государственное казенное учреждение Самарской области «Комплексный центр социального обслуживания населения Поволжского округа»

ПОЛИТИКА БЕЗОПАСНОСТИ КОРПОРАТИВНОЙ СЕТИ ГКУ СО «КЦСОН ПОВОЛЖСКОГО ОКРУГА»

Новокуйбышевск

2024

**СОДЕРЖАНИЕ**

[ВВЕДЕНИЕ 3](#_Toc163742210)

[1. ТЕРМИНЫ И СОКРАЩЕНИЯ В СФЕРЕ ПОЛИТИКИ БЕЗОПАСНОСТИ СЕТИ 5](#_Toc163742211)

[2. ОБЩИЕ ПОЛОЖЕНИЯ ПОЛИТИКИ БЕЗОПАСНОСТИ СЕТИ 6](#_Toc163742212)

[3. ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ДОСТУПА И РЕГИСТРАЦИИ 7](#_Toc163742213)

[4. ТРЕБОВАНИЯ ПО ЗАЩИТЕ ОТ ВРЕДОНОСНОГО ПО 8](#_Toc163742214)

[5. ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ РЕСУРСОВ СЕТИ ИНТЕРНЕТ 9](#_Toc163742215)

[6. КОНТРОЛЬ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ СЕТИ 10](#_Toc163742216)

# ВВЕДЕНИЕ

Политика информационной безопасности (Политика) является частью системы обеспечения информационной безопасности (СОИБ) ГКУ СО «КЦСОН Поволжского округа» (далее - Компания).

Политика определяет высокоуровневые цели, содержание и основные направления деятельности по обеспечению информационной безопасности (ИБ) Компании. Положения Политики являются основополагающими и детализируются применительно к одной или нескольким областям ИБ, видам и технологиям деятельности Компании в других нормативных документах по обеспечению ИБ.

Действие Политики распространяется на все информационные активы Компании независимо от их места установки и использования. Требования Политики ИБ обязательны для соблюдения всем персоналом Компании, а также сотрудниками сторонних организаций, имеющим доступ к информационным активам Компании.

Политика разработана в соответствии с международными стандартами и рекомендациями по информационной безопасности, применимыми нормами международного права, законодательством стран присутствия Компании, включая страну ее местопребывания, а также внутренней нормативно-правовой базой Компании.

В основе разработки Политики лежат следующие документы и стандарты:

* Концепция информационной безопасности Компании;
* Положение о служебной и коммерческой тайне Компании;
* Положение о работе с персональными данными в Компании;
* Инструкция по делопроизводству;
* ISO/IEC 17799:2005 (второе издание) (с 2007 года - ISO/IEC 27002) Информационные технологии. Кодекс практики по управлению информационной безопасностью;
* ISO/IEC 27001:2005 Информационные технологии. Методы защиты. Системы управления информационной безопасностью. Требования;
* ГОСТ Р ИСО/мЭк 17799-2005 Информационные технологии. Практические правила управления информационной безопасностью;
* ГОСТ Р ИСО/мЭк 27001-2006 Информационные технологии. Методы и средства обеспечения безопасности. Системы управления информационной безопасностью. Требования.

# ТЕРМИНЫ И СОКРАЩЕНИЯ В СФЕРЕ ПОЛИТИКИ БЕЗОПАСНОСТИ СЕТИ

Политика безопасности сети (ПБС) - набор правил, процедур и рекомендаций, направленных на обеспечение безопасности сети компании.

Вредоносное программное обеспечение (ВПО) - программы, способные нанести ущерб компьютерным системам, сетям и данным.

VPN (Virtual Private Network) - виртуальная частная сеть, обеспечивающая защищенное соединение между удаленными устройствами.

АИС - автоматизированная информационная система.

ИБ - информационная безопасность.

СОИБ - система обеспечения информационной безопасности. НСД - несанкционированный доступ.

ОСОИБ - ответственный сотрудник по обеспечению информационной безопасности.

ПО - программное обеспечение.

СКЗИ - средства криптографической защиты информации.

СУБД - система управления базами данных.

# ОБЩИЕ ПОЛОЖЕНИЯ ПОЛИТИКИ БЕЗОПАСНОСТИ СЕТИ

Целями политики безопасности сети являются обеспечение конфиденциальности, целостности и доступности данных, защита сетевой инфраструктуры, предотвращение и реагирование на угрозы безопасности.

Положения политики распространяются на все сотрудников, администраторов систем, поставщиков услуг и внешних пользователей, имеющих доступ к корпоративной сети.

Все сотрудники обязаны соблюдать политику безопасности сети и проходить обучение и аудиты по безопасности на регулярной основе.

# ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ДОСТУПА И РЕГИСТРАЦИИ

Все сотрудники обязаны использовать уникальные учетные записи для доступа к сети и ресурсам компании.

Необходимо использовать сильные пароли и механизмы двухфакторной аутентификации для повышения уровня безопасности.

Логи доступа и регистрации должны быть включены и регулярно мониторироваться на предмет несанкционированных действий.

# ТРЕБОВАНИЯ ПО ЗАЩИТЕ ОТ ВРЕДОНОСНОГО ПО

Все устройства, подключенные к корпоративной сети, должны быть обязательно защищены антивирусным программным обеспечением.

Настройка антивирусного ПО на автоматический режим сканирования всех файлов и папок при загрузке или доступе, с последующим удалением обнаруженных угроз.

Рекомендуется регулярное проведение обновлений и патчей для всех установленных программ, включая Microsoft Office 2010, Adobe Acrobat Reader, VLC Media Player и др., чтобы устранить известные уязвимости и защитить систему от возможных атак.

Настройка брандмауэра на всех устройствах для блокирования вредоносного сетевого трафика, за исключением разрешенных портов и протоколов.

Настройка строгих политик безопасности паролей, включая требование сложных паролей и сроков их смены, а также использование механизмов двухфакторной аутентификации.

Необходимо проводить обучение сотрудников по базовым мерам безопасности, таким как неразглашение паролей, неоткрывание подозрительных вложений в электронной почте и осторожное поведение в Интернете.

# ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ РЕСУРСОВ СЕТИ ИНТЕРНЕТ

Установка и настройка расширений браузеров Microsoft Edge и Yandex для блокировки вредоносных сайтов, рекламы и отслеживания пользователей.

Включение защиты от фишинговых атак на уровне браузера, чтобы предотвратить переход на поддельные или вредоносные сайты.

Регулярное обновление браузеров и расширений до последних версий для закрытия известных уязвимостей.

Настройка политик безопасности для использования приложений, связанных с Интернетом, таких как Zoom, с акцентом на конфиденциальность и безопасность сетевых соединений.

Проведение обучения сотрудников по правилам безопасного поведения в Интернете, распознаванию угроз и предотвращению атак.

# КОНТРОЛЬ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ СЕТИ

Проводятся регулярные аудиты сетевой инфраструктуры на предмет уязвимостей и соблюдения правил безопасности.

Запрещается использование несанкционированных средств и сервисов, которые могут представлять угрозу для безопасности сети.

Разрабатывается и поддерживается план реагирования на инциденты безопасности для оперативного устранения угроз и восстановления после атак.