Информационные технологии в управлении персоналом

Понятие информационной безопасности

Безопасность информации (данных) – состояние защищенности информации (данных), при котором обеспечены ее (их) конфиденциальность, доступность и целостность.

Безопасность информации (данных) определяется отсутствием недопустимого риска, связанного с утечкой информации по техническим каналам, несанкционированными и непреднамеренными воздействиями на данные и (или) на другие ресурсы автоматизированной информационной системы, используемые при применении информационной технологии.

Безопасность информации (при применении информационных технологий) (англ. IT security) — состояние защищенности информационной технологии, обеспечивающее безопасность информации, для обработки которой она применяется, и информационную безопасность автоматизированной информационной системы, в которой она реализована.

Безопасность автоматизированной информационной системы – состояние защищенности автоматизированной информационной системы, при котором обеспечиваются конфиденциальность, доступность, целостность, подотчетность и подлинность ее ресурсов.

В качестве стандартной модели безопасности часто приводят модель из трех категорий:

- **Конфиденциальность** (англ. confidentiality) – состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право;
- **Целостность** (англ. integrity) – избежание несанкционированной модификации информации;
- **Доступность** (англ. availability) – избежание временного или постоянного сокрытия информации от пользователей, получивших права доступа.

Выделяют и другие не всегда обязательные категории модели безопасности:

- **Неотказуемость** или **апеллируемость** (англ. non-repudiation) – невозможность отказа от авторства;
- **Подотчетность** (англ. accountability) – обеспечение идентификации субъекта доступа и регистрации его действий;
- **Достоверность** (англ. reliability) – свойство соответствия предусмотренному поведению или результату;
- **Аутентичность** или **подлинность** (англ. authenticity) – свойство, гарантирующее, что субъект или ресурс идентичны заявленным.

Методы обеспечения информационной безопасности

Задача обеспечения информационной безопасности должна решаться системно. Это означает, что различные средства защиты (аппаратные, программные, физические, организационные и т.д.) должны применяться одновременно и под централизованным управлением. При этом компоненты системы должны «знать» о существовании друг друга, взаимодействовать и обеспечивать защиту как от внешних, так и от внутренних угроз.

- средства идентификации и аутентификации пользователей (так называемый «комплекс 3А»);
- средства шифрования информации, хранящейся на компьютерах и передаваемой по сетям;
- межсетевые экраны;
- виртуальные частные сети;
- средства контентной фильтрации;
- инструменты проверки целостности содержимого дисков;
- средства антивирусной защиты;
- системы обнаружения уязвимостей сетей и анализаторы сетевых атак.

- **«Комплекс 3А»** включает *аутентификацию* (или идентификацию), *авторизацию* и *администрирование*. Идентификация и авторизация – это ключевые элементы информационной безопасности. Функция авторизации отвечает за то, к каким ресурсам конкретный пользователь имеет доступ. Функция администрирования заключается в наделении пользователя определенными идентификационными особенностями в рамках данной сети и определении объема допустимых для него действий.

- **Системы шифрования** позволяют минимизировать потери в случае несанкционированного доступа к данным, хранящимся на жестком диске или ином носителе, а также перехвата информации при ее пересылке по электронной почте или передаче по сетевым протоколам. Задача данного средства защиты – обеспечение *конфиденциальности*.

- **Межсетевой экран** представляет собой систему или комбинацию систем, образующую между двумя или более сетями защитный барьер, предохраняющий от несанкционированного попадания в сеть или выхода из нее пакетов данных. Основной принцип действия межсетевых экранов – проверка каждого пакета данных на соответствие входящего и исходящего IP-адреса базе разрешенных адресов.

- Эффективное средство защиты от потери конфиденциальной информации – **фильтрация** содержимого входящей и исходящей электронной почты.

- Все изменения на рабочей станции или на сервере могут быть отслежены администратором сети или другим авторизованным пользователем благодаря технологии **проверки целостности** содержимого жесткого диска (integrity checking). Это позволяет обнаруживать любые действия с файлами (изменение, удаление или же просто открытие) и идентифицировать активность вирусов, несанкционированный доступ или кражу данных авторизованными пользователями.

- Современные **антивирусные технологии** позволяют выявить многие известные вирусные программы через сравнение кода подозрительного файла с образцами, хранящимися в антивирусной базе. Кроме того, разработаны технологии моделирования поведения, позволяющие обнаруживать вновь создаваемые вирусные программы. Обнаруживаемые объекты могут подвергаться лечению, изолироваться (помещаться в карантин) или удаляться.

- **Фильтры спама** значительно уменьшают непроизводительные трудозатраты, связанные с разбором спама, снижают трафик и загрузку серверов, улучшают психологический фон в коллективе и уменьшают риск вовлечения сотрудников компании в мошеннические операции. Кроме того, фильтры спама уменьшают риск заражения новыми вирусами, поскольку сообщения, содержащие вирусы (даже еще не вошедшие в базы антивирусных программ), часто имеют признаки спама и отфильтровываются.

- **Системы обнаружения уязвимостей** компьютерных сетей и **анализаторы сетевых атак** безопасно моделируют распространенные атаки и способы вторжения и определяют, что именно хакер может увидеть в сети и как он может использовать ее ресурсы.

- **Резервное копирование** – один из основных методов защиты от потери данных с четким соблюдением установленных процедур (регулярность, типы носителей, методы хранения копий и т.д.).

Бизнес-моделирование как метод управления

Предприятие – это совокупность персонала, оборудования, производственных площадей и других элементов, объединенных структурно для того, чтобы при определенных условиях достичь установленных целей путем производства некоторого объема товаров (услуг).

Управление предприятием условно можно разделить на следующие сегменты:

- управление финансами;
- управление средствами производства;
- управление материальными потоками;
- управление персоналом и т.д.

Для осуществления бизнес-процессов в масштабах предприятия необходимо, чтобы работники своевременно имели надежные данные для принятия управленческих решений, а также получали оперативную информацию для выполнения своих каждодневных функций.

Под ***бизнес-процессом*** в общем случае понимается деятельность, имеющая определенные входные и выходные параметры и связанная с получением прибыли или достижением результата.

Для коммерческих организаций бизнес-процесс обычно связан с тем или иным основным направлением деятельности (например, производство того или иного вида продукции, проведение исследований и разработок или операции на фондовом рынке).

Для государственных или некоммерческих организаций бизнес-процесс может заключаться в обработке информации и подготовке управленческих решений.

Персонал и вопросы управления ими рассматриваются в качестве отдельного бизнес-процесса, который в информационном аспекте взаимодействует с другими бизнес-процессами. Для большинства организаций тематика управления персоналом в общем случае не является основной деятельностью и может быть отнесена к обеспечивающим бизнес-процессам наряду с обеспечением оборудованием и бухгалтерским учетом.

В рамках одного бизнес-процесса можно выделить ряд ***бизнес-функций***, связанных с выполнением отдельных задач.

Например, в рамках процесса управления персоналом традиционно принято выделять такие бизнес-функции, как:

- учет персонального состава работников;
- планирование и подбор кадров;
- табельный учет.

На практике при реализации комплексных автоматизированных систем управления персоналом к этой области относят также функции ведения штатного расписания и расчета зарплаты, притом что на большинстве предприятий эти функции выполняются отдельными подразделениями, такими как планово-экономический отдел, ОТиЗ или расчетные группы в бухгалтерии.

Причина заключается в том, что выполнение этих функций в значительной степени базируется на информации, вводимой и обрабатываемой в задачах собственно кадрового учета.

Для каждого бизнес-процесса можно построить целую иерархию функций, например, такая функция кадрового учета, как аттестация персонала, в свою очередь может включать следующие подфункции:

- планирование проведения аттестации;
- учет фактических аттестационных признаков;
- расчет результирующих аттестационных признаков;
- анализ результатов аттестации.

Отдельные функции могут служить для реализации учета, осуществления контроля, планирования и регулирования, а также проведения анализа результатов управления процессом.

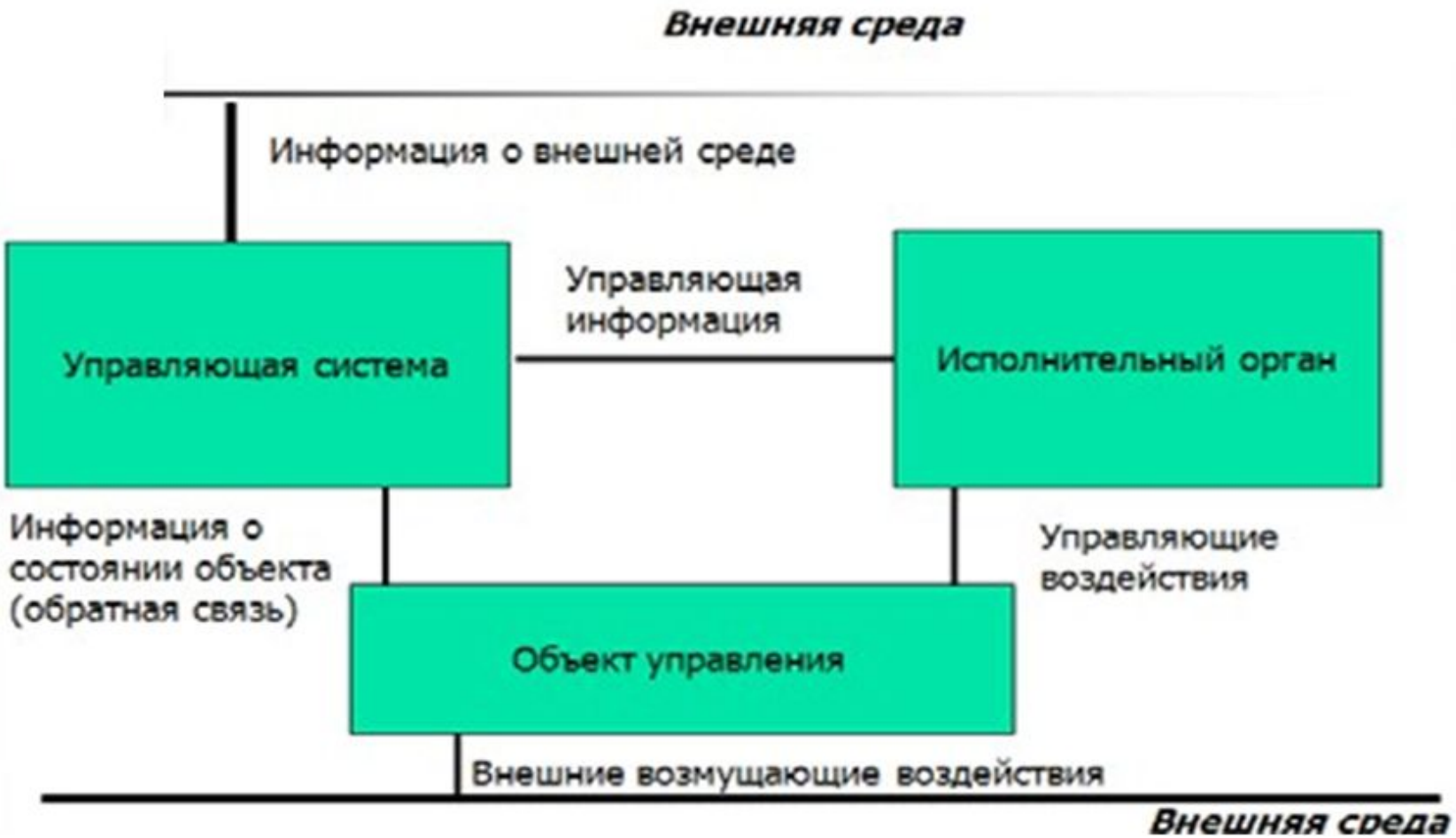
Процессы	Задачи управления				
	Учет	Контроль	Планирование	Регулирование	Анализ
Обеспечение персоналом	Персональный состав работников Текучесть кадров Рабочее время Травматизм Выполнение производственных заданий	Соблюдение трудовой дисциплины Выполнение производственных заданий Планирование выполнения программы повышения квалификации	Потребность в кадрах Прогнозирование потребности в кадрах Проведение аттестации Расчет трудовых показателей Обработка результатов социологических опросов	Согласование с производственным и процедурами Распределение персонала по рабочим местам Координация плана инструктажа по технике безопасности	Качественный и количественный состав персонала Причины текучести кадров Динамика изменения профессионального состава кадров за период

Организацию, как любой экономический объект, следуя основным положениям кибернетики, можно рассматривать в качестве регулируемой динамической информационной системы.

Под информационной системой в кибернетике понимается упорядоченное множество ее элементов, образующих определенную целостность.

Устойчивость и целостность системы, ее жизнеспособность и функционирование определяются информационным обменом между ее элементами. Способы и качество информационного обмена определяют процесс поддержания системы в заданных оптимальных параметрах. Этот процесс и получил название управления.

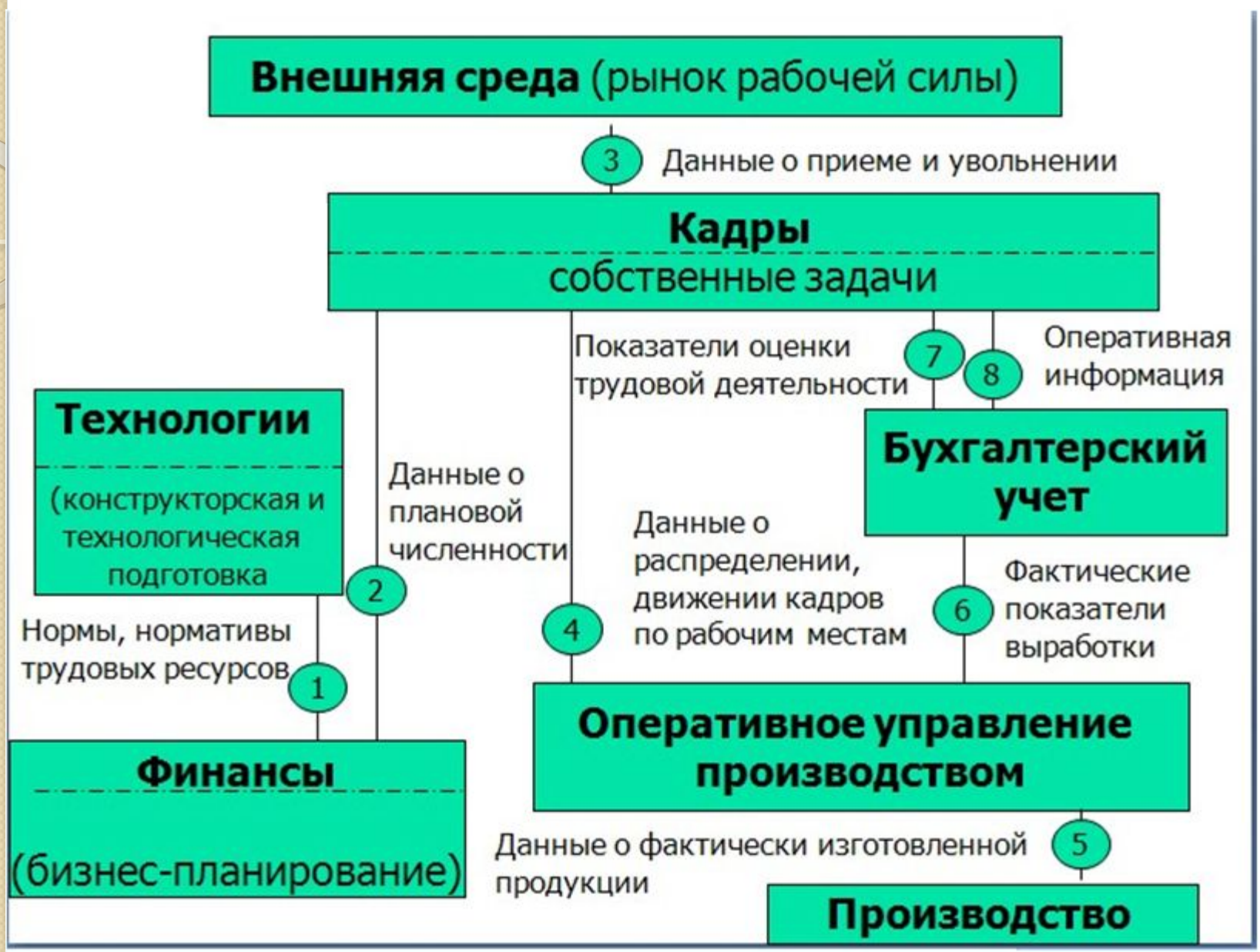
Принципиальная схема системы управления



Чтобы управлять, надо знать, как реагирует на управляющий сигнал объект управления, т.е. необходимо наличие сигнала, который называется обратной связью.

На основании информации, получаемой через обратную связь, орган управления вырабатывает управляющие (корректирующие) информационные воздействия, способные поддерживать работоспособность объекта управления в заданном режиме.

Принцип обратной связи универсален. Он лежит в основе функционирования регулируемых динамических систем в природе, технике, социальных системах и в экономике как их составной части.


Внешняя среда (рынок рабочей силы)
3
Данные о приеме и увольнении
Кадры
собственные задачи
Показатели оценки трудовой деятельности
7
8
Оперативная информация
Технологии
(конструкторская и технологическая подготовка
Данные о плановой численности
Бухгалтерский учет
Данные о распределении, движении кадров по рабочим местам
Фактические показатели выработки
2
4
6
Нормы, нормативы трудовых ресурсов
1
Оперативное управление производством
Финансы
(бизнес-планирование)
Данные о фактически изготовленной продукции
5
Производство

На практике реализация в информационной системе предприятия функций управления персоналом может потребовать следующих составляющих программного обеспечения:

- модуль кадрового учета;
- модуль управления штатным расписанием – для планирования численности работников, фонда заработной платы;
- модуль расчета заработной платы;
- система управления документами (СУД);
- юридическая справочная система;
- экспертные системы – для проведения аналитических исследований.

Совокупность задач, решаемых в отделе кадров можно разделить на две группы: работа непосредственно с людьми и работа с информацией.

В настоящее время автоматизированное управление кадрами дублируется бумажными документами. Это можно объяснить, с одной стороны, консерватизмом работников, традициями, недоверием к вычислительной технике и страховкой от непредвиденных обстоятельств, а с другой – несовершенством законодательной базы в области электронного документооборота.