УТВЕРЖДЕНО

Приказом директора

№ от « » 20 г.

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БК «СТД»

Москва 2019 г.

СОДЕРЖАНИЕ

1. Перечень используемых определений, обозначений и сокращений.

2. Вводные положения.

##### 2.1 Введение.

##### 2.2 Цели.

##### 2.3 Задачи.

### 3. Политика информационной безопасности БК «СТД».

##### 3.1 Назначение Политики информационной безопасности.

##### 3.2 Основные принципы обеспечения информационной безопасности.

##### 3.3 Соответствие Политики информационной безопасности действующему законодательству.

##### 3.4 Ответственность за реализацию Политики информационной безопасности.

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

##### 3.6 Учетные записи.

##### 3.7 Использование паролей.

##### 3.8 Защита автоматизированного рабочего места.

### 4. Профилактика нарушений Политики информационной безопасности.

##### 4.1 Ликвидация последствий нарушения Политики информационной безопасности.

4.2 Ответственность за нарушение Политики информационной безопасности.

### 4.3. Неформальная модель возможных нарушителей.

### 5. Меры обеспечения информационной безопасности.

### 6. Техническая концепция в области обеспечения безопасности информации.

7. Заключительные положения.

1. Перечень используемых определений, обозначений и сокращений.

ИБ — Информационная безопасность.

СЗИ — Средство защиты информации.

СУИБ — Система управления информационной безопасностью.

ЭВМ — Электронная — вычислительная машина, персональный компьютер.

БК - Букмекерская контора.

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 несанкционированного доступа 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 Букмекерской Конторы “Сегодня Твой День” (далее — БК «СТД»).

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 БК «СТД» 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 БК «СТД» 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 БК «СТД» от возможного нанесения материального, физического, морального или иного ущерба, посредством случайного или преднамеренного воздействия на информацию, ее носители, процессы обработки и передачи, а так же обеспечение эффективной работы всего информационно-вычислительного комплекса при осуществлении деятельности, указанной в Положении о деятельности БК «СТД».

Общее руководство обеспечением ИБ осуществляется Генеральным директором БК «СТД». Ответственность за организацию мероприятий по обеспечению ИБ и контроль за соблюдением требований ИБ несет администратор ИБ. Ответственность за функционирование информационных систем БК «СТД» несет администратор информационной системы.

Должностные обязанности администратора ИБ и системного администратора закрепляются в соответствующих инструкциях.

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

Сотрудники БК «СТД» обязаны соблюдать порядок обращения с конфиденциальными документами, носителями ключевой информации и другой защищаемой информацией, соблюдать требования настоящей Политики и других внутренних документов БК «СТД» 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 БК «СТД» обладает собственный персонал. Действия персонала могут быть мотивированы злым умыслом (при этом злоумышленник может иметь сообщников как внутри, так и вне БК «СТД»), либо иметь непреднамеренный ошибочный характер.

На основе вероятностной оценки определяется перечень актуальных угроз безопасности, который отражается в «Модели угроз».

Для противодействия угрозам ИБ на БК «СТД» 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 БК «СТД». 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 информационной системы БК «СТД».

Настоящая Политика вводится в действие Приказом Генерального директора БК «СТД»

и распространяется на все структурные подразделения БК «СТД» 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 БК «СТД».

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

### 3. Политика информационной безопасности БК «СТД».

##### 3.1 Назначение Политики информационной безопасности.

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

Политика информационной безопасности относятся к административным мерам обеспечения ИБ и определяют стратегию БК «СТД» 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 БК «СТД».

##### 3.2 Основные принципы обеспечения информационной безопасности.

Основными принципами обеспечения ИБ являются следующие:

* постоянный и всесторонний анализ информационного пространства БК «СТД» с целью выявления уязвимостей информационных активов;
* своевременное обнаружение проблем, потенциально способных повлиять на ИБ БК «СТД», 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 БК «СТД», а также повышать трудоемкость технологических процессов обработки информации;
* контроль эффективности принимаемых защитных мер;
* персонификация и адекватное разделение ролей и ответственности между сотрудниками БК «СТД», 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 администратор ИБ.

Ответственность за реализацию Политики возлагается:

* в части, касающейся разработки и актуализации правил внешнего доступа - на администратора ИБ;
* в части, касающейся контроля доведения правил Политики до сотрудников БК «СТД», а также иных лиц (см. область действия настоящей Политики) - на администратора ИБ;
* в части, касающейся исполнения правил Политики — на каждого сотрудника БК «СТД», 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 БК «СТД» 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 информационными ресурсами БК «СТД» осуществляется только после его ознакомления с настоящей Политикой, а также после ознакомления пользователей с «Порядком работы пользователей» БК «СТД», а также иными инструкциями пользователей отдельных информационных систем. Согласие на соблюдение правил и требований настоящей Политики подтверждается подписями сотрудников в журналах ознакомления.
* Допуск персонала к работе с информацией БК «СТД» осуществляется после ознакомления с «Порядком организации работы с материальными носителями»,
* «Порядком организации работы с электронными носителями». Правила допуска к работе с информационными ресурсами лиц, не являющихся сотрудниками БК «СТД», 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 БК «СТД». Регистрационные учетные записи подразделяются на:

* пользовательские — предназначенные для идентификации/аутентификации пользователей информационных активов БК «СТД»;
* системные — используемые для нужд операционной системы;
* служебные — предназначенные для обеспечения функционирования отдельных процессов или приложений.
* Каждому пользователю информационных активов БК «СТД» 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 БК «СТД». 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 БК «СТД» 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 БК «СТД» 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.

* Администратор ИБ, используя данные, полученные в результате применения инструментальных средств контроля (мониторинга) безопасности информации информационных систем, должен своевременно обнаруживать нарушения ИБ, факты осуществления несанкционированного доступа к защищаемым ИР и предпринимать меры по их локализации и устранению.
* В случае обнаружения подсистемой защиты информации факта нарушения ИБ или осуществления несанкционированного доступа к защищаемым информационным ресурсам, информационным системам рекомендуется уведомить администратора ИБ, и далее следовать указаниям.
* Действия администратора ИБ 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 информационных систем, 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 БК «СТД» в рамках своих служебных обязанностей и полномочий.
* На основании ст. 192 Трудового кодекса Российской Федерации сотрудники, нарушающие требования Политики информационной безопасности БК «СТД», 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 БК «СТД» 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 БК «СТД» несут ответственность в соответствии со статьями 272, 273 и 274 Уголовного кодекса Российской Федерации.

### 4.3. Неформальная модель возможных нарушителей.

Нарушитель - это лицо, которое предприняло попытку выполнения запрещенных операций (действий) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради игры или удовольствия, с целью самоутверждения и т.п.) и использующее для этого различные возможности, методы и средства.

Злоумышленник - нарушитель, действующий намеренно из корыстных, идейных или иных побуждений;

Система обеспечения информационной безопасности БК «СТД» должна строиться исходя из предположений о следующих возможных типах нарушителей в системе (с учетом категории лиц, мотивации, квалификации, наличия специальных средств и др.):

* Некомпетентный (невнимательный) пользователь - сотрудник БК «СТД» (или подразделения другой организации, являющийся легальным пользователем информационной системы БК «СТД»), который может предпринимать попытки выполнения запрещенных действий, доступа к защищаемым ресурсам информационной системы с превышением своих полномочий, ввода некорректных данных, нарушения правил и регламентов работы с информацией и т.п., действуя по ошибке, некомпетентности или халатности без злого умысла и использующий при этом только штатные (предоставленные) средства.
* Любитель - сотрудник БК «СТД» (или подразделения другого организации, являющийся зарегистрированным пользователем информационной системы БК «СТД»), пытающийся нарушить систему защиты без корыстных целей или злого умысла или для самоутверждения. Для преодоления системы защиты и совершения запрещенных действий он может использовать различные методы получения дополнительных полномочий доступа к ресурсам, недостатки в построении системы защиты и доступные ему штатные средства (несанкционированные действия посредством превышения своих полномочий на использование разрешенных средств). Помимо этого он может пытаться использовать дополнительно нештатные инструментальные и технологические программные средства, самостоятельно разработанные программы или стандартные дополнительные технические средства.
* Внутренний злоумышленник - сотрудник БК «СТД» (или подразделения другого ведомства, зарегистрированный как пользователь системы), действующий целенаправленно из корыстных интересов или мести за нанесенную обиду, возможно в сговоре с лицами, не являющимися сотрудниками БК «СТД». Он может использовать весь набор методов и средств взлома системы защиты, включая агентурные методы, пассивные средства (технические средства перехвата), методы и средства активного воздействия (модификация технических средств, подключение к каналам передачи данных, внедрение программных закладок и использование специальных инструментальных и технологических программ), а также комбинации воздействий, как изнутри, так и извне БК «СТД».
* Внешний злоумышленник - постороннее лицо, действующее целенаправленно из корыстных интересов, мести или из любопытства, возможно в сговоре с другими лицами. Он может использовать весь набор методов и средств взлома системы защиты, включая агентурные методы, пассивные средства (технические средства перехвата), методы и средства активного воздействия (модификация технических средств, подключение к каналам передачи данных, внедрение программных закладок и использование специальных инструментальных и технологических программ), а также комбинации воздействий, как изнутри, так и извне БК «СТД».

Внутренним нарушителем может быть лицо из следующих категорий сотрудников БК «СТД»:

* зарегистрированные пользователи информационной системы БК «СТД»;
* сотрудники БК «СТД», не являющиеся зарегистрированными пользователями и не допущенные к ресурсам информационной системы БК «СТД», но имеющие доступ в здания и помещения;
* персонал, обслуживающий технические средства корпоративной информационной системы БК «СТД»;
* сотрудники подразделений БК «СТД», задействованные в разработке и сопровождении программного обеспечения;
* сотрудники подразделений обеспечения безопасности БК «СТД»;
* руководители различных уровней.

Категории лиц, которые могут быть внешними нарушителями:

* уволенные сотрудники БК «СТД»;
* представители организаций, взаимодействующих по вопросам технического обеспечения БК «СТД»;
* клиенты БК «СТД»;
* посетители (представители фирм, поставляющих технику, программное обеспечение, услуги и т.п.);
* представители конкурирующих организаций;
* члены преступных организаций, сотрудники спецслужб или лица, действующие по их заданию;
* лица, случайно или умышленно проникшие в корпоративную информационную систему БК «СТД» из внешних телекоммуникационных сетей (хакеры).

### 5. Меры обеспечения информационной безопасности

Все меры обеспечения безопасности информационной системы БК «СТД» подразделяются на:

* правовые (законодательные);
* морально-этические;
* технологические;
* организационные (административные);
* физические;
* технические (аппаратурные и программные).

**Законодательные (правовые) меры защиты**

К правовым мерам защиты относятся действующие в стране законы, указы и нормативные акты, регламентирующие правила обращения с информацией, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения этих правил. Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом информационной системы БК «СТД».

**Морально-этические меры защиты**

К морально-этическим мерам относятся нормы поведения, которые традиционно сложились или складываются по мере распространения информационных технологий в обществе. Эти нормы большей частью не являются обязательными, как законодательно утвержденные нормативные акты, однако, их несоблюдение может привести к падению авторитета, престижа человека, группы лиц или БК «СТД» в целом. Морально-этические нормы бывают как неписаные, так и писаные, то есть оформленные в некоторый свод (устав) правил или предписаний. Морально-этические меры защиты являются профилактическими и требуют постоянной работы по созданию здорового морального климата в коллективах подразделений.

**Технологические меры защиты**

К данному виду мер защиты относятся разного рода технологические решения и приемы, основанные на использовании некоторых видов избыточности (структурной, функциональной, информационной, временной и т.п.) и направленные на уменьшение возможности совершения сотрудниками ошибок и нарушений в рамках предоставленных им прав и полномочий. Примером таких мер является использование процедур двойного ввода ответственной информации, инициализации ответственных операций только при наличии согласования нескольких лиц, процедур проверки реквизитов исходящих и входящих сообщений, периодическое подведение общего баланса всех счетов и т.п.

**Организационные (административные) меры защиты**

Организационные (административные) меры защиты - это меры организационного характера, регламентирующие процессы функционирования системы обработки данных, использование ее ресурсов, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации.

### 6. Техническая концепция в области обеспечения безопасности информации.

Реализация технической концепции в области обеспечения безопасности информации должна исходить из предпосылки, что невозможно обеспечить требуемый уровень защищенности информации не только с помощью одного отдельного средства (мероприятия), но и с помощью их простой совокупности. Необходимо их системное согласование между собой (комплексное применение), а отдельные разрабатываемые элементы информационной системы должны рассматриваться как часть единой информационной системы в защищенном исполнении при оптимальном соотношении технических (аппаратных, программных) средств и организационных мероприятий.

Основными направлениями реализации технической концепции обеспечения безопасности информации БК «СТД» являются:

* обеспечение защиты информационных ресурсов от хищения, утраты, утечки, уничтожения, искажения или подделки за счет несанкционированного доступа и специальных воздействий;
* обеспечение защиты информации от утечки по техническим каналам при ее обработке, хранении и при передаче по каналам связи.

Система обеспечения безопасности информации БК «СТД» должна предусматривать комплекс организационных, программных и технических средств и мер по защите информации в процессе ее обработки и хранения, при передаче информации по каналам связи, при ведении конфиденциальных переговоров, раскрывающих сведения с ограниченным доступом, при использовании технических и программных средств.

В рамках указанных направлений технической концепции обеспечения безопасности информации осуществляются:

* реализация разрешительной системы допуска исполнителей (пользователей, обслуживающего персонала) к работам, документам и информации; реализация системы инженерно-технических и организационных мер охраны, предусматривающей многорубежность и равнопрочность построения охраны (территории, здания, помещения) с комплексным применением современных технических средств охраны, обнаружения, наблюдения, сбора и обработки информации, обеспечивающих достоверное отображение и объективное документирование событий;
* ограничение доступа в здания и помещения, где проводятся работы конфиденциального характера и размещены средства информатизации и коммуникации, на которых обрабатывается (хранится, передается) информация, а также непосредственно к самим средствам информатизации и коммуникациям;
* разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защита информации в информационной системе БК «СТД»;
* учет документов, информационных массивов, регистрация действий пользователей и обслуживающего персонала, контроль за несанкционированным доступом и действиями пользователей, обслуживающего персонала и посторонних лиц;
* предотвращение внедрения в корпоративную информационную систему БК «СТД» программ-вирусов, программных закладок.
* реализация инфраструктуры с открытым ключом, криптографическая защита информации ограниченного пользования, обрабатываемой и передаваемой средствами вычислительной техники по открытым каналам связи;
* надежное хранение документов и машинных носителей информации, ключей (ключевой документации) и их обращение, исключающее хищение, подмену и уничтожение;
* необходимое резервирование технических средств и дублирование массивов и носителей информации;
* обеспечение акустической защиты помещений, в которых обсуждается информация конфиденциального характера;
* противодействие оптическим и лазерным средствам наблюдения.

7. Заключительные положения.

Требования настоящей Политики могут развиваться другими внутренними нормативными документами БК «СТД», которые дополняют и уточняют ее.

В случае изменения действующего законодательства и иных нормативных актов настоящая Политика и изменения к ней применяются в части, не противоречащей вновь принятым законодательным и иным нормативным актам. В этом случае Ответственное подразделение обязано незамедлительно инициировать внесение соответствующих изменений.

Внесение изменений в настоящую Политику осуществляется на периодической и внеплановой основе:

* периодическое внесение изменений в настоящую Политику должно осуществляться не реже одного раза в 24 месяца;
* внеплановое внесение изменений в настоящую Политику может производиться по результатам анализа инцидентов информационной безопасности, актуальности, достаточности и эффективности используемых мер обеспечения информационной безопасности, результатам проведения внутренних аудитов информационной безопасности и других контрольных мероприятий.

Ответственным за внесение изменений в настоящую Политику является руководитель Ответственного подразделения.