Приложение №1
к Приказу №56 от «20» декабря 2015г.

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АО «АГЕНТСТВО «ВЭРТАС»

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Дата введения – 01.01.2016

1. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящая политика информационной безопасности АО Агентство «Вэртас» (далее Политика) разработана с учетом требований федерального законодательства, а также требований других нормативных и организационно-распорядительных документов АО Агентство «Вэртас» (далее Компания) по вопросам обеспечения информационной безопасности (ИБ).

Политика определяет позицию руководства Компании в отношении ИБ, основные цели, направления и меры обеспечения ИБ, которыми Компания руководствуется в своей деятельности.

В рамках Политики руководство Компании заявляет, что:

- информационные технологии играют важную роль в достижении бизнес-целей Компании;
- информация является ценным активом Компании, требующим защиты независимо от форм ее представления;
- в своей деятельности Компания сталкивается с широким спектром угроз ИБ как внутреннего, так и внешнего характера, реализация которых может привести к ущербу (финансовые потери, юридические взыскания, потеря репутации, дезорганизация и т.д.);
- стратегической целью Компании в области ИБ является обеспечение функционирования и использования информационных технологий с учетом принимаемых рисков получения возможного ущерба от реализации угроз ИБ;
- стратегической задачей в области ИБ является построение системы управления ИБ, основанной на методологии управления рисками, учитывающей бизнес-требования, а также правовые требования ИБ.

Исполнение положений настоящей политики ИБ является обязательным для всех работников Компании.

2. ЦЕЛИ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.

Основными целями Политики являются:

- обеспечение единых подходов к обеспечению ИБ в рамках Компании;
- создание методологической основы для разработки внутренних документов по ИБ в Компании;
- определение форм участия руководства Компании в решении проблем ИБ.

Основными целями процесса обеспечения ИБ в Компании являются:

- создание условий для устойчивого функционирования информационной инфраструктуры Компании;
- поддержание необходимого уровня ИБ в Компании, соответствующего требованиям федерального законодательства, нормативным и организационно-распорядительных документов Компании.

3. НАПРАВЛЕНИЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Обеспечение ИБ в Компании осуществляется по следующим направлениям:

- управление ИБ;
- идентификация и классификация объектов защиты;
- организация работы с персоналом по вопросам ИБ;
- управление инцидентами ИБ;
- обеспечение непрерывности бизнес-процессов;

- обеспечение ИБ при эксплуатации средств обработки, хранения и передачи информации и использовании информационных ресурсов;
- обеспечение соответствия требованиям по ИБ.

Данные направления реализуются организационными и техническими мерами.

4. УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ВНУТРИ КОМПАНИИ

Организация и обеспечение управления ИБ в Компании осуществляется ее руководителем.

Руководство Компании постоянно поддерживает необходимый уровень ИБ путем внедрения системы обеспечения ИБ, а также распределения обязанностей и ответственности работников Компании за ее внедрение и осуществление.

Организация плановой, непрерывной и целенаправленной работы по осуществлению мер обеспечения ИБ и контролю их выполнения в Компании возлагается на Заместителя Генерального директора – Руководителя отдела Информационных технологий (далее Руководитель ОИТ).

На Руководителя ОИТ возложены следующие функции:

- планирование работ по ИБ;
- контроль эффективности реализуемых мер обеспечения ИБ и внесение рекомендаций по их совершенствованию;
- координация действий по обеспечению ИБ с представителями различных подразделений Компании;
- контроль выполнения и пересмотр политик ИБ объектов защиты.

С учетом особенностей конкретных объектов информационной инфраструктуры в Компании осуществляется:

- определение полномочий работников в отношении защищаемых информационных ресурсов;
- администрирование и контроль средств и механизмов безопасности;
- контроль выполнения работниками требований в области ИБ.

Функции администрирования и контроля средств и механизмов безопасности в Компании распределяются между подразделениями, эксплуатирующими объекты защиты информационной инфраструктуры, и Руководителя ОИТ:

- администрирование встроенных механизмов безопасности средств обработки, хранения и передачи информации, а также дополнительных средств защиты осуществляется работниками подразделений, отвечающих за их эксплуатацию;
- контроль функционирования и настройки механизмов безопасности, а также соблюдения требований по ИБ осуществляется Руководителем ОИТ.

В Компании организуется администрирование ИБ, направленное на обеспечение установленных правил доступа к объектам информационной инфраструктуры, порядка обращения с защищаемой информацией при ее обработке, хранении и передаче.

Администратором ИБ назначается, как правило, работник структурного подразделения, эксплуатирующего защищаемые объекты информационной инфраструктуры.

На администратора ИБ возлагается ответственность по предотвращению несанкционированного доступа к защищаемой информации.

Обязанности работников Компании по обеспечению ИБ зависят от занимаемой должности и определяются их должностными инструкциями.

В каждом структурном подразделении назначается работник, ответственный за обеспечение ИБ, перечень обязанностей которого разрабатывается с учетом специфики работы подразделения.

В Компании ежегодно разрабатывается план мероприятий по обеспечению ИБ на будущий год, в том числе мероприятий по контролю состояния ИБ.

5. ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ РАБОТЕ С ВНЕШНИМИ ОРГАНИЗАЦИЯМИ

При организации доступа сторонних организаций к защищаемым информационным ресурсам в Компании осуществляются мероприятия по обеспечению ИБ:

- определение рисков, связанных с предоставлением доступа сторонней организации к конфиденциальной информации;
- формирование на основе оценки рисков перечня мероприятий по обеспечению ИБ при предоставлении доступа сторонней организации к конфиденциальной информации Компании и их реализация;
- заключение соглашения о конфиденциальности со сторонними организациями, которым предоставляется доступ к конфиденциальной информации Компании.

Порядок представления информации органам государственной власти, а также передачи материалов средствам массовой информации, вопросы обеспечения ИБ при допуске на объекты защиты Компании представителей сторонней организации регламентируются нормативными, организационно-распорядительными и информационными документами Компании в области ИБ.

6. ИДЕНТИФИКАЦИЯ И КЛАССИФИКАЦИЯ ОБЪЕКТОВ ЗАЩИТЫ

В целях обеспечения ИБ в Компании осуществляется идентификация объектов защиты информационной инфраструктуры, определение степени их критичности, классификация и назначение ответственных за их безопасную эксплуатацию.

Идентификация объектов защиты, определение степени критичности и их классификация осуществляются в соответствии с требованиями Компании. Идентифицированные и классифицированные объекты защиты отражаются в инвентаризационной документации, маркируются и для них назначаются владельцы — работники Компании, ответственные за безопасную эксплуатацию объектов защиты.

Процедуры повторяются ежегодно. Внеплановые процедуры идентификации и классификации объектов защиты выполняются в случае внесения существенных изменений в информационную инфраструктуру Компании.

На основе классификации объектов защиты информационной инфраструктуры определяются применяемые по отношению к ним меры безопасности. Процедуры обработки информации и правила безопасного использования объектов защиты определяются их политиками ИБ, а также другими нормативными и организационно-распорядительными документами Компании в области ИБ.

7. ОРГАНИЗАЦИЯ РАБОТЫ С ПЕРСОНАЛОМ ПО ВОПРОСАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

7.1. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПРИ ЗАКЛЮЧЕНИИ И ВО ВРЕМЯ ДЕЙСТВИЯ ТРУДОВОГО ДОГОВОРА

В целях повышения уровня обеспечения информационной безопасности при приеме на работу новых работников осуществляется доведение до них правил обеспечения ИБ и устанавливается ответственность за их нарушение.

Обязанности работников Компании по соблюдению правил ИБ определяются должностными инструкциями и конкретизируются нормативными и организационно-распорядительными документами Компании в области ИБ.

При приеме на работу Компания заключает с работником соглашение о конфиденциальности.

В Компании обеспечивается сохранность заключенных соглашений о конфиденциальности.

Все работники Компании при вступлении в должность проходят первичный инструктаж, предусматривающий ознакомление с правилами и мерами ИБ.

Для работников Компании реализуются мероприятия повышения осведомленности в области ИБ.

Работники, отвечающие за обеспечение ИБ, регулярно проходят повышение квалификации, знакомятся с изменениями в федеральном законодательстве, нормативных и организационно-распорядительных документах Компании в области ИБ.

Работники Компании, имеющие доступ к информации, подлежащей защите, несут ответственность за ее разглашение и утрату, а также за нарушение установленного порядка обеспечения ИБ.

Работники, разгласившие подлежащую защите информацию или нарушившие установленный порядок обращения с ней, а также работники, по вине которых произошла ее утрата или искажение, несут ответственность в соответствии с действующим законодательством Российской Федерации.

7.2. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПРИ УВОЛЬНЕНИИ И ИЗМЕНЕНИИ УСЛОВИЙ ТРУДОВОГО ДОГОВОРА

В целях обеспечения ИБ при увольнении и изменении условий трудового договора в Компании осуществляется контроль возврата технических средств обработки, хранения и передачи информации, своевременного прекращения прав доступа работников к объектам защиты Компании.

Напоминание увольняемым работникам о принятых ими обязательствах по соблюдению в тайне конфиденциальных сведений и доведение до них срока сохранения в тайне сведений, с которыми они были ознакомлены, выполняются Руководителем ОИТ.

В Компании определяется порядок контроля возврата увольняемыми взятых во временное пользование технических средств.

При увольнении работника (изменении условий трудового договора) его права доступа к информационным ресурсам незамедлительно аннулируются (приводятся в соответствие с новыми условиями).

Специалист по кадрам своевременно уведомляет подразделение ИБ об увольнении (изменении условий трудового договора) работников.

8. УПРАВЛЕНИЕ ИНЦИДЕНТАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

8.1. ОПОВЕЩЕНИЕ ОБ ИНЦИДЕНТАХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В целях предотвращения нарушений ИБ в Компании принимаются меры по оповещению об инцидентах ИБ.

Работники Компании обязаны сообщать Руководителю ОИТ о любых замеченных или предполагаемых нарушениях безопасности, а также выявленных уязвимостях в соответствии с установленным в Компании порядком.

8.2. РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В целях реагирования на инциденты ИБ осуществляется их регистрация и анализ, а также принятие необходимых мер по исключению их повторения.

В Компании назначаются работники, ответственные за реагирование на инциденты ИБ, имеющие соответствующую подготовку.

Реагирование на инциденты ИБ осуществляется в соответствии с принятым в Компании порядком.

8.3. ОБЕСПЕЧЕНИЕ НЕПРЕРЫВНОСТИ БИЗНЕС-ПРОЦЕССОВ

В целях обеспечения поддержки и восстановления бизнес-процессов осуществляются профилактические и восстановительные мероприятия по обеспечению бесперебойного функционирования информационной инфраструктуры Компании.

Состав мероприятий по обеспечению бесперебойного функционирования информационной инфраструктуры Компании определяется с учетом оценки рисков ИБ.

Мероприятия по обеспечению бесперебойного функционирования информационной инфраструктуры Компании подвергаются тестированию и регулярному пересмотру.

9. ПОРЯДОК ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ЭТАПАХ ЖИЗНЕННОГО ЦИКЛА ОБЪЕКТОВ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Информационная безопасность информационной инфраструктуры Компании обеспечивается на всех стадиях жизненного цикла ее объектов с учетом ролей всех вовлеченных в этот процесс сторон (разработчиков, заказчиков, поставщиков продуктов и услуг, эксплуатирующих организаций и надзорных органов).

Жизненный цикл объекта информационной инфраструктуры Компании включает следующие этапы:

- обоснование требований к объекту;
- разработка (модернизация) объекта;
- ввод объекта в эксплуатацию;
- эксплуатация объекта;
- вывод объекта из эксплуатации.

Руководитель ОИТ в части сопровождения вопросов ИБ участвует во всех этапах жизненного цикла объектов информационной инфраструктуры Компании.

Для наиболее важных объектов информационной инфраструктуры Компании может разрабатываться программа сопровождения и обеспечения ИБ в течение их жизненного цикла.

Порядок обеспечения ИБ информационной инфраструктуры Компании на всех этапах жизненного цикла ее объектов определяется их политиками ИБ, а также другими нормативными и организационно-распорядительными документами Компании в области ИБ.

10. ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ЭКСПЛУАТАЦИИ СРЕДСТВ ОБРАБОТКИ, ХРАНЕНИЯ И ПЕРЕДАЧИ ИНФОРМАЦИИ И ИСПОЛЬЗОВАНИИ ИНФОРМАЦИОННЫХ РЕСУРСОВ

10.1. ФИЗИЧЕСКАЯ ЗАЩИТА ОБЪЕКТОВ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ.

В целях предотвращения несанкционированного доступа к объектам защиты информационной инфраструктуры Компании обеспечивается физическая защита мест их эксплуатации (размещения).

Технические средства обработки, хранения и передачи информации размещаются в запираемых шкафах, располагаемых в специализированных помещениях, доступ посторонних лиц к которым ограничивается.

Порядок обеспечения физической защиты мест эксплуатации (размещения) объектов защиты определяется их политиками ИБ.

10.2. ЗАЩИТА ТЕРРИТОРИЙ, ЗДАНИЙ И ПОМЕЩЕНИЙ

В целях обеспечения защиты информации и технических средств обработки, хранения и передачи информации обеспечивается защита территорий, зданий и помещений Компании.

В центральном офисе Компании устанавливается пропускной режим, препятствующий бесконтрольному посещению его охраняемых помещений. Порядок посещения и поведения в зданиях и помещениях Компании регламентируется нормативными и организационно-распорядительными документами Компании в области ИБ.

Здания и помещения Компании обеспечиваются техническими средствами охраны, системами контроля доступа и пожарной безопасности.

При проведении работ на охраняемых территориях Компании, в его зданиях и защищаемых помещениях третьими лицами обеспечивается контроль их деятельности.

Порядок защиты помещений, в которых располагаются технические средства (серверы, централизованные хранилища данных, сетевое оборудование и средства защиты информации), определяется политиками ИБ объектов защиты

информационной инфраструктуры, а также другими нормативными и организационно-распорядительными документами Компании в области ИБ.

10.3. ОРГАНИЗАЦИЯ БЕЗОПАСНОЙ ЭКСПЛУАТАЦИИ СРЕДСТВ ОБРАБОТКИ, ХРАНЕНИЯ И ПЕРЕДАЧИ ИНФОРМАЦИИ

В целях обеспечения ИБ объектов информационной инфраструктуры в Компании устанавливаются правила безопасной эксплуатации средств обработки, хранения и передачи информации.

Принимаются меры по обеспечению использования средств обработки, хранения и передачи информации только по целевому назначению.

Функции по администрированию и контролю эксплуатации средств обработки, хранения и передачи информации возлагаются на специально выделенных для этого работников.

Правила эксплуатации средств обработки, хранения и передачи информации, используемые в Компании, определяются политиками ИБ объектов защиты.

10.4. ЗАЩИТА ОТ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

В целях предотвращения проникновения, обнаружения и нейтрализации вредоносного ПО в Компании создается система защиты информационной инфраструктуры Компании от вредоносного ПО.

В Компании используются сертифицированные на соответствие требованиям безопасности информации средства защиты от вредоносного ПО. Архитектура системы защиты от вредоносного ПО обеспечивает многоуровневую (эшелонированную) защиту.

Порядок организации защиты информационной инфраструктуры Компании от вредоносного ПО определяется политиками ИБ объектов защиты.

10.5. РЕЗЕРВИРОВАНИЕ ИНФОРМАЦИОННЫХ РЕСУРСОВ И ТЕХНИЧЕСКИХ СРЕДСТВ ОБРАБОТКИ, ХРАНЕНИЯ И ПЕРЕДАЧИ ИНФОРМАЦИИ

10.5.1. РЕЗЕРВНОЕ КОПИРОВАНИЕ ИНФОРМАЦИОННЫХ РЕСУРСОВ

В целях обеспечения возможности восстановления информационных ресурсов в случае их утраты или нарушения целостности в Компании осуществляется их резервное копирование.

Способ и периодичность резервного копирования, сроки хранения резервных копий определяются в зависимости от назначения и особенностей системы, в которой информация обрабатывается, а также от ценности информации.

Порядок резервного копирования информационных ресурсов определяется политиками ИБ объектов защиты.

10.5.2. РЕЗЕРВИРОВАНИЕ СРЕДСТВ ОБРАБОТКИ, ХРАНЕНИЯ И ПЕРЕДАЧИ ИНФОРМАЦИИ

В целях обеспечения бесперебойного функционирования информационной инфраструктуры Компании осуществляется резервирование критически важных средств обработки, хранения и передачи информации.

Перечень критически важных средств обработки, хранения и передачи информации формируется в результате проведения идентификации и классификации объектов защиты.

Порядок резервирования средств обработки, хранения и передачи информации определяется политиками ИБ объектов защиты.

10.6. ОБЕСПЕЧЕНИЕ СЕТЕВОЙ БЕЗОПАСНОСТИ

В целях обеспечения защиты информации, непрерывного и устойчивого функционирования информационной инфраструктуры в Компании осуществляются мероприятия по обеспечению сетевой безопасности.

Обеспечение сетевой безопасности достигается защитой корпоративной сети передачи данных, сетевых сервисов и сетевой инфраструктуры. Порядок обеспечения сетевой безопасности определяется соответствующими политиками ИБ.

10.7. ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ОБРАЩЕНИИ СО СЪЕМНЫМИ НОСИТЕЛЯМИ ИНФОРМАЦИИ

В целях предотвращения разглашения, утечки или утраты информации в Компании применяются меры защиты съемных носителей информации.

В Компании разрешается применение только зарегистрированных установленным порядком съемных носителей информации.

Осуществляется мониторинг использования съемных носителей. Утилизация неиспользуемых носителей осуществляется только с обеспечением гарантированного уничтожения содержащейся на них информации.

Порядок обеспечения ИБ при обращении со съемными носителями информации определяется соответствующими политиками ИБ, а также другими нормативными и организационно-распорядительными документами Компании в области ИБ.

10.8. ЗАЩИЩЕННЫЙ ОБМЕН ИНФОРМАЦИЕЙ

В целях предотвращения разглашения, утечки или утраты информации в Компании применяются меры по защите информации при ее передаче различными методами.

Порядок защиты обмена информацией определяется политиками ИБ объектов защиты, а также другими нормативными и организационно-распорядительными документами Компании в области ИБ.

10.9. ЗАЩИТА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

В целях поддержания работоспособности программного обеспечения (ПО) в Компании осуществляются меры по устранению уязвимостей ПО, а также другие меры защиты.

Устранение уязвимостей ПО достигается регулярным централизованным получением и установкой обновлений, предоставляемых разработчиками ПО. Обновление ПО возлагается на работников отдела ИТ.

Порядок защиты ПО определяется политиками ИБ объектов защиты, а также другими нормативными и организационно-распорядительными документами Компании в области ИБ.

10.10. РЕГИСТРАЦИЯ И УЧЕТ СОБЫТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В целях своевременного выявления нарушений ИБ в Компании осуществляется контроль событий ИБ.В Компании осуществляется регистрация и учет в журналах событий технических средств обработки, хранения и передачи информации событий, которые могут быть связаны с нарушениями ИБ. Журналы событий регулярно анализируются Руководителем ОИТ. Результаты регистрации и учета событий используются при проведении мероприятий по управлению инцидентами ИБ.

Порядок осуществления контроля событий ИБ определяется политиками ИБ объектов защиты, а также другими нормативными и организационно-распорядительными документами Компании в области ИБ.

10.11. КОНТРОЛЬ ЗАЩИЩЕННОСТИ

В целях своевременного и эффективного реагирования на опубликованные и выявленные уязвимости, а также устранения недостатков в конфигурации технических средств обработки, хранения и передачи информации в информационной инфраструктуре Компании принимаются меры контроля защищенности.

Контроль защищенности осуществляется Руководителем ОИТ. Перечень объектов контроля защищенности определяется по результатам идентификации и классификации объектов защиты.

Порядок осуществления контроля защищенности определяется политиками ИБ объектов защиты, а также другими нормативными и организационно-распорядительными документами Компании в области ИБ.

10.12. КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА

В целях обеспечения конфиденциальности, целостности и аутентичности обрабатываемой, хранимой и передаваемой информации в информационной инфраструктуре Компании применяются сертифицированные установленным порядком криптографические средства защиты.

Электронные документы, для которых необходимо обеспечить целостность и аутентичность защищаются с помощью электронной цифровой подписи.

При передаче информации ограниченного доступа вне контролируемых зон, в том числе при использовании беспроводных сетей, применяются средства криптографической защиты информации.

При использовании мобильных устройств информация ограниченного доступа, хранимая на них, защищается с использованием криптографических средств.

Порядок применения средств криптографической защиты определяется политиками ИБ объектов защиты, а также другими нормативными и организационно-распорядительными документами Компании в области ИБ.

11. КОНТРОЛЬ ДОСТУПА

11.1. УПРАВЛЕНИЕ ДОСТУПОМ ПОЛЬЗОВАТЕЛЕЙ

В целях обеспечения безопасности и устойчивого функционирования информационной инфраструктуры в Компании осуществляется управление доступом пользователей к ее информационным ресурсам, прикладным системам и соответствующим техническим средствам объектов защиты.

Пользователи наделяются минимальными правами доступа и привилегиями, необходимыми им для выполнения служебных задач. Наделение пользователей правами доступа и привилегиями основывается на установленной в Компании формализованной процедуре предоставления прав доступа. Целесообразно при этом использовать принцип ролевого управления доступом. Права доступа и привилегии пользователей подлежат регулярному пересмотру.

Порядок управления доступом пользователей определяется политиками ИБ объектов защиты, а также другими нормативными и организационно-распорядительными документами Компании в области ИБ.

11.2. ОТВЕТСТВЕННОСТЬ ПОЛЬЗОВАТЕЛЕЙ

В целях предотвращения несанкционированного доступа, а также компрометации или утраты информации и средств обработки информации определяется ответственность пользователей за соблюдение правил доступа при использовании АРМ.

Пользователи несут ответственность за соблюдение установленных правил при выборе и использовании паролей. Парольная политика и правила использования паролей определяются нормативными и организационно-распорядительными документами Компании в области ИБ.

Пользователям запрещено работать под чужими учетными записями, а также сообщать свои пароли и передавать средства аутентификации другим пользователям. При оставлении АРМ пользователями предпринимаются меры по защите их от несанкционированного доступа.

Порядок использования АРМ определяется политиками ИБ объектов защиты.

11.3. КОНТРОЛЬ ДОСТУПА К ОПЕРАЦИОННОЙ СИСТЕМЕ (ОС)

В целях предотвращения несанкционированного доступа к объектам защиты информационной инфраструктуры Компании осуществляется контроль доступа к ОС.

Работа пользователей в ОС осуществляется под учетными записями с ограниченными правами. Доступ к ОС предоставляется пользователям только после прохождения процедур идентификации и аутентификации.

Управление учетными записями пользователей, их принадлежностью к группам пользователей, правами и привилегиями, а также политикой парольной защиты осуществляется сотрудниками отдела ИТ.

Меры контроля доступа к ОС определяются политиками ИБ объектов защиты.

11.4. КОНТРОЛЬ ДОСТУПА К ПРИКЛАДНЫМ СИСТЕМАМ И ИНФОРМАЦИОННЫМ РЕСУРСАМ

В целях предотвращения несанкционированного доступа к информации и нарушения функционирования информационной инфраструктуры в Компании обеспечивается контроль доступа к прикладным системам и информационным ресурсам.

Доступ к прикладным системам и информационным ресурсам предоставляется пользователям после прохождения ими процедур идентификации и аутентификации. При наличии технической возможности целесообразно осуществлять единую аутентификацию в прикладных системах и ОС.

Меры контроля доступа определяются политиками ИБ объектов защиты.

11.5. КОНТРОЛЬ ДОСТУПА К СЕТЕВЫМ СЕРВИСАМ

В целях предотвращения несанкционированного использования сетевых сервисов в информационной инфраструктуре Компании осуществляется контроль доступа к сетевым сервисам.

Доступ к сетевым сервисам предоставляется пользователям объектов защиты только ввиду служебной необходимости. Порядок разрешения и осуществления доступа пользователей к сетевым сервисам, меры контроля доступа определяются соответствующими политиками ИБ, а также другими нормативными и организационно-распорядительными документами Компании в области обеспечения ИБ.

11.6. КОНТРОЛЬ СЕТЕВОГО ДОСТУПА

В целях предотвращения несанкционированного доступа в информационную инфраструктуру Компании и к ее информационным ресурсам в Компании осуществляется контроль сетевого доступа.

Контроль сетевого доступа включает:

- контроль информационных потоков внешнего взаимодействия корпоративной сети передачи данных;
- контроль информационных потоков внешнего взаимодействия с информационными системами предприятия;
- контроль внутренних информационных потоков ЛВС;
- контроль удаленного подключения к ЛВС.

Меры контроля сетевого доступа определяются политиками ИБ объектов защиты.

11.7. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПРИ УДАЛЕННОМ ДОСТУПЕ И ИСПОЛЬЗОВАНИИ МОБИЛЬНЫХ УСТРОЙСТВ

В целях защиты от несанкционированного доступа в информационную инфраструктуру Компании и к защищаемым информационным ресурсам, а также от ее утечки в Компании принимаются меры по обеспечению безопасности при осуществлении удаленного доступа и использовании мобильных устройств.

При удаленном подключении пользователей к объектам защиты осуществляется контроль подключения, предусматривающий применение средств усиленной аутентификации и средств криптографической защиты информационного обмена (защищенных виртуальных сетей).

Перед подключением к информационной инфраструктуре Компании все мобильные устройства проверяются на наличие вредоносного ПО и необходимых обновлений системного ПО.

При использовании беспроводных подключений к объектам защиты применяются меры защиты беспроводных сетей.

Меры обеспечения безопасности при использовании мобильных устройств и при осуществлении удаленного доступа определяются политиками ИБ объектов защиты.

11.8. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ В БЕСПРОВОДНЫХ СЕТЯХ

В целях защиты от несанкционированного доступа к информационной инфраструктуре Компании и информации в Компании принимаются меры по обеспечению безопасности беспроводных сетей.

Целесообразность применения беспроводных сетей обосновывается проведением оценки рисков с учетом возможных угроз ИБ, связанных с использованием беспроводных сетей.

Подключение пользовательских устройств к беспроводной сети Компании согласовывается с отделом ИТ.

Меры обеспечения безопасности беспроводных сетей определяются политиками ИБ объектов защиты.

11.9. КОНТРОЛЬ ДОСТУПА К СЕТЕВОМУ ОБОРУДОВАНИЮ

В целях обеспечения безопасности сетевой инфраструктуры Компании осуществляется управление доступом администраторов к сетевому оборудованию.

В информационной инфраструктуре Компании обеспечивается защита физического и логического доступа к диагностическим и конфигурационным портам сетевого оборудования и сетевых средств защиты. Создается выделенная сеть управления сетевым оборудованием. При управлении сетевым оборудованием и средствами защиты без использования выделенной сети управления осуществляется криптографическая защита каналов управления.

Доступ к управлению сетевым оборудованием и средствами защиты предоставляется только сотрудникам отдела ИТ.

Меры контроля доступа определяются политиками ИБ объектов защиты.

12. ОБЕСПЕЧЕНИЕ СООТВЕТСТВИЯ ТРЕБОВАНИЯМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

12.1. ОБЕСПЕЧЕНИЕ СООТВЕТСТВИЯ ПРАВОВЫМ ТРЕБОВАНИЯМ

В соответствии с законодательством Российской Федерации, требованиями нормативных и организационно-распорядительных документов Компании осуществляются меры по защите информации ограниченного доступа.

Защита информации ограниченного доступа в Компании обеспечивается организацией:

- режима коммерческой тайны (КТ);
- защиты персональных данных работников Компании.

Допускается использование только официально приобретенного лицензионного ПО.

В составе объектов информационной инфраструктуры используются сертифицированные по требованиям безопасности информации или разрешенные к применению средства защиты информации.

Для защиты информации ограниченного доступа криптографическими методами в соответствии с законодательством Российской Федерации используются сертифицированные по требованиям безопасности информации криптографические средства защиты.

12.2. ОРГАНИЗАЦИЯ РЕЖИМА КОММЕРЧЕСКОЙ ТАЙНЫ

В Компании устанавливается порядок, предусматривающий правовые, организационные и технические меры по охране информации, содержащей КТ, и иной конфиденциальной информации.

Перечень мер по защите КТ и иной конфиденциальной информации регламентируется Федеральным законом 29.07.2004 № 98-ФЗ «О коммерческой тайне», а также нормативными и организационно-распорядительными документами Компании в области ИБ.

12.3. ОРГАНИЗАЦИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

В Компании устанавливается порядок защиты персональных данных работников, предусматривающий правовые, организационные и технические меры по их охране.

Перечень мер по защите персональных данных регламентируется Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», а также нормативными и организационно-распорядительными документами Компании в области ИБ.

12.4. ОБЕСПЕЧЕНИЕ СООТВЕТСТВИЯ ОРГАНИЗАЦИОННЫМ И ТЕХНИЧЕСКИМ ТРЕБОВАНИЯМ

В целях предотвращения нарушений ИБ осуществляется контроль выполнения требований нормативных и организационно-распорядительных документов Компании в области ИБ.

К числу мер контроля относятся:

- регулярный контроль руководителями структурных подразделений выполнения требований ИБ;
- внутренние проверки Руководителем ОИТ соответствия существующих процедур обеспечения ИБ предъявляемым требованиям;
- анализ выявленных несоответствий и установление причин их возникновения;
- реализация корректирующих мер и устранение выявленных несоответствий.

12.5. КОНТРОЛЬ СОСТОЯНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В целях определения соответствия принимаемых мер безопасности внутренним документам Компании по ИБ, выявления угроз ИБ и принятия мер по противодействию им в Компании осуществляется контроль состояния ИБ.

Контроль состояния ИБ осуществляется:

- проведением плановых (внеплановых) внешних проверок независимыми организациями и специалистами;
- проведением внутренних плановых (внеплановых) проверок и постоянным мониторингом, осуществляемыми Руководителем ОИТ Компании.

Контроль состояния ИБ осуществляется путем интервьюирования руководителей и работников структурных подразделений, анализа документации, осуществления инструментальных проверок.

Результаты проведения контроля состояния ИБ документируются.

13. ОТВЕТСТВЕННОСТЬ РУКОВОДСТВА И РАБОТНИКОВ

Руководство Компании отвечает за состояние ИБ в Компании и обеспечивает реализацию Политики, включая регулярный контроль ее исполнения, актуализацию и выделение необходимых для обеспечения ИБ ресурсов, а также организацию осведомленности и обучения работников в области обеспечения ИБ.

Ответственность за обеспечение ИБ объектов защиты Компании возлагается на работников, ответственных за их эксплуатацию.

Работники Компании обязаны:

- соблюдать требования настоящей политики ИБ и других нормативных и организационно-распорядительных документов Компании в области ИБ;
- использовать технические средства обработки информации только в служебных целях;
- осуществлять информирование Руководителя ОИТ о выявленных инцидентах ИБ.

Работникам Компании запрещается нарушать установленные правила обеспечения ИБ и скрывать факты возникновения инцидентов ИБ.

Работники Компании, не выполняющие требования настоящей политики ИБ или требования нормативных и организационно-распорядительных документов Компании в области ИБ, могут быть привлечены к ответственности установленным порядком.

14. ПОРЯДОК ПЕРЕСМОТРА ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Политика пересматривается с периодичностью не реже одного раза в 5 лет. При пересмотре Политики учитываются результаты контроля эффективности обеспечения ИБ за предыдущий период.

Процедура пересмотра Политики включает:

- анализ и выявление несоответствий действующей Политики текущим условиям;
- разработку предложений по совершенствованию Политики;
- утверждение новой редакции Политики.

При осуществлении процедуры пересмотра учитываются:

- результаты контроля состояния ИБ и предложения структурных подразделений о совершенствовании процедур обеспечения ИБ;
- изменения в организационной структуре и информационной инфраструктуре Компании;
- изменения в законодательной и нормативной базе по ИБ, произошедшие с момента утверждения предыдущей Политики;
- результаты анализа произошедших инцидентов ИБ, а также уязвимости и угрозы, выявленные в Компании за время, прошедшее с момента утверждения предыдущей Политики;
- изменения в управлении ИБ, включая изменения в распределении ресурсов и обязанностей при обеспечении ИБ.