

УТВЕРЖДАЮ

Генеральный директор
ООО «Сатурн»

Соколов А.А.

«__» _____ 2018 г.

ПРОЕКТ

СИСТЕМА МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

ПОЛИТИКА
ПРЕДОСТАВЛЕНИЯ ДОСТУПА
К ИНФОРМАЦИОННЫМ РЕСУРСАМ

[ИБ-102]

2018г.

Оглавление

Введение	3
1. Термины и сокращения	Ошибка! Закладка не определена.
2. Цели политики	3
3. Область применения политики	4
4. Ключевые требования	Ошибка! Закладка не определена.
12. Сведения о документе	5
13. Срок действия и порядок внесения изменений.....	6
14. История изменений.....	7

Введение

Согласованные, формализованные процессы предоставления доступа к информационным ресурсам являются одним из базовых механизмов защиты информации в информационных системах Компании.

Под субъектами доступа понимаются как пользователи ИС Компании, так и служебные учетные записи, необходимые для функционирования информационных систем. Формализованные процессы, позволяющие контролировать организацию правил.

1. Термины и определения

Для целей настоящего документа используются следующие основные понятия:

- 1.1. **Субъект доступа** – это лицо или процесс, действия которого регламентируются правилами разграничения доступа.
- 1.2. **Информационный ресурс** (информационный объект доступа) - организованная по определенным принципам и тематической направленности совокупность документированной информации, включающая базы данных и знаний, другие массивы информации.
- 1.3. **Информационная система** - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.
- 1.4. **Владелец информационного ресурса** – это лицо, осуществляющее владение и пользование указанным информационным ресурсом и реализующее полномочия распоряжения ресурсом.
- 1.5. **Владелец информационной системы** – это лицо, осуществляющее владение и пользование указанной информационной системой и реализующее полномочия распоряжения информационной системой.
- 1.6. **Защищаемая информация** - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.
- 1.7. **Коммерческая тайна** - режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.
- 1.8. **Информация, составляющая коммерческую тайну**, - сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны;
- 1.9. **Доступ к защищаемой информации** - ознакомление определенных лиц с защищаемой информацией с согласия ее владельца или на ином законном основании при условии сохранения конфиденциальности этой информации.
- 1.10. **Уровень полномочий субъекта доступа** - совокупность прав доступа субъекта доступа.

- 1.11. **Передача защищаемой информации** - передача защищаемой информации и зафиксированной на материальном носителе, ее обладателем контрагенту на основании договора в объеме и на условиях, которые предусмотрены договором, включая условие о принятии контрагентом установленных договором мер по охране ее конфиденциальности;
- 1.12. **Контрагент** - сторона гражданско-правового договора, которой владелец защищаемой информации передал эту информацию.
- 1.13. **Разглашение защищаемой информации** - действие или бездействие, в результате которых защищаемая информация в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия владельца такой информации либо вопреки трудовому или гражданско-правовому договору.

2. Цели политики

Основными целями настоящей Политики являются:

- 2.1. Создание единого подхода к обеспечению информационной безопасности при предоставлении доступа к информационным ресурсам компании.
- 2.2. Определение порядка и требований, реализация которых обязательна для обеспечения эффективности деятельности компании, сохранения репутации и выполнения компанией своих обязательств перед контрагентами.
- 2.3. Разграничение полномочий и определение ответственности за обеспечение информационной безопасности при предоставлении доступа к информационным ресурсам компании.

3. Область применения политики

Настоящая Политика применяется ко всем информационным ресурсам и информационным системам компании, а также ко всем лицам, имеющим любую форму доступа к любым информационным ресурсам компании.

Настоящая Политика регламентирует порядок предоставления доступа к информационным ресурсам компании, порядок контроля соблюдения Политики и ответственность за ее несоблюдение.

4. Общие принципы предоставления доступа к ресурсам

- 4.1. Предоставление доступа к информационным ресурсам и информационным системам компании не может осуществляться без согласия Владельца информационного ресурса или информационной системы.
- 4.2. Предоставление доступа сотруднику компании не может осуществляться без ведома его непосредственного руководителя.
- 4.3. Уровень полномочий субъекта доступа должен соответствовать принципу минимальной достаточности для решения поставленных перед субъектом доступа (пользователем) функциональных задач и/или должностных обязанностей.
- 4.4. Предоставление доступа к информационным ресурсам и информационным системам компании не может быть полным и неограниченным по времени.
- 4.5. Предоставление доступа для третьих лиц (не являющихся сотрудниками компании) должно осуществляться только на основе действующих договоров и/или соглашений.

- 4.6. Лицо, инициирующее предоставление доступа, обязано представить соответствующее обоснование необходимости предоставления доступа.
- 4.7. Лицо, которому предоставляется доступ (субъект доступа) должно быть ознакомлено с Политикой использования ресурсов компании.
- 4.8. Предоставление доступа к ресурсам компании может осуществляться только в законных целях, не противоречащих интересам компании и Законодательству Российской Федерации.

5. Порядок предоставления доступа к ресурсам

Общий порядок предоставления доступа к ресурсам компании включает следующие этапы:

- 1) Инициатор оформляет заявку на предоставление доступа к информационным активам и/или информационным системам компании.
- 2) Заявка проходит согласование у владельцев информационных активов и/или информационных систем компании.
- 3) Заявка проходит согласование в Дирекции по безопасности.
- 4) Обслуживающее подразделение осуществляет предоставление доступа на установленный период времени.
- 5) Завершение предоставления доступа обслуживающим подразделением с уведомлением Инициатора и владельцев информационных активов и/или информационных систем компании.

- 5.1. Инициатор предоставления доступа
- 5.2. Форма заявки на предоставление доступа
- 5.3. Порядок прохождения заявки на согласование
- 5.4. Конфликт интересов и разрешение споров

6. Контроль

Компания оставляет за собой право защищать свою репутацию путём регулярного контроля использования работниками Информационных ресурсов Компании.

Контроль использования коммерческого программного обеспечения осуществляется согласно

Список ознакомления

Все сотрудники компании.

разработан

Директор по ИБ	_____	Волков Д.Д.
----------------	-------	-------------

Согласовано

Юрист	_____	_____
	“ ____ ” _____ 2018г	
Начальник Отдела управления качеством	_____	_____
	“ ____ ” _____ 2018г	

7. Сведения о документе

- 7.1. Настоящая Политика разработана в соответствии с действующим законодательством РФ в

области защиты информации.

- 7.2. Методологической основой для разработки настоящей Политики является Концепция информационной безопасности Компании.
- 7.3. Настоящая Политика является методологической основой для разработки всех нормативных документов, касающихся обеспечения информационной безопасности в Компании.
- 7.4. Настоящая Политика разрабатывается и согласуется с членами Комиссии по защите информации.
- 7.5. Настоящая Политика вступает в действие с момента утверждения ее Генеральным директором Компании.

8. Срок действия и порядок внесения изменений

- 8.1. Срок действия настоящей Политики – один год с момента утверждения.
- 8.2. По истечении срока действия (или ранее - при необходимости) Политика подлежит пересмотру. Внесение изменений в Политику осуществляет ответственный за ИБ в Компании. Пересмотренная Политика утверждается генеральным директором Компании.

ЛИСТ СОГЛАСОВАНИЙ

к Политике информационной безопасности

РАЗРАБОТАЛ:

СОГЛАСОВАНО

9. История изменений

№	Дата	Версия	Предмет изменений	Автор
1.				
2.				
3.				