ответственность за соблюдение настоящей Политики и может привлекать другие структурные подразделения, поставщиков услуг и руководство ООО ПК «СЕВАСТОПОЛЬ» для поддержания и контроля ее соблюдения.

## 4. Соответствие

4.1. Соответствие Политике обязательно для ООО ПК «СЕВАСТОПОЛЬ». Нарушение соответствия настоящей Политики повлечет дисциплинарную, административную и/или уголовную ответственность в соответствии с действующим законодательством Российской Федерации и локальными нормативными документами ООО ПК «СЕВАСТОПОЛЬ».

## 5. Цели информационной безопасности

Целями ООО ПК «СЕВАСТОПОЛЬ» в области обеспечения информационной безопасности являются:

5.1. Поддержание стратегии развития бизнеса компании посредством защиты персональных данных и коммерческой тайны.

5.2. Соблюдение требований российского законодательства и нормативных документов, регламентирующих порядок обработки и защиты персональных данных и коммерческой тайны.

5.3. Создание процесса управления рисками информационной безопасности.

5.4. Управление выявленными рисками информационной безопасности на приемлемом уровне посредством разработки и внедрения планов минимизации рисков.

5.5. Повышение уровня осведомленности всего персонала по вопросам обеспечения информационной безопасности.

5.6. Установление ответственности за обеспечение и управление информационной безопасностью в компании.

## 6. Обеспечение информационной безопасности

### 6.1. Организация информационной безопасности.

В ООО ПК «СЕВАСТОПОЛЬ» разработаны, поддерживаются и внедряются политики, процедуры и стандарты обеспечения информационной безопасности для защиты конфиденциальности, целостности и доступности своих информационных активов.

### 6.2. Управление доступом.

Доступ к информационным системам компании контролируется на протяжении всего жизненного цикла учетной записи: от первоначальной идентификации и аутентификации пользователя до предоставления, изменения и блокировки прав доступа. Права доступа для учетных записей пользователей в информационных системах предоставляются с использованием принципа минимальных привилегий и периодически пересматриваются. Пароли соответствуют требованиям политики компании к их сложности и периодически меняются.

### 6.3. Непрерывность бизнеса и аварийное восстановление.

ООО ПК «СЕВАСТОПОЛЬ» защищает критически важные информационные активы от последствий серьезных сбоев или аварий путем разработки и реализации планов обеспечения непрерывности и восстановления деятельности. ООО ПК «СЕВАСТОПОЛЬ» обеспечивает резервное копирование критически важных данных и стремится к предотвращению сбоев, обеспечению своевременного восстановления критических данных после сбоев, а также к поддержанию выполнения критически важных бизнес-процессов во время сбоев, сохраняя при этом конфиденциальность информации.

#### **6.4. Управление коммуникациями и сетевой безопасностью.**

Для обеспечения эффективного управления коммуникациями и сетевой безопасностью внедрены различные системы и сервисы защиты сетевой инфраструктуры, такие как: межсетевые экраны, системы предотвращения и обнаружения вторжения, системы и сервисы защиты от атак типа отказа в обслуживании (DDoS) и средства контроля и защиты доступа к беспроводным сетям и в сеть Интернет, а также реализована сегментация сети для того, чтобы ООО ПК «СЕВАСТОПОЛЬ» защищал свои информационные активы от их компрометации как со стороны внешних, так и со стороны внутренних нарушителей.

##### **6.4.1 Системы предотвращения и обнаружения вторжения.**

Системы предотвращения и обнаружения вторжения развернуты в компании на уровне сетевой инфраструктуры и на уровне конечных пользовательских устройств. Безопасность сетевой инфраструктуры находится под круглосуточным мониторингом.

##### **6.4.2 Защита инфраструктуры беспроводных сетей.**

Инфраструктура беспроводных сетей в офисах ООО ПК «СЕВАСТОПОЛЬ» защищена с помощью механизмов контроля доступа, аутентификации, шифрования и контроля появления несанкционированных точек доступа.

##### **6.4.3 Защита от атак типа отказа в обслуживании.**

Защита от DDoS-атак строится в ООО ПК «СЕВАСТОПОЛЬ» по принципу эшелонированной защиты:

- защита от атак типа DDoS на пограничных устройствах поставщика услуг Интернет;
- использование внешних провайдеров защиты от DDoS-атак;
- использование внутренних систем предотвращения DDoS-атак в компании.

##### **6.4.4 Защита доступа в Интернет.**

Сотрудникам ООО ПК «СЕВАСТОПОЛЬ» предоставляется доступ в Интернет только для исполнения своих должностных обязанностей. Фильтрация доступа осуществляется в соответствии с установленными правилами. Дополнительные доступы предоставляются только по согласованию с руководством и подразделением информационной безопасности.

##### **6.5 Безопасность рабочих станций и ноутбуков.**

Безопасность корпоративных рабочих станций и ноутбуки сотрудников обеспечивается, но не ограничивается, за счет применения следующих средств защиты:

- средства антивирусной защиты, встроенного в рабочие сборки операционных систем по умолчанию и настроенного на регулярное сканирование и получение актуальных обновлений антивирусных баз;
- средств шифрования дисков на корпоративных ноутбуках сотрудников;
- средств блокировки записи данных на съемные носители информации;
- средств удаленного подключения сотрудников к корпоративной сети с многофакторной аутентификацией.

##### **6.6. Соблюдение нормативных требований.**

ООО ПК «СЕВАСТОПОЛЬ» соблюдает российские законодательные и регуляторные требования по информационной безопасности.

##### **6.7. Криптографическое управление.**

В ООО ПК «СЕВАСТОПОЛЬ» применяются криптографические средства защиты информации для поддержания конфиденциальности информации, обеспечения проверки целостности и электронных подписей. Требования к алгоритмам шифрования и длине ключей при хранении, передаче по каналам связи и использовании информации, определены в порядке криптографической защите информации.

##### **6.8. Управление инцидентами информационной безопасности.**

В рамках управления инцидентами информационной безопасности ООО ПК «СЕВАСТОПОЛЬ» проводит следующие работы:

- осуществляет координирование инцидентов информационно безопасности;
- осуществляет своевременное расследование инцидентов информационной безопасности;
- оценивает риск, связанный с инцидентом информационной безопасности;
- внедряет корректирующие защитные меры в целях минимизации риска от инцидента информационной безопасности,

##### **6.9. Управление рисками информационной безопасности.**

ООО ПК «СЕВАСТОПОЛЬ» управляет рисками информационной безопасности по всем процессам обеспечения защиты информации. Оценка рисков проводится на регулярной основе и для различных активов: процессы, технологии, информационные системы, люди, информация. Регулярный процесс оценки рисков информационной безопасности проводится для решения следующих задач:

- идентификация всех информационных, программных и физических активов;
- выявление угроз и уязвимостей информационной безопасности;
- количественная оценка риска информационной безопасности;
- обработка риска информационной безопасности для выделения средств на минимизацию факторов, представляющих наибольший риск;
- внедрение средств и технологий защиты информации в областях, обеспечивающих максимальное снижение рисков для персональных данных и коммерческой тайны клиентов.

#### **6.10. Регистрация и мониторинг событий.**

В ООО ПК «СЕВАСТОПОЛЬ» внедрены требования к регистрации событий, процессу мониторинга и анализу активностей сотрудников в инфраструктуре и информационных системах. ООО ПК «СЕВАСТОПОЛЬ» соблюдает все соответствующие юридические, нормативные и договорные требования, применимые к регистрации и мониторингу событий.

#### **6.11. Управление изменениями.**

Все изменения в информационной инфраструктуре производятся в соответствии с внедренными процессами управления изменениями, управления конфигурациями, а также процессами управления техническими ресурсами.

#### **6.12. Физическая безопасность и безопасность окружающей среды.**

ООО ПК «СЕВАСТОПОЛЬ» применяет защитные меры для предотвращения несанкционированного доступа в свои офисы, а также обеспечивает физическую защиту информационных активов от возможных природных стихийных угроз.

Меры, применяемые ООО ПК «СЕВАСТОПОЛЬ», включают, но не ограничиваются:

- системы контроля доступа;
- системы видеонаблюдения;
- системы охранной и пожарной сигнализации;
- сейфы и специализированные шкафы.

#### **6.13. Защита информации при управление жизненным циклом информационных систем.**

ООО ПК «СЕВАСТОПОЛЬ» принимает меры обеспечения защиты информации на всех этапах жизненного цикла информационных систем (ввод в эксплуатацию, эксплуатация, вывод из эксплуатации, модернизация), в том числе определение состава мер, должный контроль, контроль отсутствия уязвимостей защиты информации, чтобы гарантировать выявление и своевременное устранение и/или минимизацию рисков информационной безопасности.

#### **6.14. Управление уязвимостями и обновлениями.**

На регулярной основе ООО ПК «СЕВАСТОПОЛЬ» проводит анализ уязвимостей своей информационной инфраструктуры и обеспечивает установку обновлений безопасности программного обеспечения. Управление и контроль исправления уязвимостей в инфраструктуре осуществляется за счет регулярного мониторинга и взаимодействия подразделений.

#### **6.15. Защита от утечек информации.**

Предотвращение утечек информации осуществляется за счет регулярного мониторинга каналов утечки информации, применения технических средств контроля, организационных мер защиты и обучения работников ООО ПК «СЕВАСТОПОЛЬ».

Каналы контроля включают в себя, но не ограничиваются:

- исходящую электронную почту;
- передачу и загрузку файлов в Интернет;
- корпоративные мессенджеры;
- печать документов.

ООО ПК «СЕВАСТОПОЛЬ» контролирует утечку данных, чтобы предотвратить риски кражи, а также случайной передачи или преднамеренного раскрытия конфиденциальной информации.

#### **6.16. Анализ защищенности.**

Внутренний и внешний анализ защищенности инфраструктуры ООО ПК «СЕВАСТОПОЛЬ» проводится на регулярной основе. Кроме того, может быть заказан внешний анализ защищенности инфраструктуры специалистами вендора для обеспечения дополнительной уверенности в эффективности применяемых методов и средств защиты информации.

#### **6.17. Информационная безопасность вендоров\партнеров.**

В ООО ПК «СЕВАСТОПОЛЬ» выстроен процесс для проведения первоначальной и постоянной комплексной проверки партнеров, которые заключают официальные деловые соглашения. Каждый партнер, которому планируется предоставить доступ к защищаемой информации, подписывает соглашение о неразглашении и/или соглашение о конфиденциальности.