Н. В. Гришина, М. В. Мецатунян, И. А. Русецкая

ВЛИЯНИЕ СОЦИАЛЬНО-ПСИХОЛОГИЧЕСКИХ АСПЕКТОВ НА ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СУБЪЕКТОВ ИНФОРМАЦИОННЫХ ОТНОШЕНИЙ

Данная статья — это результат очередного этапа исследований по теме «Построение и анализ модели взаимодействия субъектов информационных отношений в едином информационном конкурентном пространстве с целью обеспечения информационной безопасности», проводимого в рамках инициативного проекта, поддержанного Российский фондом фундаментальных исследований.

Рассмотрение информационного пространства с точки зрения взаимодействия субъектов информационных отношений приводит к представлению его в виде сложной системы процессов различной природы.

Проблемы обеспечения информационной безопасности субъектов информационных отношений должны рассматриваться как многосоставные, включающие в себя необходимый анализ целого ряда факторов, среди которых необходимо упомянуть следующие:

– организационно-правовая составляющая — ряд аспектов, позволяющих сформировать концепцию информационной безопасности каждого из субъектов, включенного в информационную среду, а также реализовать на базе этой концепции комплекс организационных мер как основу комплексной системы защиты информации и создать нормативно-методическую базу, обеспечивающую их реализацию;

– техническая составляющая — совокупность инженерно-технических, программно-аппаратных и иных технических мер, средств и ресурсов, позволяющих реализовать принятую предприятием концепцию информационной безопасности.

Целью данной статьи является рассмотрение социально-психологических факторов как базы организационно-правовой составляющей концепции информационной безопасности предприятия.

Реализацию поставленной цели исследования должно обеспечить решение задач, предусматривающих анализ требований, необходимых для создания:

– благоприятного психологического климата в коллективе предприятия, помогающего осуществлению политики информационной безопасности;

– системы мотивации, материального и морального поощрения сотрудников, которая может благоприятно повлиять на обеспечение информационной безопасности при взаимодействии субъектов информационных отношений;

– системы обучения и повышения компетентности специалистов области информационной безопасности, а также повышения информированности сотрудников в вопросах информационной безопасности и защиты информации.

Достижение целей деятельности субъекта информационных отношений осуществляется посредством совместной деятельности сотрудников. Для обеспечения необходимого уровня взаимодействия между всеми участниками информационных отношений необходимо координировать эту деятельность.

Внешние отношения охватывают связи партнеров, конкурентов, клиентов и других субъектов информационного пространства между собой, включая государственные правоохранительные, контролирующие и другие органы, предприятия и учреждения.

Внутренние отношения — это связи, возникающие в рамках конкретного субъекта информационных отношений, образующиеся с момента приема сотрудника на работу и определяющие организацию служебного и отчасти внеслужебного времени, выплату денежного содержания, установление льгот и гарантий, увольнение сотрудника, а также связи с данным предприятием

после увольнения. Эти внутренние отношения могут существенно влиять на состояние единой конкурентной информационной среды, в которой происходит взаимодействие субъектов.

Работа с персоналом подразумевает деятельность руководства организации и трудового коллектива, направленную на наиболее полное использование трудовых и творческих способностей каждого сотрудника, создание элементов корпоративной культуры, препятствующих возникновению желания нанести вред своей организации.

Человеческий фактор должен постоянно учитываться в долговременной стратегии функционирования каждого субъекта информационных отношений и в его текущей деятельности, являться основным элементом построения действенной и эффективной системы защиты информационных ресурсов.

Каждый сотрудник, работающий с конфиденциальной информацией, потенциально является или может стать в силу обстоятельств источником конфиденциальных сведений для конкурентов. Каждый из источников, особенно ставший им случайно, может быть опасным для фирмы при несанкционированном разглашении защищаемых сведений.

Несанкционированное использование информации происходит в значительном числе случаев в результате отсутствия должного уровня корпоративной культуры, безответственности и недостаточной обученности персонала.

От персонала информация легко переходит к злоумышленнику по следующим причинам [1]:

- слабого знания персоналом требований и правил защиты информации, неумения распознать злоумышленника и противодействовать его устремлениям;
- злостного невыполнения сотрудником правил;
- использования экстремальных ситуаций в помещениях организации и происшествий с персоналом: пожара (или инсценирования пожара), нападения, отключения электропитания в помещении организации и т. п.;
- ошибочных или безответственных действий персонала.

В корпоративную культуру организации как совокупность норм и правил поведения сотрудников в различных ситуациях должны быть внесены как положения, касающиеся поведения персонала при общении с представителями других субъектов единого конкурентного поля, так и пункты, определяющие поведение работников при столкновении со злонамеренными действиями конкурентов.

При этом обязательными принципами построения корпоративной культуры каждого из субъектов информационных отношений должны стать следующие:

– создание здорового психологического климата в коллективе фирмы;

– осознание каждым сотрудником важности соблюдения целей и норм обеспечения информационной безопасности;

– достаточный уровень подготовки в области защиты информации у всех сотрудников, работающих с конфиденциальной информацией;

– создание системы мотивации сотрудников;

– создание системы и практики контроля за соблюдением норм защиты информации;

– создание системы реагирования на нарушения в области режима конфиденциальности;

– создание системы ответственности персонала при утечке и утрате конфиденциальной информации.

Структурно здоровый психологический климат должен включать следующие основные элементы:

1. Изучение и анализ качеств сотрудников;

2. Создание условий для продвижения работников по службе, повышения заработной платы и других форм поощрения;

3. Организация обучения или переподготовки сотрудников;

4. Организация системы персональной ответственности за дисциплинарные нарушения, в том числе нарушения режима конфиденциальности;

5. Участие руководства в решении проблем сотрудников и урегулировании конфликтных ситуаций;

6. Поддержание духа единой компании и неформального общения между сотрудниками;

7. Привлечение подчиненных к формулированию идей, целей и выработке решений.

Одним из важнейших условий построения корпоративной культуры субъекта информационных отношений, как было указано выше, является создание грамотной системы мотивации сотрудников. Трудовая мотивация — побуждение человека к труду, являющееся результирующей системой внутренних побудительных элементов, таких как потребности, интересы, ценностные ориентации, с одной стороны, с другой — отражаемые и фиксируемые сознанием человека факторы внешней среды, так называемые внешние стимулы, побуждающие к трудовой деятельности [2]. Все эти элементы представляют собой сложную систему мотивов, под влиянием которых в сознании человека формируется как отношение к труду, так и программа трудового поведения.

В системе мер мотивации, как правило, принято выделять меры положительного и отрицательного стимулирования [3].

Меры положительного стимулирования призваны развивать позитивные качества сотрудников. Сущность такого рода мер сводится к применению различных форм морального и материального поощрения, связанных со стремлением вознаградить сотрудников за достижение конкретных результатов в работе.

Меры отрицательного стимулирования предполагают применение различных форм наказания, таких как критика, замечания, выговоры, предупреждения о неполном служебном соответствии, а также увольнение как крайняя мера дисциплинарного взыскания.

Можно выделить следующие перспективные направления исследований трудовой мотивации:

1. Изучение роли планирования как возможного мотивационного фактора труда.

2. Исследование роли образцов для подражания.

3. Исследование роли внешних и внутренних оценок трудовой деятельности.

4. Исследование вопроса о гласности заработной платы [4].

5. Определение баланса между мерами материального и морального поощрения.

6. Планирование и организация тренингов, позволяющих объединить сотрудников в команду и позволяющих сотрудникам службы безопасности предприятия и службы персонала изучить их личные и деловые характеристики, а также особенности их поведения в различных ситуациях.

7. Понимание сотрудником значимости своей трудовой деятельности, которая должна быть закреплена нормативными документами.

8. Индивидуальный подход к процессу мотивации для каждого сотрудника.

Текущая работа с персоналом, обладающим конфиденциальной информацией, помимо мотивации, подразумевает [1]:

– обучение и систематическое инструктирование работников;

– проведение регулярной воспитательной работы с персоналом, работающим с конфиденциальными сведениями и документами;

– постоянный контроль за выполнением персоналом требований по защите конфиденциальной информации;

– аналитическую работу по изучению степени осведомленности персонала в области конфиденциальных сведений;

– проведение служебных расследований по фактам утраты информации и нарушений персоналом требований по защите информации;

– совершенствование методики текущей работы с персоналом.

Обязательной составляющей текущей работы с персоналом должно стать обучение сотрудников правилам работы с конфиденциальной информацией, документами и базами данных, а также методике защиты информации в различных, в том числе экстремальных, ситуациях.

Процесс обучения сотрудников нормам информационной безопасности должен быть систематическим и регулярным, поскольку сама организация системы безопасности требует постоянного учета новых факторов, появление которых связано с изменениями информационного поля конкурентной среды.

Обучение работника должно начинаться с момента получения им допуска к работе с конфиденциальными сведениями и заканчиваться при увольнении. Обычная периодичность обучения для работающих сотрудников составляет раз в 3–5 лет, как правило, после аттестации или перезаключения контракта. Однако инструктажи и совещания должны проводиться по мере необходимости.

Задачами обучения должны являться:

1. Информирование о целях и принципах организации комплексной системы защиты информации, нормах и правилах защиты;

2. Информирование о потенциальных угрозах конфиденциальной информации, каналах и методах несанкционированного доступа к ней злоумышленников;

3. Обучение принципам работы сотрудников с конфиденциальными сведениями, документами и базами данных;

4. Обучение персонала действиям в чрезвычайных ситуациях, которые могут повлиять на состояние информационной безопасности.

Учебные занятия могут проводиться на базе специализированных учебных заведений, институтов повышения квалификации, а также с участием приглашенных специалистов.

Методика обучения включает [1]:

1. Наличие специализированных программ обучения для обеспечения лекционных курсов и практических занятий;

2. Проведение лекций, семинаров и собеседований как общего плана, так и по конкретным направлениям защиты;

3. Решение ситуационных задач, связанных с выполнением необходимых требований по защите конфиденциальной информации, изучение методов противодействия злоумышленнику;

4. Практическую ситуационную учебу по действиям персонала при общении со злоумышленником и в экстремальных ситуациях;

5. Проведение деловых игр, обучающих методам противодействия замыслам злоумышленника.

Важной особенностью обучения должен являться индивидуальный подход к подготовке каждого сотрудника, предполагающий получение им необходимых и достаточных знаний по указанной выше проблематике. Предоставление сотруднику излишней информации, не требующейся ему по роду выполняемой работы, может сыграть отрицательную роль в организации режима конфиденциальности субъекта информационных отношений.

Руководство и топ-менеджмент компании, другие сотрудники, владеющие инсайдерской информацией, а также лица, непосредственно участвующие в создании и разработке новой продукции или решений, должны обучаться отдельно от остальных сотрудников с учетом имеющегося у них большого объема важных конфиденциальных сведений.

Отдельным аспектом обучения работников, в основные служебные функции которых входит внешнее сотрудничество с другими субъектами информационной среды, должно стать информирование о возможных действиях конкурентной разведки этих субъектов и правилах защиты информации при проведении деловых переговоров, участии во внешних совещаниях и открытых мероприятиях и раскрытии информации о деятельности своей организации.

По окончании обучения должна проводиться проверка усвоения сотрудниками полученных знаний.

Наряду с обучением по мере необходимости должны проводиться также совещания-инструктажи по обеспечению информационной безопасности, в процессе которых до сотрудников должна быть доведена актуальная информация о положении дел в области информационной безопасности предприятия, новых факторах и возникающих угрозах безопасности, принятии руководством фирмы новых решений и внутренних документов в области обеспечения защиты информации.

Таким образом, системы мотивации, материального и морального поощрения сотрудников, обучения и повышения их компетентности в вопросах обеспечения информационной безопасности и создание благоприятного психологического климата каждого субъекта информационных отношений направлены на решение следующих проблем информационной безопасности при взаимодействии субъектов конкурентной среды:

– обеспечение каждого субъекта конкурентной среды информацией соответствующего качества;

– выявление сотрудников, которые могут при определенных условиях или обстоятельствах оказывать неблагоприятное влияние на положение субъекта информационной среды в конкурентном пространстве, и устранение этих обстоятельств и условий;

– выявление и нейтрализация исходящих от персонала угроз информационной безопасности субъекта информационных отношений;

– выявление факторов информационных рисков, исходящих от возможных действий сотрудников фирмы и возникающих при раскрытии и предоставлении информации о субъекте информационных отношений с целью организации открытого информационного пространства, налаживания информационных связей между субъектами и инвестиционной политики;

– выявление репутационных рисков для субъекта информационных отношений, которые могут возникнуть в результате ошибочных или несанкционированных действий сотрудников, их предупреждение, устранение и нейтрализация;

– обеспечение норм информационной безопасности при организации различных форм сотрудничества представителей субъектов единого информационного пространства;

– получение информации о конкурентах от сотрудников других фирм с использованием при этом методов легальной разведки;

– обнаружение и устранение попыток негативного воздействия на информационную среду со стороны сотрудников фирмы и конкурентов, а также анализ их причин и последствий.

Заключение

В результате проведенного анализа были сформулированы факторы, влияющие на уровень информационной безопасности субъекта информационных отношений, которые могут учитываться при построении модели взаимодействия субъектов информационных отношений. Степень влияния факторов в данной статье не анализировалась, да такая задача и не ставилась.

СПИСОК ЛИТЕРАТУРЫ:

1. *Корнеев И. К., Степанов Е. А.* Защита информации в офисе. М.: ТК Велби, Изд-во «Проспект», 2008. — 80 с.
2. Экономический словарь. URL: http://abc.informbureau.com.
3. *Стрельцов А. А.* Организационно-правовое обеспечение информационной безопасности: Учебное пособие для студентов вузов. М.: Издательский центр «Академия», 2008. — 256 с.
4. *Пряжников Н. С.* Психологический смысл труда. 3-е изд. М.: Изд-во Московского психолого-социального института, 2010. — 74 с.