Функции по защите информации руководителя предприятия

Тябин Алексей
ОТЗИ 20501.10

Защита информации на предприятии — регламентация производственной деятельности и взаимоотношений субъектов (сотрудников предприятия) на нормативно-правовой основе, исключающая или ослабляющая нанесение ущерба данному предприятию.

- Система мер по защите информации в широком смысле слова должна строиться исходя из тех начальных условий и факторов, которые, в свою очередь, определяются состоянием устремленности разведок противника либо действиями конкурента на рынке товаров и услуг, направленными на овладение информацией, подлежащей защите.

- Это правило действует как на государственном уровне, так и на уровне конкретного предприятия.

защита информации:

- Организация работы с персоналом;
- Организация внутриобъектового и пропускного режимов и охраны;
- Организация работы с носителями сведений;
- Комплексное планирование мероприятий по защите информации;
- Организация аналитической работы и контроля.

Защита информации является организационным началом, так называемым «ядром» в общей системе защиты конфиденциальной информации предприятия. От полноты и качества решения руководством предприятия и должностными лицами организационных задач зависит эффективность функционирования системы защиты информации в целом. Роль и место организационной защиты информации в общей системе мер, направленных на защиту конфиденциальной информации предприятия, определяются исключительной важностью принятия руководством своевременных и верных управленческих решений с учетом имеющихся в его распоряжении сил, средств, методов и способов защиты информации и на основе действующего нормативно-методического аппарата.

- Роль руководства предприятия в решении задач по защите информации трудно переоценить. Основными направлениями деятельности, осуществляемой руководителем предприятия в этой области, являются: планирование мероприятий по защите информации и персональный контроль за их выполнением, принятие решений о непосредственном доступе к конфиденциальной информации своих сотрудников и представителей других организаций, распределение обязанностей и задач между должностными лицами и структурными подразделениями, аналитическая работа и т.д. Цель принимаемых руководством предприятия и должностными лицами организационных мер — исключение утечки информации и, таким образом, уменьшение или полное исключение возможности нанесения предприятию ущерба, к которому эта утечка может привести.

Руководитель предприятия выполняет следующие функции по защите информации:

1) утверждает стратегию (политику) и концепцию защиты объекта;

2) утверждает планы работы по обеспечению информационной безопасности;

3) утверждает состав специальных комиссий, участвующих в работе по защите информации;

4) утверждает Перечень сведений, составляющих КИ;

5) разрешает проведение конфиденциальных переговоров;

6) выделяет ресурсы для создания и функционирования системы защиты информации;

7) подписывает приказы, договора, контракты, локальные нормативные акты предприятия по защите информации.

Руководитель несет ответственность за:

- за организацию работы по защите информации на предприятии;
- допуск и доступ к конфиденциальной информации;
- неразглашение конфиденциальной информации.

- Один из основных подходов к созданию системы защиты информации заключается во всестороннем анализе состояния защищенности информационных ресурсов предприятия с учетом устремленности конкурирующих организаций к овладению конфиденциальной информацией и, тем самым, нанесению ущерба предприятию. Важным элементом анализа является работа по определению перечня защищаемых информационных ресурсов с учетом особенностей их расположения (размещения) и доступа к ним различных категорий сотрудников (работников других предприятий).

- Работу по проведению такого анализа непосредственно возглавляет руководитель предприятия и его заместители по направлениям деятельности. Изучение защищенности информационных ресурсов основывается на положительном и отрицательном опыте работы предприятия, накопленном в течение последних нескольких лет, а также на деловых связях и контактах предприятия с организациями, осуществляющими аналогичные виды деятельности.

- Руководитель предприятия несет персональную ответственность за организацию и проведение необходимых мероприятий, направленных на исключение утечки сведений, отнесенных к конфиденциальной информации, и утрат носителей информации. Он обязан:

- знать фактическое состояние дел в области защиты информации, организовывать постоянную работу по выявлению и закрытию возможных каналов утечки конфиденциальной информации;
- определять обязанности и задачи должностным лицам и структурным подразделениям предприятия в этой области;
- проявлять высокую требовательность к персоналу предприятия в вопросах сохранности конфиденциальной информации;
- оценивать деятельность должностных лиц и эффективность мероприятий по защите информации.

- В зависимости от объема работ по защите информации руководителем предприятия создается структурное подразделение по защите информации, либо назначаются штатные специалисты по этим вопросам. Подразделение по защите информации является самостоятельным структурным подразделением. Штатная численность подразделения по защите информации и его структура определяются руководителем предприятия. Указанные подразделения (штатные специалисты) подчиняются непосредственно руководителю предприятия или его заместителю.

1. Начальник службы защиты информации, приказом руководителя предприятия назначается во главе группы компетентных сотрудников, которые высказывают свои предложения по объему, уровню и способам обеспечения сохранности конфиденциальной информации.

2. Руководитель группы, обладая соответствующей квалификацией в этой области, с привлечением отдельных специалистов формирует предварительный список сведений, которые в дальнейшем войдут в «Перечень сведений, составляющих конфиденциальную информацию предприятия».

3. Руководитель группы на основе этого списка определяет и представляет на согласование необходимые к защите объекты (оборудование для обработки и обращения информации, программное обеспечение, коммуникации для передачи конфиденциальных данных, носители информации, персонал, допущенный к работе с использованием коммерческой и иной тайны).

4. Анализируются существующие меры защиты соответствующих объектов, определяется степень их недостаточности, неэффективности, физического и морального износа.

5. Изучаются зафиксированные случаи попыток несанкционированного доступа к охраняемым информационным ресурсам и разглашения информации.

6. На основе опыта предприятия, а также используя метод моделирования ситуаций, группа специалистов выявляет возможные пути несанкционированных действий по уничтожению информации, ее копированию, модификации, искажению, использованию и т. п. Угрозы ранжируются по степени значимости и классифицируются по видам воздействия.

7. На основе собранных данных оценивается возможный ущерб предприятия от каждого вида угроз, который становится определяющим фактором для категорирования сведений в «Перечне» по степени важности, например — для служебного пользования, конфиденциально, строго конфиденциально.

8. Определяются сферы обращения каждого вида конфиденциальной информации: по носителям, по территории распространения, по допущенным пользователям. Для решения этой задачи группа привлекает руководителей структурных подразделений и изучает их пожелания.

9. Группа подготавливает введение указанных мер защиты.

- К задачам СлЗИ относятся:

Своевременное выявление угроз защищаемой информации компании, причин и условий их возникновения и реализации.

Выявление и максимальное перекрытие потенциально возможных каналов и методов несанкционированного доступа к информации.

Отработка механизмов оперативного реагирования на угрозы, использование юридических, экономических, организационных, социально-психологических, инженерно-технических средств и методов выявления и нейтрализации источников угроз безопасности компании.

Организация специального делопроизводства, исключающего несанкционированное получение конфиденциальной информации.

Начальник СлЗИ является новой штатной единицей. На эту должность необходимо взять профессионала и специалиста в области защиты информации, а также хорошо знающего юридическую сторону этой проблемы, имеющего опыт руководства и координации работы подобных служб. Требования – высшее профессиональное образование и стаж работы в области защиты информации не менее 5 лет, хорошее знание законодательных актов в этой области, принципов планирования защиты.

Руководитель СлЗИ должен выполнять следующие функции:

вырабатывать политику обеспечения защиты информации и обеспечивать ее реализацию;

отвечать за функционирование СлЗИ и обеспечение защиты конфиденциальной информации;

осуществлять планирование и непосредственное руководство работой СлЗИ, нести персональную ответственность за выполнение службой возложенных на нее задач, за неукоснительное исполнение подчиненными своих должностных обязанностей и правил внутреннего трудового распорядка;

принимать личное участие в проведении наиболее сложных мероприятий по обеспечению защиты информации в компании;

разрабатывать планы действий в чрезвычайных ситуациях, проводить регулярную учебу с подчиненными;

руководить проведением служебных расследований;

организовывать взаимодействие СлЗИ с другими подразделениями;

разработка инструкций по работе с коммерческой тайной для персонала, допущенного к работе с документами, ее содержащую;

организовывать разработку рекомендаций по совершенствованию функционирования СЗИ;

осуществлять руководство отделом охраны;

кроме того, выполнять функции юриста: разработка, ведение и обновление основополагающих документов с целью закрепления в них требований обеспечения безопасности и защиты конфиденциальной информации.

Вопросы:

1) Какие функции по защите информации выполняет руководитель предприятия?
2) За что несет ответственность руководитель предприятия?
3) Кто назначает руководителя СлЗИ?

Используемые источники:

1) http://www.bezopasnik.org/article/19.htm
2) http://www.abc-people.com/typework/economy/e-confl-8.htm
3) http://gendocs.ru/v35243/?cc=21&view=txt