ВОПРОСЫ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОГО ОБЕСПЕЧЕНИЯ ДЕЯТЕЛЬНОСТИ ПРЕДПРИЯТИЯ

SECURITY ISSUES OF INFORMATION SUPPORT OF THE ENTERPRISE

L. Shvedova

Summary. For a modern Manager, the issue of providing information for the purpose of making a management decision is most often associated with information technology and information systems, as well as with the availability of those software products that allow you to systematize and efficiently process the available information.

In the modern world, all information technologies (oral, written, computer) are involved, each of which performs a key, important role in the formation of a single information space. Management of a modern enterprise is currently at a stage of development, when there is a replacement of old traditional information technologies to new ones in many areas of activity: production, marketing, Finance.

This article discusses the concept of» information «and» information security», and also the main issues related to these concepts. In particular, the article touches upon the issues of information security of modern enterprises.

Keywords: information, information security, management decisions, information technology, business processes, a single information space.

Шведова Лариса Евгеньевна
К.т.н., ФГАОУ ВО «КФУ им. В. И. Вернадского»
Таврическая академия (структурное подразделение),
Республика Крым, г. Симферополь
larisashvedova@yandex.ru

Аннотация. Для современного руководителя вопрос обеспечения информацией с целью принятия управленческого решения чаще всего связан с информационными технологиями и информационными системами, а также с наличием тех программных продуктов, которые позволяют систематизировать и качественно обрабатывать имеющуюся информацию.

В современном мире задействованы все информационные технологии (устная, письменная, компьютерная), каждая из которых выполняет ключевую, значимую роль в формировании единого информационного пространства. Управление современным предприятием находится в настоящее время на таком этапе развития, когда происходит замена старых традиционных информационных технологий на новые во многих сферах деятельности: производстве, маркетинге, финансах.

В данной статье рассмотрены понятия «информация» и «информационная безопасность», а также рассмотрены основные вопросы, связанные с данными понятиями. В частности в статье, затронуты вопросы по обеспечения информационной безопасности современных предприятий.

Ключевые слова: информация, информационная безопасность, управленческие решения, информационные технологии, бизнес процессы, единое информационное пространство.

В толковом словаре С. И. Ожегова и Н. Ю. Шведовой слово «информация» трактуется следующим образом: информация — это сведения об окружающем мире и протекающих в нем процессах, воспринимаемые человеком или специальным устройством; информация — сообщения, осведомляющие о положении дел, о состоянии чего-нибудь[3].

В словаре русского языка Ефремовой Т. Ф., кроме вышеперечисленных определений по С. И. Ожегову, приводятся следующие определения понятия «информация»: [7]

- «это обмен сведениями между людьми и специальными устройствами»;
- «обмен сигналами в животном и растительном мире».

В словаре Н. Д. Ушакова, кроме объединяющих характеристик данного определения информация представляет собой «сведения, сообщения, сигнал, обмен, появляется слово, отражающее действие — информировать, осведомлять, т.е. информация (сообщение) уже связано с процессом, а именно, с процессом передачи знаков, сигналов, сообщений» [8].

В практической деятельности менеджеры многих организаций сталкиваются со многими преградами, проблемами: техническими, организационными, финансовыми, психологическими. В этих условиях необходимы осознанные решения: с одной стороны, нельзя отказываться от проверенных традиционных технологий работы с информацией, а, с другой стороны, необходимо внедрять новые информационные системы и технологии в управлении организацией. Подходить к данному вопросу нужно с точки зрения системного и синергетического подходов.

Системный подход к информационному обеспечению менеджмента предполагает: во-первых, рассмотрение его как одного из элементов системы управления; во-вторых, оно само состоит из нескольких составных частей, каждая из которых относительно самостоятель-

Таблица 1. Примеры угроз информационной безопасности[1]

Направления обеспечения безопасности	Техногенные		Природные
	Преднамеренные	Случайные	
Контроль физического доступа	Бомбардировка	Сон вахтерши	Торнадо
Сохранность оборудования	Вандализм	Запыление	Шаровые молнии
Управление коммуникациями	Прослушивание сети	Флуктуации в сети	Магнитные бури
Защита информационных хранилищ	Взлом парольной системы	Сбой криптосредств	Грибки
Управление непрерывностью деятельности	Последствие DOS-атаки	Последствия тестов на проникновения	Карстовые процессы
Соответствие законодательству	Компьютерное пиратство	Тиражирование персональных данных	Природные пожары

ная и имеет свои закономерности развития; в-третьих, информационное обеспечение рассматривается как динамичная система, находящаяся в постоянном развитии, причем скорость изменения отдельных составляющих может быть различна.

Таким образом, система информационного обеспечения — это совокупность данных о целях, состоянии, направлениях развития объекта и окружающей его среды, организованная во взаимосвязанных потоках сведений. Система, включающая в себя методы получения, хранения, поиска, обработки данных и выдачи их пользователю для возможностей реализации управленческих функций и наиболее полного удовлетворения потребностей менеджеров всех уровней управления в информации, позволяющей разработать, принять и реализовать выполнение оптимальных решений, которые обеспечивают достижение главных целей организации.

Здесь отметим, что эффективная реализация основных управленческих функций (планирование, организация, мотивация и контроль), а тем более дополнительных функций (связующие процессы: коммуникация) предъявляет особые требования к управленческим информационным системам (УИС). И деятельность, связанная с информационным обеспечением процесса принятия управленческих решений на предприятиях и в организациях, на которых она осуществляется «по старинке», и традиционными способами, приводит к информационному дефициту, тем самым создает проблемы в достижении главных целей хозяйствующих субъектов. Именно, на данном этапе проблемы информационного обеспечения менеджмента связаны не столько с поиском нужной информации, сколько с ее качеством — достоверностью, обоснованностью и объемом.

Здесь необходимо отметить информационное обеспечение работы предприятия неразрывно связано с обеспечением информационной безопасности предприятия.

Данный факт обусловлен тем, что любая конфиденциальная для бизнеса информация входит в сферу повышенного интереса конкурирующих компаний. Для недобросовестных конкурентов, коррупционеров и других злоумышленников особый интерес представляет информация о составе менеджмента предприятий, их статусе и деятельности фирмы. Доступ к конфиденциальной информации и ее изменение могут нанести существенный урон финансовому положению компании. Причиной утечки информации, если отсутствует должное обеспечение информационной безопасности организации, могут быть различные случайности, вызванные неопытностью сотрудников.

Под информационной безопасностью (ИБ) обычно понимают состояние (свойство) защищенности ресурсов информационной системы в условиях наличия угроз в информационной сфере. Защита информации — это процесс, направленный на обеспечение информационной безопасности. [1]

Информационная безопасность предполагает обеспечение защиты данных от хищений или изменений как случайного, так и умышленного характера. Система

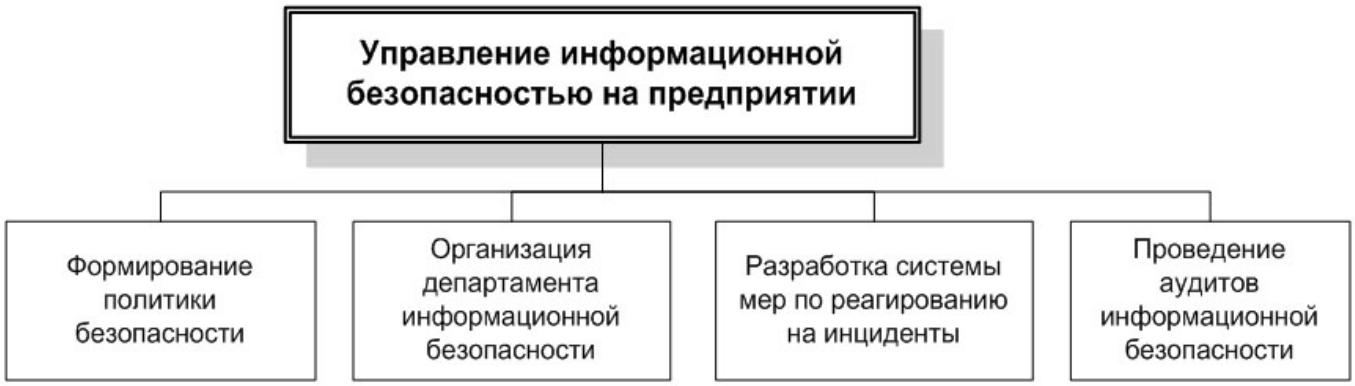

Рис. 1. Структура организационной деятельности в сфере информационной безопасности на предприятии (Составлено автором)

обеспечения информационной безопасности организации — эффективный инструмент защиты интересов собственников и пользователей информации.

Система управления информационной безопасностью (Information Security Management System) является частью общей системы управления, базирующейся на анализе рисков и предназначенной для проектирования, реализации, контроля, сопровождения и совершенствования мер в области информационной безопасности. Систему составляют организационные структуры, политика, действия по планированию, обязанности, процедуры, процессы и ресурсы.

Основная цель обеспечения комплексной системы безопасности информации для защиты предприятия должна представлять собой следующее:

- Создать благоприятные условия для нормального функционирования в условиях нестабильной среды;
- Обеспечить защиту собственной безопасности;
- Возможность на законную защиту собственных интересов от противоправных действий конкурентов;
- Обеспечить сотруднику сохранностью жизни и здоровья.
- Предотвращать возможность материального и финансового хищения, искажения, разглашения и утечки конфиденциальной информации, растраты, производственные нарушения, уничтожение имущества и обеспечить нормальную производственную деятельность.

Качественная безопасность информации для специалистов — это система мер, которая обеспечивает:

- Защиту от противоправных действий;
- Соблюдение законов во избежание правового наказания и наложения санкций;
- Защиту от криминальных действий конкурентов;
- Защиту от недобросовестности сотрудников.

Эти меры применяются в следующих сферах:

- Производственной (для сбережения материальных ценностей);
- Коммерческой (для оценки партнерских отношений и правовой защиты личных интересов);
- Информационной (для определения ценности полученной информации, ее дальнейшего использования и передачи, как дополнительный способ от хищения);
- Для обеспечения предприятия квалифицированными кадрами.

Обеспечение безопасности информации любого коммерческого предприятия основывается на следующих критериях:

- Соблюдение конфиденциальности и защита интеллектуальной собственности;
- Предоставление физической охраны для персонала предприятия;
- Защита и сохранность имущественных ценностей.

При создавшейся за последние годы на отечественном рынке обстановке рассчитывать на качественную защиту личных и жизненно важных интересов можно только при условии:

- Организации процесса, ориентированного на лишение какой-либо возможности в получении конкурентом ценной информации о намерениях предприятия, о торговых и производственных возможностях, способствующих развитие и осуществление поставленных предприятием целей и задач;
- Привлечение к процессу по защите и безопасности всего персонала, а не только службы безопасности.

Далее сформулируем рекомендации для формирования надежной и эффективной системы информационной безопасности предприятия:

- Все используемые средства для защиты информационной безопасности должны быть доступными для пользователей и простыми для технического обслуживания.
- Каждого пользователя, имеющего доступ к конфиденциальной информации предприятия, нужно обеспечить минимальными полномочиями, необходимыми для выполнения конкретной работы.
- Система защиты информационной безопасности должна быть максимально автономной.
- Необходимо предусмотреть возможность отключения защитных механизмов в ситуациях, когда они являются помехой для выполнения работ (обслуживание информационных серверов, персональных компьютеров и иных электронно-вычислительных средств, связанных с обработкой и передачей информации в электронном виде[9]).
- Разработчики системы информационной безопасности должны учитывать максимальную степень враждебности окружения, то есть предполагать самые наихудшие намерения со стороны злоумышленников и возможность обойти все защитные механизмы предприятия[9].
- Наличие и место расположение защитных механизмов должно быть конфиденциальной информацией.

Таким образом, сделаем вывод о том, что система обеспечения информационной безопасности организации рассматривается как целый комплекс принятых управленческих решений, направленных на выявление и предотвращение внешних и внутренних угроз.

Эффективность принятых мер основывается на определении таких факторов, как степень и характер угрозы, аналитическая оценка кризисной ситуации и рассматривание других неблагоприятных моментов, представляющих опасность для развития предприятия и достижения поставленных целей. Обеспечение информационной безопасности организации должно основываться на принятии таких мер, как:

- Анализ потенциальных и реальных ситуаций, представляющих угрозу безопасности информации предприятия;
- Оценка характера угроз безопасности информации;
- Принятие и комплексное распределение мер для определения угрозы;
- Реализация принятых мер по предотвращению угрозы.

ЛИТЕРАТУРА

1. Дорофеев Александр Владимирович, Марков Алексей Сергеевич, Менеджмент информационной безопасности: основные концепции (Information security management: basic concepts) Вопросы кибербезопасности № 1(2) — 2014
2. Емельянова Н. З. Защита информации в персональном компьютере: Учебное пособие / Н. З. Емельянова, Т. Л. Партыка, И. И. Попов. — М.: Форум, 2013. — 368 с.
3. Ефремова Т. Ф. Современный словарь русского языка три в одном: орфографический, словообразовательный, морфемный: около 20000 слов, около 1200 словообразовательных единиц. — М.: АСТ, 2010. — 699 с. — ISBN978–5–17–069855–4.
4. Жук А. П. Защита информации: Учебное пособие / А. П. Жук, Е. П. Жук, О. М. Лепешкин, А. И. Тимошкин. — М.: ИЦ РИОР, НИЦ ИНФРА-М, 2013. — 392 с.
5. Ищейнов В. Я. Защита конфиденциальной информации: Учебное пособие / В. Я. Ищейнов, М. В. Мецатунян. — М.: Форум, 2013. — 256 с.
6. Малюк А. А. Защита информации в информационном обществе: Учебное пособие для вузов / А. А. Малюк. — М.: ГЛТ, 2015. — 230 с.
7. Ожегов С. И., Шведова Н. Ю. Толковый словарь русского языка: 80000 слов и фразеологических выражений / Российская академия наук. Институт русского языка им. В. В. Виноградова. — 4-е изд., дополненное. — М.: Азбуковник, 1999. — 944 с. — ISBN5–89285–003-X.
8. Толковый словарь русского языка: в 4 т. / гл. ред. Б. М. Волин, Д. Н. Ушаков (т. 2–4); сост. Г. О. Винокур, Б. А. Ларин, С. И. Ожегов, Б. В. Томашевский, Д. Н. Ушаков; под ред. Д. Н. Ушакова. — М.: Государственный институт «Советская энциклопедия» (т. 1): ОГИЗ (т. 1): Государственное издательство иностранных и национальных словарей (т. 2–4), 1935–1940. (2-е издание словаря вышло в 1947–1948 годах.) Словарь содержит 85289 слов.
9. Хорев П. Б. Программно-аппаратная защита информации: Учебное пособие / П. Б. Хорев. — М.: Форум, 2013. — 352 с.
10. Шаньгин В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — М.: ДМК, 2014. — 702 с.
11. Шаньгин В. Ф. Комплексная защита информации в корпоративных системах: Учебное пособие / В. Ф. Шаньгин. — М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2013. — 592 с.

Журнал «Современная наука: актуальные проблемы теории и практики»