Политика информационной безопасности издательства

Цели информационной безопасности

Основной целью, на достижение которой направлена ПИБ, является минимизация ущерба от событий, таящих угрозу безопасности информации, посредством их предотвращения или сведения их последствий к минимуму.

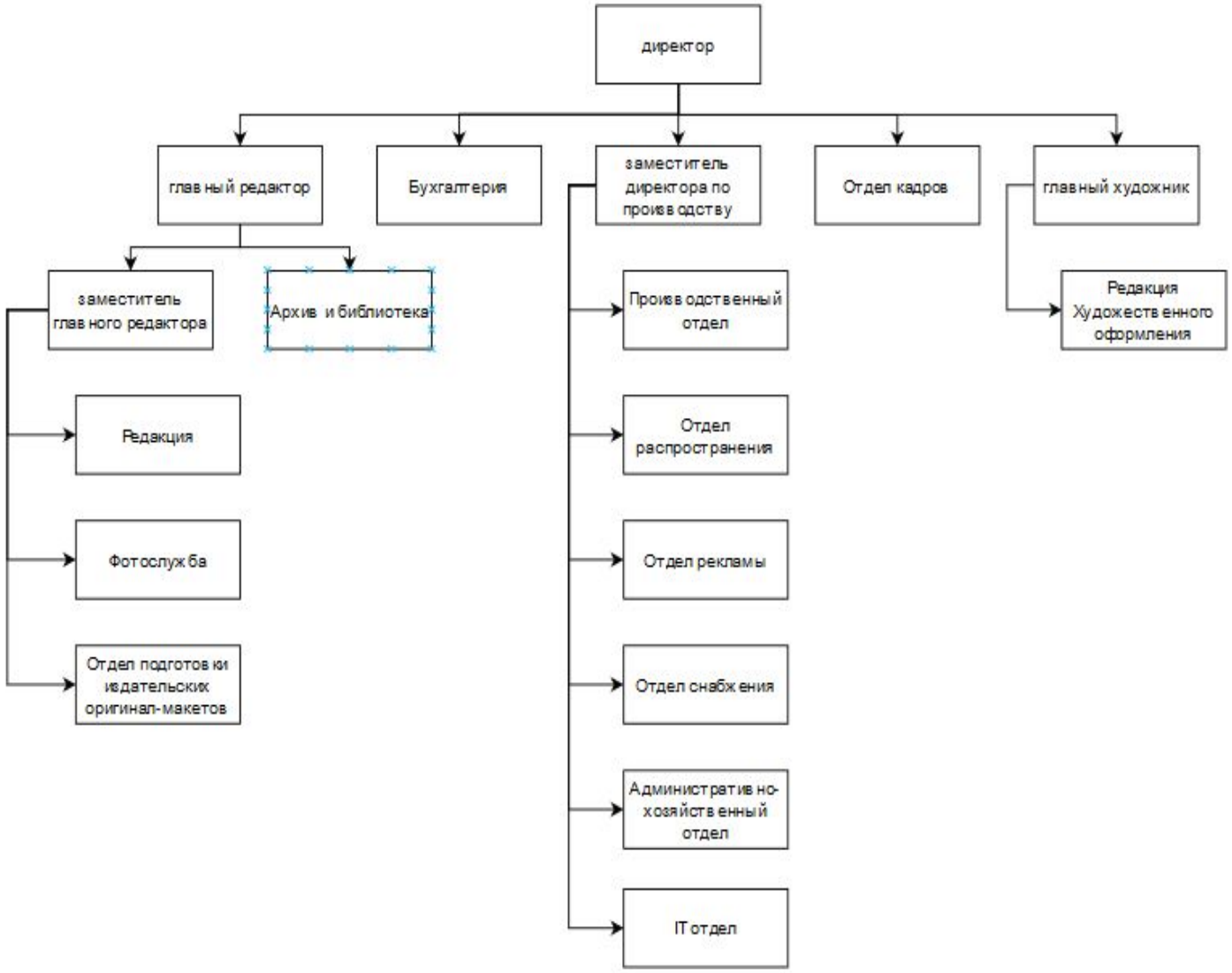
Для достижения цели необходимо обеспечивать решение следующих задач:

- 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 вмешательств в процесс функционирования Информационной Системы (ИС) посторонних лиц;
- Соответствие требованиям законодательства по информационной безопасности Республики Беларусь, нормативно-методических документов и договорным обязательствам в части ИБ;

Для достижения цели необходимо обеспечивать решение следующих задач:

- 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;

Структура компании



Объекты защиты

- коммерческая тайна издательства, данные о ее договорах, финансовых взаимоотношениях, бухгалтерская информация;
- коммерческая тайна клиентов и партнеров организации, данные об их активах, имуществе, платежах, произошедших страховых событиях;
- персональные данные сотрудников компании и сотрудников клиентов, эта информация иногда включает номера автомобилей, водительских удостоверений, кредитных карт;

Все массивы информации содержатся как на бумажных, так и на электронных носителях.

Основные объекты обеспечения ИБ

- информационные ресурсы, содержащие сведения, отнесенные в соответствии с действующим законодательством и внутренними нормативными документами компании к конфиденциальной информации;
- средства и системы информатизации, на которых производится обработка, передача и хранение защищаемой информации.
- программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение) автоматизированной системы компании, с помощью которых производится обработка защищаемой информации;

Основные объекты обеспечения ИБ

- процессы Компании, связанные с управлением и использованием информационных ресурсов;
- помещения, в которых расположены средства обработки защищаемой информации;
- рабочие помещения и кабинеты работников компании, помещения компании, предназначенные для ведения закрытых переговоров и совещаний;
- персонал компании, имеющий доступ к защищаемой информации.

Основные угрозы и их источники

действия внутреннего или внешнего злоумышленника (несанкционированный, в том числе удаленный доступ с целью нарушения работоспособности ИВС, кражи, удаления или модификации информации, несанкционированного распространение материальных носителей за пределами организации);

наблюдение за источниками информации;

подслушивание конфиденциальных разговоров и акустических сигналов работающих механизмов;

перехват электрических, магнитных и электромагнитных полей, электрических сигналов и радиоактивных излучений;

разглашение информации компетентными людьми;

Основные угрозы и их источники

несанкционированное распространение информации через поля и электрические сигналы, случайно возникшие в аппаратуре;

воздействие стихийных сил (наводнения, пожары и т. п.);

сбои и отказы в аппаратуре сбора, обработки и передачи информации;

отказы системы электроснабжения;

воздействие мощных электромагнитных и электрических помех (промышленных и природных).

Оценка рисков. Условная численная шкала для оценки ущерба издательства от НСД

Величина ущерба	Описание
0	Раскрытие информации принесет ничтожный моральных и финансовый ущерб издательству
1	Ущерб от атаки есть, но он незначителен, основная работа и положение издательства на рынке не затронуты
2	Работа издательства приостанавливается на некоторое время, за это время издательство несет убытки, но положение на рынке и количество клиентов меняется не значительно
3	Значительные потери на рынке и в прибыли. От издательства уходит основная часть клиентов.
4	Потери очень значительны, издательство теряет позиции на рынке. Для восстановления положения требуются крупные финансовые займы.
5	Издательство прекращает существование

Вероятностно-временная шкала реализации несанкционированного доступа к информационным ресурсам

Вероятность события	Средняя частота события (НСД)
0	Данный вид атаки отсутствует
0,1	Реже, чем раз в год
0,2	Около 1 раза в год
0,3	Около 1 раза в месяц
0,4	Около 1 раза в неделю
0,5	Практически ежедневно

Оценка рисков

Описание атаки	Ущерб	Вероятность	Риск (Ущерб*Вероятность)
Спам (переполнение почтового ящика)	1	0,4	0,4
Копирование жесткого диска из центрального офиса	3	0,1	0,3
Непреднамеренный рассказ конфиденциальной информации сотрудниками издательства	3	0,4	1,2
Раскрытие основных планов и стратегий развития издательства	4	0,1	0,4
Раскрытие личных данных клиентов издательства	3	0,2	0,6
Итого	2.8	0.24	0.58

обеспечения требуемого уровня защищенности информационных ресурсов

Информационная безопасность издательства должна обеспечиваться целым комплексом мер, среди которых:

- административно-правовые;
- организационные;
- программно-технические

Данные меры следует применять совместно. Опираться система защиты должна на управление персоналом компании и контроль над ним. Меры технического характера не менее важны, но не могут существовать в отрыве от организационных мер.

Вывод

Комплексное применение современных технических средств в работе службы безопасности издательства может обеспечить высокий уровень защиты информации от утечек и несанкционированного доступа.

Следует учитывать, что все предпринимаемые действия должны в полной мере соответствовать требованиям законодательства. В частности, нарушение конфиденциальности данных юридической фирмы и их клиентов зачастую приводит к вымогательству и шантажу, инсайдерской торговле и недобросовестной конкуренции. Это не только нанесет урон репутации – юридическая фирма понесет ответственность – начиная от финансовой и закачивая уголовной