Научный руководитель: Сотникова Анна Николаевна

к.г.н., преподаватель ФСПО НАН ЧОУ ВО Академии ИМСИТ

Волошина Екатерина Васильевна

студент 18-СПО-Ф 01 НАН ЧОУ ВО Академии ИМСИТ

ОСНОВНЫЕ ПРОБЛЕМЫ РОССИЙСКИХ ПРЕДПРИЯТИЙ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Под информационной безопасностью понимают состояние защищенности информационной среды, обеспечивающее ее формирование и развитие [4,с. 73]

Предприятиям управление не может эффективно проводиться без достаточной оперативной, надежной, своевременной и достоверной информации. Информация является основой управленческого процесса, и от того, насколько она совершенна, во многом зависит качество управления предприятием. Информационная деятельность менеджера требует от него четкой организации процесса сбора, анализа и обработки информации, причем он должен уметь определять важность или второстепенность поступающей информации. Опытный менеджер также должен уметь упорядочивать коммуникации и обмен информацией в рамках предприятия и фирмы.

Управляющая система получает от управляемой системы информацию о состоянии заданных ею технико-экономических параметров в процессе производственной и финансово-хозяйственной деятельности. На основе полученной информации управляющая система (менеджмент) вырабатывает команды управления и передает их в управляемую систему для исполнения. Информация, которая функционирует на предприятии в процессе управления, может быть классифицирована следующим образом:

- по форме отображения (визуальная, аудиовизуальная и смешанная);

- по форме представления (цифровая, буквенная, кодированная);

- по роли в процессе управления (аналитическая, прогнозная, отчетная, научная, нормативная)

- по качеству (достоверная, вероятностно достоверная, недостоверная, ложная);

- по возможности использования (необходимая, достаточная, избыточная);

- по степени обновляемое (постоянная, переменная);

- по степени деятельности предприятия (экономическая, управленческая, социальная, технологическая);

- по источнику возникновения (внутриорганизационная, внешняя);

- по степени преобразования (первичная, производная, обобщенная);

- по виду носителя (печатный текст, микрофильм, кинофильм, видеофильм, машинный носитель);

- по времени поступления (периодическая, постоянная, эпизодическая, случайная) [2, с. 75].

Из вышеизложенного следует, что информационная безопасность предприятия неразрывно связана с формами управления предприятия.

В условиях постоянного роста количества известных и появления новых видов информационных угроз перед крупными предприятиями всё чаще встаёт задача обеспечения надёжной защиты корпоративных сетей от вредоносных программ и сетевых атак.

Работа с информацией в современных условиях отличается не только массивом и многообразием ресурсов, постоянным обновлением технологий ее обработки, повышенным вниманием и контролем над персоналом, но и грамотным уровнем управления фирмой.

Известно, что процесс массового внедрения компьютерной техники и информационных технологий наряду с прогрессивным началом неизбежно создает и дополнительные проблемы. Они связаны с реальными угрозами безопасности предприятий, с потерей стратегически важной информации, а вместе с этим и утратой управляемости компании.

В целях сокращения побочных явлений повсеместного использования новых информационных технологий руководство организаций определяет стратегию своей деятельности в информационной сфере. Стержневым началом такой стратегии должна быть информационная безопасность, определяемая как состояние защищенности интересов предприятий или организации в информационной сфере. Все направления деятельности предприятия, в которых прямо или косвенно используются информационные технологии, фокусируются в рамках обеспечения информационной безопасности.

Как показывает международная практика, основная проблема в сфере обеспечения информационной безопасности заключается в создании единого эффективного механизма, который позволял бы своевременно применять на практике нормативно-правовые, законодательные акты, отвечающие существующим социально-политическим и экономическим условиям и достижениям в области информационных технологий. Развитие технологий, сферы информатизации делает актуальным вопрос обеспечения информационной безопасности.

Проблема обеспечения информационной безопасности имеет две составляющие - технологическую и идеологическую. Первая - связана с

разработкой и внедрением информационных ресурсов, системы защиты информационных баз, вторая - с распространением информации, ее воздействием на жизнь личности, общества, государства.

Практически любая новая технология влечет за собой социально-экономические изменения в обществе, влияет на международные отношения. На сегодняшний день можно говорить о создании общемирового информационного пространства. Информация, информационные технологии характеризуются такими свойствами как трансграничность, проницаемость, имеют возможность повсеместного использования, становятся доступными вне зависимости от национальных границ.

Под угрозами информации принято понимать потенциальные или реально возможные действия по отношению к информационным ресурсам, приводящие к неправомерному овладению охраняемыми сведениями.

Такими действиями являются:

- ознакомление с информацией различными путями и способами без нарушения ее целостности;

- модификация информации в криминальных целях как частичное или значительное изменение состава и содержания сведений;

- разрушение (уничтожение) информации как акт вандализма с целью прямого нанесения материального ущерба.

В конечном итоге противоправные действия с информацией приводят к нарушению ее конфиденциальности, полноты, достоверности и доступности, что в свою очередь приводит к нарушению, как режима управления, так и его качества в условиях ложной или неполной информации. Каждая угроза влечет за собой определенный ущерб - моральный или материальный, а защита и противодействие угрозе призвано снизить его величину, в идеале - полностью,

реально - значительно или хотя бы частично. Но и это удается далеко не всегда [7, с. 65].

В общем, факт получения охраняемых сведений злоумышленниками или конкурентами называют утечкой. Однако одновременно с этим в значительной части законодательных актов, законов, кодексов, официальных материалов используются и такие понятия, как разглашение сведений и несанкционированный доступ к конфиденциальной информации [1, с. 89].

Разглашение - это умышленные или неосторожные действия с конфиденциальными сведениями, приведшие к ознакомлению с ними лиц, не допущенных к ним. Разглашение выражается в сообщении, передаче, предоставлении, пересылке, опубликовании, утере и в других формах обмена и действий с деловой и научной информацией.

Несанкционированный доступ - это противоправное преднамеренное овладение конфиденциальной информацией лицом, не имеющим права доступа к охраняемым секретам. Несанкционированный доступ к источникам конфиденциальной информации реализуется различными способами: от инициативного сотрудничества, выражающегося в активном стремлении "продать" секреты, до использования различных средств проникновения к коммерческим секретам. Для реализации этих действий злоумышленнику приходится часто проникать на объект или создавать вблизи него специальные посты контроля и наблюдения - стационарных или в подвижном варианте, оборудованных самыми современными техническими средствами.

Если исходить из комплексного подхода к обеспечению информационной безопасности, то такое деление ориентирует на защиту информации как от разглашения, так и от утечки по техническим каналам и от несанкционированного доступа к ней со стороны конкурентов и злоумышленников. Такой подход к классификации действий, способствующих

неправомерному овладению конфиденциальной информацией, показывает многогранность угроз и многоаспектность защитных мероприятий, необходимых для обеспечения комплексной информационной безопасности.

А так же рассматривается отсутствие высокой трудовой дисциплины, психологическая несовместимость, случайный подбор кадров, слабая работа кадров по сплочению коллектива.

Финансовое же подавление включает такие понятия, как инфляция, бюджетный дефицит, коррупция, хищение финансов, мошенничество; психическое давление может выражаться в виде хулиганских выходок, угрозы и шантажа, энергоинформационного воздействия.

Основными угрозами информации являются ее разглашение, утечка и несанкционированный доступ к ее источникам. Каждому из условий неправомерного овладения конфиденциальной информацией можно поставить в соответствие определенные каналы, определенные способы защитных действий и определенные классы средств защиты или противодействия.

Из вышесказанного следует, что информационная безопасность предприятия - это состояние защищённости корпоративных данных, при которой обеспечивается их конфиденциальность, целостность, аутентичность и доступность. Обеспечение информационной безопасности предприятия возможно только при системном и комплексном подходе к защите.

Основные проблемы и пути их решения в области информационной безопасности должны учитываться не только актуальные компьютерные угрозы и уязвимости, но и человеческий фактор персонала предприятий..

Список используемой литературы

1. Информационные технологии в профессиональной деятельности: Учеб. пособие. - М.: Проспект, 2014. - 448 с.

2. Новые информационные коммуникационные технологии в образовании / В.А. Трайнев, В.Ю. Теплышев, И.В. Трайнев. - 2-е изд. - М.: Издат.-торговая корпорация Дашков и К, 2014. - 320 с.

3. Федеральный закон «Об участии в международном информационном обмене» от 04.07.1996 г. №85-ФЗ.

4. Волоткин А.В., Маношкин А.П. Информационная безопасность. М.: НТЦ «ФИОРД-ИНФО», 2016. - 235 с.

5. Управление персоналом современной организации / Под ред. Шекшня С.В. -М.: Интел-Синтез, 2013 - 368с.

6. Управление персоналом организации. Под ред. Кибанова А.Я., - 3-е изд., доп. и перераб. - М.: ИНФРА-М, 2014. - 238 с.

7. Родичев Ю.А. Информационная безопасность. Учебное пособие - М.: Академия, 2015. - 356 с.