Политика информационной безопасности ООО «Клин»

Утверждена приказом Генерального директора ООО «Клин» № 1337 от 15.09.2020 г.

Булгаков Алексей БАСО-02-20

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 «Клин».

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 на ООО “Клин” 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, 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.

2.1 Введение.

Политика информационной безопасности ООО «Клин» 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.

2.2 Цели.

Основными целями Политики информационной безопасности являются защита информации ООО «Клин» 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 ООО «Клин».

Общее руководство обеспечением ИБ осуществляется Генеральным директором ООО «Клин», Булгаковым Алексеем Алексеевичем. Ответственность за организацию мероприятий по обеспечению ИБ и контроль за соблюдением требований ИБ несет АИБ. Ответственность за функционирование информационных систем ООО «Клин» несет администратор информационной системы.

Должностные обязанности АИБа и системного администратора закрепляются в соответствующих инструкциях.

Руководители структурных подразделений ООО «Клин» несут ответственность за обеспечение выполнения требований ИБ в своих подразделениях.

Сотрудники ООО «Клин» обязаны соблюдать порядок обращения с конфиденциальными документами, носителями ключевой информации и другой защищаемой информацией, соблюдать требования настоящей Политики и других внутренних документов ООО «Клин» по вопросам обеспечения ИБ.

2.3 Задачи.

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.

Наибольшими возможностями для нанесения ущерба ООО «Клин» обладает собственный персонал. Действия персонала могут быть мотивированы злым умыслом (при этом злоумышленник может иметь сообщников как внутри, так и вне ООО «Клин»), либо иметь непреднамеренный ошибочный характер.

Для противодействия угрозам ИБ на ООО «Клин» 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.

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 ООО «Клин». Необходимо учитывать, что с течением времени меняется характер угроз, поэтому следует своевременно, используя данные мониторинга и аудита, обновлять модели угроз и нарушителя.

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.

Задачами настоящей политики являются:

- описание организации СУИБ;
- определение порядка сопровождения ИС ООО «Клин».

Настоящая Политика вводится в действие приказом Генерального директора ООО «Клин», Булгакова Алексея Алексеевича и распространяется на все структурные подразделения ООО «Клин» 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.

Политика признается утратившей силу на основании приказа Генерального директора ООО «Клин», Булгакова Алексея Алексеевича.

2.4 Порядок внесения изменений.

Изменения в Политику вносятся приказом Генерального директора ООО «Клин», Булгакова Алексея Алексеевича. Инициаторами внесения изменений в Политику информационной безопасности являются:

- Генеральный директор ООО «Клин», Булгаков Алексей Алексеевич;
- руководители подразделений (управлений, отделов, цехов и т. д.) ООО «Клин»;
- администратор информационной безопасности.

Плановая актуализация настоящей Политики производится ежегодно и имеет целью приведение в соответствие определенных политикой защитных мер реальным условиям и текущим требованиям к защите информации.

Внеплановая актуализация Политики информационной безопасности производится в обязательном порядке в следующих случаях:

- при изменении внутренних нормативных документов (инструкций, положений, руководств), касающихся ИБ ООО «Клин»;
- при происшествии и выявлении инцидента (инцидентов) по нарушению ИБ, влекущего ущерб ООО «Клин».

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

3. Политика информационной безопасности ООО «Клин».

3.1 Назначение Политики информационной безопасности.

Политика информационной безопасности ООО «Клин» — это совокупность норм, правил и практических рекомендаций, на которых строится управление, защита и распределение информации в ООО «Клин».

Политика информационной безопасности относятся к административным мерам обеспечения ИБ и определяют стратегию ООО «Клин» в области ИБ.

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.

Все документально оформленные решения, формирующие Политику, должны быть утверждены на ООО «Клин».

3.2 Основные принципы обеспечения информационной безопасности

Основными принципами обеспечения ИБ являются следующие:

- постоянный и всесторонний анализ информационного пространства ООО «Клин» с целью выявления уязвимостей информационных активов;
- своевременное обнаружение проблем, потенциально способных повлиять на ИБ ООО «Клин», корректировка моделей угроз и нарушителя;
- разработка и внедрение защитных мер, адекватных характеру выявленных угроз, с учетом затрат на их реализацию. При этом меры, принимаемые для
- обеспечения ИБ, не должны усложнять достижение уставных целей ООО «Клин», а также повышать трудоемкость технологических процессов обработки информации;
- контроль эффективности принимаемых защитных мер;
- персонификация и адекватное разделение ролей и ответственности между сотрудниками ООО «Клин», исходя из принципа персональной и единоличной ответственности за совершаемые операции.

3.3 Соответствие Политики информационной безопасности действующему законодательству

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.

3.4 Ответственность за реализацию Политики информационной безопасности

Ответственность за разработку мер обеспечения защиты информации несёт АИБ.

Ответственность за реализацию Политики возлагается:

- в части, касающейся разработки и актуализации правил внешнего доступа -на АИБа;
- в части, касающейся контроля доведения правил Политики до сотрудников ООО «Клин», а также иных лиц (см. область действия настоящей Политики) — на АИБа;

- в части, касающейся исполнения правил Политики — на каждого сотрудника ООО «Клин», согласно их должностным и функциональным обязанностям, и иных лиц, попадающих под область действия настоящей Политики.

3.5 Порядок подготовки персонала по вопросам информационной безопасности и допуска его к работе.

- Обучение сотрудников ООО «Клин» в области ИБ проводится согласно плану, утвержденному Генеральным директором предприятия.
- Подписи сотрудников об ознакомлении заносятся в «Журнал проведения инструктажа по информационной безопасности».
- Допуск персонала к работе с защищаемыми ИР ООО «Клин» осуществляется только после его ознакомления с настоящей Политикой, а также после ознакомления пользователей с «Порядком работы пользователей» ООО «Клин», а также иными инструкциями пользователей отдельных ИС. Согласие на соблюдение правил и требований настоящей Политики подтверждается подписями сотрудников в журналах ознакомления.
- Допуск персонала к работе с информацией ООО «Клин» осуществляется после ознакомления с «Порядком организации работы с материальными носителями»,
- «Порядком организации работы с электронными носителями». Правила допуска к работе с ИР лиц, не являющихся сотрудниками ООО «Клин», определяются на договорной основе с этими лицами или с организациями, представителями которых являются эти лица.

3.6 Учетные записи.

Настоящая Политика определяет основные правила присвоения учетных записей пользователям информационных активов ООО «Клин». Регистрационные учетные записи подразделяются на:

- пользовательские — предназначенные для идентификации/аутентификации пользователей информационных активов ООО «Клин»;
- системные — используемые для нужд операционной системы;
- служебные — предназначенные для обеспечения функционирования отдельных процессов или приложений.
- Каждому пользователю информационных активов ООО «Клин» назначается уникальная пользовательская регистрационная учетная запись. Допускается привязка более одной пользовательской учетной записи к одному и тому же пользователю (например, имеющих различный уровень полномочий).
- 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.

- Системные регистрационные учетные записи формируются операционной системой и должны использоваться только в случаях, предписанных документацией на операционную систему.
- Служебные регистрационные учетные записи используются только для запуска сервисов или приложений.
- Использование системных или служебных учетных записей для регистрации пользователей в системе категорически запрещено.

3.7 Использование паролей.

Настоящая Политика определяет основные правила парольной защиты на ООО «Клин». Положения Политики закрепляются в «Порядке по организации парольной защиты»

3.8 Защита автоматизированного рабочего места.

- Настоящая Политика определяет основные правила и требования по защите информации ООО «Клин» от неавторизованного доступа, утраты или модификации.
- Положения данной Политики определяются в соответствии с используемым техническим решением.

4. Профилактика нарушений Политики информационной безопасности.

- Под профилактикой нарушений Политики информационной безопасности понимается проведение регламентных работ по защите информации, предупреждение возможных нарушений ИБ на ООО «Клин» и проведение разъяснительной работы по ИБ среди пользователей.
- Положения определены документами «Об обучении сотрудников правилам защиты информации» и «Порядком технического обслуживания средств вычислительной техники».

4.1 Ликвидация последствий нарушения Политики информационной безопасности.

- 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.
- В случае обнаружения подсистемой защиты информации факта нарушения ИБ или осуществления НСД к защищаемым ИР, ИС рекомендуется уведомить АИБа, и далее следовать указаниям.
- Действия АИБа и администратора информационной системы при признаках нарушения Политики информационной безопасности регламентируются следующими внутренними документами:

- регламентом пользователя;
- Политикой информационной безопасности;
- регламентом администратора информационной безопасности;
- регламентом системного администратора.
- 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.

4.2 Ответственность за нарушение Политики информационной безопасности.

- Ответственность за выполнение правил Политики информационной безопасности несет каждый сотрудник ООО «Клин» в рамках своих служебных обязанностей и полномочий.
- На основании ст. 192 Трудового кодекса Российской Федерации сотрудники, нарушающие требования Политики информационной безопасности ООО «Клин», могут быть подвергнуты дисциплинарным взысканиям, включая замечание, выговор и увольнение с работы.
- Все сотрудники несут персональную (в том числе материальную) ответственность за прямой действительный ущерб, причиненный ООО «Клин» в результате нарушения ими правил Политики информационной безопасности (Ст. 238 Трудового кодекса Российской Федерации).
- 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 ООО «Клин» несут ответственность в соответствии со статьями 272, 273 и 274 Уголовного кодекса Российской Федерации.