УДК 004.056.5:658.5

Т.В. Карлова, Н.М. Кузнецова, А.Ю. Бекмешов

ОПТИМИЗАЦИЯ ДОСТУПА К ИНФОРМАЦИОННЫМ РЕСУРСАМ В ПРОМЫШЛЕННОСТИ

Рассмотрен вопрос определения оптимального количества уровней доступа к информационным ресурсам в зависимости от принятой политики информационной безопасности и масштаба организации.

Ключевые слова: разграничение доступа, защита информации, уровень доступа, информационные ресурсы.

Политика информационной безопасности – документ, определяющий управление защитой информационных ресурсов предприятия.

В качестве основного метода защиты информационных ресурсов можно использовать автоматизированные системы разграничения доступа [1; 2]. При использовании подобных систем необходимо определение оптимального количества уровней доступа сотрудников к информационным структурам предприятия.

Рассмотрим предприятия малого, среднего и крупного бизнеса.

Для предприятия малого бизнеса характерно наличие небольшого количества сотрудников. К сотрудникам относятся:

- руководство предприятия;
- управленческий персонал;
- исполнители (разработчики).

Экономическими расчётами и бухгалтерией предприятий малого бизнеса занимается, как правило, небольшое количество сотрудников. Также для предприятий малого бизнеса характерно частое совмещение обязанностей управления процессом разработки и руководства.

Для предприятия среднего бизнеса характерно наличие дополнительных отделов, не связанных напрямую с проектами и разработками предприятия: отдела кадров, экономических отделов. Также предприятия среднего бизнеса имеют чёткое разделение обязанностей между руководством и управленческим персоналом. Таким образом, к сотрудникам предприятия среднего бизнеса относятся:

- руководство предприятия;
- управленческий персонал;
- исполнители (разработчики);
- сотрудники отдела кадров;
- сотрудники экономических служб.

Как правило, на предприятиях малого и среднего бизнеса исполнители выполняют как разработку, так и тестирование, написание сопровождающей документации.

Предприятия крупного бизнеса представляют собой корпорации масштаба страны. Для таких организаций характерно наличие большого количества департаментов, а также чёткого разделения обязанностей сотрудников согласно их принадлежности к отделам и подразделениям.Для предприятий крупного бизнеса характерно разделение обязанностей исполнителей при разработке, а также наличие нескольких уровней управления.

Таким образом, к сотрудникам предприятия крупного бизнеса относятся:

- руководство предприятия;
- сотрудники высшего уровня управления (так называемые топ-менеджеры);
- сотрудники уровня управления подразделениями (в том числе филиалами);
- сотрудники уровня управления отделами;

– разработчики;
– сотрудники отдела тестирования;
– сотрудники отдела кадров;
– сотрудники экономических служб;
– сотрудники отдела управления качеством;
– сотрудники отдела контроля нормативной документации;
– сотрудники отдела маркетинга;
– сотрудники отдела снабжения;
– сотрудники вспомогательных отделов;
– сотрудники отдела информационной безопасности.

Важно отметить, что современные предприятия стараются уменьшить количество уровней управления с целью повышения надёжности всей системы менеджмента [3].

Определение количества уровней доступа сотрудников к информационным ресурсам для предприятий малого бизнеса. Так как сотрудники предприятия малого бизнеса находятся в едином информационном пространстве, не стоит создавать более двух уровней доступа. Как показано на рис. 1, к первому, более строгому уровню относится руководство предприятия, ко второму – управленческий персонал и исполнители.

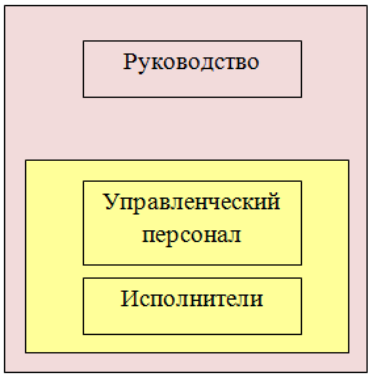

Рис. 1. Уровни доступа сотрудников к информационным ресурсам на предприятиях малого бизнеса

Важно отметить, что наличие «красного» уровня доступа также предполагает доступ к информации более низкого уровня – «жёлтого». Таким образом, руководство предприятия малого бизнеса должно иметь неограниченный доступ ко всему информационному пространству.

Определение количества уровней доступа сотрудников к информационным ресурсам для предприятий среднего бизнеса. Для предприятий среднего бизнеса характерно наличие нескольких уровней доступа к информационным ресурсам. Так как персонал организации составляют сотрудники не только отделов разработки, но и экономических отделов и отдела кадров, следует разделять доступ как минимум на три уровня:

1. Уровень доступа к стратегически важной информации («красный») – уровень для руководства организации. Предполагается доступ к информации о контрактах, партнёрах, запланированных сделках и т.д.

2. Уровень доступа к важной информации («желтый») – уровень для сотрудников отделов разработки. «Жёлтый» уровень предполагает доступ ко всей информации о разработках (информация о технических заданиях, методиках выполнения, об имеющихся оборудовании и материалах и т.д.). С целью оптимизации производственного процесса исполнители должны находиться в едином информационном пространстве. Разделение информационного пространства для исполнителей на дополнительные уровни доступа приведет к замедлению процесса разработки.

3. Уровень доступа к конфиденциальной информации («зелёный») – уровень для сотрудников экономических отделов и отдела кадров. Уровень предполагает доступ к информации, связанной с проектами организации, но не содержащей стратегически важных данных (персональные данные сотрудников, данные о расходах и доходах организации).

Уровни доступа представлены на рис. 2.

Стрелочками отмечены возможные запросы информации, относящейся к другому уровню доступа. Согласно рис. 2, руководство предприятия может осуществлять любой запрос информации к любому уровню, в то время как сотрудники, относящиеся к «желто-

му» и «зелёному» уровням доступа могут получать информацию другого уровня («зеленого» и «жёлтого» соответственно) только частично.

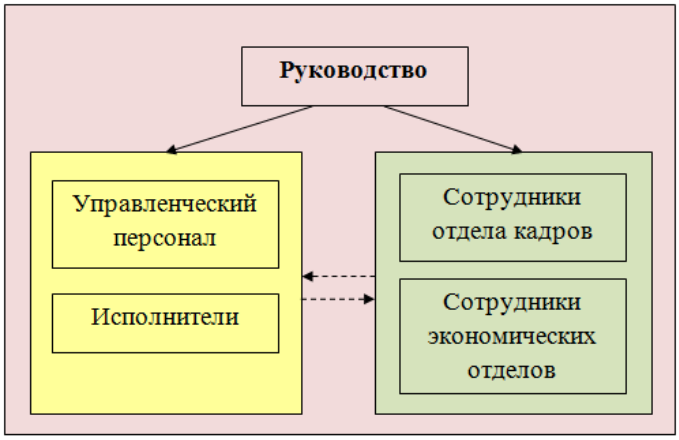

Рис. 2. Уровни доступа сотрудников к информационным ресурсам на предприятиях среднего бизнеса

Определение количества уровней доступа сотрудников к информационным ресурсам для предприятий крупного бизнеса. Для предприятий крупного бизнеса характерно наличие сложной инфраструктуры отделов и подразделений. Как правило, штат сотрудников такого предприятия составляет более тысячи человек. На предприятии такого масштаба требуется наличие тщательно сформулированной политики информационной безопасности, а также разграничения доступа.

Необходимо выделять как минимум четыре уровня доступа к информационным ресурсам (рис. 3).

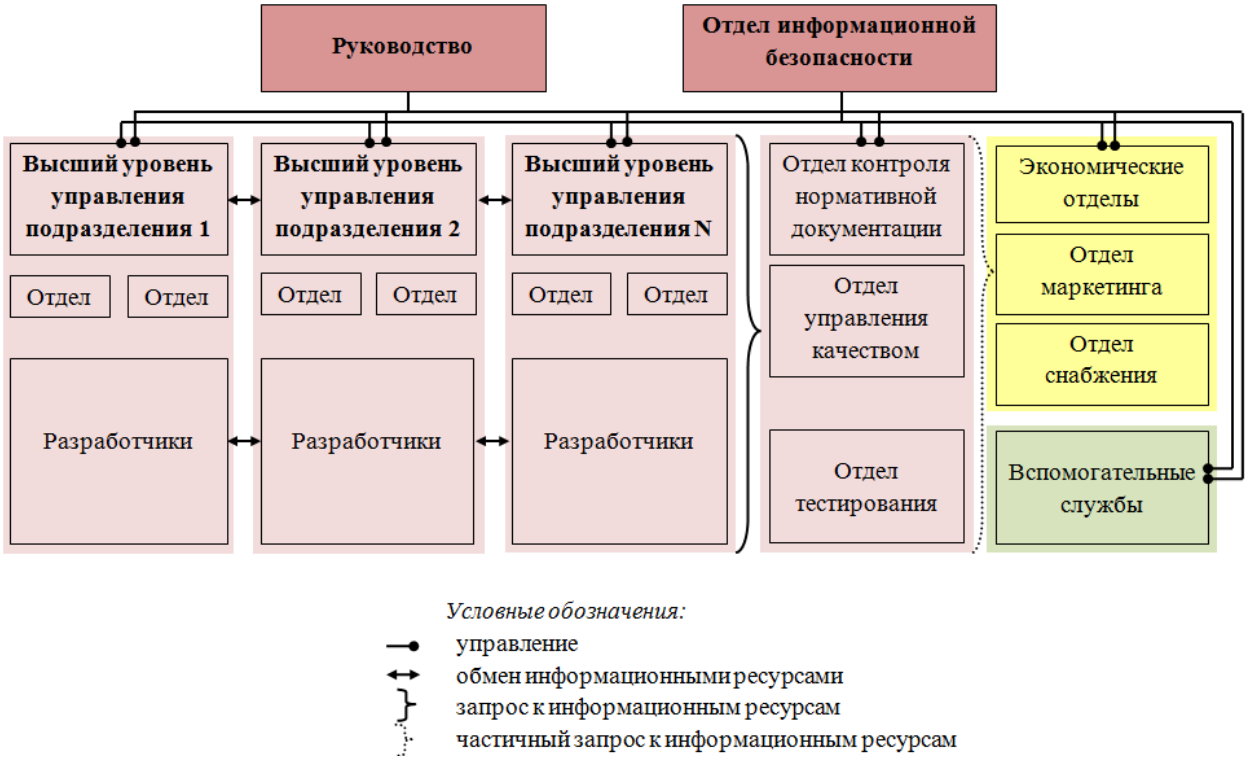

Рис. 3. Уровни доступа сотрудников к информационным ресурсам на предприятиях крупного бизнеса

Как показано на рис. 3, руководство предприятия и сотрудники отдела информационной безопасности, осуществляющие контроль, имеют самый высокий уровень доступа – «тёмно-красный».

К «красному» уровню доступа относятся:

– отделы предприятия, занятые непосредственно разработкой проектов;

– отделы, занимающиеся сопровождением проектов (отдел контроля нормативной документации, отдел управления качеством, отдел тестирования); сотрудники данных отделов заняты обработкой стратегически важной информации о проектах организации.

К «желтому» уровню доступа относятся те структурные подразделения предприятия, которые выполняют обработку информации, связанной с проектами организации, но не содержащей совершенно секретных данных.

К «зелёному» уровню доступа относятся те структурные подразделения предприятия, которым нет необходимости в ознакомлении с информацией о разработках предприятия.

Важно отметить, что разработчики должны находиться в едином информационном пространстве, информационный обмен в котором должен осуществляться без дополнительных барьеров. Также крайне необходимо вовремя предоставлять разработчику как можно более полное описание поставленной задачи, уточнения требований заказчиков, данные о датах сдачи проектов. Утаивание от разработчика информации, связанной с техническим заданием, является как минимум нерациональным.

Таким образом, количество уровней доступа к информационным ресурсам предприятия зависит от масштаба предприятия. Представленные в статье схемы разграничения являются обобщением и носят рекомендательный характер. При проектировании системы разграничения доступа количество уровней может быть изменено согласно требованиям политики информационной безопасности предприятия.

СПИСОК ЛИТЕРАТУРЫ

1. Карлова, Т.В. Разработка концепции обеспечения многоуровневого доступа к конфиденциальной информации / Т.В.Карлова, Н.М.Кузнецова // Вестник МГТУ «Станкин». – 2011. - № 2 (14). – С.87-90.
2. Карлова, Т.В. Автоматизированная система разграничения доступа к конфиденциальной информации с модулем контроля на основе усовершенствованного криптоаналитического метода «грубой силы» / Т.В.Карлова, Н.М.Кузнецова // Известия Кабардино-Балкарского государственного университета. – 2012. – Т. 2. - № 4. – С. 90-92.
3. Карлова, Т.В. Социодинамическое моделирование в производственной среде / Т.В.Карлова, А.Ю.Бекмешов // Вестник МГТУ «Станкин». – 2012. - Т. 2. - № 2 (21). - С. 35-37.

Материал поступил в редколлегию 15.06.15.