ПОЛИТИКА
информационной безопасности

**г. Москва, 2023 г.**

**Содержание**

[1. Термины и сокращения 3](#_Toc148005972)

[1.1. Термины 3](#_Toc148005973)

[1.2. Сокращения 3](#_Toc148005974)

[2. Введение 3](#_Toc148005975)

[3. Общие положения 4](#_Toc148005976)

[4. Объект защиты 4](#_Toc148005977)

[5. Классификация информационных ресурсов 5](#_Toc148005978)

[6. Модель угроз и нарушителей ИБ 5](#_Toc148005979)

[6.1. Общие положения 5](#_Toc148005980)

[6.2. Классификация угроз ИБ 5](#_Toc148005981)

[6.3. Последствия реализации угроз ИБ 6](#_Toc148005982)

[7. Управление рисками ИБ 7](#_Toc148005983)

[8. Требования по обеспечению ИБ 7](#_Toc148005984)

[8.1. Общие требования по обеспечению ИБ 7](#_Toc148005985)

[8.2. Требования по обеспечению ИБ при назначении и распределении ролей и обеспечении доверия к персоналу 9](#_Toc148005986)

[8.3. Требования по обеспечению ИБ на стадиях жизненного цикла ИС 10](#_Toc148005987)

[8.4. Требования по обеспечению ИБ при управлении доступом и регистрацией 11](#_Toc148005988)

[8.5. Требования по защите от вредоносного ПО 12](#_Toc148005989)

[8.6. Требования по обеспечению ИБ при использовании ресурсов сети Интернет 12](#_Toc148005990)

[8.7. Требования по обеспечению ИБ при использовании СКЗИ 13](#_Toc148005991)

[9. Организация деятельности по обеспечению ИБ 13](#_Toc148005992)

[10. Нормативно-методическое обеспечение ИБ 15](#_Toc148005993)

[11. Технологическое обеспечение ИБ 16](#_Toc148005994)

[12. Кадровое обеспечение ИБ 16](#_Toc148005995)

[13. Контроль обеспечения ИБ 17](#_Toc148005996)

## Термины и сокращения

## Термины

Основные термины определены в документе «Политика информационной безопасности ООО «\_\_\_\_\_\_\_». Термины и определения по информационной безопасности».

## Сокращения

АИС - автоматизированная информационная система.

ИБ - информационная безопасность.

СОИБ - система обеспечения информационной безопасности.

НСД - несанкционированный доступ.

ОСОИБ - ответственный сотрудник по обеспечению информационной безопасности.

ПО - программное обеспечение.

СКЗИ - средства криптографической защиты информации.

СУБД - система управления базами данных.

## Введение

Политика информационной безопасности (далее - Политика) является частью системы обеспечения информационной безопасности (СОИБ) ООО «\_\_\_\_\_\_\_» (далее - Компания).

Политика определяет высокоуровневые цели, содержание и основные направления деятельности по обеспечению ИБ Компании. Положения Политики являются основополагающими и детализируются применительно к одной или нескольким областям ИБ, видам и технологиям деятельности Компании в других нормативных документах по обеспечению ИБ.

Политика разработана под цели и задачи Компании и является рекомендательной для дочерних компаний кроме пункта 9 данной Политики.

Действие Политики распространяется на все информационные активы Компании независимо от места их установки и использования. Требования Политики обязательны для выполнения всем персоналом Компании, а также персоналом сторонних организаций, имеющим доступ к информационным активам Компании.

Политика разработана в соответствии с положениями международных стандартов и рекомендаций по ИБ, применимых норм международного права, законодательства стран присутствия Компании, включая страну местопребывания Компании, внутренней нормативно-правовой базой Компании, в том числе:

* Концепцией информационной безопасности Компании;
* Положением о служебной и коммерческой тайне Компании;
* Положением о работе с персональными данными в Компании;
* Инструкцией по делопроизводству;
* ISO/IEC 17799:2005 (second edition) (c 2007 года — ISO/IEC 27002) Information Technology. Code of practice for information security management;
* ISO/IEC 27001:2005 Information technology. Security techniques. Information security management systems. Requirements;
* ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью;
* ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.

## Общие положения

Для решения стоящих перед ней задач Компания использует информационные активы, являющиеся частью всех активов Компании, и включающие информацию, а также процессы и средства её обработки.

Информационные активы, используемые Компанией, подвержены действию угроз ИБ. Целью деятельности по обеспечению ИБ является защита информационных активов Компании от реализации угроз ИБ и связанной с этим возможности нанесения ущерба Компании.

Обеспечение ИБ осуществляется посредством реализации мер защиты информации, выбираемых на основе анализа защищаемых информационных активов, модели угроз и нарушителей ИБ, а также рисков ИБ.

Реализуемые меры защиты информации должны обеспечивать сохранность требуемых свойств ИБ информационных активов.

Основными свойствам ИБ являются конфиденциальность, целостность и доступность. Дополнительными свойствами ИБ, в том числе, являются аутентичность, функциональность, учетность и отказоустойчивость.

Обеспечение ИБ в Компании осуществляется Системой обеспечения ИБ (СОИБ), реализующей процессы защиты информации и управления ИБ.

## Объект защиты

Защите подлежат все информационные активы, принадлежащие Компании и используемые Компанией в своей деятельности, в том числе:

* информационные ресурсы (файлы, базы данных, архивированная информация, документация и др.);
* технологические процессы обработки информации (платёжные, технологические процессы и др.);
* программное обеспечение (прикладное и системное программное обеспечение, утилиты, средства разработки и др.);
* технические средства информатизации (компьютерное и телекоммуникационное оборудование, носители информации и др.);
* помещения, используемые для реализации информационных процессов.

В целях анализа рисков ИБ и выбора мер защиты все защищаемые информационные активы подлежат инвентаризации и классификации. Классификация информационных активов основана на требованиях по обеспечению ИБ использующих их бизнес-процессов.

Рекомендуемые правила инвентаризации и классификации информационных активов определены в документе «Политика информационной безопасности» ООО «\_\_\_\_\_\_\_». Методика инвентаризации и классификации информационных активов».

## Классификация информационных ресурсов

Классификация информационных ресурсов по уровню конфиденциальности, содержащейся в них информации, осуществляется в соответствии с требованиями Положения о служебной и коммерческой тайне (далее Положение о СКТ), Положения о работе с персональными данными в Компании и Инструкции по делопроизводству.

Вся информация, используемая в Компании, относится по уровню конфиденциальности к одной из 2-х категорий:

* открытая;
* конфиденциальная.

К ***открытой информации*** относятся:

* сведения, полученные из внешних открытых источников;
* сведения, явно определённые в установленном Положением о СКТ порядке в качестве открытой информации для публикации или предоставления внешним организациям.

Открытая информация может неограниченно распространяться как внутри, так и вне Компании. Требования по обеспечению ИБ открытой информации включают обеспечение целостности, доступности и дополнительных свойств ИБ в случае необходимости.

К ***конфиденциальной информации***относятся:

* сведения, содержащие служебную и коммерческую тайну в соответствии с Положением о СКТ;
* персональные данные, относящиеся к конфиденциальным в соответствии Положением о работе с персональными данными в Компании;
* сведения, имеющие гриф "конфиденциально", «служебная информация».

Порядок обеспечения сохранности конфиденциальной информации определяется Положением о СКТ и Инструкцией по делопроизводству.

Требования по обеспечению ИБ конфиденциальной информации включают обеспечение конфиденциальности, целостности, доступности и дополнительных свойств ИБ в случае необходимости.

## Модель угроз и нарушителей ИБ

## Общие положения

Модель угроз и нарушителей определяет основные принципы классификации источников рисков ИБ, подлежащих учёту при создании, поддержании и совершенствовании СОИБ.

Конкретный перечень источников угроз, выбор методов и средств противодействия, а также подходы к оценке эффективности защиты зависят от защищаемого уровня ИС.

## Классификация угроз ИБ

Угрозы ИБ по природе их возникновения разделяется на две категории: объективные и субъективные.

К объективным угрозам ИБ относятся угрозы, вызванные воздействиями объективных физических процессов или стихийных природных явлений, не зависящих от деятельности человека. Объективные угрозы ИБ могут нарушить целостность и доступность информации.

К объективным угрозам относятся:

* природные факторы, такие как стихийные бедствия, электромагнитные явления и биологические факторы;
* техногенные факторы, такие как аварии электроснабжения, дефекты аппаратно-программного обеспечения, сбои при предоставлении телекоммуникационных услуг.

К субъективным угрозам ИБ относятся угрозы, связанные с деятельностью человека и направленные на нарушение доступности, целостности или конфиденциальности информации.

Среди них можно выделить:

* непреднамеренные угрозы, вызванные несовершенством организации бизнес-процессов, ошибочными действиями персонала и т.п.;
* преднамеренные угрозы, порождаемые злоумышленными действиями нарушителя ИБ.

Угрозы ИБ могут быть реализованы нарушителем ИБ на каждом из основных уровней ИС, включая:

* приложения (программное обеспечение, используемое Компанией);
* аппаратные средства (серверы, рабочие станции, принтеры и другое компьютерное оборудование);
* сетевые устройства (коммутаторы, межсетевые экраны, точки доступа и др.);
* сетевые подключения (сетевые соединения между аппаратными средствами, а также подключения к внешним сетям);
* помещения.

Все нарушители ИБ разделяются на следующие категории:

* внешние нарушители ИБ, не имеющие санкционированного доступа к активам Компании (хакеры, фрикеры и др.);
* внутренние нарушители ИБ, имеющие права доступа к АИС Компании и реализующие угрозы ИБ как в рамках своих полномочий, так и за их пределами;
* комбинированные, действующие в сговоре внешние и внутренние нарушители ИБ.

## Последствия реализации угроз ИБ

Реализация угрозы ИБ может привести к нарушению свойств ИБ. В результате нарушения конфиденциальности информационных активов защищаемая информация может стать известной неполномочным лицам, логическим объектам или процессам. Нарушение целостности информационных активов может привести к несанкционированному изменению информации, а нарушение доступности может нарушить доступ полномочных пользователей к информации.

В результате реализации угроз ИБ Компании может быть нанесён ущерб, который может быть обусловлен:

* частичной или полной невозможностью продолжения деятельности;
* необходимостью восстановления нарушенных свойств ИБ защищаемых информационных активов;
* частичной или полной невозможностью выполнения обязательств перед клиентами, контрагентами и другими сторонами;
* нарушением требований законодательства, надзорных и регулирующих органов;
* потерей деловой репутации.

## Управление рисками ИБ

Угрозы ИБ влияют на операционные риски Компании, связанные с несовершенной организацией или ненадлежащей реализацией бизнес-процессов. Для обеспечения приемлемого уровня рисков ИБ принимаются меры по защите ИС Компании.

Разработка экономически обоснованных мер по совершенствованию обеспечения ИБ Компании осуществляется на основе оценки рисков ИБ. При обработке рисков ИБ принимаются решения по их оптимизации за счет реализации мер защиты, переноса, отказа или принятия остаточных рисков.

Оценка и обработка рисков ИБ осуществляется в соответствии с документом «Политика информационной безопасности ООО «\_\_\_\_\_\_\_». Методика оценки рисков информационной безопасности».

## Требования по обеспечению ИБ

## Общие требования по обеспечению ИБ

***Законность.***

Меры обеспечения ИБ Компании должны соответствовать применимым нормам международного права, законодательства стран присутствия Компании, включая страну местопребывания Компании, внутренней нормативно-правовой базе Компании.

***Комплексность и координация.***

В обеспечении ИБ должны принимать участие руководящие органы, структурные подразделения и персонал Компании. Для обеспечения ИБ необходимо согласованное применение всех доступных правовых, организационных и технических мер, перекрывающих в совокупности все существенные каналы реализации угроз ИБ. Ответственность за организацию и координацию деятельности по обеспечению ИБ должна быть возложена на специально уполномоченное лицо.

***Компетентность и специализация.***

Решения, влияющие на уровень обеспечения ИБ, включая выбор средств информатизации и защиты информации, распределение обязанностей персонала, информационного взаимодействия с бизнес-партнёрами и др., должны быть согласованы с уполномоченным лицом по ИБ.

***Непрерывность.***

Обеспечение ИБ должно представлять собой непрерывный процесс, осуществляемый на всех этапах процессов и всех стадиях жизненного цикла ИС. Процесс обеспечения ИБ должен включать стадии планирования, реализации, контроля и анализа, поддержки и совершенствования системы.

***Осведомленность.***

Персонал Компании, а также сотрудники внешних организаций - клиентов и контрагентов Компании, должны быть осведомлены о требованиях по обеспечению ИБ в объёме, требуемом для выполнения их служебных обязанностей. Нормативные документы по ИБ должны полностью разъяснять предмет, обязательства и меры ответственности, как со стороны Компании, так и со стороны осведомляемого лица или организации. Уровень осведомленности персонала в области ИБ подлежит регулярному контролю со стороны уполномоченных лиц по ИБ.

***Знание своих клиентов и сотрудников.***

Компания должна обладать необходимой для обеспечения ИБ информацией о своих клиентах и сотрудниках. Эта информация должна поддерживаться в актуальном состоянии и использоваться при принятии решений по обеспечению ИБ.

***Эшелонирование.***

Для повышения уровня защищённости, система защиты должна строиться эшелонировано. Обнаружение и противодействие угрозам ИБ должно обеспечиваться независимыми уровнями (эшелонами) защиты таким образом, чтобы компрометация одного уровня не приводила компрометации всей системы защитных мер. Наряду с защитой периметра Компании от внешних угроз, должна быть обеспечена организация и защита внутренних периметров в местах размещения критичных информационных активов. Система ИБ должна включать независимые эшелоны защиты на уровнях:

* физического доступа к носителям данных, серверам, системам резервного копирования, и прочему оборудованию;
* доступа к межсетевым соединениям и локальной вычислительной сети Компании;
* доступа к операционным системам;
* доступа к приложениям и данным.

Специальные меры должны быть предприняты для защиты систем управления, мониторинга, учетности и аудита ИБ.

***Приоритет мер предупреждения.***

Процесс обеспечения ИБ Компании должен быть ориентирован на профилактику и своевременное выявление предпосылок возникновения и реализации угроз ИБ.

***Минимизация привилегий, разделение полномочий.***

Каждому пользователю должны предоставляться минимально необходимые для выполнения его должностных обязанностей права по доступу к информационным активам. Права одного пользователя не должны давать возможности нарушения ИБ.

***Минимум общего ресурса защиты.***

Во всех возможных случаях должны использоваться персонифицированные средства идентификации и аутентификации пользователей ИС.

***Полнота контроля.***

Система ИБ должна обеспечивать выполнение явно определенной политики безопасности при каждом обращении к каждому защищаемому информационному активу. Политика безопасности должна строиться на основе принципа «все, что явно не разрешено - запрещено».

***Доступность услуг и сервисов.***

Информационные активы должны быть доступны легальным пользователям в течение определённого нормативными документами времени. Для критически важных информационных активов должны быть разработаны планы обеспечения непрерывности деятельности и восстановления работоспособности после прерываний.

***Простота реализации и применения.***

Средства защиты должны быть максимально просты и понятны в реализации и использовании. Простота используемых средств защиты должна признаваться дополнительным фактором защищенности.

***Централизация управления.***

Организационные и технические меры обеспечения ИБ Компании должны быть максимально централизованы и обеспечивать функционирование системы безопасности по единым правовым, организационным, функциональным и методологическим принципам. Централизация управления средствами ИБ должна обеспечивать максимальную информированность персонала, обоснованность, оперативность и минимальные затраты на координацию решений.

***Гибкость управления и применения.***

Система ИБ должна перестраиваться с минимальными затратами времени и ресурсов при изменениях бизнес-процессов и требований к защите, а также обеспечивать защиту не только от известных угроз ИБ, но и от угроз, появление которых возможно в будущем.

***Адекватность и экономическая обоснованность защитных мер.***

Применяемые защитные меры должны быть адекватны модели угроз и нарушителей, а также учитывать соотношение между величиной затрат на их реализацию и возможным ущербом от реализации угроз.

***Плановая и бюджетная основа деятельности.***

Деятельность по обеспечению ИБ должна осуществляться на основе плана и бюджета доходов и расходов Компании в части расходов по обеспечению ИБ.

## Требования по обеспечению ИБ при назначении и распределении ролей и обеспечении доверия к персоналу

Роли персонала, участвующего в реализации бизнес процессов Компании, должны быть определены и документально зафиксированы. Роли должны быть персонифицированы, ответственность за надлежащее исполнение ролей должна быть зафиксирована в трудовых договорах и/или должностных регламентах.

В целях снижения рисков нарушения ИБ не рекомендуется в рамках одной роли совмещать функции разработки, сопровождения и эксплуатации программного обеспечения, администрирования ИБ и использования ИС, исполнения операций обработки информации и контроля результатов их исполнения.

При приёме на работу, влияющую на обеспечение ИБ, должна осуществляться проверка подлинности представленных документов, заявляемой квалификации, точности и полноты биографических фактов, а также контроль профессиональных навыков и оценка профессиональной пригодности. Порядок и результаты проверки должны быть документально зафиксированы.

Весь персонал Компании, а также лица, принимаемые на работу по срочным трудовым договорам, для прохождения практики или стажировки и др. обязаны дать письменное обязательство о неразглашении конфиденциальной информации в соответствии с "Положением о коммерческой и служебной тайне".

Обязанности по выполнению требований по обеспечению ИБ должны включаться в трудовые договора и/или должностные регламенты. Нарушение требований по обеспечению ИБ должно рассматриваться как неисполнение должностных обязанностей.

## Требования по обеспечению ИБ на стадиях жизненного цикла ИС

Формирование требований по обеспечению ИБ осуществляется для следующих обобщенных стадий жизненного цикла ИС:

* разработка технического задания;
* проектирование;
* создание и тестирование;
* приемка и ввод в действие;
* эксплуатация;
* сопровождение и модернизация;
* снятие с эксплуатации.

В зависимости от объёма и метода выполнения работ (собственная или заказная разработка, приобретение и др.) допускается опускать или объединять отдельные стадии.

Разработка технических заданий и приёмка ИС должна осуществляться по согласованию, а ввод в действие, эксплуатация, сопровождение, модернизация и снятие с эксплуатации под контролем уполномоченного лица по ИБ.

Привлекаемые на договорной основе для разработки средств защиты информации специализированные организации должны иметь выданные в установленном порядке лицензии на осуществление данного вида деятельности.

В договоры на разработку или поставку ИС должны включаться положения по сопровождению поставляемых изделий в течение всего срока службы или поставке технических средств и документации, позволяющих осуществлять сопровождение и эксплуатацию ИС без участия поставщика.

При разработке технических заданий на системы АИС следует учитывать, что защита данных должна обеспечиваться в условиях:

* попыток доступа к информации анонимных, неавторизованных злоумышленников при использовании сетей общего пользования;
* возможности ошибок авторизованных пользователей систем;
* возможности ненамеренного или неадекватного использования конфиденциальных данных авторизованными пользователями.

На стадии сопровождения (модернизации) необходимо обеспечить защиту от неумышленного или умышленного несанкционированного раскрытия, модификации или уничтожения информации, а также от отказа в обслуживании или снижения качества обслуживания.

Создание и тестирование изменений ИС должны осуществляться с использованием выделенной операционной среды, не влияющей на выполнение бизнес-процессов. При внесении изменений в ИС должна проводиться проверка работоспособности системы.

При выполнении работ должны приниматься необходимые меры обеспечения ИБ, в том числе в отношении лицензионных данных, исходных кодов и дистрибутивов ПО, криптографической информации и тестовых данных.

При эксплуатации ИС должны регулярно выполняться процедуры контроля работоспособности реализованных в ИС защитных мер.

При снятии с эксплуатации необходимо обеспечивать:

* сохранение архивов электронных документов и протоколов электронного взаимодействия, ведение и сохранность которых в течение определенного срока предусмотрены нормативными документами или договорами Компании;
* удаление информации, несанкционированное использование которой может нанести ущерб деятельности Компании, из постоянной памяти АИС и с внешних носителей.

## Требования по обеспечению ИБ при управлении доступом и регистрацией

Порядок управления доступом к различным видам информационных активов должен быть регламентирован. Регламент управления доступом должен включать, в том числе, описание информационных активов, уровней предоставляемого доступа и определять процедуры управления доступом.

Процедуры управления доступом должны:

* предусматривать предоставление пользователям минимально необходимых для выполнения их должностных обязанностей прав доступа к информационным активам;
* обеспечивать изменение прав доступа пользователей при изменении их должностных обязанностей;
* исключать возможность неконтролируемого предоставления прав доступа;
* определять порядок действий в случае компрометации используемых для получения доступа реквизитов.

Для управления доступом могут использоваться встроенные в АИС, сертифицированные установленным образом или разрешенные к применению Департаментом безопасности Компании средства.

Доступ к информационным активам Компании должен предоставляется только зарегистрированным пользователям с использованием средств идентификации, аутентификации и авторизации. Учётная запись должна однозначно идентифицировать пользователя и определять его права по доступу к информационным активам.

Данные регистрации о предоставлении доступа и использовании АИС должны регулярно контролироваться и анализироваться с целью обнаружения неправомерных действий.

АИС и все её компоненты должны обеспечивать, в том числе, возможность регистрации операций, связанных с назначением и распределением прав доступа, с изменением регистрационных данных, а также финансовых транзакций.

Компоненты АИС должны реализовывать защитные меры, обеспечивающие невозможность отказа от авторства производимых операций.

В договоры с клиентами и контрагентами, в случае необходимости, следует включать положения, предусматривающие необходимый уровень взаимодействия в случае возникновения инцидентов ИБ, требующих совместного реагирования.

## Требования по защите от вредоносного ПО

Средства защиты от вредоносного ПО должны обеспечивать противодействие проникновению вредоносного ПО в АИС Компании, а также обнаружение и устранение обнаруженного вредоносного ПО.

Средства защиты должны контролировать все возможные пути проникновения и распространения вредоносного ПО, включая ресурсы сети Интернет, электронную почту, съёмные носители и мобильные устройства, программное обеспечение, разделяемые файловые ресурсы, а также обеспечивать автоматическую загрузку обновлений.

Порядок установки, настройки, сопровождения и эксплуатации средств защиты от вредоносного ПО должен быть регламентирован. Должны быть определены, в том числе, процедуры контроля за правильностью функционирования, отключением и обновлением средств защиты, отражения и устранения последствий заражения вредоносным ПО.

## Требования по обеспечению ИБ при использовании ресурсов сети Интернет

Компания осуществляет предоставление Сотрудникам доступа к сети Интернет для производственной и собственной хозяйственной деятельности, получения и распространения информации, связанной с деятельностью Компании, информационно-аналитической работы, обмена электронными сообщениями, в том числе электронной почтой Интернет, получения обновлений программного обеспечения и баз данных АИС Компании.

Для исключения использования в неустановленных целях Компания осуществляет ограничение доступа и контроль использования ресурсов сети Интернет.

При использовании сети Интернет для доступа к внутренним ресурсам АИС Компании должны приниматься меры защиты, обеспечивающие противодействие нарушениям ИБ ИС, идентификацию, аутентификацию и авторизацию пользователей, а также конфиденциальность, целостность, доступность, учётность и отказоустойчивость при обмене информацией.

При использовании электронной почты должны приниматься меры защиты от проникновения вредоносного ПО, массовых несанкционированных рассылок (СПАМа), утечки конфиденциальной информации. Сообщения электронной почты должны архивироваться. Хранение и доступ к архивам сообщений должны осуществляться в установленном порядке.

## Требования по обеспечению ИБ при использовании СКЗИ

Средства криптографической защиты информации (СКЗИ) могут применяться для обеспечения целостности, конфиденциальности, отказоустойчивости и других свойств ИБ в соответствии с моделью угроз и нарушителей ИБ.

Применяемые СКЗИ должны быть сертифицированы установленным образом, или разрешены к применению в Компании в установленном порядке, или соответствовать требованиям договора с контрагентом (клиентом) Компании.

При применении СКЗИ в ИС должна поддерживаться непрерывность протоколирования работы СКЗИ, а также целостность программного обеспечения, взаимодействующего со СКЗИ.

Порядок применения СКЗИ, включая процессы ввода в действие, внесения изменений, эксплуатации, восстановления работоспособности после сбоев, снятия с эксплуатации, управления ключами, использования носителей ключевой информации включая действия при смене и компрометации ключей, должен быть регламентирован.

Ключи СКЗИ должны изготавливаться Компанией или их владельцами самостоятельно. В случае изготовления ключей сторонними организациями или лицами, организационные и правовые последствия таких действий должны быть отражены в соответствующих договорах.

## Организация деятельности по обеспечению ИБ

Деятельность структурных подразделений и отдельных должностных лиц по защите информационных активов организуется и координируется СОИБ. В функционировании СОИБ принимают участие:

* Руководитель по информационным технологиям Компании;
* ответственный сотрудник по обеспечению ИБ (ОСОИБ);
* структурные подразделения Компании;
* персонал Компании.

Департамент безопасности Компании осуществляет общее руководство и контроль обеспечения ИБ. Для текущего управления деятельностью по обеспечению ИБ, в региональных представительствах Компании, Департамент безопасности назначает ответственного сотрудника по обеспечению ИБ (ОСОИБ), утверждает нормативные документы и планы по совершенствованию ИБ, выделяет ресурсы на обеспечение ИБ, контролирует состояние ИБ Компании.

ОСОИБ осуществляет планирование, организацию, совершенствование и контроль деятельности по обеспечению ИБ, а также несёт ответственность за состояние ИБ Компании.

Выполнение обязанностей ОСОИБ может совмещаться с выполнением иных функциональных обязанностей, исключая виды деятельности, приводящие к возникновению конфликта интересов.

В функциональные обязанности ОСОИБ входит:

* организация, планирование и контроль выполнения мероприятий по обеспечению ИБ;
* участие в формировании заявки о планируемых доходах и расходах ИТ в части расходов по обеспечению ИБ;
* подготовка предложений по разработке и совершенствованию нормативной документации по обеспечению ИБ;
* выработка требований к реализации мер обеспечения ИБ;
* участие в проверке уровня защищённости информационных активов, систем и бизнес- процессов Компании, подготовка предложений по предотвращению нарушений ИБ;
* участие в рассмотрении инцидентов ИБ, подготовка предложений по применению санкций в отношении нарушителей режима обеспечения ИБ;
* участие в подготовке документации и проведении работ по созданию и модификации ИС на стадиях жизненного цикла;
* взаимодействие, в случае необходимости, с организациями и уполномоченными органами страны местопребывания Компании по вопросам, относящимся обеспечению ИБ и лицензированию деятельности по защите информации;
* инструктаж и консультирование персонала Компании по вопросам обеспечения ИБ.
* ОСОИБ вправе:
* получать от структурных подразделений информацию, необходимую для выполнения своих функций;
* вносить мотивированные предложения Департаменту безопасности об ограничении или приостановке функционирования АИС или бизнес-процессов в случае возникновения угроз ИБ деятельности Компании.

Структурные подразделения осуществляют деятельность по обеспечению ИБ в объёме возложенных на них задач и функций.

***Отдел информационных технологий:***

* участвует в разработке нормативно-технической документации по обеспечению ИБ процессов автоматизированной обработки и передачи информации;
* реализует технические меры по обеспечению ИБ в АИС в соответствии с требованиями нормативных документов по обеспечению ИБ;
* осуществляет мониторинг защищённости АИС, выявление и пресечение попыток реализации угроз нарушения ИБ;
* осуществляет администрирование ряда средств обеспечения ИБ АИС в соответствии с требованиями нормативных документов;
* осуществляет резервирование и восстановление информационных ресурсов, обрабатываемых в электронном виде;
* обеспечивает непрерывность функционирования и восстановление после сбоев АИС Компании.

***Юридический отдел:***

* разрабатывает и реализует правовые меры обеспечения ИБ;
* осуществляет мониторинг соответствия внутренних нормативных актов Компании законодательству стран присутствия Компании, относящегося к вопросам обеспечения ИБ;
* контролирует правильность оформления договорных отношений Компании с персоналом, клиентами и контрагентами Компании на соответствие требованиям законодательства и нормативных документов Компании по обеспечению ИБ.

Обязанность по обеспечению ИБ в соответствии с нормативной документацией ИБ должна быть включена в должностные регламенты персонала Компании. Персонал Компании выполняет требования по обеспечению ИБ в рамках исполнения своих должностных обязанностей. Руководители всех уровней организуют работу по обеспечению ИБ в подконтрольных им подразделениях.

Нарушение требований по обеспечению ИБ рассматривается как ненадлежащее исполнение должностных обязанностей. Виновные подлежат ответственности в установленном порядке.

## Нормативно-методическое обеспечение ИБ

Деятельность по обеспечению ИБ Компании должна быть документирована. Комплекс нормативных документов по ИБ должен обеспечивать систематическое изложение правил и требований по осуществлению деятельности по защите информации, как для Компании в целом, так и для отдельных бизнес-процессов и функциональных ролей.

В состав комплекса нормативных документов по обеспечению ИБ входят:

* Политика ИБ (настоящий документ) и поддерживающие её документы;
* Регламент парольной защиты;
* Инструкция пользователя ИАС;
* прочие документы, определяющие требования ИБ к процедурам и ролям.

Политика ИБ является основополагающим документом и определяет высокоуровневые цели, содержание и основные направления деятельности по обеспечению ИБ. Политика ИБ подлежит утверждению руководством Компании.

Частные политики ИБ детализируют положения Политики ИБ для отдельных направлений деятельности по обеспечению ИБ. Документы, содержащие положения частных политик ИБ, могут быть введены в действие посредством утверждения руководством Компании или приказом Главного акционера Компании.

Документы, содержащие требования ИБ к процедурам и ролям (регламенты, инструкции и др.) определяют требования к процессам обеспечения ИБ и порядок действий персонала по обеспечению ИБ при реализации отдельных бизнес-процессов, работе с отдельными информационными системами и видами активов с необходимой для обеспечения надёжной защиты информационных активов детальностью.

Указанные в настоящем пункте документы подлежат согласованию с ответственным сотрудником по обеспечению ИБ и утверждаются руководителями структурных подразделений, ответственными за выполнение регламентируемых видов деятельности.

Нормативная документация по обеспечению ИБ должна предусматривать документальное оформление свидетельств выполнения деятельности по обеспечению ИБ.

Нормативные документы по обеспечению ИБ должны пересматриваться и совершенствоваться на регулярной основе с учётом изменений законодательства и нормативных актов по обеспечению ИБ страны местопребывания Компании, внутренних нормативных документов Компании и результатов контроля состояния ИБ Компании. Изменённые нормативные документы подлежат утверждению в установленном порядке.

## Технологическое обеспечение ИБ

Технологическое обеспечение ИБ включает программные и аппаратные средства, реализующие установленные меры защиты.

Технологическое обеспечение ИБ должно удовлетворять основным требованиям по обеспечению ИБ и, в том числе, осуществлять:

* выявление существующих уязвимостей автоматизированных информационных систем;
* обнаружение и защиту от вредоносного ПО;
* обнаружение и предотвращение сетевых атак;
* защиту, в том числе криптографическую, конфиденциальной информации;
* защиту от нежелательной почтовой корреспонденции;
* мониторинг и аудит событий ИБ;
* контроль использования съемных носителей информации и подключаемых устройств.

## Кадровое обеспечение ИБ

В рамках кадрового обеспечения ИБ в Компании должен быть организован процесс повышения осведомленности и контроля знаний персонала по вопросам ИБ.

Квалификация персонала в области ИБ должна соответствовать требованиям, предъявляемым к безопасности информационных активов, необходимых для исполнения возложенных функциональных обязанностей.

Формой повышения осведомлённости и контроля знаний персонала в области ИБ может являться инструктаж, осуществляемый уполномоченными лицами Компании, посещение авторизованных курсов повышения квалификации, использование методов дистанционного обучения.

## Контроль обеспечения ИБ

Исполнение требований по соблюдению ИБ подлежит регулярному контролю.

Руководители всех уровней должны контролировать соблюдение требований по обеспечению ИБ в руководимых ими подразделениях.

Ответственный сотрудник по обеспечению ИБ должен осуществлять постоянный контроль обеспечения ИБ Компании и регулярно информировать руководителя Департамента безопасности о результатах проводимой работы.

Отдел внутреннего контроля осуществляет независимую проверку (аудит) эффективности и надёжности функционирования СОИБ не реже одного раза в год.