УДК 331.5; 658.3

МЕТОДЫ РАБОТЫ С ПЕРСОНАЛОМ В РАМКАХ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Н.П. Лонцих[1], Е.П. Кунаков[2]
Иркутский национальный исследовательский технический университет,
664074, Россия, г. Иркутск, ул. Лермонтова, 83.
В статье затрагивается тема организации системы защиты информации и работы с персоналом в рамках системы защиты информации. Значительное внимание уделяется методам управления персоналом в рамках системы защиты информации. Особое внимание уделено устранению причины раскрытия защищаемой информации путем повышения мотивации персонала организации.
Ключевые слова: защита информации; система защиты информации; управление персоналом; методы управления персоналом; персонал.

TOOLS OF PERSONNEL POLICY WITHIN INFORMATION SECURITY SYSTEM
N. Lontsikh, E. Kunakov
Irkutsk National Research Technical University,
83 Lermontov Str., Irkutsk, Russia, 664074.
The article discusses the arrangement of information security systems and personnel policy in this field. The authors pay special attention to personnel management methods within the in-formation security system. They concentrate on removal of the causes of protected infor-mation disclosure by enhancing the motivation of the personnel.
Keywords: information security; information security system; personnel management; methods of personnel management; staff.

На сегодняшний день информация это наиболее ценный и ходовой объект в международных экономических отношениях. На международном уровне сформировалась система взглядов на информацию как на ценнейший ресурс жизнеобеспечения общества, имеющий социальное значение.

Информация, используемая в предпринимательской и иной деятельности весьма разнообразна. Вся эта информация представляет различную ценность для хозяйствующего субъекта и, соответственно, ее разглашение может привести к угрозам экономической безопасности различной степени тяжести.

В современном обществе неизбежность и целесообразность использования информационных технологий и глобальных коммуникаций влечет за собой неотвратимость угроз информационной безопасности.

Обеспечение информационной безопасности организации является одним из приоритетных направлений деятельности высшего руководства компании. Очевидно, что надежность защиты информации напрямую зависит от ее ценности. Для защиты информации компании требуется комплекс мер, образующих систему.

В рамках системы защиты информации в организации обычно используются следующие методы работы с персоналом [1]:

- обучение;
- инструктажи;
- индивидуальная и воспитательная работа;
- проверка уровня знаний;
- контроль.

Обучение – начальный этап работы с персоналом в приобретении теоретических знаний и практических навыков обеспечения защиты информации. Процесс обучения сотрудников предприятия должен быть постоянным и планомерным, так как система защиты информации предприятия развивается и совершенствуется за счет внедрения новых элементов.

Задачи обучения персонала предприятия включают изучение:

- нормативно-методических документов по защите информации;
- структуры, сил и средств системы защиты информации предприятия;

[1] Лонцих Наталья Павловна, кандидат педагогических наук, доцент, e-mail: palon@list.ru
Lontsikh Natalia, Candidate of Pedagogy, Associate Professor, e-mail: palon@list.ru
[2] Кунаков Егор Петрович, аспирант, e-mail: egor-kunakov@mail.ru
Kunakov Yegor, a postgraduate student, e-mail: egor-kunakov@mail.ru

• установленных норм и правил защиты информации на предприятии, а также стандартов предприятия, положений о службе безопасности (режимно-секретном отделе);

• возможных угроз защите информации, их характера и возможных способов проявления;

• порядка работы сотрудников предприятия с носителями информации с учетом установленных требований по режиму секретности [1].

В ходе обучения используются следующие инструменты:

• лекции, семинары и практические занятия;

• тестирование сотрудников и оценка уровня их подготовленности;

• решение различных ситуационных задач, связанных с защитой информации;

• решение интеллектуальных задач, направленных на получение сотрудниками предприятия навыков прогнозирования различных ситуаций;

• использование специализированных программ обучения.

Обучение персонала проводится раздельно в зависимости от занимаемой должности и, соответственно, доступу к информации — высшее руководство, их заместителей, начальники структурных подразделений, рядовые сотрудники предприятия. При выборе форм и методов обучения персонала учитывают уровень профессиональной подготовленности сотрудника, стаж работы по конкретной специальности, специфику решаемых им задач по защите информации и результатов контроля за деятельностью сотрудника по выполнению установленных требований защиты информации.

Инструктажи применяется для информирования сотрудников о положениях принятых нормативно-методических документов и требований вышестоящих органов государственной власти. Во время инструктажей особое внимание должно уделяться анализу практической работы по предотвращению возникновения угроз защиты информации.

Метод индивидуальной и воспитательной работы заключается в систематическом воздействии на процесс формирования и развития сотрудника в цепях наиболее полного обеспечения сохранности информации, с которой он сталкивается во время выполнения своих должностных обязанностей.

Цель проверки уровня знаний — с помощью оценки знания сотрудниками предприятия положений нормативно-методических и внутренних организационно-распорядительных документов определить степень подготовленности каждого сотрудника к выполнению практических задач по защите информации. Проверка уровня знаний проводится как руководством предприятия, так и сотрудниками режимно-секретного подразделения, службы безопасности, подразделения охраны.

Контроль в работе с персоналом предприятия применяется для оценки эффективности работы каждого сотрудника предприятия по обеспечению защиты информации. Контроль может быть периодическим (плановым) и внезапным. Проводится сотрудниками штатных подразделений предприятия, решающих задачи по организации защиты информации.

Основными формами контроля над сотрудниками в системе информационной безопасности можно выделить:

• проверки знаний и правильного соблюдения положений документов по защите информации;

• отчеты и доклады руководителей подразделений о результатах работы подчиненных;

• периодическая аттестация сотрудников, допущенных к защищаемой информации;

• самоконтроль сотрудников.

«Проблемный» персонал

Отдельно хотелось раскрыть такую группу в составе сотрудников организации как «проблемный» персонал. "Проблемным" с позиций обеспечения безопасности организации следует расценивать тот персонал, который может выступать потенциальным источником причинения ущерба компании. Типичной ошибкой является деление работников на тех, кто создает угрозы безопасности организации, и кто не представляет такого рода опасности, автоматически занося первых в разряд "проблемного" персонала.

Нередко встречаются попытки систематизации работников с позиций потенциальной опасности для организации. В числе критериев системы предлагают принимать во внимание: срок трудового договора, специфику работы, личные амбиции, конфликтный характер и т.п. В большей степени предлагаемые системы и критерии их классификации носят абстрактный, теоретический характер. Формирование категории "проблемного" персонала в основном зависит от конкретной ситуации, складывающейся в организации.

Высшее руководство должно обеспечить соответствующий социально-психологический климат внутри организации. Необходимо своевременно обращать внимание на следующие факторы:

• отсутствие действенной системы материальных стимулов;

• отсутствие гарантии долговременной занятости работников;

• отсутствие возможностей для карьерного роста;

- расстановка сотрудников без учета их способностей и желаний;
- отношение к сотрудникам как к простым исполнителям воли руководства;
- использование взысканий в качестве инструмента стимулирования работоспособности;
- психотравмирующая практика увольнений.

Стоит остановиться на некоторых группах работников, которые могут быть отнесены к числу потенциально опасных для безопасности компании. Формирование групп во многом обусловлено именно внутренними факторами, имеющими место в организации:

1. Повышено конфликтный персонал. Конфликты в организации всегда имели место. Однако больший риск заложен не столько в самом конфликте, сколько в его причинах. Далеко не всегда развитие конфликта осуществляется по схеме "начальник всегда прав". Золотое правило руководителя в таком случае, - признав ошибочность, несостоятельность своих решений, действий, предупредить развитие конфликта. Серьезную опасность в рассматриваемом аспекте несут те конфликты, которые оставляют "осадок" обиды, незаслуженного наказания со стороны руководителя. Такого рода работники, как правило, в большей степени восприимчивы к наказанию, в них значительно развито чувства повышенной несправедливости. Последний, независимо от его заслуг, способен из чувства мести (реже зависти, корысти) подорвать деятельность если не всей организации, то отдельного ее подразделения.

2. Подверженные воздействию. Здесь речь пойдет о людях с сильной внушаемостью, имеющими определенного рода зависимость. Именно значительная сила внушения и зависимости заставляет последних менять свои жизненные приоритеты, принципы, ценности.

3. Карьеристы. Для достижения поставленных целей эти лица могут не побрезговать никакими способами и средствами. Повышенную опасность представляют в том случае, если в силу занимаемого положения получают доступ к информации о персонале компании. Главная цель выбора методов - достижение цели выслужиться, завоевать более высокий социальный статус.

4. Недовольные (амбициозные). К данной группе относятся работники, обладающие довольно завышенной самооценкой, имеющие определенные знания, навыки, опыт, но которые в силу объективных (субъективных) причин не могут их реализовать на работе [2].

В таких случаях усматривается два варианта:

а) человек вырос из рамок своей должности, но его не пускают дальше;

б) человек не способен к дальнейшему росту, но жаждет всеобщего признания (почета, уважения, славы и т.п.).

В первом случае дело чаще всего заканчивается тем, что такой работник переходит на работу в иную фирму, не исключен вариант, что и к конкурентам. Во втором случае данный работник, используя складывающуюся ситуацию, обладая достаточной информацией о деятельности организации, не получая поощрения от руководства, может оказывать негласное содействие конкурентам.

В приведенный перечень могут быть также включены: работники, заключившие срочный трудовой договор и планирующие в ближайшее время его расторгнуть. Повышенное внимание следует обращать на руководящий состав организации. Последние имеют довольно большие информационные возможности. Также следует отметить лиц, работающих по совместительству, занимающихся научной, преподавательской или творческой деятельностью сверх основной работой. Они порой неосознанно могут переносить значимую для организации информацию от одного работодателя к другому.

Мотивация персонала, как один из значимых аспектов
в системе информационной безопасности

Особое место в деятельности высшего руководства предприятия и руководителей структурных подразделений по работе с персоналом занимают методы мотивации сотрудников, направленные на эффективное и качественное выполнение возложенных на них задач на фоне строгого соблюдения норм и правил защиты информации.

Мотивация действий сотрудников предприятия является основой общей организаторской и управленческой функции руководителя любого уровня. При отсутствии мотивации любая организационная, планирующая, координирующая и иная управленческая работа теряет всякий смысл. В самом общем виде мотивация — это процесс побуждения сотрудника предприятия к деятельности во имя достижения определенных целей с помощью внутриличностных и внешних факторов. В основе побуждения лежит совокупность потребностей, интересов, желаний, целевых установок, ценностных ориентации, ожиданий сотрудника [3].

Основные факторы, обусловливающие результативность труда персонала, — готовность, возможность и условия для результативной деятельности.

Готовность к добросовестному выполнению должностных обязанностей определяется тем, насколько сотрудник склонен их выполнять. Она основывается на мотивационных составляющих личности сотрудника, а именно:

- на уровне потребностей и интересов;
- целевых установках; ценностных ориентациях;
- желаниях; удовлетворенности работой;
- ожидании вознаграждения в зависимости от результатов труда и т. п.

Отзывы всего одного сотрудника могут хорошо сказаться как на мотивации других сотрудников, так и на повышении качества работы в целом.

Возможности сотрудника, позволяющие ему результативно выполнять его должностные обязанности и поставленные задачи, определяются как потенциал или совокупность его физиологических, интеллектуальных и профессиональных способностей.

Потенциал сотрудника зависит от уровня его знаний, образования, квалификации, возрастных данных, состояния здоровья, выносливости, энергии и т. п.

Условия представляют собой совокупность внешних стимулирующих факторов, влияющих на результативность труда персонала и находящихся вне его прямого контроля.

В целях построения эффективной системы мотивации персонала высшее руководство предприятия должно обеспечить:

- удовлетворение первичных потребностей персонала предприятия — физиологических, потребностей в безопасности и защищенности;
- условия для удовлетворения вторичных потребностей персонала — социальных потребностей в уважении и самовыражении.

Выделяют три основные группы методов мотивации: [3]

- методы непосредственной мотивации труда;
- методы властной, принудительной мотивации;
- методы стимулирования труда (морального, материального, трудового).

Методы непосредственной мотивации труда характеризуются прямым воздействием на личность сотрудника. К этой группе относятся методы убеждения, внушения и агитации.

Методы властной, принудительной мотивации основаны на реальном принуждении или потенциальной возможности применить принуждение: выполнении указаний, приказов, распоряжений и других директивных решений.

Методы стимулирования труда направлены на создание такой ситуации, которая побуждает сотрудника действовать определенным образом, и включают:

- моральное стимулирование — направлено на удовлетворение потребностей сотрудника в уважении и признании со стороны коллектива, к наиболее распространенным методам морального стимулирования относятся поощрения, награждение медалями, почетными знаками, присвоение почетных званий;
- материальное стимулирование — направлено на повышение уровня благосостояния персонала, реализуется в денежной форме (выплата премий, различных надбавок, повышение заработной платы, привлечение к участию в прибылях) и неденежной форме (выделение путевок на отдых, предоставление жилья, поездки за город и кемпинговые палатки);
- трудовое стимулирование — направлено на удовлетворение потребностей сотрудника в самовыражении и заключается в предоставлении ему возможности служебного роста, а также перевода (назначения) на должности, более соответствующие его реальным возможностям, способностям и интересам.

Мотивация сотрудников может быть достигнута тремя путями [3]:

- поощрение за выполнение правил;
- информирование персонала;
- наказание за нарушение;

Сочетание этих методов в совокупности приносит наибольший эффект, чем их использование по отдельности.

Поощрения являются самым эффективным средством мотивации сотрудников и (как и наказания) делятся на два основных вида – материальные и нематериальные.

В качестве денежного поощрения может выступать одноразовая премия - ежегодная или ежеквартальная. К видам материальной мотивации относятся те средства, которые сотрудник получает не напрямую – оплата мобильной связи, бесплатные обеды, клубные карты, полисы дополнительного медицинского страхования, компенсация проезда, обучение за счет фирмы, оплачиваемые отгулы или дополнительные дни к отпуску.

Однако материальное поощрение не всегда является рентабельным и эффективны, особенно в работе системы защиты информации. Поэтому целесообразно сочетать его с нематериальным. Не-

которые руководители скептически относятся к такому виду стимулирования, но если он тщательно продуман и грамотно внедрен, результативность может быть такой же высокой, как и при применении денежного поощрения.

Прежде чем вводить систему нематериальных поощрений, высшему руководству необходимо выяснить, как каждый конкретный работник позиционирует себя по отношению к организации, ее целям. Здесь возможны два варианта. Первый – сотрудник не считает себя частью организации и не отождествляет свои интересы с корпоративными, что может негативно сказаться как на работе сотрудника, так и на сохранности защищенных данных. Во втором случае работник ощущает себя полноценным членом команды и считает, что его труд – нечто большее, чем просто выполнение трудовых обязанностей, а также сотрудник осознает важность сохранения конфиденциальной информации и последствий ее разглашения для всей компании в целом.

Если имеет место первая «модель отношений» сотрудника и организация, то главной задачей нематериального стимулирования будет смещение приоритетов работника ко второй модели.

Рассмотрим информирование. Важным этапом информирования являются инструктажи, они могут быть вводными, дополнительными, периодическими. Вводные инструктажи нужны новым сотрудникам, приступающим к работе. Во многих случаях для дисциплинированных сотрудников достаточно грамотного вводного инструктажа, чтобы они выполняли необходимые правила довольно долгий период времени. По возможности вводный инструктаж нужно проводить очно или по телефону, бумажные и электронные материалы не так эффективны, но их также необходимо предоставлять для того, чтобы сотрудник при желании мог найти нужную информацию и при возникновении сомнений, правильно ли он поступает, обратиться к этим материалам. Очень важно, чтобы сама форма подачи инструктажа была доступной.

Дополнительные инструктажи проводятся в случае выявления нарушений. Можно инструктировать как конкретного человека, который был виноват в нарушении, так и группу сотрудников и даже весь коллектив в случае участившихся нарушений.

Кроме инструктажей, а также в дополнение к ним существует тестирование по результатам проведенного обучения. Во многих организациях проводят проверку знаний по охране труда и по результатам таких испытаний могут не допустить до работы. С точки зрения информационной безопасности, правильно организовать тестирование перед доступом сотрудника к работе с защищаемой информацией. Естественно, вопросы теста должны быть максимально направлены на практику. Вопросы должны быть простыми и относиться именно к рабочему процессу, а не к тому, какие выдержки из законодательства должен выучить сотрудник.

Очень часто в дополнение к инструктажам используются плакаты, памятки с правилами безопасности. Можно использовать информационную рассылку, проводить беседы с отдельными сотрудниками. Особое внимание стоит уделить информированию ключевых сотрудников: люди, которые имеют широкие полномочия, либо доступ к материальным ценностям и различным категориям конфиденциальной информации.

Нужно показывать сотрудникам, что информационная безопасность важна, хотя она и не приносит никакого дохода. Для повышения мотивации сотрудника работать эффективнее, можно показать, что от этого вырастет доход компании и, как следствие, его заработок. Мотивируя соблюдать правила безопасности, можно лишь показать, какие проблемы возникнут, если эти правила не соблюдать.

Наказание может быть различным, и стоит заметить, что очень важной мерой является предупреждение, особенно по отношению к небольшим нарушениям. Во многих случаях предупреждения достаточно, чтобы в последующем нарушение не повторялось. Сотрудники могут нарушать правила, даже не осознавая, что они делают что-то запрещенное, либо думая, что за ними никто не следит и соблюдение правил необязательно. Широко применяется методика показательных наказаний, ее эффективность обусловлена неформальным обменом информацией между сотрудниками. Наказав одного из сотрудников, вы предупреждаете всех остальных.

Наказание может быть различным, и стоит заметить, что очень важной мерой является предупреждение, особенно по отношению к небольшим нарушениям. Во многих случаях предупреждения достаточно, чтобы в последующем нарушение не повторялось. Сотрудники могут нарушать правила, даже не осознавая, что они делают что-то запрещенное, либо, думая, что за ними никто не следит и соблюдение правил необязательно. Широко применяется методика показательных наказаний, ее эффективность обусловлена неформальным обменом информацией между сотрудниками. Наказав одного из сотрудников, вы предупреждаете всех остальных. Распространять информацию о том, что сотрудник был наказан необязательно, «сарафанное радио» сделает это за вас.

Очень действенным наказанием является лишение каких-либо прав. Ни одному сотруднику не понравится оправдываться и доказывать, что он не виноват. К тому же объяснительные часто прохо-

дят через руководство организации и не способствуют повышению статуса сотрудника, могут повлиять на развитие его карьеры.

Также на территории РФ очень распространен метод воздействия основанный на материальных стимулах, например лишение премии. Лишение премии очень эффективно бывает в тех случаях, когда сотрудник заинтересован в том, чтобы дальше продолжать работать в организации. Такие сотрудники вынесут для себя урок и больше не повторят нарушения, в то время как недооцененные сотрудники, которые уже раздумывали об увольнении, укрепятся в своем решении уйти либо начнут производить злоумышленные действия сознательно и более изощренными способами.

На сегодняшний день у руководства большинства организаций не остается сомнений в необходимости серьезно заботиться об информационной безопасности. Здесь и необходимость сохранения информации, и обеспечение безопасности носителей. Современные информационные системы позволяют защитить данные компании от внешних злоумышленников. Однако большинство проблем информационной безопасности лежит внутри компании, а не за ее пределами. К одной из проблем отнесен персонал организации, который работает с информацией и ее носителями. В решении проблемы информационной безопасности значительное место занимает выбор эффективных методов работы с персоналом.

Библиографический список

1. Аверчиков В.И., Рытов М.Ю. Служба защиты информации – организация и управление: учеб. пособие для вузов. М. : ФЛИНТА, 2011. 186 с.

2. Погодина И.В. Если работник не умеет хранить деловые секреты // Трудовое право. 2009. № 10. С. 23–42.

3. Кибанов А.Я. Мотивация и стимулирование трудовой деятельности: учебник / А.Я. Кибанов [и др.]. М. : ИНФРА-М, 2010. 524 с.