УДК 005.95 + 004.056 Вестник УрФО № 3(21) / 2016, с. 38–46

Астахова Л. В., Овчинникова Л. О.

КАДРОВЫЕ ПРОБЛЕМЫ ПОСТРОЕНИЯ СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ НА ПРЕДПРИЯТИИ

В статье рассматриваются кадровые проблемы построения системы управления» информационной безопасностью (СУИБ) и приводятся способы их решения. Научная новизна статьи состоит в выявлении недооценки кадровых проблем в международных стандартах по управлению информационной безопасностью, обосновании системы управления мотивации сотрудников как части СУИБ, предложениях по внесению дополнений в ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности» на основе разработанной системы.

Ключевые слова: *информационная безопасность, система управления, функции управления, мотивация сотрудников*

Astakhova L. V., Ovchinnikova L. O.

PERSONNEL PROBLEMS OF CONSTRUCTION CONTROL SYSTEMS INFORMATION SAFETY AT THE ENTERPRISE

The article deals with personnel problems of building systems Management »Information Security (ISMS) and how they are solutions. The scientific novelty of this paper is to identify the underestimation of personnel problems in international standards for information management safety management system justification motivation of employees as a of the ISMS for amendment proposals to GOST R ISO / IEC 27002-2012 "Information technology. Methods and security features. vault standards and information security management rules "based on developed system.

Keywords: *information security management system functions management, employee motivation*

В современных условиях функционирования предприятий одной из важнейших задач является построение системы информационной безопасности (ИБ). При построении данной системы используются различные экономические ресурсы: финансовые, трудовые и т.д., ограниченность которых порождает актуальные кадровые проблемы реализации СУИБ, которые значительно снижают производительность и эффективность функционирования как самой системы, так и организации в целом. Этим обусловлена актуальность статьи, поскольку выявление и решение кадровых проблем – ключевая задача при построении СУИБ. Ее решение позволяет продуктивно распределять ресурсы предприятия, направленные на создание системы управления информационной безопасностью. В статье предложены эффективные методы решения кадровых проблем и минимизации их негативного влияния на работу предприятия.

Организация процесса управления безопасностью (Security Management) усложняется тем обстоятельством, что на предприятиях, помимо автоматизированных бизнес-процессов, существуют бизнес-процессы, не реализуемые на ЭВМ, но попадающие в сферу обеспечения информационной безопасности, например, процессы кадровой службы по найму персонала [3]. С.Э. Ковалев считал, что изначальной причиной сложившейся ситуации является решение управленческих задач при помощи только технических средств, что является недостаточным в плане реализации защиты информационной безопасности [4]. Для предотвращения угрозы информационной безопасности, связанной с людьми, необходима совокупность организационно-правовых и организационно-технических мероприятий, которые исключали бы (или сводили к минимуму) возможность возникновения опасности утечки, утраты или искажения информации ограниченного доступа.

При оценке критичности каждого информационного актива предприятия уделяется большое внимание персоналу. Тот факт, что более двух третей ущербов, имеющих злонамеренный характер, исходит от персонала предприятия, свидетельствует о том, что угрозы, исходящие от человека, должны быть дифференцированы в отдельный вид угроз безопасности информации – HR-угрозы, а уязвимости – в HR-уязвимости объектов защиты информации.

Л.В. Астахова в своей статье «Проблема оценки HR-уязвимости объекта защиты информации» утверждает, что проблема нормативной недооценки HR-угроз и уязвимостей связана, во-первых, с приоритетностью технических мер защиты информации, во-вторых, со сложностью формализации процессов работы с персоналом и, наконец, с неразработанностью методологических проблем организационной защиты информации [1].

На сегодня внутренний нарушитель занимает первое место среди основных угроз ИБ. Причиной этого является тот факт, что в большинстве организаций периметр контролируемой зоны защищен достаточно надежно, а сотрудники организации имеют непосредственный доступ к информационной системе для выполнения своих служебных обязанностей. Следовательно, технические средства защиты в гораздо меньшей степени обеспечивают безопасность информации от внутреннего нарушителя.

В ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности» (п.8) регламентируются правила и методы работы с персоналом, в целях обеспечения конфиденциальности, целостности и доступности информационных активов на предприятии. Для комплексного обеспечения безопасности, связанной с персоналом, принимаются организационные меры на всех трех стадиях взаимодействия человека с нанимающей его организацией: трудоустройства, занятости и увольнения.

Целью работы с сотрудниками во время трудоустройства является обеспечение уверенности в том, что сотрудники осознают свои обязанности и способны выполнять предусмотренные для них роли и снижение риска хищения, мошенничества или нецелевого использования средств обработки информации. Целью работы с сотрудниками во время занятости являются осведомление персонала об угрозах и проблемах, связанных с информационной безопасностью, о мере их ответственности и обязательствах, а также оснащение всем необходимым для поддержки политики безопасности организации, что снижает риск человеческого фактора. Целью работы с сотрудниками во время увольнения является обеспечение уверенности в том, что сотрудники покидают организацию или меняют занятость таким образом,

Таблица 1

Цели работы с сотрудниками на разных этапах взаимодействия с работодателем и соответствующие им нормативные документы

Цель	Нормативные документы
Во время трудоустройства	
Документальное определение и оформление ролей и обязанностей, которые должны быть определены и доведены до претендентов на работу до их трудоустройства.	• Приказ Минздравсоцразвития РФ от 22.04.2009 № 205. [7] • ГОСТ Р ИСО/МЭК 27002-2012. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности. (п. 5.1 Политика информационной безопасности). [2]
Предварительная тщательная проверка всех кандидатов.	• ГОСТ Р ИСО 19011-2012. Руководящие указания по аудиту систем менеджмента (п. 7 Компетентность и оценка аудиторов). [5]
Согласование и подписание трудового договора.	• Ст. 16 ТК РФ. Основания возникновения трудовых отношений. [6] • Ст. 57 ТК РФ. Содержание трудового договора. [6]
Во время занятости	
Регистрация обязанностей руководства.	• ГОСТ Р ИСО 19011-2012. Руководящие указания по аудиту систем менеджмента. (п.7 «Компетентность и оценка аудиторов»). [5]
Осуществление формального дисциплинарного процесса, применяемый в отношении сотрудников, совершивших нарушение безопасности.	• Федеральный закон от 29.07.2004 N 98-ФЗ (ред. от 12.03.2014) "О коммерческой тайне" (статья 14. Ответственность за нарушение настоящего ФЗ). [13] • Федеральный закон от 27.07.2010 N 224-ФЗ (ред. от 21.07.2014) "О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации" (статья 11. Меры по предотвращению, выявлению и пресечению неправомерного использования инсайдерской информации и (или) манипулирования рынком)[19]
Во время увольнения	
Прекращение трудового взаимодействия между работником и работодателем.	• Ст. 81 ТК РФ. Расторжение трудового договора по инициативе работодателя. [6]

что это не влияет на безопасность информационных активов на предприятии [2].

Цели работы с сотрудниками на разных этапах взаимодействия с работодателем и соответствующие им нормативные документы, позволяющие интегрировать требования данного стандарта в работу организаций по обеспечению информационной безопасности, представлены в Таблице 1:

Анализируя данные Таблицы 1, можно сделать вывод о том, что все этапы взаимодействия сотрудника с работодателем разработаны недостаточно в теории информационной безопасности, особенно - увольнение сотрудников. Тем не менее, есть источники (книги, статьи, сайты), которые могут, наряду с другими материалами, освещающими практическую сторону кадрового обеспечения защиты информации в организации, решить проблему внедрения стандарта ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности» (п.8).

Методам работы с сотрудниками на различных этапах взаимодействия посвящены разные источники, например:

1. Во время трудоустройства:

• Документальное определение и оформление ролей и обязанностей, которые должны быть определены и доведены до претендентов на работу до их трудоустройства: наглядные примеры и образцы политики информационной безопасности и парольных политик [8, 9].

2. Во время занятости:

• Регистрация обязанностей руководства: перечень и описание ролей и компетен-

ций руководителя, осуществляющего управление и контроль информационной безопасности [10], перечень аспектов, на которые должен обращать внимание руководитель во избежание утраты, разглашения или изменения сотрудниками данных, принадлежащих клиентам организации [18].

• Осведомление, обучение и тренинг в области информационной безопасности: проводится анализ угроз безопасности реализуемых через атаку на персонал организации и методы противодействия им [12], проблемы подготовки и переподготовки специалистов в рамках реализации системы управления ИБ [11], примеры и анализ нарушений ИБ инсайдерами [20], перечисление преимущества электронного обучения сотрудников и примеры его применения [21], предпочтительные методы осведомления сотрудников о кибер-безопасности [21].

3. Во время увольнения:

Четкое определение и установление обязанностей в отношении прекращения занятости или смены занятости, ответственность и служебные обязанности, продолжающие оставаться действительными после прекращения занятости, аннулирование прав доступа и возврат всех информационных и материальных активов, принадлежащих организации: описывается значение заключительного интервью для выявления брешей и уменьшение психологической подавленности и недовольства бывших сотрудников [14], рекомендации по поведению сотрудников службы безопасности в процессе увольнения персонала для предотвращения негативных последствий [15], практические советы по выявлению и удалению брешей в системе безопасности предприятия, которые может использовать уволенный сотрудник [16], документальное оформление ответственности и обязанностей работника при увольнении [17].

На основании приведенных источников можно сделать вывод об отсутствии в российских стандартах по управлению информационной безопасностью описания практической реализации такой функции управления как мотивация.

Мотивация - это внутренняя потребность, преображенная в побудительную причину действий и поведения человека в конкретной ситуации [23]. Эффективно построенная система мотивирования персонала формирует нормальную психологическую среду человека, которая, в свою очередь, способствует уменьшению HR-угроз. Знания и навыки персонала - главный источник длительного процветания компании только в том случае, если работник добровольно посвящает ей себя и свой труд. Поэтому организация, ориентированная на долгосрочное развитие и успех уделяет особое внимание обеспечению сотрудников благоприятными условиями труда для реализации их потенциала.

Разработка и реализация способов стимулирования персонала закрепляются в кадровых документах, таких как кадровая политика, Положение о персонале, правила внутреннего трудового распорядка, трудовые договора и др. [24].

В связи с изложенным, целесообразно дополнить стандарт ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности» (п.8 «Безопасность, связанная с персоналом») методами мотивирования сотрудников. Предлагается использовать все рекомендации, связанные с выполнением функции мотивации, а также с функциями планирования, организации и контроля, которые так или иначе влияют на мотивирование сотрудников.

Анализируя рассмотренные источники, целесообразно разработать рекомендации для работодателя, которые помогут ему эффективно управлять кадрами в рамках обеспечения информационной безопасности на всех стадиях взаимодействия работника и организации.

Р. Мэтьюз, А.И. Агеев, Б.В. Куроедов [23] выделяли три группы мотивации персонала: материальные факторы, психологические факторы, факторы мотивации. На каждой стадии взаимодействия сотрудника и организации присутствует хотя бы одна группа факторов.

Основываясь на системе трех стадий работы сотрудника (найм, работа, увольнение) и четырех функций управленческой деятельности (планирование, организация, мотивация, контроль) можно представить систему управления мотивацией в виде таблицы (Таблица 2).

В пункте 8.1 «Перед трудоустройством» ГОСТ Р ИСО/МЭК 27002-2012 следует внести дополнения, касающиеся мотивирования сотрудника на этапе найма.

Целью работы с сотрудниками во время трудоустройства является стимулирование

Таблица 2

Система управления мотивацией в структуре СУИБ с точки зрения функционального подхода

	Планирование	**Организация**	**Мотивация руководства**	**Контроль**
На этапе приема	Разработка политики ИБ и Положения по работе с персоналом, содержащего описание соотношения должности сотрудника и соответствующей ей степени угрозы ИБ.	Реализация политики ИБ (анкетирование, собеседование, рекомендации, ознакомление с правами и обязанностями, проверка предоставленных данных соискателем) и Положения по работе с персоналом.	Разработка руководителем отдела ИБ и представление руководству аналитической справки «Персонал как источник угроз ИБ»; возможно сравнение справки с Отчетом, ежегодно составляемом аналитическим центром компании InfoWatch для убеждения руководства о введении Положения по приему персонала.	Положение об аудите работы с персоналом (проверка компетенций работников, осуществляющих набор персонала, их осведомленности в области ИБ, проверка организации процесса набора персонала).
На этапе работы	Разработка Положения о мотивации (включая пункт о самореализации сотрудника как фактора повышения уровня ИБ), разработка системы финансового и организационного обеспечения системы мотивации.	Реализация Положения о работе с персоналом, (анкетирование для определения вектора развития мотивации руководства и сотрудников, направление на обучение, введение дифференцированной оценки персонала как источника угроз).	Ознакомление высшего руководства и руководителей подразделений с результатами мониторинга причин реализации HR-угроз, материальное и иное стимулирование.	Положение об аудите работы персонала, аттестация, анкетирование об уровне компетенций и осведомленности в области ИБ, дисциплинарные взыскания.
На этапе увольнения	Парольные политики, Инструкция об увольнении (установление этапов увольнения и их содержания).	Реализация парольной Политики (смена паролей увольняемого сотрудника), реализация Положения об увольнении (передача информации и материальных носителей и др.).	Ознакомление руководства с отчетами об увольнениях сотрудников с наличием инцидентов ИБ, дисциплинарные взыскания в отношении руководителей подразделений, в которых произошел инцидент ИБ.	Положение об аудите работы по увольнению сотрудников, соглашение о неразглашении информации ограниченного доступа уволенного сотрудника.

персонала путем установки должного уровня требований к соискателям. Данные требования рекомендуется прописывать в Политике информационной безопасности, а также в Положении о работе с персоналом в виде отдельного перечня для каждой должности компетенций и личностных качеств, которыми должен обладать работник. Названные документы следует разрабатывать, принимая во внимание все варианты использования трудовых ресурсов предприятия, для того чтобы максимально реализовывать потенциал сотрудников. На их базе проводится отбор претендентов на должность с использованием анкетирования, собеседования и тд. После отбора и утверждения кандидатов необходимо ознакомить их со своими обязанностями и правами, для обеспечения уверенности в их осведомленности.

В пункт 8.1 «В течение занятости» ГОСТ Р ИСО/МЭК 27002-2012 следует внести дополнения, касающиеся мотивирования сотрудника на этапе его непосредственной работы в организации.

Целью работы с сотрудниками во время занятости является повышение качества как внешних, так и внутренних мотивирующих сил сотрудника. Руководству важно понимать, что немаловажным аспектом, на который стоит обратить особое внимание, является сонаправленность целей работника и организации. При несовпадении стремлений предприятия и сотрудника мотивация последнего теряет ценность, поэтому смысл мотивационных механизмов заключается в достижении максимального удовлетворения потребностей как организации, так и работника.

Для определения основных мотивирующих сил работников может применяться анонимное анкетирование, содержащее вопросы об уровне удовлетворенности условиями работы, о пожеланиях к работе организации, а также графы с предложениями по улучшению результатов мотивирования. На основании анкетирования разработать план мотивации как предприятия в целом, так и отдельных отделов.

Что касается материальной мотивации, стоит составить план премий и дополнительных выплат. Важно соблюдать баланс и избегать ситуаций, когда компетентный работник, получая значительные вознаграждения, начинает лениться, будучи уверенным в том, что руководство примет любой уровень его работы. В то же время, нерадивый сотрудник, получая вознаграждение, формирует установку, что руководство устраивает то качество работы, которое он предоставляет.

Важным аспектом материальной мотивации является предоставление улучшенного страхового и пенсионного пакетов, санаторно-курортного лечения, а также закрепление сотрудника за сотрудничающим с организацией медицинским центром. Также можно предоставлять сотруднику те предметы и услуги, которые прямо не необходимы для выполнения им своих обязанностей, но значительно облегчают жизнь (предоставление служебного транспорта, оплата сотовой связи и тд.).

Для улучшения психологической обстановки в коллективе регулярно проводятся «летучки», планерки и тд., где открыто или анонимно обсуждаются интересующие вопросы, а также устраиваются корпоративы в неформальной обстановке.

Кроме того, сотрудник нуждается в признании как руководством, так и всем коллективом. Если сотруднику не внушается его значимость и важность командной работы, он быстро теряет мотивацию не только к дальнейшему росту, но и к элементарному выполнению своих обязанностей. Способов признания сотрудника множество: вручение грамоты, подарка, благодарственного письма, публичное поздравление, возможность повышения образования по специальности. В данном контексте перечисленные способы несут нематериальную ценность: они выражают степень оценки сотрудника как руководством и коллективом.

Следует принимать во внимание степень заинтересованности и внимательности к деталям руководства в реализации мер, направленных на улучшение психологического климата предприятия и укрепление командного духа, так как именно от него будет зависеть точность постановки целей и эффективность принимаемых мер по мотивированию персонала. Недооцененный персонал может начать халатно относиться к своим обязанностям, что может привести к пренебрежению своими служебными обязанностями и, как следствие, к угрозе нарушения информационной безопасности. [25]

Что касается факторов самореализации, то важнейшим способом является обучение и повышение квалификации сотрудника. [26] Возможно создание системы профессиональной аттестации и планирования служебного роста с целью стимулирования профессионального развития. [27, 28]. Квалифицированный и мотивированный сотрудник – ценнейший актив организации. Получая от организации возможность повысить свою компетентность, сотрудник реализует свою потребность к самосовершенствованию. Но необходимо помнить, что следует убедиться в заинтересованности сотрудника в профессиональном росте и в готовности к этому росту, в противном случае навязывание ненужных сотруднику мероприятий только ослабит его заинтересованность в росте.

Важно уделять внимание творческой составляющей обязанностей работника. Если выполняемые сотрудником действия монотонны, следует разнообразить его деятель-

ность, ввести дробные перерывы и по возможности модифицировать трудовой процесс. Также при грамотном определении внутренних мотивирующих факторов сотрудника можно давать ему задания, в которых он сможет реализовать свои самые сильные качества, это поможет раскрыть его профессиональный потенциал и подтолкнуть к дальнейшему развитию. [29]

В пункт 8.3 «Прекращение или смена занятости» ГОСТ Р ИСО/МЭК 27002-2012 следует внести дополнения, касающиеся мотивирования сотрудника на этапе его ухода из организации.

Целью мотивирования сотрудников во время увольнения являются четкое определение и установление обязанностей в отношении прекращения занятости или смены занятости. Сотрудник должен четко осознавать, как то или иное действие или бездействие может отразиться на его положении в организации, какие дисциплинарные меры на него могут быть возложены при невыполнении своих обязанностей.

Ответственность и служебные обязанности, продолжающие оставаться действительными после прекращения занятости, должны содержаться в договорах с сотрудниками. Основным способом контролирования данного аспекта является подписание договора о неразглашении, в котором сотрудник обязуется в течение определенного закрепленного в договоре промежутка времени не передавать сведения ограниченного доступа третьим лицам. Также возможна выплата компенсаций сотруднику за соблюдение данного договора.

Аннулирование прав доступа и возврат всех информационных и материальных активов, принадлежащих организации следует четко зафиксировать в парольных политиках и документах, закрепляющих порядок возврата информационных и материальных активов. Установленные дисциплинарные меры, применяемые при несоблюдении этих правил, лишат сотрудника соблазна покинуть место работы, не завершив должным образом свое взаимодействие с организацией.

Стадия увольнения характеризуется самыми жесткими мерами мотивирования персонала, которые могут обеспечить уверенность в том, что при увольнении сотрудника или смене его занятости, в лице данного работника исключаются угрозы информационной безопасности предприятия.

Приведенные выше меры можно использовать для формирования системы управления мотивацией сотрудника, что позволит значительно снизить уровень HR-угроз. Данные меры могут быть введены в полной мере или частично.

Таким образом, научная новизна статьи заключается в выявлении недооценки кадровых проблем в международных стандартах по управлению информационной безопасностью; обосновании системы управления мотивации сотрудников как части СУИБ, выявлении ее специфики; разработке предложений по внесению дополнений в ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности» на основе разработанной системы управления мотивации сотрудников как части СУИБ.

Примечания

1. Астахова, Л.В. Проблема оценки HR-уязвимости объекта защиты информации / Л. В. Астахова / Вестник УрФО: Безопасность в информационной сфере. – 2011. – № 1. – с. 26-33.

2. ГОСТ Р ИСО/МЭК 27002-2012. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности. – Введ. 2014-01-01.— М.: ФГУП «СТАНДАРТИНФОРМ», 2014.— 106 с. (взамен ГОСТ Р ИСО/МЭК 17799-2005).

3. Волкодаева, А.В. Проектирование эффективной системы информационной безопасности предприятия / А.В. Волкодаева / Научный журнал НИУ ИТМО. Серия «Экономика и экологический менеджмент». – 2015. – №3. – с. 193-200.

4. Барбашин, С.С. Принципы, методы и практика построения системы управления информационной безопасностью предприятия / С.С. Барбашин, В.И. Карпова, С.С. Марчуков // Горный информационно-аналитический бюллетень (ГИАБ). – 2008. – с. 192-199.

5. ГОСТ Р ИСО 19011-2012. Руководящие указания по аудиту систем менеджмента. – Введ. 2013-02-01.— М.: ОАО «ВНИИС», 2013.— 41 с. (взамен ГОСТ Р ИСО 19011-2003).

6. Трудовой кодекс Российской Федерации: [федер. закон: принят Гос. Думой 21 дек. 2001 г.: по состоянию на 1 янв. 2002 г.]. – М. Омега-Л 2006. – 184 с.

7. Приказ Минздравсоцразвития РФ от 22.04.2009 № 205 «Об утверждении Единого квалификационного справочника должностей руководителей, специалистов и служащих, раздел «Квалификационные характеристики должностей руководителей и специалистов по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, противодействию техническим разведкам и технической защите информации».

8. Парольная политика [Электронный ресурс] // SecurityPolicy.ru – Документы по информационной безопасности: сайт. – Электрон. текстов. дан. – [Б.м.], 2016. – Режим доступа: http://securitypolicy.ru/index.php/Парольная_политика – Загл. с экрана.

9. Политика информационной безопасности [Электронный ресурс] // SecurityPolicy.ru – Документы по информационной безопасности: сайт. – Электрон. текстов. дан. – [Б.м.], 2016. – Режим доступа: http://securitypolicy.ru/index.php/ Политика_информационной_безопасности – Загл. с экрана.

10. National Cyber Security Devision, United States Department of Homeland Security «IT Security Essential Body of Knowledge (EBK): A Competency and Functional Framework for IT Security. Workforce Development. Information Security and Privacy Advisory Board Meeting December 7, 2007». – October 2008.

11. Бабков, И.Н. Обучение персонала как составная часть проблемы обеспечения информационной безопасности энергосистемы // И.Н. Бабков, В.М. Шатунов // Защита информации. Конфидент. – 2004. – №3, с. 53-58.

12. Бойдало, М.К. Персонал организации как уязвимость в системе информационной безопасности: атаки и противодействие им / М.К. Бойдало, Г.П. Жигулин // Научно-технический вестник Поволжья. – 2015. - №3. – с.89-91.

13. Федеральный закон от 29.07.2004 N 98-ФЗ (ред. от 12.03.2014) «О коммерческой тайне» [Электронный ресурс] // КонсультантПлюс: сайт. – Электрон. текстов. дан. – [Б.м.], 2016. – Режим доступа: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=160225;div=LAW;dst=100114,0;rnd=203280.26559209473736645.

14. Низола, Д.А. Безболезненное увольнение работников / Д.А. Низола, Л.В. Тарасова / Новое слово в науке: перспективы развития. – 2015. – № 2. – с. 391-393.

15. Бугаян, С.А. Обеспечение кадровой безопасности предприятия // Russ. acad. j., RAJ . 2013. №3 (25). URL: http://cyberleninka.ru/article/n/obespechenie-kadrovoy-bezopasnosti-predpriyatiya.

16. Барамба, С. Они увольняются, а с «учетными записями» разбираться нам! / С. Барамба / Системный администратор. – 2014. – №10. – с. 44-46.

17. Соглашение о неразглашении конфиденциальной информации [Электронный ресурс] // Бесплатный архив юридических документов peopleandlaw.ru – Электрон. текстов. дан. – [Б.м.], 2016. – Режим доступа: https://peopleandlaw.ru/soglashenie/soglashenie-o-nerazglashenii-konfidentsialnoj-informatsii – Загл. с экрана.

18. Levy, M Protecting customer data: with personal information at risk, internal auditors must provide assurance for the many facets that make up data security / M. Levy / Internal Auditor. – August 2015. – Vol. 72 Issue 4. – с. 32/

19. Федеральный закон от 27.07.2010 N 224-ФЗ (ред. от 21.07.2014) «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации» [Электронный ресурс] // КонсультантПлюс: сайт. – Электрон. текстов. дан. – [Б.м.], 2016. – Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_103037.

20. Shorpshire, J. A canonical analysis of international information security breaches by insiders / J. Shorpshire / Information manager & computer security. – 2009. – №17. – с. 296-310.

21. Hagen J. The long-term effects of information security e-learning on organizational learning / J. Hagen / Information management & computer security. – 2011. – №19. – с. 140-154.

22. Abawajy, J. User preference of cyber security awareness delivery methods / J. Abawajy / Behaviour & Information Technology. – 2014. – №33. – с. 236-247.

23. Подосинников Е.Ю. Мотивация трудовой деятельности инженернотехнического персонала предприятия: измерение и анализ / Е. Ю. Подосинников, А. С. Кулешов, С. С. Железняков / Ученые записки. Электронный научный журнал Курского государственного университета. – 2015. – № 3 (35).

24. Пожарская, Е.Л. Мотивация поведения персонала как психологическая основа экономической безопасности предприятия, организации / Е.Л. Пожарская / Актуальные проблемы гуманитарных и естественных наук. – 2015. – № 4-2.

25. ГОСТ Р ИСО/МЭК 27004-2011 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения. – Введ. 2012-01-01. [Электронный ресурс] // Техэксперт: сайт. – Электрон. текстов. дан. – [Б.м.], 2016. – Режим доступа: http://docs.cntd.ru/document/gost-r-iso-27004-2011 (Пункт 6).

26. ГОСТ Р ИСО/МЭК 27001 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. – Введ. 2008-02-01. [Электронный ресурс] // Техэксперт: сайт. – Электрон. текстов. дан. – [Б.м.], 2016. – Режим доступа: http://docs.cntd.ru/document/gost-r-iso-mek-27001-2006 (Пункт 5).

27. СТО БР ИББС-1.2-2014 «Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0-2014»

28. СТО БР ИББС-1.0-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» (Пункт 8.9).

29. Трудникова, И.А., «Актуальные проблемы гуманитарных и естественных наук» // И.А. Трудникова, Е.Г. Новосельцева /Волгоградский государственный университет № 4-1 – 2015 Стр. 266-270.

Астахова Людмила Викторовна, доктор педагогических наук, профессор, профессор кафедры «Защита информации» Южно-Уральского государственного университета. 454080, г. Челябинск, пр. Ленина, д. 76. E-mail: lvastachova@mail.ru

Овчинникова Людмила Олеговна, студентка кафедры «Защита информации» » Южно-Уральского государственного университета. 454080, г. Челябинск, пр. Ленина, д. 76.

Astakhova Ludmila Viktorovna, Doctor of Sciences (Pedagogy), Professor, South Ural State University (National Research University), Chelyabinsk, Russia. E-mail: lvastachova@mail.ru

Ovchinnikova Ludmila Olegovna, a student of the Department «Information Security», «South-Ural State University. 454080, Chelyabinsk, Lenina ave., D. 76