Политика информационной безопасности

1. **Перечень используемых определений, обозначений и сокращений.**

АИБ — Администратор информационной безопасности.

ИБ — Информационная безопасность.

ИР — Информационные ресурсы.

ИС — Информационная система.

НСД — Несанкционированный доступ.

СЗИ — Средство защиты информации.

СУИБ — Система управления информационной безопасностью.

ЭВМ — Электронная — вычислительная машина, персональный компьютер.

Администратор информационной безопасности — специалист или группа специалистов организации, осуществляющих контроль за обеспечением защиты информации в ЛВС, а также осуществляющие организацию работ по выявлению и предупреждению возможных каналов утечки информации, потенциальных возможностей осуществления НСД к защищаемой информации.

Доступ к информации — возможность получения информации и ее использования.

Идентификация — присвоение субъектам доступа (пользователям, процессам) и объектам доступа (информационным ресурсам, устройствам) идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информация — это актив, который, подобно другим активам, имеет ценность и, следовательно, должен быть защищен надлежащим образом.

Информационная безопасность — механизм защиты, обеспечивающий конфиденциальность, целостность, доступность информации; состояние защищенности информационных активов общества в условиях угроз в информационной сфере. Угрозы могут быть вызваны непреднамеренными ошибками персонала, неправильным функционированием технических средств, стихийными бедствиями или авариями (пожар, наводнение, отключение электроснабжения, нарушение телекоммуникационных каналов и т. п.), либо преднамеренными злоумышленными действиями, приводящими к нарушению информационных активов общества.
Информационная система — совокупность программного обеспечения и технических средств, используемых для хранения, обработки и передачи информации, с целью решения задач подразделений ООО “Бермуды” (далее — “Компания”).

Информационные ресурсы — совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий.

Конфиденциальность — доступ к информации только авторизованных пользователей.

Несанкционированный доступ к информации — доступ к информации, нарушающий правила разграничения уровней полномочий пользователей.

Политика информационной безопасности — комплекс взаимоувязанных руководящих принципов и разработанных на их основе правил, процедур и практических приемов, принятых в Компании для обеспечения его информационной безопасности.

Регистрационная (учетная) запись пользователя — включает в себя имя пользователя и его уникальный цифровой идентификатор, однозначно идентифицирующий данного пользователя в операционной системе (сети, базе данных, приложении и т. п.). Регистрационная запись создается администратором при регистрации пользователя в операционной системе компьютера, в системе управления базами данных, в сетевых доменах, приложениях и т. п. Она также может содержать такие сведения о пользователе, как Ф. И. О., название подразделения, телефоны, E-таН и т. п.

Угрозы информации — потенциально существующая опасность случайного или преднамеренного разрушения, несанкционированного получения или модификации данных, обусловленная структурой системы обработки, а также условиями обработки и хранения данных, т. е. это потенциальная возможность источника угроз успешно выявить определенную уязвимость системы.

Уязвимость — недостатки или слабые места информационных активов, которые могут привести к нарушению информационной безопасности при реализации угроз в информационной сфере.

2. Вводные положения.

1. Политика информационной безопасности Компании определяет цели и задачи системы обеспечения ИБ и устанавливает совокупность правил, требований и руководящих принципов в области ИБ, которыми в последствии руководствуется в своей деятельности.
2. Основными целями Политики информационной безопасности являются защита информации Компании от возможного нанесения материального, физического, морального или иного ущерба, посредством случайного или преднамеренного воздействия на информацию, ее носители, процессы обработки и передачи, а также обеспечение эффективной работы всего информационно-вычислительного комплекса при осуществлении деятельности, указанной в Положении о деятельности Компании.
3. Общее руководство обеспечением ИБ осуществляется Генеральным директором Компании. Ответственность за организацию мероприятий по обеспечению ИБ и контроль за соблюдением требований ИБ несет АИБ. Ответственность за функционирование информационных систем Компании несет администратор информационной системы.
4. Должностные обязанности АИБа и системного администратора закрепляются в соответствующих инструкциях.
5. Руководители структурных подразделений Компании несут ответственность за обеспечение выполнения требований ИБ в своих подразделениях.
6. Сотрудники Компании обязаны соблюдать порядок обращения с конфиденциальными документами, носителями ключевой информации и другой защищаемой информацией, соблюдать требования настоящей Политики и других внутренних документов Компании по вопросам обеспечения ИБ.
7. Политика информационной безопасности направлена на защиту информационных активов от угроз, исходящих от противоправных действий злоумышленников, уменьшение рисков и снижение

потенциального вреда от аварий, непреднамеренных ошибочных действий персонала, технических сбоев, неправильных технологических и организационных решений в процессах обработки, передачи и хранения информации и обеспечение нормального функционирования технологических процессов.

8. Наибольшими возможностями для нанесения ущерба Компании обладает собственный персонал. Действия персонала могут быть мотивированы злым умыслом (при этом злоумышленник может иметь сообщников как внутри, так и вне Компании), либо иметь непреднамеренный ошибочный характер.
9. На основе вероятностной оценки определяется перечень актуальных угроз безопасности, который отражается в «Модели угроз».
10. Для противодействия угрозам ИБ в Компании на основе имеющегося опыта составляется прогностическая модель предполагаемых угроз и модель нарушителя. Чем точнее сделан прогноз (составлены модель угроз и модель нарушителя), тем ниже риски нарушения ИБ при минимальных ресурсных затратах.
11. Разработанная на основе прогноза Политики информационной безопасности и в соответствии с ней построенная СУИБ является наиболее правильным и эффективным способом добиться минимизации рисков нарушения ИБ для Компании. Необходимо учитывать, что с течением времени меняется характер угроз, поэтому следует своевременно, используя данные мониторинга и аудита, обновлять модели угроз и нарушителя.
12. Стратегия обеспечения ИБ заключается в использовании заранее разработанных мер противодействия атакам злоумышленников, а также программно-технических и организационных решений, позволяющих свести к минимуму возможные потери от технических аварий и ошибочных действий персонала.
13. Задачами настоящей политики являются:
    1. описание организации СУИБ;
    2. определение порядка сопровождения ИС Компании.
14. Настоящая Политика вводится в действие приказом Генерального директора Компании и распространяется на все структурные подразделения Компании и обязательна для исполнения всеми его сотрудниками и должностными лицами. Положения настоящей Политики применимы для использования во внутренних нормативных и методических документах, а также в договорах.
15. Политика признается утратившей силу на основании приказа Генерального директора Компании.

3. Порядок внесения изменений

1. Изменения в Политику вносятся приказом Генерального директора Компании. Инициаторами внесения изменений в Политику информационной безопасности являются:
    1. Генеральный директор Компании;
    2. руководители подразделений Компании
    3. администратор информационной безопасности.
2. Плановая актуализация настоящей Политики производится ежегодно и имеет целью приведение в соответствие определенных политикой защитных мер реальным условиям и текущим требованиям к защите информации.
3. Внеплановая актуализация Политики информационной безопасности производится в обязательном порядке в следующих случаях:
    1. при изменении внутренних нормативных документов (инструкций, положений, руководств), касающихся ИБ Компании;
    2. при происшествии и выявлении инцидента (инцидентов) по нарушению ИБ, влекущего ущерб Компании.

4. Ответственность за актуализацию Политики информационной безопасности (плановую и внеплановую) и контроль за исполнением требований настоящей Политики возлагается на АИБа.

4. Политика информационной безопасности Компании

1. Политика информационной безопасности Компании — это совокупность норм, правил и практических рекомендаций, на которых строится управление, защита и распределение информации в Компании.
2. Политика информационной безопасности относятся к административным мерам обеспечения ИБ и определяют стратегию Компании в области ИБ.
3. Политика информационной безопасности регламентируют эффективную работу СЗИ. Они охватывают все особенности процесса обработки информации, определяя поведение ИС и ее пользователей в различных ситуациях. Политика ИБ реализуется посредством административно-организационных мер, физических и программно-технических средств и определяет архитектуру системы защиты.
4. Все документально оформленные решения, формирующие Политику, должны быть утверждены в Компании.
5. Основными принципами обеспечения ИБ являются следующие:
    1. постоянный и всесторонний анализ информационного пространства Компании с целью выявления уязвимостей информационных активов;
    2. своевременное обнаружение проблем, потенциально способных повлиять на ИБ , корректировка моделей угроз и нарушителя;
    3. разработка и внедрение защитных мер, адекватных характеру выявленных угроз, с учетом затрат на их реализацию. При этом меры, принимаемые для
    4. обеспечения ИБ, не должны усложнять достижение уставных целей Компании, а также повышать трудоемкость технологических процессов обработки информации;
    5. контроль эффективности принимаемых защитных мер;
    6. персонификация и адекватное разделение ролей и ответственности между сотрудниками Компании, исходя из принципа персональной и единоличной ответственности за совершаемые операции.
6. Правовую основу Политики составляют законы Российской Федерации и другие законодательные акты, определяющие права и ответственность граждан, сотрудников и государства в сфере безопасности, а также нормативные, отраслевые и ведомственные документы, по вопросам безопасности информации, утвержденные органами государственного управления различного уровня в пределах их компетенции.
7. Ответственность за реализацию Политики возлагается:
    1. в части, касающейся разработки и актуализации правил внешнего доступа -на АИБа;
    2. в части, касающейся контроля доведения правил Политики до сотрудников Компании, а также иных лиц (см. область действия настоящей Политики) — на АИБа;
    3. в части, касающейся исполнения правил Политики — на каждого сотрудника Компании, согласно их должностным и функциональным обязанностям, и иных лиц, подпадающих под область действия настоящей Политики.
8. Обучение сотрудников Компании в области ИБ проводится согласно плану, утвержденному Генеральным директором предприятия.
9. Подписи сотрудников об ознакомлении заносятся в «Журнал проведения инструктажа по информационной безопасности».
10. Допуск персонала к работе с защищаемыми ИР Компании осуществляется только после его ознакомления с настоящей Политикой, а также после

ознакомления пользователей с «Порядком работы пользователей» Компании, а также иными инструкциями пользователей отдельных ИС. Согласие на соблюдение правил и требований настоящей Политики подтверждается подписями сотрудников в журналах ознакомления.

11. Допуск персонала к работе с информацией Компании осуществляется после ознакомления с «Порядком организации работы с материальными носителями»,
12. «Порядком организации работы с электронными носителями». Правила допуска к работе с ИР лиц, не являющихся сотрудниками Компании, определяются на договорной основе с этими лицами или с организациями, представителями которых являются эти лица.
13. Настоящая Политика определяет основные правила присвоения учетных записей пользователям информационных активов Компании. Регистрационные учетные записи подразделяются на:
    1. пользовательские — предназначенные для идентификации/аутентификации пользователей информационных активов Компании;
    2. системные — используемые для нужд операционной системы;
    3. служебные — предназначенные для обеспечения функционирования отдельных процессов или приложений.
14. Каждому пользователю информационных активов Компании назначается уникальная пользовательская регистрационная учетная запись. Допускается привязка более одной пользовательской учетной записи к одному и тому же пользователю (например, имеющих различный уровень полномочий).
15. В общем случае запрещено создавать и использовать общую пользовательскую учетную запись для группы пользователей. В случаях, когда это необходимо, ввиду особенностей автоматизируемого бизнес-процесса или организации труда (например, посменное дежурство), использование общей учетной записи должно сопровождаться отметкой в журнале учета машинного времени, которая должна однозначно идентифицировать текущего владельца учетной записи в каждый момент времени. Одновременное использование одной общей пользовательской учетной записи разными пользователями запрещено.
16. Системные регистрационные учетные записи формируются операционной системой и должны использоваться только в случаях, предписанных документацией на операционную систему.
17. Служебные регистрационные учетные записи используются только для запуска сервисов или приложений.
18. Использование системных или служебных учетных записей для регистрации пользователей в системе категорически запрещено.
19. Настоящая Политика определяет основные правила парольной защиты на Компании. Положения Политики закрепляются в «Порядке по организации парольной защиты»
20. Настоящая Политика определяет основные правила и требования по защите информации Компании от неавторизованного доступа, утраты или модификации.
21. Положения данной Политики определяются в соответствии с используемым техническим решением.
22. Под профилактикой нарушений Политики информационной безопасности понимается проведение регламентных работ по защите информации, предупреждение возможных нарушений ИБ в Компании и проведение разъяснительной работы по ИБ среди пользователей.
23. Положения определены документами «Об обучении сотрудников правилам защиты информации» и «Порядком технического обслуживания средств вычислительной техники».
24. АИБ, используя данные, полученные в результате применения инструментальных средств контроля (мониторинга) безопасности

информации ИС, должен своевременно обнаруживать нарушения ИБ, факты осуществления НСД к защищаемым ИР и предпринимать меры по их локализации и устранению.

25. В случае обнаружения подсистемой защиты информации факта нарушения ИБ или осуществления НСД к защищаемым ИР, ИС рекомендуется уведомить АИБа, и далее следовать указаниям.
26. Действия АИБа и администратора информационной системы при признаках нарушения Политики информационной безопасности регламентируются следующими внутренними документами:
    1. регламентом пользователя;
    2. Политикой информационной безопасности;
    3. регламентом администратора информационной безопасности;
    4. регламентом системного администратора.
27. После устранения инцидента необходимо составить акт о факте нарушения и принятых мерах по восстановлению работоспособности ИС, а также зарегистрировать факт нарушения в журнале учета нарушений, ликвидации их причин и последствий.

5. Ответственность за нарушение Политики информационной безопасности

1. Ответственность за нарушение Политики информационной безопасности.
2. Ответственность за выполнение правил Политики информационной безопасности несет каждый сотрудник Компании в рамках своих служебных обязанностей и полномочий.
3. На основании ст. 192 Трудового кодекса Российской Федерации сотрудники, нарушающие требования Политики информационной безопасности Компании, могут быть подвергнуты дисциплинарным взысканиям, включая замечание, выговор и увольнение с работы.
4. Все сотрудники несут персональную (в том числе материальную) ответственность за прямой действительный ущерб, причиненный Компании в результате нарушения ими правил Политики информационной безопасности (Ст. 238 Трудового кодекса Российской Федерации).
5. За неправомерный доступ к компьютерной информации, создание, использование или распространение вредоносных программ, а также нарушение правил эксплуатации ЭВМ, следствием которых явилось нарушение работы ЭВМ (автоматизированной системы обработки информации), уничтожение, блокирование или модификация защищаемой информации, сотрудники Компании несут ответственность в соответствии со статьями 272, 273 и 274 Уголовного кодекса Российской Федерации.