Коровяковская Н.И.
Алтайский государственный университет.
Научный руководитель - Черкасова О.Г., к.и.н.

ДОЛЖНОСТНЫЕ ИНСТРУКЦИИ КАК СРЕДСТВО РЕАЛИЗАЦИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Информационная безопасность - это комплекс мер по обеспечению безопасности информационных активов предприятия, то есть свойство информации сохранять конфиденциальность, целостность и доступность (а также и свойство сохранять аутентичность, подотчётность, неотказуемость и надёжность). Информационную безопасность можно обеспечить только в случае комплексного подхода, а также при помощи система менеджмента информационной безопасности, так как разрешение каких-то отдельных вопросов (технических или организационных) не решит проблему информационной безопасности в целом, а вот как раз этого главного принципа большинство сегодняшних руководителей в г. Барнауле не понимают и вследствие чего являются жертвами злоумышленников.

Система менеджмента информационной безопасности – часть общей системы менеджмента, основанная на использовании методов оценки бизнес-рисков для разработки, внедрения, функционирования, мониторинга, анализа, поддержки и улучшения информационной безопасности. Она включает в себя организационную структуру, политики, деятельность по планированию, распределение ответственности, практическую деятельность, процедуры, процессы и ресурсы.

Комплексный подход по обеспечению безопасности осуществляется с помощью разработки и внедрением руководством предприятия стратегии информационной безопасности. Стратегия – средство достижения желаемых результатов, комбинация из запланированных действий и быстрых решений по адаптации фирмы к новым возможностям получения конкурентных преимуществ и новым угрозам ослабления её конкурентных позиций.

В соответствии со ГОСТ Р ИСО/МЭК 27001-2006, организация должна разработать, внедрить, обеспечить функционирование, вести мониторинг, анализировать, поддерживать и непрерывно улучшать документированную систему менеджмента информационной безопасности применительно ко всей деловой деятельности организации и рискам, с которыми она сталкивается.

Одним из средств реализации стратегии информационной безопасности предприятия является документация. По данному национальному стандарту документация по системе менеджмента информационной безопасности должна включать в себя записи решений руководства, позволяющие обеспечивать контроль выполнения решений руководства и политик организации, а также обеспечивать воспроизводимость документированных результатов.

Руководство организации должно разрабатывать политику системы менеджмента информационной безопасности; обеспечивать разработку её целей и планов; определять функции и ответственности в области

информационной безопасности; доводить до сведения всех сотрудников организации информации о важности достижения целей информационной безопасности и соответствия её требованиям политики и стратегии информационной безопасности, об их ответственности перед законом, а также о необходимости непрерывного совершенствования в реализации мер информационной безопасности; проводить анализ системы менеджмента информационной безопасности и т.д.

Организация должна обеспечить необходимую квалификацию персонала, на который возложены обязанности выполнения задач в рамках системы менеджмента информационной безопасности путем определения требуемого уровня знаний и навыков для персонала, который выполняет работу, влияющую на систему менеджмента информационной безопасности; организации обучения персонала или принятия других мер для удовлетворения указанных потребностей; оценки результативности предпринятых действий; ведения записей об образовании, подготовке, навыках, опыте и квалификации сотрудников.

Также немаловажно обеспечить понимание всеми соответствующими сотрудниками значимости и важности деятельности в области информационной безопасности, и их роли в достижении целей система менеджмента информационной безопасности.

Организация должна постоянно повышать результативность системы менеджмента информационной безопасности посредством уточнения политики информационной, целей информационной безопасности, использования результатов аудитов, анализа контролируемых событий, корректирующих и предупреждающих действий, а также использования руководством результатов анализа системы менеджмента информационной безопасности.

Руководство организации должно постоянно поддерживать заданный уровень информационной безопасности путем внедрения системы менеджмента, а также путем распределения обязанностей и ответственности персонала за ее обеспечение. Оно также должно определить и внедрить процедуры получения разрешения на использование новых средств обработки информации, должно определять и условия конфиденциальности или вырабатывать соглашения о неразглашении информации в соответствии с целями защиты информации и регулярно их пересматривать.

Действия по обеспечению информационной безопасности должны координироваться представителями различных подразделений организации, имеющими соответствующие функции и должностные обязанности.

Реализация стратегии информационной безопасности осуществляется посредством разработанных Отделом кадров должностных инструкций и использования их в работе предприятия.

«Должностные инструкции являются одним из основных организационно-правовых документов, определяющих задачи, функции, основные права, обязанности и ответственность работника при осуществлении им трудовой функции согласно занимаемой должности, квалификационные требования, предъявляемые к лицу, занимающему определённую должность».

В настоящее время во многих организациях и на предприятиях (в большей части негосударственных) отсутствует практика разработки и введения должностных инструкций. Между тем, их введением достигается ряд целей, как определяет Т.В. Кузнецова: рациональное разделение труда; правильный подбор кадров, их расстановка и использование; укрепление служебной дисциплины в организации; повышение эффективности деятельности организации; создание организационно-правовой основы служебной деятельности сотрудников; повышение ответственности сотрудника за результаты его деятельности, осуществляемой на основании трудового контракта; обеспечение объективности при аттестации сотрудника, его поощрении и при наложении на него дисциплинарного взыскания; разрешение трудовых споров.

Из целей выводятся правила безопасности, описывающие, кто, что и при каких условиях может делать. Чем подробнее правила, чем более формально они изложены, тем проще поддержать их выполнение программно-техническими средствами.

Библиографический список

1. Трудовой кодекс Российской Федерации. – Новосибирск, 2008.
2. ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования». – М., 2008.
3. Общероссийский классификатор профессий рабочих, должностей служащих и тарифных разрядов от 26 декабря 1994 г.
4. Постановление Минтруда РФ от 10.11.1992 N 31 (ред. от 24.11.2008) «Об утверждении тарифно-квалификационных характеристик по общеотраслевым профессиям рабочих».
5. Постановление Минтруда РФ от 06.06.1996 N 32 (с изм. от 20.02.2002) «Об утверждении разрядов оплаты труда и тарифно-квалификационных характеристик (требований) по общеотраслевым должностям служащих».
6. Государственная система документационного обеспечения управления (ГСДОУ): Основные положения: Общие требования к документам и службам документационного обеспечения управления. – М., 1991.
7. В.А. Галатенко. Основы информационной безопасности. Курс лекций. Учебное пособие. Издание второе, исправленное / Под ред. члена-корреспондента РАН В.Б. Бетелина. – М.: ИНТУИТРУ «Интернет-университет Информационных Технологий», 2004 - 264 с.
8. Егоршин А. П. Управление персоналом: Учебник для вузов. - 4-е изд., испр. -Н. Новгород: НИМБ, 2003. - 720 с.
9. Игнатьев В.А. Информационная безопасность современного коммерческого предприятия: Монография. — Старый Оскол: ООО «ТНТ», 2005. — 448 с.

10. Костян И.А. Должностная инструкция: нужна или нет? // Справочник кадровика. – 2007. - №3. – С. 92-99.

11. Кузнецова Т.В. Делопроизводство (документационное обеспечение управления). – 4-е изд. испр. и дополн. - М., 2003.

12. Основы информационной безопасности. Учебное пособие для вузов / Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. - М.: Горячая линия - Телеком, 2006. - 544 с.

13. Травин В.В. Менеджмент персонала предприятия: Учеб.-практ. пособие / В.В. Травин, В.А. Дятлов — 5-е изд. — М.: Дело. 2003. — 272 с.

14. Управление персоналом: Учеб. для вузов/ Под ред. Т.Ю.Базарова, Б.Л. Еремина. — М.: Банки и биржи; ЮНИТИ, 1998. — 423 с.

15. Экономика труда и социальных отношений / Под ред. Г.Г. Меликьяна, Р.П. Колосовой. — М.: Изд-во МГУ, Изд-во ЧеРо, 1996. — 623 с.