УДК 004.056

ОРГАНИЗАЦИОННО-УПРАВЛЕНЧЕСКИЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЙ

© 2016 Балановская А.В., Волкодаева А.В.

ЧОУ ВО «Международный институт рынка», г. Самара, Россия

Статья посвящена рассмотрению организационно-управленческого аспекта защиты данных на трех уровнях в системе обеспечения информационной безопасности предприятия. Определяется значение мероприятий организационно-управленческого характера по обеспечению информационной безопасности предприятия. Проводится связь между законодательным, административным, организационным и программно-техническим уровнем защиты информации.

Ключевые слова: информационная безопасность, организационные меры защиты информации, уровень.

Информационная безопасность предприятия является функциональным элементом системы обеспечения его стратегического развития. Ее основная задача – обеспечить стабильность существования предприятия в настоящем и перспективы его устойчивого развития в будущем [1]. В комплексной системе обеспечения информационной безопасности предприятий учитываются современные правовые и организационно-управленческие мероприятия, а также программно-технические средства противодействия внешним и внутренним угрозам, что обеспечивает состояние защищенности информации и перспективы развития информационных технологий.

Актуальность разработки организационно-управленческого аспекта информационной безопасности предприятия заключается в создании надежного механизма защиты информации на административно-правовой и организационно-технической основе, что исключало бы (или сводило к минимуму) возможность возникновения опасности доступа к конфиденциальной информации. Несанкционированное использование конфиденциальных сведений предприятия в значительной мере обусловливаются не техническими аспектами, а злоумышленными действиями и халатностью пользователей или специалистов по их защите. Персонал предприятия, как виновник нарушения актуальности и непротиворечивости информации, склонен к умышленной или неумышленной фильтрации. Искажение информации является одной из основных трудностей в коммуникационной системе предприятия, определяющей ухудшение функционирования системы информационной безопасности [5].

Преднамеренное искажение информации:
- не информирование членами коллектива других сотрудников о своих основных достижениях;
- несогласие с сообщением и искажение информации в личных целях;
- фильтрация (упрощение большего объема сведений);
- желание получить одобрение руководителя и страх перед наказанием.

Непреднамеренное искажение информации:
- слабая мотивация и, как следствие, не выполнение ряда должностных полномочий;
- неудовлетворительный морально-нравственный климат и затруднения в межличностном общении;
- беспечность, халатность;
- многоуровневая система управления, где каждый уровень склонен корректировать и фильтровать сообщение.

Обозначенные выше трудности коммуникационной системы предприятия разделены на преднамеренные и непреднамеренные способы искажения информации на предприятия и данное деление условно, поскольку они взаимосвязаны между собой, поскольку. Например, не информирование членами коллектива других сотрудников о своих основных достижениях может быть следствием слабой трудовой мотивации и стимулирования.

В организационно-управленческом аспекте защиты данных предприятия используются различные мероприятия, предполагающие

регламентацию деятельности и взаимоотношений исполнителей на нормативно-правовой основе. Необходимо четко разграничивать законодательный, административный, организационный и программно-технический уровни защиты информации (таблица 1).

Таблица 1 – Уровни защиты информации в системе информационной безопасности предприятия

Уровень защиты информации	Методы и средства защиты информации
Законодательный уровень	1. Государственные стандарты. 2. Законы Российской Федерации в области защиты информации (защиты государственной тайны). 3. Указы Президента РФ в области защиты информации (защиты государственной тайны). 4. Постановления Правительства РФ в области защиты информации (защиты государственной тайны). 5. Внутренние нормативные документы предприятия в области защиты информации от несанкционированного доступа. 6. Сертификация и лицензирование.
Административный уровень	1. Политика информационной безопасности. 2. Распорядительство.
Организационный уровень	1. Организационное регламентирование. 2. Организационное нормирование. 3. Организационное инструктирование.
Программно-технический уровень	1. Аппаратные средства защиты. 2. Программные средства защиты. 3. Защитные преобразования.

Рассмотрим взаимосвязь обозначенных уровней защиты информации в общей системе информационной безопасности предприятия. Основополагающим будет являться законодательный уровень, поскольку ГОТы, законы, постановления, указы, нормативные акты и стандарты регламентируют правила использования и обработки конфиденциальной информации и меры ответственности за нарушения этих правил. Нормативно-правовая база Российской Федерации в области защиты информации и обеспечения ее безопасности ложится в основу системы контроля предприятия.

Надстройкой данного уровня является три последующих подуровня, включающихся в работу по обеспечению информационной безопасности предприятия одновременно. На административном уровне создается регламентирующий документ «Политика информационной безопасности предприятия» [4], включающий в себя ряд разделов, определяющих принятие документированных управленческих решений и разработанных превентивных мер по защите информационных ресурсов. К основным разделам «Политики информационной безопасности предприятия» следующие разделы:

1. Вводная часть (определяет актуальность и заинтересованность различных групп сотрудников предприятия в защите информации, дается описание объекта защиты, определяются цели и задачи защиты информации, принципы политики информационной безопасности).
2. Юридический раздел (ссылки на законодательные, нормативные акты, внутренние документы распорядительного характера, регламентирующие и деятельность предприятия, и его персонала по защите информационных ресурсов).
3. Штатный раздел (описание подразделений, групп и т.д., отвечающих за работы в области информационной безопасности; описание должностей с точки зрения информационной безопасности, организация обучения, порядок реагирования на нарушение режима и т.д.).

4. Организационный раздел (описание мер, направленных на обеспечение непрерывной работы организации, порядок разработки и внедрения систем, правила разграничения доступа к производственной информации) [3]
5. Технический раздел (освещает вопросы физической защиты информации), описывает подход к управлению компьютерами и сетями передачи данных.

Распорядительство в системе информационной безопасности определяет решение конкретных ситуаций, требующих использования приказов, распоряжений, постановлений, резолюций и т.п. Сюда можно отнести приказ о назначении ответственного за безопасность данных предприятия, приказ об утверждении списка лиц с доступом конфиденциальной информации или приказ о назначении ответственных за журнал обращений к доступу к конфиденциальной информации.

Организационный уровень защиты информации включает организационное регламентирование, организационное нормирование и организационное инструктирование и обеспечивает организацию охраны, режима, работу с кадрами, с документами, нормы использования технических средств безопасности и процедуры информационно-анали-тической деятельности предприятия по выявлению угроз.

В каждом аспекте организационного уровня защиты информации определяется перечень задач, методов воздействия, форм контроля и регулирования, а также реакция системы (таблица 2).

Таблица 2 – Организационный уровень защиты информации

Методы воздействия	Задачи методов	Формы воздействия на объект (систему)
Организационное регламентирование	1. Повышение эффективности работ и их контроля. 2. Рационализация и упорядочение управленческой деятельности.	Законодательные акты страны и региона, нормативные акты предприятия (устав, положения, должностные инструкции и т.п.)
Организационное нормирование	1. Определение рациональных пределов возможных изменений в системе. 2. Обеспечение эффективного использования ресурсов.	Правила внутреннего распорядка, нормы и нормативы, технологические схемы, графики и т.п.
Организационное инструктирование	1. Оказание методической и информационной помощи. 2. Создание условий для осуществления процесса управления	Схемы организационного построения предприятия и расположения функциональных подразделений, порядок работы организации, внутриорганизационные инструкции, инструктажи по технике безопасности.

В системе обеспечения информационной безопасности важную роль играет организационное регламентирование как основа правового регулирования защиты информации предприятия. Организационная регламентация защиты данных включает:
1. Организация и координирование службы безопасности предприятия на основе обеспечения ее нормативно-методической документацией по защите информации.
2. Составление перечня защищаемой информации и его регулярное обновление. Определение регламента доступа к защищаемой информации с определением списка допускаемых к ней лиц.
3. Работа с персоналом по инструктированию работы с защищаемой информацией и применению санкций при нарушениях; организация рабочего места специалистов по информационной защите и другого персонала при работе с конфиденциальной информацией.
4. Разработка технологии защиты, обработки и хранения информации и порядка защиты информации при несанкционированном доступе, системы охраны территории

предприятия (пропускной режим, видеонаблюдение).
5. Приобретение, установка и эксплуатация технических средств защиты информации предприятия.
6. Разработка системы контроля мероприятий по определению уровня эффективности информационной безопасности предприятия.

К мероприятиям организационно-управленческого характера по обеспечению информационной безопасности предприятия можно отнести информирование персонала о правилах работы с конфиденциальной информацией, мерах ответственности за нарушение, процедурах защиты и хранения информации, организацию охраны территорий, создание организационных структур по обеспечению безопасности информационных ресурсов, организацию конфиденциального делопроизводства предприятия. Создание организационной структуры органов информационной безопасности предприятия рекомендуется в виде единой вертикали, подчиненной высшему руководству предприятия через механизм вхождения представителей этого руководства в совет по информационной безопасности. Практика показывает, что на многих предприятиях, данная рекомендация выполняется только в части выделения ответственных за информационную безопасность работников в подразделениях информационных технологий. На крупных предприятиях создаются подразделения информационной безопасности, которые в большинстве случаев не имеют достаточных полномочий и влияния. Некоторые крупные поставщики продуктов и услуг в области комплексных информационно-технических решений предлагают дополнительно услуги аутсорсинга информационных технологий, включая и вопросы информационной безопасности. Сейчас спрос на аутсорсинг в части обеспечения информационной безопасности предприятия достаточно ограничен.

Организационный аспект обеспечения информационной безопасности предприятия является одним из важнейших ее элементов, так как от принятых к реализации действий в значительной степени зависит эффективность всей деятельности по поддержанию системы информационной безопасности на должном уровне [7]. Правильное решение вопросов создания органов информационной безопасности будет способствовать ускорению комплексного внедрения и поддержанию работоспособности целостной системы информационной безопасности, увязывающей правовые, административные, организационные, технологические, научно-технические и физические меры защиты информации. Организационный аспект существенным образом влияет на проведение внутреннего аудита информационной безопасности, ведение объективного анализа и мониторинга состояния информационной безопасности с выявлением нарушений и новых угроз информационной безопасности, на своевременное и объективное расследование этих нарушений с принятием защитных мер и определением степени вины сотрудников и других лиц. Роль организационного аспекта тем более возрастает, чем выше уровень зрелости предприятия по обеспечению процессов информационной безопасности, чем выше степень осознания основной специфики вопросов информационной безопасности, заключающейся в том, что проблема информационной безопасности является междисциплинарной темой, охватывающей фактически все аспекты бизнеса предприятия.

Программно-технический уровень защиты информации является технической основой защиты информации. Применение аппаратных, программных средства защиты и защитных преобразований осуществляется специализированными подразделениями в структуре управления и определяется политикой информационной безопасности предприятия. При организации формирования оптимального перечня программных средств и методов принято использовать следующую схему:
1. Определить информационные и технические ресурсы, подлежащие защите.
2. Выявить потенциально-возможные угрозы и каналы утечки информации.
3. Провести оценку уязвимости и рисков информации при возникновении угроз или утечке.
4. Определить требования к системе защиты информации.
5. Осуществить выбор средства защиты информации.

6. Внедрить и организовать использование выбранных средств (мер, способов) защиты.
7. Осуществить контроль целостности и управление системой защиты информации [2].

Программные методы, аппаратные средства и защитные преобразования не представляется возможным рассматривать отдельно от организационных мер по обеспечению информационной безопасности предприятия, так как последние включают всю совокупность действий по подбору и подготовке персонала для работы с ними и определяют строгое регламентирование процесса разработки и функционирования информационной системы на основе программно-технических средств. Таким образом, организационно-управленческий аспект создания надежного механизма защиты информации играет важную роль в обеспечении информационной безопасности предприятия [6], т.к. посягательство на использование конфиденциальных сведений предприятия в значительной мере обусловлено не техническими аспектами, а организационными мероприятиями, регламентирующими работу с программно-техническими средствами, определяющими ответственность должностных лиц по защите информации, а также исполнением нормативной базы и определением места службы по обеспечению информационной безопасности в структуре управления предприятием.

СПИСОК ИСТОЧНИКОВ

1. Горбунова О.А., Мавлявеева Ю.О. Основные направления повышения конкурентоспособности промышленного предприятия на примере ООО «Ортопласт»//Вестник Международного института рынка. 2015 №1. С.65-72.
2. Домарев В.В. Программно-технические методы и средства защиты информации [Электронный ресурс] / В.В. Домарев. – Режим доступа: http://www.bezpeka.com/files/lib_ru/book-domarev03/ch_09.pdf (дата обращения 04.04.2015 г.)
3. Герасимов Б.Н. Развитие процесса управления операционной политикой предприятия // Вестник Международного института рынка. 2015. № 1. С. 49-58.
4. Казакова А.В. Развитие системы обеспечения информационной безопасности промышленных предприятий: автореферат // Экономическая библиотека [Электронный ресурс] Режим доступа: http://economy-lib.com/razvitie-sistemy-obespecheniya-informatsionnoy-bezopasnosti-promyshlennyh-predpriyatiy#1.
5. Китаев Д.Ф., Макаров А.А., Макарова Л.В., Смольников С.Д. Информационная система для разработки имитационной модели оценки коллектива//Вестник Международного института рынка. 2016 №1. С.190-198.
6. Нестерова С.И. Инструмент управления конкурентоспособностью региона//Экономика и управление собственностью. 2015. №1. С.15-20.
7. Семкин С.Н. Основы организационного обеспечения информационной безопасности объектов информатизации: учеб. пособие / С.Н. Семкин, Э.В. Беляков, С.В. Гребенов, В.И. Козачок. - М. Гелиос АРВ, 2005. - 192 с.

ORGANIZATIONAL AND MANAGERIAL ASPECTS OF INFORMATION SECURITY COMPANIES

© 2016 Anna V. Balanovskaya, Arina V. Volkodaeva

International Market Institute, Samara, Russia

The article is devoted to the organizational and managerial aspects of data protection at three levels in the system of ensuring information security of the enterprise. The article determines the value of organizational and managerial nature to ensure information security of the enterprise. The article gives the link between the legislative, administrative, organizational, software and hardware level of information security.

Keywords: information security, organizational security measures to safeguard the information, level.