Политика информационной безопасности (далее - Политика) является частью системы управления информационной безопасности (СУИБ) ЗАО «ДЖИЭНСИ-АЛЬФА» (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 и в других нормативных документах по обеспечению ИБ.

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 и управления рисками Компании;
- Политикой обработки персональных данных в Компании;
- ISO/IEC 27001:2022; Информационная безопасность, кибербезопасность и защита персональных данных; Система менеджмента информационной безопасности; Требования
- Требованиям стандарта PCI DSS 4.0

Настоящая Политика является корпоративным документом по информационной безопасности первого уровня.

Документами, детализирующими положения корпоративной Политики применительно к одной или нескольким областям информационной безопасности, видам и технологиям деятельности Компании, являются Политика обработки персональных данных, Политика и Руководство по СУИБ, а также регламенты, которые являются документами по информационной безопасности второго уровня, оформляются как отдельные внутренние нормативные документы Компании, разрабатываются, согласовываются и утверждаются в соответствии с установленным в Компании порядком.

1. ОБЩИЕ ПОЛОЖЕНИЯ

Политика разработана с целью определения основных принципов и направлений в области информационной безопасности, кибербезопасности и охватывает все бизнес-процессы, информационные системы и документы, владельцем и пользователем которых является Компания.

Целью деятельности по управлению информационной безопасностью и кибербезопасностью в Компании является защита субъектов информационных отношений от возможного нанесения им ощутимого материального, физического, морального или иного ущерба посредством случайного или преднамеренного несанкционированного вмешательства в процесс функционирования информационной системы или несанкционированного доступа к циркулирующей в Компании (в ее системах) информации и её незаконного использования.

Основными объектами защиты системы информационной безопасности в Компании являются:

- информационные ресурсы, содержащие коммерческую тайну, конфиденциальную информацию, включая персональные данные физических лиц, сведения ограниченного распространения, а также открыто распространяемая информация, необходимая для работы Компании, независимо от формы и вида ее представления;
- работники Компании, являющиеся пользователями информационных активов и систем Компании;
- специальные контролируемые зоны, к которым относятся следующие группы ресурсов: основные информационные серверы и средства вычислительной техники, на которых осуществляется обработка и хранение информации ограниченного распространения; сетевое оборудование и серверы, обеспечивающие работу критических систем; файловые серверы, на которых хранятся данные, в том числе резервные; критичные для деятельности Компании системы и коммуникационное оборудование, обеспечивающее

внешние коммуникации; системы и средства защиты информации, объекты и помещения, в которых размещены такие системы;

- вверенные Компании информационные активы Заказчиков и Партнеров;
- вверенные Компании персональные данные.

Задачами деятельности по управлению информационной безопасностью в Компании являются:

- категорирование информационных активов путем разделения их на критичные и некритичные на основании максимального уровня критичности, хранимой и обрабатываемой в них информации;
- своевременное выявление потенциальных угроз информационной безопасности и уязвимостей в информационных активах Компании;
- исключение либо минимизация выявленных угроз;
- предотвращение инцидентов информационной безопасности или минимизация их последствий.

Основными мерами защиты конфиденциальности, целостности и доступности информационных активов Компании являются:

- управление сетевой безопасностью;
- управление уязвимостями и политиками безопасности;
- управление безопасностью конечных устройств;
- управление идентификацией и доступом;
- управление инцидентами информационной безопасности;
- управление криптографическими средствами защиты;
- управление антивирусными средствами защиты;
- обеспечение физической безопасности информационных активов;
- обеспечение безопасности при взаимодействии с контрагентами;
- обучение и повышение осведомленности персонала в вопросах ИБ;
- обеспечение безопасности интернет-ресурсов.

Поставленные основные цели защиты и решение перечисленных выше задач достигаются:

- строгим учетом всех подлежащих защите информационных активов
- регламентацией процессов обработки подлежащей защите информации, с применением средств автоматизации и действий работников структурных подразделений Компании, использующих, а также действий персонала, осуществляющего обслуживание и модификацию программных и технических средств Компании, на основе утвержденных генеральным директором Компании организационно-распорядительных документов по вопросам обеспечения информационной безопасности;
- полнотой, реальной выполнимостью и непротиворечивостью требований организационно-распорядительных документов Компании по вопросам обеспечения информационной безопасности;
- назначением и подготовкой должностных лиц (работников), ответственных за организацию и осуществление практических мероприятий по обеспечению информационной безопасности и процессов её обработки;
- наделением каждого пользователя информационного актива Компании минимально необходимыми для выполнения им своих функциональных обязанностей полномочиями по доступу;
- четким знанием и строгим соблюдением всеми работниками, использующими и обслуживающими аппаратные и программные средства Компании, требований организационно-распорядительных документов по вопросам обеспечения информационной безопасности;
- персональной ответственностью за свои действия каждого работника, участвующего в рамках своих функциональных обязанностей, в процессах обработки информации и имеющего доступ к информационным активам Компании;
- реализацией технологических процессов обработки информации с использованием комплексов организационно-технических мер защиты программного обеспечения, технических средств и данных;
- принятием эффективных мер обеспечения физической целостности технических средств и непрерывным поддержанием необходимого уровня защищенности информационных активов Компании;
- применением физических и технических (программно-аппаратных) средств защиты активов

Компании;

- разграничением потоков информации различного уровня конфиденциальности, а также запрещением передачи информации ограниченного распространения по незащищенным каналам связи;
- эффективным контролем соблюдения работниками подразделений Компании требований по обеспечению информационной и безопасности;
- юридической защитой интересов Компании при взаимодействии его подразделений с внешними организациями (связанном с обменом информацией) от противоправных действий, как со стороны этих организаций, так и от несанкционированных действий обслуживающего персонала и третьих лиц;
- проведением постоянного анализа эффективности и достаточности принятых мер и применяемых средств защиты информации, разработкой и реализацией предложений по совершенствованию системы защиты информационных активов Компании.

2. ПРИНЦИПЫ И 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.

Ориентированность на бизнес. Информационная безопасность рассматривается как процесс поддержки бизнес-процессов в Компании. Любые меры по обеспечению информационной безопасности не должны повлечь за собой серьезных препятствий деятельности 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 информационной системы. 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, сотрудников и контрагентах. Компания должна обладать необходимой для обеспечения ИБ информацией о своих клиентов, сотрудников и контрагентах. 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, учёности 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 информационных систем.

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.

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.

Обоснованность и экономическая целесообразность. Используемые возможности и средства защиты должны быть реализованы на соответствующем уровне развития науки и техники, обоснованы с точки зрения заданного уровня безопасности и должны соответствовать предъявляемым требованиям и нормам, нужно учитывать соотношение между величиной затрат на их реализацию и возможным ущербом от реализации угроз;

3. ОРГАНИЗАЦИЯ ДЕЯТЕЛЬНОСТИ ПО ОБЕСПЕЧЕНИЮ ИБ

Компания обеспечивает создание и функционирование системы управления информационной безопасностью, являющейся частью общей системы управления Компании, предназначенной для управления процессом обеспечения информационной безопасности.

Компания разрабатывает внутренние процедуры по созданию, сбору, хранению и обработке информации в информационных системах Компании. Компания осуществляет мониторинг за процессами создания, хранения и обработки информации и доступа к ней с помощью механизмов информационных систем и технических средств обеспечения безопасности. Доступ к создаваемой, хранимой и обрабатываемой информации в информационных системах Компании предоставляется работникам в соответствии с их функциональными обязанностями в соответствии с принципом наименьшего уровня привилегий.

Участниками системы управления информационной безопасностью Компании являются:

1) Менеджмент;
2) совет по информационной безопасности;
3) подразделение информационной безопасности;
4) подразделение по информационным технологиям;
5) подразделение по безопасности;

6) подразделение по работе с персоналом;
7) подразделение правового сопровождения Компании;
8) подразделение внутреннего аудита;

Менеджмент утверждает перечень защищаемой информации, включающий в том числе информацию о сведениях, составляющих служебную, коммерческую или иную охраняемую законом тайну (далее – защищаемая информация), и порядок работы с защищаемой информацией. Так же утверждает внутренние документы, регламентирующие процесс управления информационной безопасностью, порядок и периодичность пересмотра.

Компания создаёт Совет по информационной безопасности, в состав которого входят представители подразделения по информационной безопасности, подразделения по информационным технологиям, а также при необходимости представители других подразделений Компании. Руководителем Совета по информационной безопасности назначается генеральный директор компании, либо первый заместитель генерального директора, курирующий деятельность подразделения по информационной безопасности.

Совет по информационной безопасности осуществляет периодический мониторинг деятельности по обеспечению информационной безопасности и мероприятий по выявлению и анализу угроз, противодействию атакам и расследованию инцидентов информационной безопасности не реже раза в год. Процесс мониторинга деятельности по обеспечению информационной безопасности, мероприятий по выявлению и анализу угроз, а также противодействию атакам должен включать отчёт по выявлению, анализу угроз и противодействию атакам на основе данных, предоставленных подразделением информационной безопасности по количеству выявленных угроз, принятых мер и произошедших инцидентов информационной безопасности. Мониторинг мероприятий по расследованию инцидентов информационной безопасности включает в себя оценку последствий инцидентов, указание причин и планов мероприятий по предотвращению, либо уменьшению влияния инцидентов информационной безопасности.

Генеральный директор осуществляет стратегическое планирование, координацию деятельности всех подразделений Компании для организации и поддержания соответствующего уровня информационной безопасности.

Руководитель подразделения информационной безопасности обеспечивает разработку, внедрение и совершенствование документированных стандартов и процедур в области информационной безопасности и управлению рисками информационной безопасности.

Подразделение информационной безопасности обеспечивает своевременное проведение анализа информации об инцидентах информационной безопасности, который должен включать в себя раскрытие обстоятельств события, при которых стала возможна реализация инцидента информационной безопасности, при необходимости, формирует рекомендаций по внедрению защитных мер. Подразделение отвечает за осуществление категорирования информационных активов путем разделения их на критичные и некритичные на основании максимального уровня критичности хранимой и обрабатываемой в них информации.

Подразделение по информационным технологиям обеспечивает исполнение установленных требований по непрерывности функционирования информационной инфраструктуры, конфиденциальности, целостности и доступности данных информационных систем Компании (включая резервирование и (или) архивирование и резервное копирование информации) в соответствии с внутренними нормативными документами Компании, а также обеспечивает соблюдение требований информационной безопасности при выборе, внедрении, разработке и тестировании информационных систем.

Подразделение по безопасности реализует меры физической и технической безопасности, в том числе организует пропускной и внутриобъектовый режим, а также проводит профилактические мероприятия, направленные на минимизацию рисков возникновения угроз информационной безопасности при приеме на работу и увольнении работников Компании.

Подразделение по работе с персоналом обеспечивает подписание работниками Компании, а также

лицами, привлеченными к работе по договору об оказании услуг, стажерами, практикантами обязательств о неразглашении конфиденциальной информации и согласие об обработке персональных данных, а также участвует в организации процесса повышения осведомленности работников Компании в области информационной безопасности.

Юридическое подразделение осуществляет правовую экспертизу внутренних нормативных документов и внутренних документов Компании по вопросам обеспечения информационной безопасности.

Подразделение внутреннего аудита проводит оценку состояния системы управления информационной безопасностью Компании при проведении аудиторских проверок.

Бизнес-владельцы информационных систем или подсистем отвечают за соблюдение требований к информационной безопасности при создании, внедрении, модификации, предоставлении клиентам продуктов и услуг, а также формируют и поддерживают актуальность матриц доступа к информационным системам.

Руководители структурных подразделений Компании обеспечивают ознакомление работников с внутренними нормативными документами Компании, содержащими требования к информационной безопасности, а также отвечают за обеспечение в подчиненных подразделениях выполнения требований информационной безопасности внедрение мер защиты при разработке новых продуктов, услуг, бизнес-приложений, бизнес-процессов и технологий.

4. МЕНЕДЖМЕНТ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Для обеспечения и результативного управления информационной безопасностью Компания обеспечивает менеджмент рисков информационной безопасности, включающий:

- анализ влияния на информационную безопасность Компании применяемых в деятельности Компании технологий, а также внешних по отношению к Компании событий;
- выявление проблем обеспечения информационной безопасности, анализ причин их возникновения и прогнозирование их развития;
- определение моделей угроз информационной безопасности;
- выявление, анализ и оценка значимых для Компании угроз информационной безопасности;
- выявление возможных негативных последствий для Компании, наступающих в результате проявления факторов риска информационной безопасности, в том числе связанных с нарушением свойств безопасности информационных активов Компании;
- идентификацию и анализ рисковых событий информационной безопасности;
- оценку величины рисков информационной безопасности и определение среди них рисков, неприемлемых для Компании;
- обработку результатов оценки рисков информационной безопасности, базирующейся на методах управления операционными рисками;
- оптимизацию рисков информационной безопасности за счет выбора и применения защитных мер, противодействующих проявлениям факторов риска и минимизирующих возможные негативные последствия для Компании в случае наступления рисковых событий;
- оценку влияния защитных мер на цели основной деятельности Компании;
- оценку затрат на реализацию защитных мер;
- рассмотрение и оценку различных вариантов решения задач по обеспечению информационной безопасности;
- разработку планов управления рисками, предусматривающих различные защитные меры и варианты их применения, и выбор из них такого, реализация которого максимально положительно скажется на целях основной деятельности Компании и будет оптимальна с точки зрения произведенных затрат и ожидаемого эффекта;

5. УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Все множество потенциальных угроз безопасности информации делится на три класса по природе их возникновения: антропогенные, техногенные и естественные (природные).

Возникновение антропогенных угроз обусловлено деятельностью человека. Среди них можно выделить угрозы, возникающие вследствие как непреднамеренных (неумышленных) действий: угрозы, вызванные ошибками в проектировании информационной системы и ее элементов, ошибками в действиях персонала и т.п., так и угрозы, возникающие в силу умышленных действий, связанные с корыстными, идейными или иными устремлениями людей.

Возникновение техногенных угроз обусловлено воздействиями на объект угрозы объективных физических процессов техногенного характера, технического состояния окружения объекта угрозы или его самого, не обусловленных напрямую деятельностью человека.

К техногенным угрозам могут быть отнесены сбои, в том числе в работе, или разрушение систем, созданных человеком.

Возникновение естественных (природных) угроз обусловлено воздействиями на объект угрозы объективных физических процессов природного характера, стихийных природных явлений, состояний физической среды, не обусловленных напрямую деятельностью человека.

К естественным (природным) угрозам относятся угрозы метеорологические, атмосферные, геофизические, геомагнитные и пр., включая экстремальные климатические условия, метеорологические явления, стихийные бедствия.

Источники угроз по отношению к инфраструктуре Компании могут быть как внешними, так и внутренними.

6. НЕФОРМАЛЬНАЯ МОДЕЛЬ ВОЗМОЖНЫХ НАРУШИТЕЛЕЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

По отношению к Компании нарушители могут быть разделены на внешних и внутренних 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.

Система защиты информационных активов Компании строиться исходя из предположений о следующих возможных типах нарушителей (с учетом категории лиц, мотивации, квалификации, наличия специальных средств и др.):

«Неопытный (невнимательный) работник» — работник Компании (или другой организации, зарегистрированный как пользователь в информационных системах компании), который может предпринимать попытки выполнения запрещенных операций, доступа к защищаемым ресурсам Компании с превышением своих полномочий, ввода некорректных данных и т.п. действия по ошибке, некомпетентности или халатности без злого умысла и использующий при этом только штатные (доступные ему) аппаратные и программные средства.

«Любитель» — работник Компании (или другой организации, зарегистрированный как пользователь в информационных системах компании), пытающийся преодолеть систему защиты без корыстных целей и злого умысла, для самоутверждения или из «спортивного интереса». Для преодоления системы защиты и совершения запрещенных действий он может использовать различные методы получения дополнительных полномочий доступа к ресурсам (имен, паролей и т.п. других пользователей), недостатки в построении системы защиты и доступные ему штатные (установленные на рабочей станции) программы (несанкционированные действия посредством превышения своих полномочий на использование разрешенных средств). Помимо этого, он может пытаться использовать дополнительно нештатные инструментальные и технологические программные средства (отладчики, служебные утилиты), самостоятельно разработанные программы или стандартные дополнительные технические средства.

«Мошенник» — работник Компании (или другой организации, зарегистрированный как пользователь в информационных системах компании), который может предпринимать попытки выполнения незаконных технологических операций, ввода подложных данных и тому подобные действия в корыстных целях, по

принуждению или из злого умысла, но использующий при этом только штатные (установленные на рабочей станции и доступные ему) аппаратные и программные средства от своего имени или от имени другого работника (зная его имя и пароль, используя его кратковременное отсутствие на рабочем месте и т.п.).

«Внутренний злоумышленник» — работник Компании, зарегистрированный как пользователь в информационных системах компании, действующий целенаправленно из корыстных интересов или мести за нанесенную обиду, возможно, в сговоре с лицами, не являющимися работниками Компании. Он может использовать весь набор методов и средств взлома системы защиты, включая агентурные методы получения реквизитов доступа, пассивные средства (технические средства перехвата без модификации компонентов системы), 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 – из сетей общего пользования.

Внутренним нарушителем может быть лицо из следующих категорий персонала Компании:

- зарегистрированные конечные пользователи в информационных системах компании (работники Компании);
- работники, не допущенные к работе с информационными активами Компании;
- персонал, обслуживающий технические средства информационных активов (инженеры, техники);
- работники подразделений разработки и сопровождения ПО (прикладные и системные программисты);
- технический персонал, обслуживающий здания (уборщицы, электрики, сантехники и другие работники, имеющие доступ в здания и помещения, где расположены критически важные информационные системы и активы);
- работники подразделения информационной безопасности и ИТ;
- руководители различных уровней.

«Внешний нарушитель (злоумышленник)» — постороннее лицо или бывший работник Компании или другой организации, действующий целенаправленно из корыстных интересов, из мести или из любопытства, возможно в сговоре с другими лицами. Он может использовать весь набор радиоэлектронных способов нарушения информационной безопасности, методов и средств взлома систем защиты, характерных для сетей общего пользования (в особенности сетей на основе IP-протокола), включая удаленное внедрение программных закладок и использование специальных инструментальных и технологических программ, используя имеющиеся слабости протоколов обмена и системы защиты узлов сети Компании.

Категории лиц, которые могут быть внешними нарушителями:

- уволенные работники Компании;
- представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации (энерго-, водо-, теплоснабжения и т.п.);
- посетители (приглашенные представители организаций, граждане), представители фирм, поставляющих технику, программное обеспечение, услуги и т.п.;
- члены преступных организаций, работники спецслужб или лица, действующие по их заданию;
- лица, случайно или умышленно проникшие в сеть Компании из внешних (по отношению к Компании) сетей телекоммуникации («хакеры»).

Пользователи и обслуживающий персонал из числа работников Компании имеют наиболее широкие возможности по осуществлению несанкционированных действий, вследствие наличия у них определенных полномочий по доступу к ресурсам и хорошего знания технологии обработки информации и защитных мер. Действия этой группы лиц напрямую связано с нарушением действующих правил и инструкций. Особую опасность эта группа нарушителей представляет при взаимодействии с криминальными структурами или спецслужбами.

Уволенные работники могут использовать для достижения целей свои знания о технологии работы, защитных мерах и правах доступа. Полученные в Компании знания и опыт выделяют их среди других источников внешних угроз.

Криминальные структуры представляют наиболее агрессивный источник внешних угроз. Для осуществления своих замыслов эти структуры могут идти на открытое нарушение закона и вовлекать в свою деятельность работников Компании всеми доступными им силами и средствами.

Профессиональные «хакеры» имеют наиболее высокую техническую квалификацию и знания об уязвимостях программных и аппаратных средств. Наибольшую угрозу представляют при взаимодействии с работающими и уволенными работниками Компании и криминальными структурами.

Организации, занимающиеся разработкой, поставкой и ремонтом оборудования, информационных систем, представляют внешнюю угрозу в силу того, что эпизодически имеют непосредственный доступ к информационным ресурсам. Криминальные структуры и спецслужбы могут использовать эти организации для временного устройства на работу своих членов, с целью доступа к защищаемой информации и информационных активов.

7. КОНТРОЛЬ ЭФФЕКТИВНОСТИ СИСТЕМЫ ЗАЩИТЫ

Контроль эффективности защиты информации осуществляется с целью своевременного выявления и предотвращения утечки информации по техническим каналам, за счет несанкционированного доступа к ней, а также предупреждения возможных специальных воздействий, направленных на уничтожение информации, разрушение средств информатизации.

Контроль может проводиться как выделенными работниками информационной безопасности, так и привлекаемыми для этой цели компетентными организациями, имеющими лицензию на этот вид деятельности.

Оценка эффективности мер защиты информации проводится с использованием технических и программных средств контроля на предмет соответствия установленным требованиям.

Контроль может осуществляться как с помощью штатных средств системы защиты информации от несанкционированного доступа, так и с помощью специальных программных средств контроля.

8. АУДИТ

Подразделение по информационной безопасности должно обеспечить и проверить при помощи внутреннего и внешнего аудита, степень, правильность выполнения и оперативность указаний данной Политики и исходящие от него внутренних нормативных документов, а также обеспечить выполнение установленных исправительных мер с целью непрерывного совершенствования функционирования.

9. ОТВЕТСТВЕННОСТЬ ЗА СОБЛЮДЕНИЕ ПОЛОЖЕНИЙ ПОЛИТИКИ

Ответственность за поддержание положений настоящей Политики в актуальном состоянии, организацию координации, внедрения, и внесение изменений в процессы системы менеджмента информационной безопасности Компании возлагается на подразделение по информационной безопасности.

Ответственность работников Компании за невыполнение настоящей Политики определяется соответствующими положениями, включаемыми в трудовые договоры с работниками Компании, а также положениями внутренних нормативных документов Компании.

10. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

Требования настоящей Политики могут быть дополнены и уточнены другими внутренними нормативными документами Компании.

В случае изменения действующего законодательства и иных нормативных актов, а также Устава Компании настоящая Политика и изменения к ней применяются в части, не противоречащей вновь принятым законодательным и иным нормативным актам, а также Уставу Компании. 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 для отражения изменений законодательства и нормативных актов, отраслевых принципов и технических регламентов;

- 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.

Контроль за исполнением требований, устанавливаемых Политикой, возлагается на Совет по информационной безопасности.

Вопросы, не урегулированные Политикой, разрешаются в соответствии с законодательством Республики Армении.