politics_sec

Выпуск 0.0.3

июн. 17, 2026

Содержание

1 Политика информационной безопасности ООО «Бизнес Технологии»

1.1 1. Общие положения

1.1. Политика информационной безопасности ООО «Бизнес Технологии» (далее — Политика) является нормативным документом первого уровня корпоративной системы управления информационной безопасностью. Политика закрепляет официальную позицию Общества в области обеспечения информационной безопасности, определяет стратегические ориентиры, принципы, цели и основные задачи защиты информационных активов.

1.2. Деятельность Общества связана с созданием, обработкой, хранением и передачей информационных активов, включая информацию ограниченного доступа, в том числе персональные данные, программное обеспечение, информационные системы, инфраструктурные компоненты, а также процессы разработки и сопровождения. Указанные активы имеют критическую ценность для устойчивости и непрерывности бизнеса и подлежат обязательной защите.

Защита обеспечивается посредством внедрения и поддержания совокупности организационных, правовых и технических мер, направленных на предотвращение реализации актуальных угроз, снижение информационных рисков до приемлемого уровня и минимизацию потенциального ущерба.

1.3. Настоящая Политика устанавливает единые принципы и подходы к защите информационных активов от внутренних и внешних угроз, включая преднамеренные и непреднамеренные воздействия. Состав и достаточность мер защиты определяются на основе идентификации активов, анализа актуальной модели угроз, оценки уязвимостей и регулярной оценки рисков информационной безопасности.

Реализуемые меры должны обеспечивать поддержание и контроль ключевых свойств информации — конфиденциальности, целостности и доступности — на уровне, соответствующем требованиям законодательства Российской Федерации, договорным обязательствам и интересам Общества.

1.4. Локальные нормативные акты Общества, регламентирующие процессы обеспечения информационной безопасности, разрабатываются в соответствии с настоящей Политикой, подлежат обязательному согласованию с руководством и не могут ей противоречить.

1.2 2. Нормативные ссылки

2.1. Настоящая Политика разработана в соответствии с требованиями законодательства Российской Федерации, нормативных правовых актов уполномоченных государственных органов в области информационной безопасности, а также с учетом национальных стандартов и внутренних нормативных документов Общества.

2.2. Правовую основу настоящей Политики составляют следующие нормативные правовые акты Российской Федерации:

- Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон № 152-ФЗ «О персональных данных»;
- Федеральный закон № 98-ФЗ «О коммерческой тайне»;
- Федеральный закон № 63-ФЗ «Об электронной подписи»;
- Доктрина информационной безопасности Российской Федерации.

2.3. В части обеспечения безопасности персональных данных при их обработке в информационных системах Общество руководствуется требованиями:

- Приказа ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Приказа ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»;
- Приказа ФСТЭК России от 21.12.2017 № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования».

2.4. При формировании системы управления информационной безопасностью Общество учитывает положения национальных стандартов Российской Федерации, гармонизированных с международными стандартами серии ISO/IEC 27000, в том числе:

- ГОСТ Р ИСО/МЭК 27001-2021;
- ГОСТ Р ИСО/МЭК 27002-2021.

2.5. Настоящая Политика разработана с учетом внутренних нормативных документов ООО «Бизнес Технологии», формирующих корпоративную систему управления информационной безопасностью, включая Стандарт Общества «Система обеспечения информационной безопасности ООО „Бизнес Технологии“», устанавливающий архитектуру СУИБ, структуру процессов обеспечения информационной безопасности и порядок формирования нормативных документов в данной области.

2.6. В случае внесения изменений в законодательство Российской Федерации, нормативные правовые акты регуляторов либо внутренние нормативные документы Общества положения настоящей Политики подлежат пересмотру и актуализации в установленном порядке.

1.3 3. Термины, определения и сокращения

3.1. Сокращения

В настоящей Политике применяются следующие сокращения:

- АИС — автоматизированная информационная система;
- АРМ — автоматизированное рабочее место;
- ИБ — информационная безопасность;
- ИСПДн — информационная система персональных данных;
- НСД — несанкционированный доступ;
- ПДн — персональные данные;
- ПИБ — внутренние нормативные документы в области информационной безопасности;
- ПО — программное обеспечение;
- СЗИ — средства защиты информации;
- СУБД — система управления базами данных;
- СУИБ — система управления информационной безопасностью;
- УЗ — уровень защищенности ИСПДн.

При необходимости в тексте Политики могут использоваться иные общепринятые сокращения в области информационной безопасности и информационных технологий.

3.2. Основные термины и определения

В целях единообразного толкования положений настоящей Политики применяются следующие термины и определения:

1. Автоматизированная система — совокупность персонала и средств автоматизации, реализующих информационные технологии для выполнения установленных функций и обработки информации.
2. Авторизация — назначение субъекту доступа прав на выполнение определенных действий в отношении информационных ресурсов в соответствии с установленными полномочиями.
3. Аутентификация — процедура подтверждения подлинности субъекта доступа на основании предъявленных им идентификационных данных или аутентификационных факторов.
4. Безопасность информации — состояние защищенности информации, при котором обеспечиваются ее конфиденциальность, целостность и доступность.
5. Бизнес-процесс — совокупность взаимосвязанных действий и операций, направленных на создание ценности для Общества и достижение установленных целей деятельности.

6. Доступность информации — свойство информации и информационных систем, обеспечивающее возможность ее получения и использования авторизованными субъектами доступа в установленные сроки.
7. Защита информации — совокупность организационных, правовых и технических мер, направленных на предотвращение НСД, уничтожения, модификации, блокирования, копирования, распространения и иных неправомерных действий в отношении информации.
8. Идентификация — присвоение субъекту доступа уникального идентификатора и установление его соответствия заявленной учетной записи.
9. Конфиденциальная информация — информация ограниченного доступа, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации и внутренними нормативными документами Общества.
10. Информационная безопасность (ИБ) — состояние защищенности информационных активов и интересов Общества в условиях существования внутренних и внешних угроз.
11. Инцидент информационной безопасности — одно или несколько взаимосвязанных событий, которые привели или могут привести к нарушению требований информационной безопасности либо негативному влиянию на деятельность Общества.
12. Угроза информационной безопасности — совокупность условий и факторов, создающих потенциальную возможность причинения ущерба информационным активам Общества.
13. Уязвимость — недостаток или слабое место актива, процесса или меры защиты, которое может быть использовано угрозой для реализации инцидента ИБ.
14. Целостность информации — свойство информации сохранять точность, полноту и неизменность в процессе обработки, хранения и передачи.

Термины, не определенные в настоящем разделе, применяются в значениях, установленных законодательством Российской Федерации и действующими нормативными документами в области информационной безопасности.

1.4 4. Система управления информационной безопасностью

4.1. Принципы обеспечения информационной безопасности

Система управления информационной безопасностью Общества (далее — СУИБ) строится на основе следующих принципов:

1. Комплексность защиты — обеспечение защиты информационных активов посредством совокупности организационных, правовых, технических, программных и физических мер, реализуемых во взаимосвязи и с учетом характера обрабатываемой информации.
2. Системность и риск-ориентированный подход — управление ИБ осуществляется в рамках функционирования СУИБ на основе регулярной идентификации активов, анализа угроз, уязвимостей и оценки рисков.
3. Соответствие законодательству и обязательным требованиям — принимаемые меры защиты должны соответствовать требованиям законодательства Российской Федерации, нормативным актам регуляторов и договорным обязательствам Общества.
4. Минимизация и обоснованность прав доступа — доступ к информационным ресурсам предоставляется на основании принципов служебной необходимости, минимально достаточных полномочий и разграничения доступа.

5. Непрерывность контроля и совершенствование — процессы обеспечения ИБ подлежат постоянному мониторингу, анализу и совершенствованию с учетом изменений угроз, технологий и организационной структуры Общества.

4.2. Структура нормативных документов в области ИБ

Нормативное регулирование деятельности в области информационной безопасности в Обществе осуществляется на основе многоуровневой системы внутренних документов.

К документам первого уровня относится настоящая Политика, определяющая стратегические цели, принципы и общие требования в области ИБ.

Документы второго уровня конкретизируют требования Политики и устанавливают порядок реализации мер защиты по отдельным направлениям деятельности.

Документы третьего уровня детализируют реализацию положений и регламентов второго уровня и включают инструкции, методические материалы и рабочие процедуры, обеспечивающие выполнение требований ИБ на уровне конкретных процессов и ролей.

Документы разрабатываются с учетом требований законодательства Российской Федерации, нормативных актов регуляторов и внутренних стандартов Общества. Документы подлежат обязательному пересмотру при изменении нормативной базы, организационной структуры, технологической среды либо по результатам оценки эффективности СУИБ.

4.3. Управление рисками ИБ

Управление рисками ИБ является неотъемлемой частью процессов управления деятельностью Общества и реализуется в рамках СУИБ.

Оценка рисков проводится на регулярной основе, а также при внедрении новых информационных систем, изменении архитектуры ИТ-инфраструктуры, бизнес-процессов или нормативных требований. Процедуры оценки основаны на анализе актуальной модели угроз, выявлении уязвимостей и определении потенциального ущерба.

Результаты оценки рисков используются при формировании и корректировке комплекса мер защиты, определении приоритетов реализации мероприятий и распределении ресурсов. Ответственные должностные лица обеспечивают контроль реализации мероприятий по снижению рисков и мониторинг их эффективности.

Процедуры идентификации, оценки и обработки рисков информационной безопасности устанавливаются ПИБ.Р-01.

4.4. Контроль эффективности и совершенствование СУИБ

В Обществе организован систематический контроль выполнения требований настоящей Политики и внутренних нормативных документов в области ИБ.

Контроль включает проведение внутренних проверок, аудитов, анализ инцидентов информационной безопасности, а также оценку соблюдения установленных процедур. В целях повышения прозрачности и доверия со стороны контрагентов и общественности на регулярной основе привлекаются независимые внешние аудиторы для проведения оценки эффективности функционирования СУИБ.

Результаты контроля используются для корректировки мер защиты, актуализации нормативных документов и совершенствования процессов СУИБ.

Руководству Общества на регулярной основе предоставляется отчетность о состоянии информационной безопасности, уровне рисков, результатах проверок и значимых инцидентах. Это обеспечивает принятие обоснованных управленческих решений.

1.5 5. Организация обеспечения информационной безопасности

5.1. Распределение ролей и ответственности

Организация обеспечения информационной безопасности в Обществе строится на принципе распределенной ответственности.

Контроль и руководство деятельностью в области ИБ находятся в ведении высшего руководства Общества.

Функции координации, методического сопровождения и организационного управления СУИБ возлагаются на структурное подразделение, ответственное за обеспечение информационной безопасности, — отдел информационной безопасности (далее — ОИБ).

Руководители структурных подразделений обеспечивают выполнение требований ИБ в рамках курируемых направлений деятельности и несут ответственность за состояние защиты информации в подчиненных подразделениях.

5.2. Функции руководства

Руководство Общества:

- утверждает Политику и иные ключевые документы в области ИБ;
- определяет стратегические направления развития СУИБ;
- обеспечивает выделение необходимых организационных, финансовых и технических ресурсов;
- рассматривает отчеты о состоянии ИБ, результатах аудитов и расследования инцидентов;
- принимает решения о реализации корректирующих и предупреждающих мероприятий.

5.3. Функции ответственного за ИБ

Ответственный за ИБ:

- организует функционирование и развитие СУИБ;
- координирует процессы управления рисками ИБ;
- инициирует разработку, пересмотр и актуализацию внутренних нормативных документов;
- организует выявление, регистрацию и реагирование на инциденты ИБ;
- взаимодействует с уполномоченными государственными органами и внешними аудиторами в пределах своей компетенции;
- осуществляет методическое сопровождение структурных подразделений по вопросам обеспечения ИБ.

5.4. Ответственность работников

Работники Общества обязаны:

- соблюдать требования внутренних нормативных документов по ИБ;
- использовать информационные ресурсы исключительно в рамках служебных обязанностей;
- незамедлительно информировать ОИБ и своего непосредственного руководителя о выявленных инцидентах, подозрительных событиях и уязвимостях;
- проходить обучение и проверку знаний в области информационной безопасности.

Нарушение требований ИБ влечет применение мер ответственности в соответствии с законодательством Российской Федерации и внутренними актами Общества.

5.5. Взаимодействие с внешними организациями

Взаимодействие с контрагентами, подрядчиками и иными третьими лицами осуществляется на договорной основе с обязательным включением условий о соблюдении требований информационной безопасности и защите конфиденциальной информации.

Передача информации третьим лицам допускается при условии определения ее статуса, установления необходимого режима доступа и применения адекватных мер защиты.

Общество взаимодействует с уполномоченными государственными органами в порядке и объеме, предусмотренных законодательством Российской Федерации.

Порядок предоставления доступа подрядчикам и сторонним организациям устанавливается ПИБ.Р-02.

5.6. Обучение и осведомленность

В Обществе реализуется система повышения осведомленности работников в области информационной безопасности.

Обучение проводится при приеме на работу, а также на регулярной основе в процессе трудовой деятельности. Программы обучения охватывают вопросы защиты персональных данных, противодействия социальной инженерии, фишингу, целевым атакам, вредоносному программному обеспечению и иным актуальным угрозам.

Практическая часть обучения может включать тренировки, разбор типовых сценариев атак и имитационные мероприятия, направленные на отработку навыков распознавания угроз.

Результаты обучения подлежат учету и анализу в рамках процессов совершенствования СУИБ.

5.7. Использование информационных и ИТ-ресурсов

Общество обеспечивает безопасное использование информационных и ИТ-ресурсов на основе принципов служебного назначения, соблюдения конфиденциальности, защиты информации, минимизации рисков инцидентов и ответственности работников за соблюдение установленных правил.

Подробные требования и процедуры использования ИТ-ресурсов устанавливаются ПИБ.Р-03.

1.6 6. Управление информационными активами

Процессы идентификации, учета, классификации и обработки информационных активов в Обществе регулируются ПИБ.П-01. Настоящий раздел Политики закрепляет ключевые принципы управления информационными активами, которые детализируются в указанном нормативном документе.

6.1. Идентификация и учет активов

Все информационные активы Общества подлежат обязательной идентификации и учету. Каждому активу назначается владелец, ответственный за определение требований к его защите, оценку рисков и контроль соблюдения мер безопасности.

Перечень активов поддерживается в актуальном состоянии и регулярно пересматривается в рамках процессов управления ИБ.

6.2. Классификация и категорирование информации

Информация классифицируется по уровням конфиденциальности, важности для бизнеса и потенциального ущерба при ее раскрытии, модификации или утрате. Классификация определяет требования к хранению, обработке, передаче и уничтожению информации.

Категорирование информационных систем, обрабатывающих персональные данные (ИСПДн), осуществляется в соответствии с законодательством Российской Федерации и внутренними нормативными документами Общества, с определением уровней защищенности (УЗ) и соответствующих мер защиты.

6.3. Правила обращения с информацией

Обработка информации осуществляется в пределах полномочий пользователей и должностных обязанностей.

Передача информации по открытым или незащищенным каналам допускается только при использовании сертифицированных средств защиты информации, соответствующих установленным требованиям.

Уничтожение носителей информации и электронных копий осуществляется с применением процедур, исключающих возможность восстановления данных, в соответствии с внутренними регламентами Общества.

1.7 7. Управление доступом

Процессы управления доступом к информационным системам и ресурсам Общества регламентируются ПИБ.Р-04. Настоящий раздел Политики закрепляет ключевые принципы предоставления, использования и контроля доступа к информационным ресурсам, которые детализируются в указанном нормативном документе.

7.1. Принципы управления доступом

Доступ к информационным ресурсам и системам предоставляется на основе принципов минимально необходимого и достаточного доступа, разграничения полномочий, а также персональной ответственности пользователей за соблюдение правил ИБ.

7.2. Управление учетными записями

Процедуры создания, изменения и блокирования учетных записей регламентированы внутренними документами. Неиспользуемые или неактивные учетные записи подлежат своевременному отключению.

7.3. Идентификация и аутентификация

Все пользователи информационных систем идентифицируются с использованием уникальных учетных данных.

Для критически значимых систем при необходимости применяется усиленная аутентификация, включая многофакторные механизмы и регулярную проверку подлинности пользователей.

7.4. Привилегированный доступ

Привилегированные права предоставляются только по согласованию с владельцем ресурса и в пределах утвержденных полномочий. Использование привилегированных учетных записей подлежит обязательной регистрации и мониторингу.

Периодический пересмотр и актуализация предоставленных привилегий осуществляются в соответствии с установленными процедурами.

7.5. Контроль доступа к системам и сетевой инфраструктуре

Применяются технические средства разграничения доступа, включая межсетевые экраны, системы обнаружения вторжений, сегментацию сети и другие механизмы защиты от несанкционированного доступа.

7.6. Удаленный доступ и мобильные устройства

Удаленный доступ к информационным системам осуществляется исключительно через защищенные каналы связи с применением сертифицированных криптографических средств.

Использование мобильных устройств регламентируется внутренними документами и допускается только при соблюдении требований безопасности, включая защиту конфиденциальной информации и контроль доступа.

1.8 8. Обеспечение безопасности при эксплуатации ИТ-инфраструктуры

Требования к эксплуатации технических и программно-аппаратных средств защиты информации, включая средства защиты сетевой инфраструктуры, системы обнаружения и предотвращения вторжений, антивирусную защиту и средства мониторинга событий безопасности, устанавливаются ПИБ.П-02.

Настоящий раздел Политики закрепляет базовые принципы обеспечения безопасности ИТ-инфраструктуры. Положения подразделов 8.1–8.4 реализуются в соответствии с указанным нормативным документом.

8.1. Сетевая безопасность

Общество применяет многоуровневую модель защиты сетевой инфраструктуры, включающую сегментацию сети, межсетевые экраны, системы обнаружения и предотвращения вторжений, а при необходимости — сертифицированные средства защиты информации.

8.2. Защита от вредоносного ПО

На рабочих станциях и серверах внедряются сертифицированные средства антивирусной защиты и механизмы централизованного обновления, обеспечивающие своевременное обновление сигнатур и корректировку правил обнаружения угроз.

8.3. Защита от целевых и сетевых угроз

Общество реализует комплекс мероприятий по противодействию целевым атакам (APT), фишингу, DDoS и другим угрозам из сети Интернет, включая:

- мониторинг и анализ сетевого трафика;
- централизованный сбор и анализ событий безопасности;
- применение средств фильтрации и предотвращения атак;
- обучение сотрудников методам защиты от целевых атак, фишинга и других киберугроз;
- проведение регулярного тестирования защищенности инфраструктуры.

8.4. Регистрация и мониторинг событий

Ведется централизованный сбор, хранение и анализ событий информационной безопасности. Журналы регистрации защищаются от несанкционированного доступа и модификации.

8.5. Резервное копирование и восстановление

Организуются процедуры регулярного резервного копирования данных с проверкой корректности восстановления и периодическим тестированием планов восстановления после инцидентов.

Требования к организации резервного копирования и тестированию восстановления устанавливаются ПИБ.П-03.

8.6. Криптографическая защита информации

Криптографическая защита информации применяется в соответствии с требованиями законодательства и внутренними нормативными документами Общества. Используемые средства криптографической защиты соответствуют установленным требованиям и обеспечивают защиту конфиденциальности и целостности информации.

Порядок применения и эксплуатации криптографических средств защиты информации определяется ПИБ.Р-05.

8.7. Физическая безопасность

Доступ в серверные помещения и критически важные зоны ограничен и контролируется с использованием систем управления доступом, видеонаблюдения и иных средств физической защиты.

Требования к физической защите помещений и оборудования устанавливаются ПИБ.П-04.

1.9 9. Безопасность разработки и сопровождения программного обеспечения

Требования к обеспечению информационной безопасности на этапах жизненного цикла разработки программного обеспечения устанавливаются ПИБ.П-05. Настоящий раздел Политики закрепляет основные принципы обеспечения безопасности разработки, реализуемые в рамках указанного нормативного документа.

9.1. Требования ИБ на этапах жизненного цикла ПО

Требования информационной безопасности учитываются на всех этапах жизненного цикла программного обеспечения — от формирования требований до эксплуатации и сопровождения. Выполняются анализ угроз, оценка рисков и проектирование мер защиты для разрабатываемых решений.

9.2. Управление изменениями

Все изменения в информационных системах и программных продуктах проходят процедуру согласования, тестирования, документирования и утверждения в соответствии с внутренними регламентами.

9.3. Контроль защищенности

Проводится анализ исходного кода, тестирование на уязвимости, проверка соблюдения стандартов безопасной разработки и иные мероприятия, направленные на контроль защищенности ПО на всех этапах его жизненного цикла.

1.10 10. Управление инцидентами информационной безопасности

Процессы выявления, регистрации, расследования и реагирования на инциденты информационной безопасности регламентируются ПИБ.Р-06.

10.1. Выявление инцидентов

Организованы процедуры раннего обнаружения инцидентов ИБ на основе мониторинга и сообщений пользователей. Выявление осуществляется через постоянный мониторинг событий безопасности, анализ журналов систем и приложений, а также обработку сообщений пользователей о подозрительной активности.

Для повышения эффективности выявления применяются автоматизированные инструменты и методы корреляции событий.

10.2. Регистрация и реагирование

Все инциденты ИБ подлежат обязательной регистрации с фиксацией времени, источника и характера события. Инциденты классифицируются по степени критичности и потенциальному влиянию на бизнес-процессы.

Общество обеспечивает своевременное реагирование, включая оперативное устранение угроз, уведомление ответственных лиц и, при необходимости, привлечение внешних специалистов.

10.3. Анализ причин и корректирующие меры

После локализации инцидента проводится детальный анализ его причин и последствий. На основе результатов расследования разрабатываются корректирующие меры, направленные на восстановление нормального функционирования систем, минимизацию ущерба и предотвращение повторного возникновения аналогичных инцидентов.

10.4. Информирование и отчетность

При критических инцидентах Общество обеспечивает информирование руководства, соответствующих подразделений и, при необходимости, регуляторов.

Формируется отчет о каждом инциденте с описанием обстоятельств, принятых мер и предложений по улучшению процессов ИБ.

1.11 11. Обеспечение непрерывности деятельности

Общество реализует мероприятия по обеспечению устойчивости критичных бизнес-процессов, включая разработку и актуализацию планов восстановления деятельности после сбоев и инцидентов.

Планы восстановления периодически тестируются и корректируются с учетом выявленных недостатков, изменений в инфраструктуре, информационных системах и организационной структуре.

Подробности процедур разработки, тестирования и корректировки планов восстановления закреплены в ПИБ.Р-07.

1.12 12. Обеспечение соответствия требованиям

12.1. Соответствие законодательству Российской Федерации

Общество обеспечивает соблюдение применимых требований законодательства Российской Федерации в области информационной безопасности, включая нормативные акты, регулирующие обработку, хранение и передачу информации, а также деятельность в сфере ИТ.

12.2. Защита персональных данных

Обработка персональных данных в Обществе осуществляется в соответствии с требованиями Федерального закона № 152-ФЗ «О персональных данных», подзаконных нормативных правовых актов и внутренних нормативных документов Общества.

Порядок обработки и защиты персональных данных определяется ПИБ.П-06, ПИБ.Р-08 и связанными внутренними документами.

12.3. Коммерческая тайна

Режим коммерческой тайны устанавливается, поддерживается и контролируется в соответствии с Федеральным законом № 98-ФЗ «О коммерческой тайне» и внутренними регламентами Общества. Доступ к информации, составляющей коммерческую тайну, осуществляется на основании разграничения прав и обязательств работников.

Порядок отнесения информации к коммерческой тайне, а также правила ее обработки и защиты определяются ПИБ.П-07.

12.4. Внутренний контроль и аудит

В Обществе организован систематический внутренний контроль соблюдения требований ИБ. Проводятся плановые и внеплановые проверки, включающие аудит процессов, анализ инцидентов, оценку эффективности мер защиты и соблюдения регламентов.

1.13 13. Ответственность за нарушение требований ИБ

13.1. Работники Общества и иные лица, имеющие доступ к информационным ресурсам и информационным системам Общества, обязаны соблюдать требования настоящей Политики и иных внутренних нормативных документов в области информационной безопасности.

13.2. Лица, допустившие нарушение требований информационной безопасности, несут ответственность в соответствии с законодательством Российской Федерации, локальными нормативными актами Общества, а также условиями заключенных трудовых или гражданско-правовых договоров.

13.3. В зависимости от характера и последствий нарушения к виновным лицам могут применяться меры дисциплинарной, материальной, административной или иной ответственности в порядке, установленном законодательством Российской Федерации и внутренними документами Общества.

13.4. При выявлении нарушений требований информационной безопасности в Обществе могут проводиться служебные проверки для установления обстоятельств произошедшего, определения степени ответственности причастных лиц и принятия необходимых организационных и корректирующих мер.

1.14 14. Заключительные положения

14.1. Настоящая Политика вступает в силу и применяется в порядке, установленном внутренним стандартом Общества «Система управления информационной безопасностью ООО „Бизнес Технологии“».

14.2. Порядок разработки, согласования, утверждения, актуализации и отмены настоящей Политики определяется стандартом Общества «Система управления информационной безопасностью ООО „Бизнес Технологии“».

14.3. Требования настоящей Политики являются обязательными для всех работников Общества, а также для иных лиц, имеющих доступ к информационным ресурсам и информационным системам Общества в рамках договорных отношений.

14.4. Контроль соблюдения требований настоящей Политики осуществляется подразделением, ответственным за обеспечение информационной безопасности.

14.5. В случае противоречия положений настоящей Политики и иных внутренних нормативных документов Общества в области информационной безопасности приоритет имеют положения настоящей Политики.