Утверждено

Приказом № 10 Генерального директора ПАО «ЧЕЛметБанк»

Михайловым Ярославом

от 30.03.2021 г.

Политика информационной безопасности ООО «ЧЕЛметБанк»

Челябинск 2021

Основной целью, на достижение которой направлены все положения настоящей Политики, является защита информационных ресурсов .

|  |  |
| --- | --- |
| Виды угроз: | Характер угроз: |
| Несанкционированный доступ | Умышленные |
| Утечка информации | Случайные |
| Потеря данных | Случайные |
| Мошенничество | Умышленные |
| Кибер-терроризм | Умышленные |
| Вымогательство | Умышленные |
| Взлом | Умышленные |

Для достижения устранения угроз необходимо обеспечивать эффективное решение

**Следующих задач:**

* создание механизма оперативного реагирования на угрозы ИБ;
* соответствие требованиям Федерального законодательства, нормативно - методических документов ФСБ России, ФСТЭК России и договорным обязательствам в части ИБ.
* своевременное выявление, оценка и прогнозирование источников угроз ИБ;
* предотвращение и/или снижение ущерба от реализации угроз ИБ;
* защита от вмешательства в процесс функционирования ИС посторонних лиц;

**1.Общие положения**

Настоящая политика информационной безопасности предусматривает принятие необходимых мер в целях защиты активов от случайного или преднамеренного изменения, раскрытия или уничтожения, а также в целях соблюдения конфиденциальности, целостности и доступности информации, обеспечения процесса автоматизированной обработки данных в «ЧЕЛметБанк».

Ответственность за соблюдение информационной безопасности несет каждый сотрудник «ЧЕЛметБанк», при этом первоочередной задачей является обеспечение безопасности всех активов «ЧЕЛметБанк». Это значит, что информация должна быть защищена не менее надежно, чем любой другой основной актив компании. Главные цели «ЧЕЛметБанк» не могут быть достигнуты без своевременного и полного обеспечения сотрудников информацией, необходимой им для выполнения своих служебных обязанностей.

В настоящей Политике под термином «сотрудник» понимаются все сотрудники компании. На лиц, работающих в «ЧЕЛметБанк» по договорам гражданско-правового характера, в том числе прикомандированных, положения настоящей Политики распространяются в случае, если это обусловлено в таком договоре.

**1.1. Цель и назначение.**

Основной целью, на достижение которой направлены все положения настоящей Политики, является защита информационных ресурсов от возможного нанесения им какого – либо ущерба.

Для достижения цели необходимо:

· своевременное выявление, оценка и прогнозирование источников угроз ИБ;

· создание механизма оперативного реагирования на угрозы ИБ;

· защита от вмешательства в процесс функционирования ИС посторонних лиц;

· обеспечение непрерывности критических бизнес-процессов;

· достижение адекватности мер по защите от угроз ИБ;

**1.2. Область применения настоящей Политики**

Настоящая Политика распространяется на все бизнес-процессы Учреждения и обязательна для применения всеми сотрудниками и руководством Учреждения, а также пользователями его информационных ресурсов.

Настоящая политика распространяется на информационные системы учреждения.

Лица, осуществляющие разработку внутренних документов Учреждения, регламентирующих вопросы информационной безопасности, обязаны руководствоваться настоящей Политикой

**2. Требования.**

**2.1. Ответственность за информационные активы**

В отношении всех собственных информационных активов Компании, активов, находящихся под контролем компании, а также активов, используемых для получения доступа к инфраструктуре «ЧЕЛметБанк», должна быть определена ответственность соответствующего сотрудника компании.

.

**2.2. Контроль доступа к информационным системам**

**2.2.1. Общие положения**

Основными пользователями информации в информационной системе Учреждения являются сотрудники структурных подразделений. Уровень полномочий каждого пользователя определяется индивидуально. Каждый сотрудник пользуется только предписанными ему правами по отношению к информации, с которой ему необходимо работать в соответствии с должностными обязанностями. Каждый пользователь должен иметь свою учетную запись.

Регистрируемые учётные записи подразделяются на:

· Пользовательские – предназначенные для аутентификации пользователей ИР Учреждения;

· Системные – используемые для нужд операционной системы;

· Служебные – предназначенные для функционирования отдельных процессов или приложений.

**2.2.2. Доступ третьих лиц к системам Компании**

Каждый сотрудник обязан немедленно уведомить руководителя Департамента информационных технологий и руководителя Департамента защиты информации обо всех случаях предоставления доступа третьим лицам к ресурсам корпоративной сети.

Доступ третьих лиц к информационным системам компании должен быть обусловлен производственной необходимостью. В связи с этим, порядок доступа к информационным ресурсам Компании должен быть четко определен, контролируем и защищен.

**3. Структура документов**

В целях создания взаимосвязанной структуры нормативных документов Учреждения в области обеспечения информационной безопасности, разрабатываемые и обновляемые нормативные документы должны соответствовать следующей иерархии:

|  |
| --- |
| Политика информационной безопасности |
| Инструкции, регламенты, |
| Документы, подтверждающие исполнение нормативных актов верхних уровней |

1) Настоящая Политика является внутренним нормативным документом по ИБ первого уровня.

2) Документы второго уровня – инструкции, порядки, регламенты и прочие документы, описывающие действия сотрудников Учреждения по реализации документов первого и второго уровня.

3) Документы третьего уровня – отчётные документы о выполнении требований документов верхних уровней.

**4. Оценка и обработка рисков**

В учреждении должны быть определены требования к безопасности путём методической оценки рисков. Результаты оценки должны определять соответствующую реакцию руководства, приоритеты управления рисками ИБ и набор механизмов контроля для защиты от этих рисков.

**5. Защита оборудования и безопасность**

Сотрудники должны постоянно помнить о необходимости обеспечения физической безопасности оборудования, на котором хранятся информация «ЧЕЛметБанк».

Сотрудникам запрещено самостоятельно изменять конфигурацию аппаратного и программного обеспечения. Все изменения производят авторизованные специалисты Департамента информационных технологий, после согласования изменений с Департаментом защиты информации.

**6. Контроль доступа**

Основными пользователями информации в информационной системе Учреждения являются сотрудники структурных подразделений.

Уровень полномочий каждого пользователя определяется индивидуально.

Допуск пользователей к работе с информационными ресурсами должен быть строго регламентирован.

Каждому пользователю, допущенному к работе с конкретным информационным активом

В общем случае запрещено создавать и использовать общую пользовательскую учётную запись для группы пользователей.

Одновременное использование одной общей пользовательской учётной записи разными пользователями запрещено.

Служебные учётные записи используются только для запуска и работы сервисов или приложений.

Использование системных или служебных учётных записей для регистрации пользователей в системе категорически запрещено.

**6.2. Управление паролями**

Пароли – средство проверки личности пользователя для доступа к ИС или сервису, обеспечивающее идентификацию и аутентификацию на основе сведений, известных только пользователю.

**7. Ответственность**

Ответственность за поддержание положений настоящей Политики в актуальном состоянии, создание, внедрение, координацию и внесение изменений в процессы СУИБ Учреждения лежит на руководстве отдела ИС СМТ.

Все руководители несут прямую ответственность за реализацию Политики и её соблюдение персоналом в соответствующих подразделениях.

Работники Учреждения несут персональную ответственность за соблюдение требований документов СУИБ и обязаны сообщать обо всех выявленных нарушениях в области информационной безопасности в отдел ИС СМТ.

Нарушение требований нормативных актов Учреждения по обеспечению ИБ является чрезвычайным происшествием и будет служить поводом и основанием для проведения служебного расследования.