УДК 331.45

© Игорь Алексеевич Тогунов
д-р мед. наук, доцент кафедры менеджмента,
Владимирский филиал РАНХиГС

© Валентин Владимирович Баганов
магистрант факультета управления, Владимирский филиал РАНХиГС

ИНСТРУМЕНТЫ ПРОТИВОДЕЙСТВИЯ УГРОЗАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ СО СТОРОНЫ СОБСТВЕННОГО ПЕРСОНАЛА

Tools to counter threats to information security of the organization from its own staff

Аннотация: *в настоящее время все большее внимание уделяется процессам, связанным с обеспечением должного уровня информационной безопасности. Именно поэтому в представленной статье проведен анализ актуального вопроса инструментов противодействия угрозам информационной безопасности организации со стороны собственного персонала.*

Annotation: *At present, more and more attention is paid to the processes related to ensuring an adequate level of information security. That is why the present article analyzes the current issue of tools to counter threats to the information security of the organization from its own staff.*

Ключевые слова: *персонал, информационная безопасность, угроза, организация, инструмент, данные.*

Keywords: *personnel, information security, threat, organization, instrument, data.*

Вместе с первыми прецедентами, связанными с утечками информации, возникло естественное желание человека обеспечить защиту собственных данных. В условиях рыночной конкуренции обеспечение информационной безопасности предприятия является едва ли не главной задачей для субъекта бизнеса. В список ключевых факторов развития компании помимо финансовых вопросов входит работа по повышению качества защиты информационных ресурсов [1].

Особое влияние на безопасное состояние информационной среды оказывает собственный персонал, так как он наиболее близок к каналам передачи и обмена данными. Существует несколько угроз информационной безопасности, в частности повышение угроз наблюдается при снижении контроля над персоналом, предоставлении больших свобод для принятия решений. Кроме того, вместе с повышением роли персонала в управлении компанией информационная безопасность бизнеса оказывается под угрозой.

Успешное функционирование организации в условиях рыночной экономики предполагает обеспечение эффективной системы мер безопасности, в том числе информационной. Экономика становится более информационно насыщенной, вопрос качественного доступа к информационным ресурсам выходит на одно из первых мест в конкурентной борьбе. Соответственно обеспечение информационной безопасности становится ключевым фактором достижения конкурентоспособности организации.

Возрастание роли угроз информационной безопасности со стороны собственного персонала в современных условиях обусловлено, с одной стороны, такими социальными тенденциями, как либерализация экономики и рынка труда; изменение сущности контроля за персоналом; повышение роли менеджмента персонала в управлении организацией; с другой стороны, в это время наблюдаются процессы усложнения труда, роли творчества и

инноваций, предоставление работникам свободы и автономии в принятии решений, что приводит к ослаблению возможности жесткого контроля за персоналом [2].

Итак, обеспечение информационной безопасности в рамках предприятия носит комплексный характер. Задача руководства – обеспечить сохранность информации и минимизировать ее потери при повреждении или получении к ней несанкционированного доступа. Чтобы минимизировать внутренние угрозы, связанные с утечкой информации, необходимо предпринять ряд мер. В частности, необходимо разработать комплекс организационных мероприятий в сфере обеспечения информационной безопасности. Это достигается через комплекс мер административного и ограничительного характера.

Нормативными документами организации должен быть предусмотрен список лиц, имеющих доступ к особо важной информации, от них должно быть получено обязательство по неразглашению информации. Кроме того, требуется предусмотреть контрольно-правовые меры. Они должны носить системный характер и контролировать соблюдение персоналом должностных инструкций и требований в них по вопросам взаимодействия с информационными базами. Распоряжениями и приказами должен быть ограничен круг лиц, имеющих доступ к конфиденциальной информации, использованы ключи доступа к информационным системам. Также должен быть внедрен в рамках модернизации программного обеспечения электронный журнал доступа к информационным базам. Данный журнал в автоматическом режиме регистрирует обращения персонала к информационным базам, идентифицирует пользователя и регистрирует действия, совершенные в информационных системах [3].

Нормативными документами компании должны регулироваться инструкции и предусматриваться новые меры по совершенствованию системы обеспечения информационной безопасности. Также рекомендуется прибегать к профилактическим мероприятиям, их цель сводится к формированию у персонала мотивов поведения. Сформированные мотивы должны побуждать персонал к беспрекословному выполнению требований, содержащихся в должностных инструкциях.

Профилактические меры должны сводиться к формированию в коллективе организации оптимального морально-нравственного состояния. Для обеспечения информационной безопасности организации должны быть проведены определенные инженерные работы. Комплекс инженерно-технических мероприятий позволяет осуществить кодирование информации для повышения безопасности передачи данных по каналам связи. Он же позволяет ограничить права доступа к информационным ресурсам. На этом этапе устанавливается тот или иной уровень доступа к информационным базам организации.

От всей информации, которая не нужна для выполнения служебных полномочий, работник ограждается. В качестве эффективного инструмента противодействия кражи информации со стороны персонала рассматривается кадровая работа. Для повышения информационной безопасности организации должны быть предусмотрены меры по совершенствованию качества работы отдела по подбору персонала. Должна быть внедрена система инструктажей. Цель данного мероприятия сводится к установлению запретов на определенные действия при получении доступа к информационным системам.

Для персонала должны быть предусмотрены обучающие занятия, их цель должна сводиться к формированию исчерпывающих навыков в вопросах обеспечения информационной безопасности. В рамках этой учебной программы сотрудники должны научиться чутко реагировать на потенциальные угрозы, тем самым повышая свою квалификацию. Повышению информационной безопасности организации способствует психологическая работа.

Для отслеживания качества работы персонала и предотвращения несанкционированного доступа к информационным системам на предприятии должна быть установлена система видеонаблюдения. Если в рамках предприятия случаются ситуации с выносом служебной информации за пределы организации, такие инциденты должны быть обнародованы. Чтобы исключить несанкционированный доступ к служебной информации, необходимо внедрить на предприятии надежную систему документооборота. При этом следует помнить о сложностях, связанных с внедрением системы электронного документооборота.

Эффективной работе с электронными данными должны быть обучены сотрудники, модернизированы каналы связи для передачи данных между разными подразделениями одной организации. Что касается правовой защиты информации организации, то она должна выстраиваться в рамках конституционных основ и гражданского права. При этом разработанные должностные инструкции не должны ущемлять права трудящихся и нарушать нормы уголовного законодательства. Организационно-правовые методы обеспечения защиты информации сводятся к введению ограничительных мер для доступа к информации.

Главная задача данных мероприятий – исключить несанкционированный доступ. Получение доступа к информации может быть направлено как на ее считывание, так и на повреждение. С целью предупреждения несанкционированного доступа к секретной информации необходимо обеспечить охрану информационных систем, передавать документы с курьерской службой. При передаче электронных документов по каналам связи требуется обеспечить идентификацию пользователя и регистрацию его действий с электронными документами [5].

Как правило, наиболее эффективным методом противодействия несанкционированному доступу является выпуск ЭЦП. Данные ключи должны храниться у ограниченного числа работников и использоваться для получения доступа к информационным системам. Таким образом, все описанные инструменты противодействия угрозам информационной безопасности организации со стороны собственного персонала подтвердили свою эффективность на практике и активно используются организациями для обеспечения безопасности информационной среды.

Список литературы

1. Водянова В. В. Экономическая безопасность. Системное представление. – М. : ГУУ, 2015.

2. Шипилов А. И., Шипилова О. А. Как обеспечить надежность персонала? // Управление персоналом. – 2016. – № 8.

3. Чумарин И. Г. Как сделать наем безопасным? // Кадры предприятия. – 2013. – № 9.

4. Курбанов Р. Формирование нравственности и морали государственных служащих в Российской Федерации // Власть. – 2015. – № 1.

5. Озерникова Т. Г. Мотивационное значение системы вознаграждений // Изв. Иркут. гос. экон. акад. – 2014. – № 1 (34).