.redev

Утверждено:
Директор
ООО «РЕДЕВ»

_____ Т.А. Пименова

Приказ № 1-ВД от 19.01.2026 г.

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЩЕСТВА С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ «РЕДЕВ»

г. Москва
2026

Содержание

1. Введение……3
2. Обозначения и сокращения……3
3. Термины и определения……3
4. Цели и принципы информационной безопасности……5
5. Основания для разработки……6
6. Область действия……6
7. Содержание политики……6
7.1. Управление информационной безопасностью……6
7.2. Объект защиты……7
7.3. Оценка и обработка рисков……8
7.4. Ответственность персонала……8
7.5. Физическая безопасность информационных ресурсов и технических средств……9
7.6. Контроль доступа и управление правами доступа……10
7.7. Политика работы с информационными системами……11
7.8. Приобретение, разработка и обслуживание систем……13
7.9. Управление инцидентами информационной безопасности……14
7.10. Управление непрерывностью и восстановлением……14
7.11. Соблюдение требований законодательства……15
7.12. Аудит информационной безопасности……15
7.13. Предоставление услуг сторонним организациям……16
7.14. Обработка персональных данных……16
7.15. Управление уязвимостями……17
7.16. Управление изменениями……17
7.17. Регистрация и мониторинг событий……17
7.18. Защита от утечек информации……17
8. Ответственность подразделений и должностных лиц……18
9. Контроль и пересмотр……19

1. Введение

Настоящая Политика информационной безопасности (далее - Политика) регламентирует в ООО «РЕДЕВ» (далее - Общество, Компания) порядок обеспечения защиты информационных активов, основные цели, принципы и задачи в области информационной безопасности, права, обязанности и ответственность работников и работодателя по соблюдению режима защиты информации, а также иные вопросы, связанные с обеспечением сохранности, целостности и доступности информационных ресурсов Общества.

Под информационной безопасностью Компания понимает состояние защищённости своих интересов (целей) от угроз в информационной сфере. Защищённость достигается обеспечением совокупности свойств информационных активов: конфиденциальности, целостности и доступности.

Информационные ресурсы составляют актив Компании. Случайные или преднамеренные воздействия на информационные ресурсы (содержание информации, ее носители, процессы обработки и передачи) могут повлечь для Компании негативные последствия.

Положения настоящей Политики направлены на определение мер и технологий защиты информационных ресурсов Компании от возможного нанесения им ущерба посредством случайного или преднамеренного воздействия.

Политика является общедоступным документом, который может предоставляться без ограничений всем заинтересованным сторонам.

2. Обозначения и сокращения

АРМ - Автоматизированное рабочее место
ИБ - Информационная безопасность
ИР - Информационный ресурс
ИС - Информационная система
ИТ - Информационные технологии
НСД - Несанкционированный доступ
ПДн - Персональные данные
ПО - Программное обеспечение
СКЗИ - Средство криптографической защиты информации

3. Термины и определения

3.1. Аутентификация - проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности.

3.2. Безопасность информации - защищенность информации от нежелательного разглашения (нарушения конфиденциальности), искажения (нарушения целостности), утраты или снижения степени доступности, а также незаконного её тиражирования.

3.3. Бизнес-процесс - последовательность технологически связанных операций по предоставлению продуктов, услуг и/или осуществлению конкретного вида деятельности Компании.

3.4. Доступность информации - состояние, характеризуемое способностью ИС обеспечивать беспрепятственный доступ к информации субъектов, имеющих на это полномочия.

3.5. Защита информации - деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на неё и нарушения её доступности.

3.6. Идентификация - присвоение субъектам и объектам доступа идентификаторов и/или сравнение предъявленного идентификатора с перечнем присвоенных.

3.7. Информационная безопасность (ИБ) - практика предотвращения несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации.

3.8. Информационная система (ИС) - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

3.9. Информационный ресурс (актив) - информация, имеющая ценность и находящаяся в распоряжении Компании, включая информацию клиентов Компании, доступ к которой получен в процессе оказания услуг.

3.10. Инцидент информационной безопасности - нежелательное или неожиданное событие ИБ, имеющее значительную вероятность нарушения бизнес-процессов или представляющее угрозу ИБ.

3.11. Конфиденциальная информация - информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством РФ или по решению ее владельца.

3.12. Несанкционированный доступ (НСД) - доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств.

3.13. Персональные данные (ПДн) - любая информация, относящаяся прямо или косвенно к определённому или определяемому физическому лицу (субъекту персональных данных).

3.14. Риск - мера, учитывающая вероятность реализации угрозы и величину возможного ущерба от этой реализации.

3.15. Целостность информации - устойчивость информации к преднамеренному или случайному воздействию, результатом которого может быть её уничтожение или искажение.

3.16. Угроза информационной безопасности (ИБ) - совокупность условий и факторов, создающих опасность нарушения информационной безопасности, приводящую к возможности потерь (ущерба).

3.17. Уязвимость - недостаток или слабое место в информационной системе или её компонентах, которое может быть использовано для реализации угрозы.

4. Цели и принципы информационной безопасности

4.1. Важнейшими целями Компании в области информационной безопасности являются:

4.1.1. минимизация рисков ИБ, которым подвержены технологии и информационные системы, используемые для достижения бизнес-целей;

4.1.2. обеспечение эффективности мероприятий по ликвидации неблагоприятных последствий реализации угроз и инцидентов ИБ;

4.1.3. соответствие требованиям законодательства и договорным обязательствам в части ИБ;

4.1.4. повышение деловой репутации и корпоративной культуры Компании;

4.1.5. достижение адекватности мер по защите от угроз ИБ.

4.2. При достижении поставленных целей Компания намерена руководствоваться следующими принципами:

4.2.1. Безусловное участие руководства. Деятельность по обеспечению ИБ инициирована и контролируется руководством Компании. Руководство выполняет те же правила, что и все работники.

4.2.2. Законность. Меры обеспечения ИБ реализуются в строгом соответствии с действующим законодательством и договорными обязательствами.

4.2.3. Экономическая целесообразность. Выбор мер ИБ осуществляется с учётом затрат на их реализацию, вероятности возникновения угроз и объёма возможных потерь.

4.2.4. Осведомленность. Документированные требования в области ИБ доводятся до сведения работников и контрагентов. Компания на периодической основе осуществляет информирование, обучение и аттестацию работников.

4.2.5. Персональная ответственность. Работники Компании несут персональную ответственность за соблюдение требований ИБ. Обязанности по обеспечению ИБ включаются в трудовые договоры и должностные инструкции.

4.2.6. Минимально необходимые права доступа. Работникам предоставляются минимально достаточные права доступа для качественного и своевременного выполнения трудовых обязанностей.

4.2.7. Учет требований ИБ в проектной деятельности. Разработка и документирование требований по обеспечению ИБ осуществляется на начальных этапах реализации проектов, связанных с обработкой, хранением и передачей информации.

4.2.8. Непрерывность. Защита информации - непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла ИС Компании.

4.2.9. Разделение функций. Запрещается совмещение в рамках одной учётной записи полномочий, позволяющих одному работнику единолично осуществлять критичные операции.

5. Основания для разработки

5.1. Настоящая Политика разработана на основе требований законодательства Российской Федерации, накопленного в Компании опыта в области обеспечения ИБ, интересов и целей Компании.

5.2. При написании отдельных положений настоящей Политики использовались следующие нормативные документы:

- ГОСТ Р ИСО/МЭК 27002-2021 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности»;
- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

6. Область действия

6.1. Настоящая Политика распространяется на все бизнес-процессы Компании, которые реализуются с использованием информационных технологий, и обязательна для применения всеми сотрудниками и руководством Компании, а также пользователями информационных ресурсов Компании.

6.2. Разработка внутренних документов Компании в части вопросов информационной безопасности должна соответствовать настоящей Политике.

6.3. Лица, осуществляющие разработку внутренних документов Компании, регламентирующих вопросы информационной безопасности, и лица, проводящие организационные и технические мероприятия, связанные с обеспечением информационной безопасности, обязаны руководствоваться настоящей Политикой.

6.4. Настоящая Политика также должна применяться при взаимодействии и обмене информацией при выполнении договорных обязательств с партнёрами и клиентами Компании.

6.5. Политика должна быть доведена до всех работников и принята ими к обязательному исполнению. Политика также должна быть доведена до контрагентов и иных третьих лиц, допущенных к информационным активам Компании, и принята ими к обязательному исполнению в части, их касающейся.

7. Содержание Политики

7.1. Управление информационной безопасностью

7.1.1. Для достижения целей Политики и решения задач по защите информации в Компании действует система управления информационной безопасностью как часть общей системы управления Компании.

7.1.2. Система управления информационной безопасностью документируется в правилах, процедурах, рабочих инструкциях. Указанные документы являются обязательными для исполнения всеми работниками Компании в части касающейся. Необходимые требования по информационной безопасности доводятся до сведения работников Компании, в том числе доводятся до сведения изменения при их внесении в документы и требования.

7.1.3. Решения о внедрении средств и систем защиты информации принимаются с учётом оценки рисков информационной безопасности и возможного ущерба при реализации угроз.

7.1.4. Вопросы непосредственной организации и обеспечения эффективного решения задач информационной безопасности возлагаются руководством на ответственные подразделения Компании. Указанные вопросы отражаются в положениях о подразделениях, должностных инструкциях.

7.1.5. При выборе средств обеспечения и контроля ИБ Компания ориентируется на использование отечественных продуктов, в том числе на использование отечественного и санкционно-устойчивого системного и прикладного ПО, вычислительной техники и сетевого оборудования.

7.2. Объект защиты

7.2.1. Информационные ресурсы

7.2.1.1. Защита информации в Компании реализуется на основе определения всех имеющихся информационных ресурсов и последующей оценкой информационных ресурсов с точки зрения их важности. Принимаемые меры по защите информации должны соответствовать ценности и важности информационных ресурсов.

7.2.1.2. Основными информационными активами Компании, подлежащими защите, являются:

- информация, составляющая коммерческую тайну, персональные данные сотрудников Компании, сотрудников и клиентов контрагентов Компании, включая персональные данные клиентов заказчиков Компании, внутренние документы Компании, иная информация, чувствительная по отношению к случайным и несанкционированным воздействиям, представленная в виде документов и информационных массивов, включая информацию заказчиков и клиентов Компании, к которой сотрудники или подрядчики Компании получают доступ в рамках выполнения работ в интересах этих заказчиков и клиентов;
- информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства обработки, передачи и отображения информации, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения;
- процессы обработки информации в ИС - информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации, процессы жизненного цикла ИС.

Для каждого ресурса должен быть назначен владелец (структурное подразделение Компании), который отвечает за соответствующую классификацию информации и ресурсов и согласует назначение и проверку прав доступа к ресурсам и привилегий.

7.2.2. Классификация информации

7.2.2.1. Все информационные ресурсы, подлежащие защите, должны быть классифицированы в соответствии с важностью и степенью доступа. Классификация информации должна быть документирована и утверждена руководством Компании.

7.2.2.2. Классификация информации должна проводиться владельцем ресурса, хранящего или обрабатывающего информацию, для определения категории ресурса. Периодически классификация должна пересматриваться для поддержания актуальности её соответствия с категорией ресурса.

7.2.2.3. Ресурсы, содержащие конфиденциальную или критичную информацию, а также персональные данные, должны иметь соответствующую пометку (гриф).

7.3. Оценка и обработка рисков

7.3.1. В Компании требования к обеспечению безопасности информационных ресурсов должны формироваться на основе оценки рисков ИБ. Оценка риска ИБ осуществляется на основании мнения экспертов (опытных сотрудников) Компании.

7.3.1. Целью управления рисками ИБ является:
- минимизация негативных последствий от реализации рисков;
- оптимизация затрат, направленных на предотвращение негативных последствий от реализации рисков.

7.3.2. Оценка рисков и выбор механизмов контроля рисков должны производиться периодически в целях:
- учета изменений бизнес-требований и приоритетов;
- анализа угроз появления новых уязвимостей в технологиях защиты информации;
- проверки сохранения эффективности реализованных мер обеспечения ИБ.

7.3.3. Обработка каждого риска Компании должна осуществляться по критериям для определения возможности принятия риска как допустимого. Риск может быть принят как допустимый, если его последствия достаточно малы, а стоимость нейтрализации не рентабельна для Компании.

Для каждого из оцененных рисков должно приниматься одно из решений по его обработке:
- применение механизмов контроля для уменьшения величины риска до приемлемого уровня;
- сознательное и объективное принятие риска как допустимого;
- нейтрализация рисков путем недопущения действий, могущих быть его причиной.

7.4. Ответственность персонала

Ответственность за соблюдение установленных правил работы с информационными ресурсами, включая соблюдение правил обеспечения информационной безопасности, должны быть доведены до сотрудника при трудоустройстве и внесены в его должностные обязанности. Сюда должны входить как

общие обязанности по реализации и поддержке Политики ИБ, так и конкретные обязанности по защите ресурсов и по соблюдению требований внутренних нормативных документов, связанных с безопасностью.

7.4.1. Условия найма

В трудовых договорах, подписываемых всеми принимаемыми на работу сотрудниками, должна быть установлена их ответственность за соблюдение требований ИБ. В трудовой договор должно быть включено согласие сотрудника на проведение контрольных мероприятий со стороны Компании по проверке выполнения требований ИБ.

В трудовых договорах, подписываемых всеми принимаемыми на работу сотрудниками, должны быть установлены их обязательства по неразглашению конфиденциальной информации, а также обязательство соблюдать требования законодательства о персональных данных.

При приёме на работу выполняются процедуры оценки благонадёжности кандидатов.

7.4.2. Ответственность руководства

Руководство Компании контролирует выполнение правил ИБ всеми сотрудниками в соответствии с установленными в Компании политиками и процедурами.

Уполномоченные руководством Компании сотрудники имеют право производить проверки:
- выполнения действующих инструкций по вопросам ИБ;
- данных, находящихся на носителях информации;
- порядка использования сотрудниками информационных ресурсов;
- содержания служебной переписки.

7.4.3. Обучение ИБ

Компания определяет необходимость проведения периодической подготовки сотрудников в области средств и технологий ИБ, принятых в Компании. Особое внимание уделяется обучению правилам работы с персональными данными и предотвращению утечек.

Проводятся регулярные обучающие мероприятия для работников, а также иных третьих лиц, допущенных к информационным активам Компании. По результатам проведённых мероприятий проводятся регулярные проверки полученных знаний.

7.4.4. Завершение или изменение трудовых отношений

При увольнении все предоставленные сотруднику права доступа к ресурсам ИС должны быть удалены. Все выданные ключи, токены, сертификаты и носители информации возвращаются по акту.

При изменении трудовых отношений удаляются только те права, необходимость в которых отсутствует в новых отношениях.

7.5. Физическая безопасность информационных ресурсов и технических средств

7.5.1. Средства обработки информации, поддерживающие критически важные информационные ресурсы Компании, должны быть размещены в защищённых помещениях, расположенных в контролируемой зоне. Такими средствами, как правило, являются: серверы, телекоммуникационное оборудование, оборудование, обеспечивающее обработку и хранение конфиденциальной информации и персональных данных.

7.5.2. Организация физической защиты:

7.5.2.1. В Компании должны быть выделены зоны (области) безопасности (в том числе особо важные и выделенные помещения), в которых должен поддерживаться режим физической безопасности.

7.5.2.2. В зонах безопасности, а также во всех офисных, вспомогательных, подсобных, технических помещениях должны быть реализованы меры по противопожарной защите, защите от аварий в системах электро-, тепло-, водо- и газоснабжения.

7.5.2.3. Лица, имеющие право на доступ в помещения Компании, должны регистрироваться, должен осуществляться контроль доступа в помещения.

7.5.2.4. Лица, не являющиеся работниками, допускаются в помещения только под контролем и в сопровождении ответственных работников Компании.

7.5.2.5. Для всех помещений назначен их владелец (распорядитель доступа). Доступ в помещения предоставляется только по согласованию с владельцем.

7.5.2.6. Входные двери помещений оборудованы механическими замками, обеспечивающими надежное закрытие помещений в нерабочее время.

7.5.2.7. Серверное и сетевое оборудование ИС расположено в запираемых серверных стойках. Доступ к данным шкафам контролируется.

7.5.2.8. В случае применения средств видеонаблюдения видеозаписи хранятся не менее 14 календарных дней.

7.5.3. Вспомогательные технические службы, такие как электропитание, водоснабжение, канализация, отопление, вентиляция и кондиционирование воздуха, должны обеспечивать гарантированную и устойчивую работоспособность компонентов ИС Компании.

7.5.4. Для хранения служебных документов и машинных носителей с защищаемой информацией помещения, в которых хранятся такие документы, снабжаются сейфами, металлическими шкафами или шкафами, оборудованными замком, а также средствами уничтожения документов на бумажных носителях и уничтожения оптических дисков.

7.5.5. В случае утилизации оборудования со всех носителей информации, которыми укомплектовано оборудование, должны гарантированно удаляться все конфиденциальные данные и персональные данные.

7.6. Контроль доступа и управление правами доступа

7.6.1. Уровень полномочий каждого сотрудника Компании определяется с учётом его обязанностей. Уровень полномочий каждого пользователя определяется индивидуально. Должно быть обеспечено использование каждым сотрудником только предписанных ему прав по отношению к информации, с которой ему необходимо

работать в соответствии с должностными обязанностями (принцип минимальных привилегий).

7.6.2. Действия всех работников Компании осуществляются от имени персонифицированной учётной записи. Наличие учетных записей, не закрепленных за конкретным работником, недопустимо.

7.6.3. Доступ к любому объекту ИС предоставляется только при наличии соответствующего разрешения. Любой доступ, не разрешенный явно, должен быть запрещен.

7.6.4. Допуск пользователей к работе с информационными ресурсами должен быть строго регламентирован. Любые изменения состава и полномочий пользователей подсистем должны производиться в установленном порядке, согласно регламенту предоставления доступа пользователей.

7.6.5. Доступ сотрудника к информационным ресурсам Компании должен быть санкционирован руководителем структурного подразделения, в котором числится, согласно штатному расписанию, данный сотрудник, и владельцами соответствующих информационных ресурсов.

7.6.6. Для идентификации и аутентификации пользователей при доступе к информационным ресурсам могут использоваться пароли, а также иные технологии. При использовании паролей должен выполняться набор требований, обеспечивающих необходимый уровень защиты паролей от компрометации (длина, сложность, периодическая смена).

7.6.7. Организация ресурсов локальной сети Компании, включая каталоги и файлы, к которым предоставляется доступ сотрудникам Компании, и их поддержка регламентируются отдельными внутренними документами.

7.7. Политика работы с информационными системами

Ответственность по установке и поддержке вычислительного оборудования и программного обеспечения всех информационных систем, функционирующих в Компании, осуществляется уполномоченным подразделением.

Комплектация персональных компьютеров аппаратными и программными средствами, расположение и сетевое подключение компьютеров обеспечивается и контролируется уполномоченным подразделением.

Все однотипные АРМ, установленные в Компании, должны иметь унифицированный набор прикладных и офисных программ, определённый назначением АРМ в бизнес-процессе Компании.

Изменение установленной аппаратной и программной конфигурации АРМ может проводиться только уполномоченным подразделением.

Уполномоченное подразделение имеет право осуществлять контроль над установленным на компьютере программным обеспечением и принимать меры по ограничению возможностей несанкционированной установки программ.

Детальные требования по организации работы в ИС Компании, требования и обязанности сотрудников при работе в ИС излагаются в отдельных документах.

7.7.1. Использование электронной почты.

Электронная почта используется для обмена в рамках ИС Компании и общедоступных сетей информацией в виде электронных сообщений и документов в электронном виде.

Функционирование электронной почты обеспечивается оборудованием, каналами связи и иными ресурсами, принадлежащими Компании.

Корпоративная электронная почта Компании предназначена исключительно для использования в служебных целях.

Каждый сотрудник Компании получает почтовый адрес в домене Компании.

Любые сообщения корпоративной электронной почты могут быть прочитаны, использованы в интересах Компании либо удалены уполномоченными сотрудниками Компании.

Запрещена пересылка конфиденциальной информации и персональных данных на внешние почтовые адреса без служебной необходимости и согласования с ответственным за ИБ.

7.7.2. Работа в публичной сети

Доступ к публичной сети (Интернет) предоставляется сотрудникам Компании в целях выполнения ими своих служебных обязанностей, требующих непосредственного подключения к внешним информационным ресурсам.

При использовании сети Интернет запрещено публиковать, загружать и распространять материалы, содержащие конфиденциальную информацию, а также персональные данные.

Содержание интернет-ресурсов, а также файлы, загружаемые из сети Интернет, подлежат обязательной проверке на отсутствие вредоносного ПО.

7.7.3. Удалённая работа с информационными ресурсами

Под удалённой работой с информационными ресурсами Компании понимается получение доступа к ИС Компании из внешней сети.

Канал связи между ИС Компании и устройством пользователя во внешней сети должен быть защищён сертифицированным средством криптографической защиты информации (СКЗИ).

Процедура управления каналом связи должна предоставлять возможность незамедлительного отключения пользователя от ИС Компании.

7.7.4. Защита от вредоносного ПО

Локальные и сетевые ресурсы Компании должны систематически проверяться антивирусным программным обеспечением, в частности должна быть обеспечена защита входящей электронной почты от проникновения вирусов и другого вредоносного ПО.

Важные данные и системная конфигурация должны периодически резервироваться, резервные копии храниться в безопасном месте.

Сотрудникам предписаны конкретные меры антивирусной безопасности, изложенные в отдельных документах Компании.

7.8. Приобретение, разработка и обслуживание систем

7.8.1. Требования безопасности для информационных систем

При описании требований к созданию новых систем или к усовершенствованию существующих необходимо учитывать потребность в средствах обеспечения безопасности. Требования к безопасности и средства защиты должны соответствовать ценности используемых ИР и потенциальному ущербу для Компании в случае сбоя или нарушения безопасности. Основой для анализа требований к безопасности и выбору мер для поддержки безопасности является оценка рисков и управление рисками.

Системные требования к ИБ и процессам, обеспечивающим защиту информации, должны быть включены на ранних стадиях проектирования ИС.

7.8.2. Корректная обработка информации

Данные, вводимые в прикладные системы, необходимо проверять, чтобы гарантировать их правильность и соответствие поставленной задаче.

7.8.3. Криптографические средства

Все используемые Компанией (приобретаемые) СКЗИ должны эксплуатироваться в полном соответствии с эксплуатационной документацией.

Управление ключами должно обеспечивать защиту от их компрометации или утраты.

Оборудование, используемое для генерации, хранения и архивирования ключей, должно быть физически защищено.

Соглашения с внешними поставщиками криптографических услуг (например, удостоверяющими центрами) об уровне предоставляемого сервиса должны охватывать вопросы ответственности, надёжности сервиса и времени реакции при предоставлении сервиса.

Криптографические системы и методы следует использовать для защиты конфиденциальной информации в случаях, когда другие средства не обеспечивают адекватной защиты.

7.8.4. Безопасность процесса разработки и обслуживания информационных систем

Внесение изменений в ПО ИС Компании должно проводиться только при наличии существенных объективных причин для внесения изменений.

До внесения изменений должно проводиться тестирование нового ПО. Тестовые среды и стенды должны быть отключены от рабочих систем во избежание влияния на рабочие системы. В тестовых системах следует избегать использования конфиденциальных данных. В случае же их вынужденного использования необходимо после тестирования конфиденциальные данные удалить.

Для сведения к минимуму риска нарушения работоспособности ИС Компания обеспечивает строгий контроль над внесением изменений в ПО и руководствуется официальными правилами внесения изменений. Эти правила должны гарантировать, что процедуры, связанные с безопасностью и соблюдением контроля, не будут нарушены. При внесении изменений доступ к ИС должен предоставляться ИТ-специалистам в минимально необходимом объёме.

7.9. Управление инцидентами информационной безопасности

В Компании должна быть разработана процедура уведомления о происшествиях в области ИБ, а также процедура реагирования на такие происшествия, включающая в себя действия, которые должны выполняться уполномоченными сотрудниками при поступлении сообщений о происшествии.

Все сотрудники должны быть ознакомлены с процедурой уведомления, а в их обязанности должна входить максимально быстрая передача информации о происшествиях в области ИБ.

Каждый инцидент ИБ должен фиксироваться и расследоваться. Результаты расследования доводятся до руководства Компании. По каждому случаю нарушения требований ИБ принимается решение о наложении на виновных лиц дисциплинарных взысканий.

7.10. Управление непрерывностью и восстановлением

В Компании реализуются планы и механизмы, направленные на обеспечение и поддержку непрерывности бизнес-процессов. Указанные планы и механизмы направлены на обеспечение возможности в случае прерывания или сбоя критически важных бизнес-процессов в установленные сроки продолжить или восстановить операции и обеспечить требуемый уровень доступности информации.

Каждый план поддержки непрерывности бизнеса должен четко определять условия начала его исполнения и сотрудников, ответственных за выполнение каждого фрагмента плана. При появлении новых требований необходимо внести поправки в принятые планы действия в нештатных ситуациях.

Для каждого плана должен быть назначен определённый владелец. Правила действия в нештатных ситуациях, планы ручного аварийного восстановления и планы возобновления деятельности должны находиться в ведении владельцев соответствующих ресурсов или процессов, к которым они имеют отношение.

Резервное копирование и восстановление информации:

- В Компании выполняется регулярное резервное копирование информации, программного обеспечения и образов ИС.

- Создаваемые резервные копии регулярно тестируются. Обеспечивается целостность создаваемых резервных копий.

7.11. Соблюдение требований законодательства

Все значимые требования, установленные действующим законодательством, подзаконными актами и договорными отношениями, а также подход Компании к обеспечению соответствия этим требованиям должны быть явным образом определены, документированы и поддерживаться в актуальном состоянии.

Необходимо соблюдение регламентированного процесса, предупреждающего нарушение целостности, достоверности и конфиденциальности ИР, содержащих персональные данные, начиная от стадии сбора и ввода данных до их хранения. Персональные данные конкретного сотрудника и процесс их обработки должен быть открытым для этого сотрудника.

В Компании должны быть внедрены соответствующие процедуры для обеспечения соблюдения законодательных ограничений, подзаконных актов и контрактных обязательств по использованию материалов, охраняемых авторским правом, а также по использованию лицензионного ПО.

Важная документация Компании должна быть защищена от утери, уничтожения и фальсификации в соответствии с требованиями законодательства, подзаконных актов, контрактных обязательств и бизнес-требований.

Система хранения и обработки должна обеспечивать четкую идентификацию записей и их периода хранения в соответствии с требованиями законов и нормативных актов. Эта система должна иметь возможность уничтожения записей по истечении периода хранения, если эти записи больше не требуются Компании.

7.12. Аудит информационной безопасности

Компания должна систематически осуществлять:

- контроль текущего уровня защищённости ИС;
- выявление и локализацию уязвимостей в системе защиты ИС;
- анализ рисков, связанных с возможностью осуществления угроз безопасности в отношении ИР;
- оценку соответствия ИС требованиям настоящей Политики;
- выработку рекомендаций по совершенствованию ИБ за счёт внедрения новых и повышения эффективности существующих мер защиты информации.

В рамках указанных действий проводятся:

- сбор и анализ исходных данных об организационной и функциональной структуре ИС, необходимых для оценки состояния ИБ;
- анализ существующей политики безопасности и других организационно-распорядительных документов по защите информации на предмет их полноты и эффективности, а также формирование рекомендаций по их разработке (или доработке);
- технико-экономическое обоснование механизмов безопасности;

- проверка правильности подбора и настройки средств защиты информации, формирование предложений по использованию существующих и установке дополнительных средств защиты для повышения уровня надёжности и безопасности ИС;

- разбор инцидентов ИБ и минимизация возможного ущерба от их проявления.

Руководство и сотрудники Компании обязаны предоставлять всю необходимую для проведения указанных работ информацию.

Аудит ИБ может быть как внутренним, так и внешним. При проведении аудитов ИБ используются стандартные процедуры документальной проверки, опрос и интервью с руководством и персоналом, а также технические процедуры тестирования.

7.13. Предоставление услуг сторонним организациям (третьими лицами)

7.13.1. Договоры об оказании услуг/ выполнении работ

В договорах об оказании услуг/выполнении работ сторонним организациям (третьими лицами) должны быть включены требования безопасности, описание, объёмы и характеристики качества предоставляемых услуг.

Для внешних подрядчиков:

- Порядок предоставления доступа к ИТ-системам Компании для внешних разработчиков (только через защищенные каналы, на строго ограниченный срок).
- Обязанность подрядчиков соблюдать требования ИБ Компании (включение отдельного пункта в договор).
- Процедура возврата оборудования и удаления доступа после завершения сотрудничества.

7.13.2. Анализ оказания услуг/выполнения работ

Услуги, отчеты и записи, предоставляемые сторонним организациям, должны постоянно проверяться и анализироваться. В отношениях со сторонней организацией должны присутствовать следующие процессы:

- контроль объема и качества услуг, оговоренных в соглашениях;
- предоставление сторонней организации информации об инцидентах ИБ, связанных с предоставляемыми услугами, и совместное изучение этой информации;
- анализ предоставленных сторонними организациями отчётов о предоставленных услугах;
- управление любыми обнаруженными проблемами.

7.14. Обработка персональных данных

7.14.1. Персональные данные являются важным информационным активом Компании. Обработка персональных данных осуществляется Компанией в строгом соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами.

7.14.2. Основные обязанности Компании как оператора персональных данных:

- Обработка персональных данных осуществляется только при наличии законных оснований (согласие субъекта, исполнение договора, требование закона и т.д.).

- Компания собирает только те персональные данные, которые являются необходимыми и достаточными для заявленной цели обработки.

- Обработка персональных данных ограничивается достижением конкретных, заранее определённых и законных целей.

- Обеспечивается конфиденциальность и безопасность персональных данных при их обработке.

- Персональные данные уничтожаются по достижении целей обработки или в случае утраты необходимости в их достижении.

- Субъектам персональных данных предоставляется информация, касающаяся обработки их персональных данных, в порядке и сроки, установленные законом.

- Компания принимает необходимые правовые, организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, предоставления, распространения.

7.14.3. Детальный порядок обработки персональных данных, включая:

- перечень категорий обрабатываемых персональных данных;
- цели обработки персональных данных;
- перечень действий, совершаемых с персональными данными;
- сроки обработки и хранения персональных данных;
- порядок передачи персональных данных третьим лицам;
- порядок уничтожения персональных данных;
- права субъектов персональных данных и порядок их реализации,

определен в отдельном документе: «Политика в отношении обработки персональных данных в ООО «РЕДЕВ».

7.15. Управление уязвимостями

В Компании организован процесс управления уязвимостями, включающий в себя постоянное выявление, анализ и устранение выявленных уязвимостей.

Проводятся регулярные работы по тестированию на проникновение как во внешние, так и во внутренние сети Компании.

7.16. Управление изменениями

В Компании организован процесс управления изменениями. Все изменения, вносимые в программное обеспечение ИС и оборудование, регистрируются и контролируются.

Определены и зафиксированы параметры безопасных конфигураций ИС и оборудования. Данные параметры в обязательном порядке применяются при настройке и восстановлении работоспособности оборудования и ИС.

7.17. Регистрация и мониторинг событий

В Компании осуществляются регулярный мониторинг и регистрация системных событий, действий пользователей и администраторов, ошибок и событий ИБ.

Все зарегистрированные события анализируются на предмет наличия признаков инцидента ИБ.

7.18. Защита от утечек информации

В Компании осуществляются мероприятия для защиты информации от её несанкционированного разглашения (утечки).

В рамках данных мероприятий осуществляется контроль следующей информации:

- информации, передаваемой в информационно-телекоммуникационную сеть Интернет;
- информации, передаваемой с использованием средств электронной почты;
- информации, передаваемой на печать;
- информации, записываемой на съёмные носители.

Распространение информации и передача информационных активов (за исключением общедоступной информации) запрещены, если только такое действие не осуществляется согласно случаям, предусмотренным законодательством Российской Федерации и внутренними документами Компании.

8. Ответственность подразделений и должностных лиц

8.1. Директор Компании при обеспечении ИБ в Компании несет ответственность:

- за утверждение Политики и внутренних документов Компании в части обеспечения ИБ;
- утверждение направлений развития ИБ в контексте снижения общих бизнес-рисков Компании;
- выделение финансовых и материальных средств, а также кадровых ресурсов для организации обеспечения ИБ;
- утверждение организационной структуры управления ИБ;
- назначение ответственных лиц за обеспечение ИБ.
- за планирование, контроль, организацию и развитие мер обеспечения и управления ИБ в Компании;
- разработку, документирование и внедрение мер обеспечения и управления ИБ;
- анализ угроз и рисков ИБ, планирование и реализацию мероприятий по снижению угроз и управлению рисками;
- выполнение требований законодательства Российской Федерации в области ИБ;
- управление применяемыми техническими средствами защиты информации, а также их сопровождение;
- организацию обучения и повышения осведомлённости работников в области ИБ.

8.2. Руководители структурных подразделений при обеспечении ИБ в Компании несут ответственность:

- за управление информационными активами, согласование прав доступа к информационным активам, принятие решений по рискам нарушения ИБ, связанным с информационными активами;
- доведение требований по обеспечению ИБ до работников подчинённых структурных подразделений;
- своевременное информирование подразделения ИБ о выявленных рисках и инцидентах информационной безопасности;
- исполнение требований подразделения ИБ по минимизации рисков ИБ, устранению условий и последствий инцидентов.

8.3. Работники Компании при обеспечении ИБ в Компании несут персональную ответственность:

- за исполнение требований внутренних документов Компании в части обеспечения ИБ;
- за сохранность своих учётных данных и действий, совершённых под их логином;
- за своевременное информирование о любых инцидентах или подозрениях на инциденты ИБ.

Нарушение требований нормативных актов Компании по обеспечению ИБ является чрезвычайным происшествием и может служить поводом и основанием для проведения расследования. За нарушение требований в области ИБ работники Компании несут персональную ответственность в соответствии с законодательством Российской Федерации.

9. Контроль и пересмотр

Общий контроль состояния ИБ осуществляется Директором Компании.

Текущий контроль соблюдения настоящей Политики осуществляется подразделениями Компании в рамках, определенных положениями о подразделениях и должностными инструкциями, а также в рамках иных контрольных мероприятий.

Настоящая Политика подлежит регулярному пересмотру в следующих случаях:

- изменения требований законодательства Российской Федерации;
- существенных изменений в информационной инфраструктуре или организационной структуре Компании;
- выявления инцидентов ИБ, свидетельствующих о неполноте или несовершенстве настоящей Политики;
- по результатам мониторинга состояния ИБ и анализа актуальных угроз.

Изменения и дополнения в настоящую Политику утверждаются Директором Компании в форме новой редакции Политики и вступают в силу с момента утверждения.