Тип работы: Контрольная работа

Предмет: Информатика основы

Содержание

1. Общие положения

1.1. Цель и задачи настоящей Политики

Основной целью, на достижение которой направлены все положения настоящей Политики, является защита информационных ресурсов от возможного нанесения им материального, физического, морального или иного ущерба, посредством случайного или преднамеренного воздействия на информацию, её носители, процессы обработки и передачи, а также минимизация рисков ИБ.

Для достижения основной цели необходимо обеспечивать эффективное решение следующих задач:

- своевременное выявление, оценка и прогнозирование источников угроз ИБ;
- создание механизма оперативного реагирования на угрозы ИБ;
- предотвращение и/или снижение ущерба от реализации угроз ИБ;
- защита от вмешательства в процесс функционирования ИС посторонних лиц;
- соответствие требованиям Федерального законодательства, нормативнометодических документов ФСБ России, ФСТЭК России и договорным обязательствам в части ИБ;
- обеспечение непрерывности критических бизнес-процессов;
- достижение адекватности мер по защите от угроз ИБ;
- изучение партнёров, клиентов, конкурентов и кандидатов на работу;
- недопущение проникновения структур организованной преступности и отдельных лиц с противоправными намерениями;
- выявление, предупреждение и пресечение возможной противоправной и иной негативной деятельности сотрудников;
- повышение деловой репутации и корпоративной культуры.

1.2. Основание для разработки

Настоящая политика разработана на основе требований законодательства Российской Федерации, накопленного в ООО «БАЗИС» опыта в области обеспечения ИБ, интересов и целей ООО «БАЗИС».

При написании отдельных положений настоящей политики использовались следующие нормативные документы:

- ГОСТ Р ИСО/МЭК 27001 «Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности»;
- РС БР ИББС-2.0-2007 «Методические рекомендации по документации в области обеспечения информационной безопасности…»;
- РС БР ИББС-2.2-2009 «Методика оценки рисков нарушения информационной безопасности»;
- РС БР ИББС-2.5-2014 «Менеджмент инцидентов информационной безопасности»;
- СТО БР ИББС-1.0-2014 «Обеспечение информационной безопасности организаций банковской системы РФ.

Общие положения».

1.3. Область применения настоящей Политики
Настоящая Политика распространяется на все бизнес-процессы ООО «БАЗИС» и обязательна для применения всеми сотрудниками и руководством Учреждения, а также пользователями его информационных ресурсов.
Настоящая политика распространяется на информационные системы учреждения.
Лица, осуществляющие разработку внутренних документов ООО «БАЗИС», регламентирующих вопросы информационной безопасности, обязаны руководствоваться настоящей Политикой.

2. Система управления информационной безопасностью
Для достижения указанных целей и задач в ООО «БАЗИС» внедряется система управления информационной безопасностью.
СУИБ документирована в настоящей политике, в правилах, процедурах, рабочих инструкциях, которые являются обязательными для всех работников ООО «БАЗИС» в области действия системы.
Документированные требования СУИБ доводятся до сведения работников ООО «БАЗИС».
Средства управления информационной безопасностью внедряются по результатам проведения оценки рисков информационной безопасности.
Стоимость внедряемых средств управления информационной безопасностью не должна превышать возможный ущерб, возникающий при реализации угроз.

2.1. Структура документов
В целях создания взаимосвязанной структуры нормативных документов ООО «БАЗИС» в области обеспечения информационной безопасности, разрабатываемые и обновляемые нормативные документы должны соответствовать следующей иерархии:

-