УДК 657

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В БУХГАЛТЕРСКОМ УЧЕТЕ

Абакарова А.А. , студентка 4 курса,

кафедры бухгалтерского учета»

Научный руководитель:

Раджабова М.Г., к.э.н., ст. преподаватель

кафедры «Бухгалтерский учет»

ФГБОУ ВПО «Дагестанский государственный университет»

aroma20008@rambler.ru

Россия, Махачкала

В современных условиях развития нашего общества важнейшим ресурсом развития стала информация - единственный продукт не убывающий, а растущий со временем. Информация сегодня - главный ресурс научно-технического и социально-экономического развития и чем больше и быстрее внедряется качественной информации в хозяйственной деятельности, тем выше уровень развития и потенциала для дальнейшего развития.

Любая предпринимательская деятельность в настоящее время невозможна без получения, накопления, хранения, обработки и использования разнообразных информационных потоков. И сегодня возникает масса проблем, связанных с обеспечением сохранности коммерческой (предпринимательской) информации как вида интеллектуальной собственности. В связи с этим все большее значение имеет организация эффективной системы информационной безопасности.

Под информационной безопасностью понимают меры по защите информации от неавторизованного доступа, разрушения, модификации, раскрытия и задержек в доступе [1]. Информационная безопасность - защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера,

которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры. [2, с. 20].

«Доктрина информационной безопасности РФ», принятая в 2000г. подтверждает актуальность данной проблемы на государственном уровне. Как в ней указывается: «Воздействию угроз информационной безопасности РФ в сфере экономики наиболее подвержены:

- системы бухгалтерского учета предприятий…независимо от формы собственности;
- системы сбора, обработки, хранения и передачи финансовой, биржевой, налоговой, таможенной информации …».

Как видно основным объектом экономической и информационной безопасности предприятия является информация бухгалтерская. Сегодня одним из основных факторов жизнеспособности любого бизнеса стало построение современной и эффективной бухгалтерской информационной системы, которая гарантирует экономическую и информационную безопасность предприятия.

Обеспечение информационной безопасности предприятия предполагает создание таких условий, при которых использование, потеря или искажение любой информации о состоянии предприятия, в том числе бухгалтерской финансовой, работниками предприятия или внешними пользователями с высокой степенью вероятности не приведут в будущем к возникновению угроз прерывания деятельности предприятия.

Можно выделить два основных вида угроз информационной безопасности:

1. случайные или непреднамеренные действия, выражающиеся в неправильной поддержке механизмов защиты и ошибками в управлении (например ни о какой защите информации не может быть и речи, если пользователи пишут пароли на бумажках и приклеивают их к мониторам,).

2. преднамеренные действия - несанкционированное получение

информации и несанкционированная манипуляция данными, ресурсами и самими информационными системами (например, попадание накопителей на жестких (оптических) дисках и магнитных лентах в руки посторонних лиц часто приводит к утечке конфиденциальной информации).

С одной стороны, информационная безопасность выступает как техническая проблема, решением которой должны заниматься специалисты в области информационных технологий. С их помощью можно обеспечить защиту информации от кражи и уничтожения. С другой стороны, данная проблема носит и управленческий характер, поскольку внедрение только технических решений не гарантирует полноту защиты информации на предприятии. Достичь приемлемого уровня экономической безопасности невозможно без соблюдения сотрудниками организации правил работы с информацией. Процесс обеспечения безопасности информационных систем, в том числе бухгалтерской, должен касаться всех сотрудников предприятия: руководство, бухгалтерию, ИТ-специалистов, руководителей технических служб и т. д.

В отношении технических средств защиты информации выделяют следующие компоненты:

• средства защиты от вирусов с использованием специализированных комплексов антивирусной профилактики;

• средства разграничения доступа к информационным ресурсам, а также защита от не санкционированного доступа к информации с использованием технологии токенов (смарт - карты, touch-memory, ключи для USB-портов и т.п.);

• средства обеспечения надежного хранения информации с использованием технологии защиты на файловом уровне (кодирование файлов и каталогов);

• средства защиты от внешних угроз при подключении к общедоступным сетям связи (например: Internet);

• средства обеспечения централизованного управления системой информационной безопасности в соответствии с согласованной и утвержденной

политикой безопасности [3].

Если рассматривать проблему обеспечения информационной безопасности с управленческой точки зрения, необходимо отметить следующее.

Предприятие является владельцем бухгалтерской информации, содержащей коммерческую тайну, поэтому должен быть определен перечень лиц, которые могут обладать, распоряжаться, определить правила обработки, а также ставить другие условия по сохранению коммерческой тайны. При условии соблюдения необходимых мер организации бухгалтерского учета собственник имеет право на юридическую защиту данных, что позволит повысить ответственность учетного персонала и сохранить активы предприятия, которые ему принадлежат.

Прежде всего, нужно определить перечень бухгалтерской информации, составляющей коммерческую тайну предприятия, а также разработать внутренние распорядительные документы в части защиты бухгалтерской информации, среди которых выделяют следующие: должностные инструкции бухгалтеров, соглашение о неразглашении информации, составляющих коммерческую тайну. Это позволит обеспечить соблюдение экономической безопасности предприятия внедрить на предприятии систему коммерческой тайны, содержит в себе механизм защиты бухгалтерской информации.

Важную роль в данной проблеме играет также защита от некачественной информации, которая поступает на предприятие извне. В результате информационной атаки, спланированной конкурентами, руководство предприятия получает недостоверную информацию о реальном состоянии дел. Дальнейшее использование этой информации для целей управления может привести к принятию ошибочных решений.

Особую актуальность приобрели проблемы защиты в интернете достоверности бухгалтерской отчетности предприятий. Согласно данным зарубежных исследований, наибольшую угрозу достоверности бухгалтерской отчетности организаций представляют:

1. внесение злоумышленниками изменений в отчетность, размещенную на сайте организации

2. умышленное искажение и последующее распространение данных отчетности в интернете;

3. создание липовых сайтов компаний и размещение на них недостоверной бухгалтерской информации и др.

Инструменты (методы, механизмы) защиты зависят от множества факторов, начиная от рода деятельности предприятия и территориального расположения, заканчивая количеством персонала на предприятия и сложившимся отношением к информационной безопасности внутри предприятия.

Исходя из вышеизложенного, каждому предприятию необходимо разрабатывать соответствующие методы и средства обеспечения информационной безопасности, связанные с:

- кадровой работой с персоналом;
- совершенствованием системы аутентификации пользователей;
- защитой информации внутри (при пересылке и хранении);
- разработкой эффективной системы защиты от внутренних угроз.

Кадровая работа с персоналом заключается, с одной стороны, в обеспечении физической безопасности работников, охране помещения и документов, разъяснительной работе, а с другой - в обеспечении строгого надзора за действиями персонала. При приеме на работу необходима проверка персонала совместно отделами безопасности и кадров. Необходимо проводить собеседования, тестирование для выявления личностных характеристик и наклонностей, а также проверять предыдущие места работ, для «наведения справок» по своим источникам информации.

Эффективная система защиты от внутренних угроз связана с грамотной пользовательской политикой внутри корпоративной (компьютерной) сети направленной на разграничение прав и уровня доступа к отдельным видам

информации, особенно к той, которая представляет коммерческую тайну, к клиентской базе данных (которая сегодня является важным ресурсом предприятия), к финансово-бухгалтерской информации и т.д. Грамотная защита всего перечисленного поможет избежать многих неприятностей.

Должен быть обеспечен постоянный контроль. Это не должна быть тотальная слежка за всем и вся, но персонал должен понимать, что его действия отслеживаются. Необходимо применять различные средства мониторинга сетевого трафика, анализа сетевой активности. Камеры видеонаблюдения и фиксация телефонных звонков оказывают тоже очень положительный эффект в плане защиты. Так как понимание персонала того, что любое их действие фиксируется, заставляет по-другому относиться не только к вопросам безопасности, но и к эффективности работы на протяжении всего рабочего дня.

Список литературы:

1. Крошилин С., Медведева Е. Безопасность информационных ресурсов предприятия: выявление угроз и методы их устранения. [Электронный ресурс]: URL: http://www.aselibrary.ru/digital_resources/journal/irr/2009/number_5/number_5_4/number_5_4977/

2. Макаренко С.И. Информационная безопасность: учебное пособие для студентов вузов. Ставрополь: СФ МГГУ им. М. А. Шолохова, 2009. 372 с.

3. Малежин О.Б. Информационная безопасность. Комплексный подход. [Электронный ресурс]: URL: http://www.elvis.ru/upload/iblock/9e0/9e07a7b7da950291dcad9cf2b2689b13.pdf (дата обращения:27.11.2014).