УТВЕРЖДАЮ

Генеральный директор
ООО «Сатурн»

Соколов А.А.

«___» _____ 2018 г.

СИСТЕМА МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

[ИБ-101]

2018г.

Оглавление

Введение 3
1. Термины и сокращения 3
2. Цели политики 4
3. Область применения политики 4
4. Ключевые требования 4
5. Классификация информации 5
6. Разграничение доступа к информации 5
7. Средства обеспечения безопасности информации 6
8. Разработка и поддержка информационных систем 7
9. Безопасность персонала 7
10. Разделение полномочий 7
11. Защита персональных данных 8
12. Сведения о документе 8
13. Срок действия и порядок внесения изменений 8
14. История изменений 9

Введение

Эффективная деятельность современного предприятия невозможна без информационной среды, обеспечивающей информационное взаимодействие, доступ к требуемой информации и удовлетворение потребности в информационных продуктах и услугах участников всех бизнес-процессов. В ООО «Сатурн» (далее – Компания) такой информационной средой является корпоративная распределенная информационно-вычислительная система.

В связи с тем, что в корпоративной информационно-вычислительной системе накапливаются и обрабатываются значительные объемы информации, а сама корпоративная информационно-вычислительная система является весьма сложной и распределенной инфраструктурой, одним из важнейших и неотъемлемых факторов, обеспечивающих ее функциональность, а также конфиденциальность, целостность и доступность размещенной в ней информации, является информационная безопасность.

Предпосылкой создания настоящего документа является необходимость определения требований и описания общего подхода к обеспечению информационной безопасности в корпоративной информационно-вычислительной системе Компании.

1. Термины и сокращения

1.1. Сокращения

Сокращение	Значение
ИБ	Информационная безопасность
СМИБ	Система менеджмента информационной безопасности
Компания	ООО «Сатурн»
ИР	Информационный ресурс
КИВС	Корпоративная информационно-вычислительная система
ПО	Программное обеспечение
ПДн	Персональные данные
ИСПДН	Информационная система персональных данных
УОБ	Управление обеспечения бизнеса
ДИТ	Дирекция по информационным технологиям
СВТ	Средства вычислительной техники

1.2. Термины

Термин	Определение
Информационная безопасность	Обеспечение конфиденциальности, целостности и доступности информации
Система управления информационной безопасностью	Та часть общей системы управления Компании, основанной на оценке бизнес рисков, которая предназначена для создания, внедрения, эксплуатации, мониторинга, анализа, сопровождения и совершенствования информационной безопасности

Термин	Определение
Ресурс	Все, что имеет ценность для Компании
Информационный ресурс	Совокупность некоторого объема информации, методов ее обработки и отображения, размещенная в информационной системе
ИТ-ресурс	Совокупность информационных ресурсов и информационных систем, технических средств связи, передачи данных и обработки информации, используемые Компанией на законных основаниях (собственность, аренда и т.д.)
Корпоративная информационно-вычислительная система	Совокупность всех информационных систем, технических средств связи, передачи данных и обработки информации, используемые Компанией на законных основаниях (собственность, аренда и т.д.)
Персональные данные	Любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация
Информационная система персональных данных	Информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств

2. Цели политики

Основными целями настоящей Политики являются:

2.1. Создание единого подхода к обеспечению информационной безопасности в Компании;

2.2. Определение требований информационной безопасности, реализация которых обязательна для обеспечения эффективности деятельности Компании, сохранения репутации и выполнения Компанией своих обязательств перед третьими лицами;

2.3. Разграничение полномочий и определение ответственности за обеспечение информационной безопасности в Компании.

3. Область применения политики

Настоящая Политика применяется ко всем информационным активам Компании, а также ко всем лицам, имеющим любую форму доступа к любым информационным активам Компании.

4. Ключевые требования

4.1. В Компании разработан и внедрен комплекс механизмов контроля, мониторинга и аутентификации для обеспечения безопасности информации, информационных ресурсов, информационных систем, аппаратного обеспечения и средств передачи данных.

4.2. В Компании производится анализ и оценка рисков, относящихся к информационной безопасности. Пересмотр рисков ИБ проводится ежегодно.

4.3. Аудит информационной безопасности проводится ежегодно. Аудит включает в себя проверку соблюдения внутренних регламентирующих документов в области ИБ, проверку правил предоставления доступа к информационным ресурсам Компании и исследование

элементов КИВС на предмет наличия возможных уязвимостей при помощи специализированных средств. Порядок проведения аудита определяется Политикой проведения аудита информационной безопасности в Компании.

4.4. В Компании на постоянной основе организовано повышение осведомленности сотрудников в вопросах, относящихся к информационной безопасности. Повышение осведомленности сотрудников проводится путем их ознакомления с регламентирующими документами в области ИБ, проведением инструктажей, а также проведением информирования посредством рассылки информационных писем и уведомлений по электронной почте. Порядок повышения осведомленности сотрудников определяется Положением по организации обучения пользователей КИВС Компании основам информационной безопасности.

4.5. Для своевременного обнаружения и предотвращения возможных утечек конфиденциальной информации, а также выявления инцидентов в области ИБ, в Компании осуществляется контроль действий пользователей КИВС. Порядок организации и выполнения контрольных мероприятий определяется Положением по организации системы контроля и мониторинга технических средств обработки, хранения и передачи и передачи информации в Компании.

4.6. Любой инцидент в области информационной безопасности фиксируется и расследуется. Результаты служебного расследования доводятся до руководителей Компании. По каждому случаю нарушения требований ИБ принимается решение о наложении на виновных лиц дисциплинарного взыскания.

4.7. В Компании составляется ежегодный отчет о состоянии информационной безопасности. Отчет включает в себя результаты аудита информационной безопасности КИВС, результаты служебных расследований по инцидентам в области ИБ, мероприятия, проведенные для снижения рисков ИБ и меры, которые необходимо предпринять для предотвращения появления новых или реализации существующих угроз ИБ в следующем отчетном периоде.

5. Классификация информации

5.1. Защите подлежит любая информация, принадлежащая Компании или переданная Компании в рамках договорных отношений. Вся информация классифицируется ее владельцами по степени конфиденциальности. Степень защиты информации выбирается в зависимости от ее категории.

5.2. Порядок категорирования и управления конфиденциальной информацией определяется Положением о коммерческой тайне Компании.

5.3. Все информационные ресурсы Компании классифицируются и защищаются в соответствии с их степенью важности для нужд бизнеса. Порядок классификации информационных ресурсов Компании определяется Регламентом управления информационными ресурсами Компании.

6. Разграничение доступа к информации

6.1. В Компании разработаны, документированы и внедрены механизмы разграничения доступа к информации в зависимости от степени конфиденциальности.

6.2. Информационные ресурсы, информационные системы и аппаратное обеспечение должны иметь необходимый и достаточный набор методов, позволяющих реализовать механизмы авторизации, аутентификации, разграничения и контроля доступа к ним.

6.3. В Компании введено ограничение доступа к информационным ресурсам КИВС. Это ограничение реализуется путем использования персональных учетных записей или специализированных аппаратно-программных средств аутентификации для всех пользователей КИВС.

6.4. Порядок управления доступом к информационным ресурсам Компании определяется Регламентом управления информационными ресурсами Компании.

7. Средства обеспечения безопасности информации

7.1. Базовый уровень безопасности информации при работе пользователей в КИВС Компании достигается путем объединения серверов и рабочих станций в домен ОС Windows. Порядок управления инфраструктурой домена определяется Доменной политикой Компании.

7.2. Защита КИВС Компании от внешних и внутренних вредоносных воздействий достигается путем использования средств межсетевого экранирования и системы обнаружения и предотвращения атак.

7.3. Обеспечение защиты КИВС Компании от вредоносного программного обеспечения осуществляется при помощи средств антивирусной защиты. Порядок работы с этими средствами определен Инструкцией по защите от вредоносного программного кода.

7.4. Для предотвращения несанкционированного доступа в КИВС Компании используются средства защиты каналов связи. Создание и администрирование защищенных каналов связи является исключительной прерогативой ДИТ. Создание и использование средств удаленного доступа в КИВС Компании любыми другими лицами в любых целях не допускается.

7.5. Для защиты конфиденциальной информации в Компании применяются криптографические средства. Перечень сведений, защищаемых при помощи криптографических средств, и порядок работы с ними, определен в Инструкции по использованию криптографических ключей в Компании.

7.6. Для предотвращения утечки конфиденциальной информации, обрабатываемой на рабочих местах пользователей КИВС, в Компании внедрена система управления съемными средствами хранения и передачи информации. Порядок работы с указанными средствами определен в Инструкции по использованию съемных средств обработки, хранения и передачи информации в Компании.

7.7. Для предотвращения нанесения Компании ущерба, связанного с потерей информации, и создания условий для обеспечения непрерывности бизнеса в части оперативного восстановления ИР в результате случайных или преднамеренных событий (действий), в Компании осуществляется резервное копирование информации. Порядок резервного копирования определяется Политикой резервного копирования информации в Компании.

7.8. Периметр безопасности на объектах Компании организован путем создания пропускного и внутриобъектового режимов, а также путем использования средств охранной, пожарной сигнализации, видеонаблюдения и контроля доступа. Порядок управления периметром безопасности определяется Инструкцией по пропускному и внутриобъектовому режиму Компании.

7.9. В Компании проводятся регулярные мероприятия по поиску и нейтрализации технических каналов утечки информации. Порядок их проведения определяется Инструкцией по

выполнению мероприятий, направленных на выявление и предупреждение утечки информации по техническим каналам в Компании.

8. Разработка и поддержка информационных систем

8.1. Для снижения риска несанкционированного доступа или внесения изменений в действующие информационные системы, в Компании организовано разделение среды разработки, тестирования и промышленных (действующих) экземпляров систем.

8.2. В Компании разработаны и внедрены механизмы контроля внесения изменений в любые элементы КИВС. Процедуры управления изменениями в КИВС определены Политикой управления изменениями информационных систем компании.

9. Безопасность персонала

9.1. Для противодействия возможным угрозам экономической и информационной безопасности, в Компании осуществляется проверка достоверности сведений, предоставляемых кандидатом при приеме на работу, и контрагентом при заключении договора. Проверка достоверности сведений проводится для всех кандидатов и контрагентов, в соответствии с действующим законодательством РФ.

9.2. Сотрудники Компании, контрагенты и иные лица, выполнение служебных или договорных обязательств которых требует наличия допуска к сведениям, составляющим коммерческую тайну (секрет производства), персональным данным и иной конфиденциальной информации, заключают соглашение о неразглашении этих сведений. Порядок допуска к работе с информацией, составляющей коммерческую тайну (секрет производства), определяется Положением о введении режима коммерческой тайны Компании.

10. Разделение полномочий

10.1. Лица, имеющие любую форму доступа к любым информационным ресурсам, размещенным в КИВС Компании, являются пользователями КИВС Компании. Порядок работы пользователя в КИВС Компании определен Инструкцией пользователя корпоративной информационно-вычислительной системы Компании по соблюдению требований информационной безопасности.

10.2. Пользователи, в должностные обязанности которых входит управление КИВС Компании, являются администраторами КИВС. Порядок работы администратора КИВС определяется Инструкцией администратора корпоративной информационно-вычислительной системы Компании по соблюдению требований информационной безопасности.

10.3. Организация мероприятий по обеспечению ИБ и контроль их выполнения, а также ответственность за состояние ИБ в Компании возложена на Дирекцию по безопасности Компании. Права и обязанности сотрудников определяются должностными инструкциями.

10.4. Выполнение технических мероприятий по обеспечению защиты КИВС Компании, указанных в п. 7.2, 7.6, 7.8 и 7.9 настоящей Политики, возложено на Дирекцию по безопасности Компании.

10.5. Выполнение технических мероприятий по обеспечению защиты КИВС Компании, указанных в п. 7.1, 7.3, 7.4, 7.5, 7.7 настоящей Политики, возложено на ИТ департамент Компании. Права и обязанности сотрудников ДИТ определяются Положением о дирекции по информационным технологиям и должностными инструкциями сотрудников.

10.6. Для поддержки процессов, связанных с построением СМИБ в Компании, и координации действий по обеспечению ИБ в Компании между представителями различных подразделений, в Компании создана Комиссия по защите информации. Комиссия является коллегиальным органом и осуществляет свою деятельность в соответствии с Положением о комиссии по защите информации Компании.

11. Защита персональных данных

11.1. Защита персональных данных физических лиц, обрабатываемых в Компании, организуется в соответствии с требованиями законодательства РФ и достигается с помощью организационных мер и технических средств.

11.2. Организационные меры защиты персональных данных определяются Положением по организации системы защиты персональных данных в Компании.

11.3. Защита ПДн, обрабатываемых в ИСПДн Компании, осуществляется техническими средствами, реализующими меры, описанные в разделе 7 настоящей Политики.

12. Сведения о документе

12.1. Настоящая Политика разработана в соответствии с действующим законодательством РФ в области защиты информации.

12.2. Методологической основой для разработки настоящей Политики является Концепция информационной безопасности Компании.

12.3. Настоящая Политика является методологической основой для разработки всех нормативных документов, касающихся обеспечения информационной безопасности в Компании.

12.4. Настоящая Политика разрабатывается и уточняется Дирекцией по безопасности Компании.

12.5. Настоящая Политика вступает в действие с момента утверждения ее генеральным директором Компании.

13. Срок действия и порядок внесения изменений

13.1. Срок действия настоящей Политики – один год с момента утверждения.

13.2. По истечении срока действия (или ранее - при необходимости) Политика подлежит пересмотру. Внесение изменений в Политику осуществляет Дирекция по безопасности Компании. Пересмотренная Политика утверждается генеральным директором Компании.

ЛИСТ СОГЛАСОВАНИЙ

к Политике информационной безопасности

РАЗРАБОТАЛ:

_____

_____

_____

СОГЛАСОВАНО

14. История изменений

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