УДК 316:42.35

КОЗАЧОК Василий Иванович – *доктор социологических наук, профессор; сотрудник Академии ФСО России (302030, Россия, г. Орел, ул. Приборостроительная, 35; kosachok@list.ru)*

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КОРПОРАЦИИ КАК ОБЪЕКТ СОЦИАЛЬНОГО УПРАВЛЕНИЯ

Аннотация. *Статья посвящена вопросу актуализации человеческого фактора в системе обеспечения информационной безопасности корпорации. Автор проводит анализ фактов утечки конфиденциальной информации по данным ведущих информационных агентств и сопоставляет источники инцидентов. В статье подтверждается зависимость роста числа утечек конфиденциальной информации по вине сотрудников при отлаженной технической системе защиты информации. Автор предлагает и обосновывает подход социальной метрики персонала, работающего в системе обеспечения информационной безопасности корпорации, и излагает предложения его реализации посредством механизмов социального управления. В основу метрики положена процедура оценки социального ядра личности – социальной компетентности, социальной готовности и социальной совместимости сотрудников, обеспечивающих защиту информации; определяются шкалы показателей социального ядра личности и приводится семантическое описание их значений в приложении к системе обеспечения информационной безопасности корпорации.*

Ключевые слова: *информационная безопасность корпорации, инциденты информационной безопасности, утечка информации, угрозы информационной безопасности, социальное управление, социальная компетентность, социальная готовность, социальная совместимость, социальное ядро личности*

Аналитики назвали 2015 г. годом утечек информации, и это не только благодаря взлому данных военного командования США в социальных сетях группировкой «Киберхалифат» и электронной почты пресс-секретаря Дмитрия Медведева Натальи Тимаковой хакерской группой «Анонимный интернационал»[1]. По данным аналитического центра *InfoWatch*, общая сумма убытков из-за утечки конфиденциальной информации выросла в 2015 г. практически на 1/4 и превысила 25 млрд долл.[2] Средняя сумма потерь от каждой значительной утечки информации составила около 31 млн долл. Отечественные корпорации не остались в стороне от процессов утечки: их потери составляют 6% общей суммы убытков. По сравнению с 2014 г. сумма урона в 2015 г. увеличилась на 33%. Общим для всех инцидентов является тот факт, что в ходе расследования было выявлено: почти 37% из них произошли по вине сотрудников, причем не по злому умыслу или сознательно, а по халатности или допущенным ошибкам. В первом полугодии 2016 г. 67% случаев утечек данных произошли по вине внутреннего нарушителя, в том числе 1% случаев утечек допустили высшие руководители организаций[3].

Россия с первого полугодия 2015 г. стабильно удерживает 2-е место по числу утечек после США. В России отмечено 118 инцидентов за 2015 г., Великобритании – 112, в США – 859, или 57% общего числа всех происшед-

[1] «Анонимный интернационал» – хакерская группировка, специализирующаяся на перехвате переписки и взломе аккаунтов высокопоставленных чиновников, политиков, крупных фирм и СМИ; публикуют полученные данные в интернет-блоге. См.: Хакерские атаки. – *Газета.ru.* 24/12/2015. Доступ: https://www.gazeta.ru/tech/2015/12/24/ 7989839/best-hacks-2015.shtml (проверено 09.11.2016).

[2] *InfoWatch* – российская компания, специализирующаяся на информационной безопасности в корпоративном секторе. См.: Международные новости утечек информации, ежегодные аналитические отчеты и статистика по инцидентам за прошедшие годы. Доступ: http://www.infowatch.ru/analytics/reports# (проверено 14.09.2016).

[3] Там же.

ших утечек[1]. За первое полугодие 2016 г. в России зарегистрированы 110 случаев утечки информации[2].

Наиболее подвержены утечкам информации медицинские (20,2%) и образовательные учреждения (14,9%), предприятия розничной торговли (10,8%), а также государственный сектор (15,9%), обладающий «совершенной» системой сохранности тайны, построенной в соответствии с профессиональными рекомендациями и систематически контролируемой специальными подразделениями.

Обобщенно распределение известных инцидентов информационной безопасности корпораций различной направленности выглядит следующим образом: внешние атаки – 32,1%, внутренний нарушитель – 65,4%, не установленные – 2,5%.

Изучение отчетов и аналитических материалов компании *InfoWatch* позволило сделать вывод, что распределение утечек информации по воздействию угроз практически не имеет субстанциальных признаков. Распределение утечек информации изучалось по двум направлениям: по вектору воздействия и по категории виновников. Анализ данных позволил зафиксировать, что по вектору воздействия возросло число утечек через внутренних нарушителей: с 53% (2010 г.) до 66,9% (первое полугодие 2016 г.). При этом снизилось число утечек через внешних злоумышленников: с 42% (2010 г.) до 33,1% (2016 г.). Анализ утечки конфиденциальной информации по категориям виновников позволяет утверждать, что наряду с постепенным снижением числа нарушений со стороны руководителей из года в год возрастает число инцидентов, происходящих по вине рядовых сотрудников корпорации. Например, рост утечек по вине сотрудника в 2013 г. составил 49,5%, в 2016 г. – 66%. Причем по вине руководителя число утечек снизилось с 6,7% (2013 г.) до 0,8% (2016 г.)[3].

В целом, происходит стабилизация показателей прироста числа утечек – около 30–35% ежегодно. Динамика роста числа инцидентов такова: с 3,4 млн в 2009 г. до 59,1 млн в 2015 г.[4]

В современной системе обеспечения информационной безопасности темпы роста числа инцидентов и, как следствие, наносимого ущерба гораздо выше темпов роста финансовых затрат на защиту информации корпораций[5]. В конечном счете, такая динамика приведет к ситуации, когда эффективность вложения средств в защиту информации становится очень низкой.

Здесь налицо проблема. С одной стороны, неуклонный рост числа нарушений диктует необходимость внесения корректирующих изменений в существующую систему управления информационной безопасностью. С другой – прослеживается перекос в техническую сторону решения проблемы: совершенствование технико-технологической составляющей обеспечения информационной безопасности корпорации [Козачок А. 2012]. Сложившееся положение привело к тому, что практически 95% инцидентов, связанных с информационной безопасностью, происходят по вине сотрудников, работающих в корпорации. Следовательно, необходимо обратить внимание на аспекты социального управления информационной безопасностью корпорации.

---

[1] Там же.

[2] Управление киберрисками во взаимосвязанном мире. Глобальное исследование по вопросам обеспечения информационной безопасности. – *PricewaterhouseCoopers*. 2015. Доступ: http://www.pwc.ru/ru/riskassurance/publications/assets/managing-cyberrisks.pdf (проверено 25.07.2016).

[3] Глобальное исследование утечек конфиденциальной информации. Доступ: https://www.infowatch.ru/node/3013 (проверено 14.09.2016).

[4] Управление киберрисками... Доступ: http://www.pwc.ru/ru/riskassurance/ publications/assets/managing-cyberrisks.pdf (проверено 25.07.2016).

[5] Там же.

Обзор практикоориентированных подходов к обеспечению информационной безопасности корпорации

Существующий арсенал подходов обоснован в работах как российских, так и зарубежных ученых. Имеющиеся подходы условно разделены на две группы.

Первая группа включает подходы, связанные с финансовой, технической и организационной стороной.

• Совершенствование программно-аппаратных средств информационной безопасности. По результатам 2015 г. расходы на эти цели увеличились почти на 10% и составили около 80 млрд долл. США[1]. Главными векторами разработки новых средств защиты является надежность и обеспечение требуемой стойкости при условии минимизации роли оператора (пользователя).

• Переработка и усиление (ужесточение) требований нормативных документов по обеспечению информационной безопасности. Операционная регламентация действий сотрудников видится организаторами систем обеспечения информационной безопасности как основное средство недопущения инцидентов. Противоречие заключается в том, что из-за разнородности операций, выполняемых персоналом корпораций, требуется разработка все большего числа инструкций и памяток, что, в свою очередь, приводит к резкому снижению остаточных знаний у сотрудников в вопросах регламентации их деятельности по защите информации.

• Увеличение затрат корпораций и организаций на поддержание требуемого уровня защищенности своих информационных ресурсов. Например, в крупных компаниях затраты по этой статье расходов составляют почти 11 млн долл. США, малые компании вынуждены тратить до 1 млн долл. США. Лавинообразный рост числа инцидентов в сфере информационной безопасности существенно снижает эффективность значительных вложений, т.к. доля ущерба, наносимого утечками, составляет от 40% до 60%[2] [Savola 2007; Журавлев, Лобжанидзе, Белоусов 2015; Воронцов, Штейнбух 2015].

Вторая группа связана с подготовкой сотрудников, регламентацией и управлением информационной безопасностью.

• Целевая подготовка сотрудников корпорации, которые по своим должностным обязанностям выполняют операции по обеспечению сохранности информации. Сознательные нарушения правил, регламентирующих требования по защите информации, имеют место и не всегда основаны на злом умысле сотрудника. В их основе могут быть социально-психологические корни, например «ложная готовность» или «социальная некомпетентность», когда сотрудник изучил и сдал зачеты по порядку обработки информации, но в силу забывчивости теперь воспроизводит их неверно, хотя внутренне он убежден в правильности выполняемых операций. Это не просто незнание (по причине забывания), а неосознание последствий и важности строгого соблюдения регламентов обращения с конфиденциальной информацией. Процесс подготовки специалистов по обеспечению безопасности информации должен сформировать у обучаемых умение и стремление к коллективному решению задач защиты информации, профессиональные компетенции (усвоенные первичные умения, доведенные до уровня навыка) [Von Solms, Van Niekerk 2013; Киреева 2013; Rao 2014; Alhogail 2015; Kretzer, Madche 2015].

• Решение социально-технических задач. Это означает, что помимо перечисленного арсенала средств защиты информации необходимо учитывать фактор персонала, процессы и технологии, которые они реализуют. Анализ тематики

[1] Там же.

[2] Там же.

современных исследований обеспечения информационной безопасности показывает, что 94% усилий исследователей направлены на совершенствование технических аспектов защиты информации. Социально-психологическим аспектам обеспечения информационной безопасности уделяется внимание менее чем в 6% исследований [Yaokumah 2016; Sohrabi Safa, Von Solms, Furnell 2016; Kearney, Kruger 2016; Beznosov, Beznosova 2007]. С другой стороны, результаты аудита оценки информационной безопасности показывают хорошую методическую обеспеченность проверок в направлениях технического анализа состояния системы обеспечения защиты информации и инструментальных испытаний [Tu, Yuan 2014; Лазуткин 2015]. В целом, социальный аспект обеспечения информационной безопасности остается вне рамок проведения аудита.

Обобщая анализ исследовательских подходов, необходимо подчеркнуть: основная причина проблемы обеспечения информационной безопасности корпорации заключается в том, что отсутствует инструментарий оценивания готовности персонала корпорации компетентно и совместно решать задачи по обеспечению информационной безопасности. Следовательно, требуется разработка метрик оценивания сотрудников корпорации и формирование социальных механизмов управления информационной безопасностью корпорации.

Социологическое обеспечение информационной безопасности корпорации

Социологическое обеспечение – это совокупность информации и алгоритмы ее обработки с целью оценки реального состояния эффективности социального управленческого воздействия на процессы обеспечения информационной безопасности корпорации, установления степени влияния факторов, его определяющих, а также предложения научно обоснованных рекомендаций по осуществлению требуемых управленческих воздействий по предотвращению инцидентов, связанных с информационной безопасностью.

Под результатами социологического обеспечения процессов управления состоянием информационной безопасности корпорации понимается предоставление руководителям или сотрудникам службы обеспечения информационной безопасности актуальной обобщенной систематизированной информации, требуемой для принятия управленческого решения на основании результатов социологического исследования сотрудников корпорации с целью формирования обоснованных управленческих решений по предотвращению утечек и хищений конфиденциальных данных.

Важным социальным аспектом проблемы защиты от утечек информации является практически устоявшееся распределение внутренних и внешних угроз. Поэтому имеет смысл говорить об уточнении модели процесса обеспечения информационной безопасности, рассматривая вектор атак в каждый момент времени как совокупность внешних и внутренних угроз, нарушающих работу системы [Велигура 2013]. Очевидно, что администрация имеет потенциальную возможность воздействовать напрямую только на поведение внутренних нарушителей с целью повышения защищенности информационных ресурсов корпорации. Внутренние угрозы – это не только персонал корпорации (руководители, системные администраторы, сотрудники), но и подрядчики (поставщики услуг – нынешние и бывшие), потребители (нынешние и бывшие) услуг (товаров) корпорации, а также бывшие сотрудники. Внешние угрозы не входят в сферу управленческого воздействия со стороны руководства корпорации. Поэтому конкретных эффективных управленческих решений по воздействию на внешних нарушителей информационной безопасности практически не существует, за исключением попыток проведения профилактической работы, направленной на соблюдение требований законности и морали.

Большинство аналитиков в области безопасности приходят к выводу, что закупка и установка дорогостоящего оборудования систем защиты информации и активная реализация организационно-режимных мероприятий – это пока единственный путь обеспечения информационной безопасности любой корпорации. Система организационно-режимных мер обеспечения информационной безопасности корпорации работает и достигает определенных результатов, однако управленческих процедур ее совершенствования практически не существует. В сложившейся ситуации в связи с достижением своего предела система организационных мер нуждается в вовлечении механизмов социального управления в арсенал защиты информации. Одним из них является формирование метрик персонала системы обеспечения информационной безопасности, а именно социологического обеспечения, которое включает методы социальной квалиметрии.

Авторская методика диагностики персонала корпорации

Цель авторской методики заключается в разработке инструмента диагностики персонала, который позволит производить эффективный подбор, расстановку персонала корпорации и управление им – в целом, комплексную систему по обеспечению информационной безопасности корпорации.

Авторская методика включает:

1) модель социального ядра личности сотрудника корпорации и подразделения по обеспечению информационной безопасности, т.е. критерии оценки социальной компетентности, социальной готовности и социальной совместимости, позволяющие произвести корреляцию оцениваемого сотрудника с определенным субтипом личности;

2) программный алгоритм выбора рациональных совокупностей субтипов социального ядра личности, наиболее предпочтительных для работы в корпорации и подразделениях по защите информации;

3) научно-практические предложения по социальному управлению персоналом корпорации и подразделением по обеспечению информационной безопасности.

Методика имеет некоторые допущения, позволяющие расширять возможности применения, и ограничения, поскольку создавалась под решение конкретных задач с учетом темпоральности исследуемого поля.

Основные допущения:

– наличие возможности получения социально-психологических метрик персонала корпорации и работающих в подсистеме обеспечения информационной безопасности;

– сотрудники корпорации в пределах своих должностных обязанностей обучены вопросам обеспечения информационной безопасности;

– аппаратно-программные комплексы и средства обеспечения информационной безопасности исправны.

Ограничения:

– исследование проводится для условий мирного времени;

– корпорация не является особорежимным объектом.

Предлагаемая методика апробирована в малых и средних корпорациях. Результаты диагностики в числовом виде отражают значение уровня социализации личности, с одной стороны, и самопроецирование индивида по отношению к окружающему его социуму – с другой. Данные, полученные по результатам диагностики, позволят оценить человека и его отношение к обществу и процессам, происходящим в нем. Реальные деяния человека, его внутренняя мотивация определяются во многом не только и не столько обстоятельствами, а в основном

результатами социализации личности. Так, например, если сотрудник в условиях необходимости выбора действия или бездействия не актуализирует интересы корпорации по обеспечению информационной безопасности, а более важным считает личную выгоду, то подобная жизненная позиция не может оставаться его «личным делом», поскольку наносит или может нанести ущерб корпорации.

Очевидно, что результат социализации любого сотрудника корпорации не является скрытым, а проявляется открыто, целенаправленно и совершенно осознанно; он остается практически устойчивым и может быть зафиксирован. Значит, информация, полученная на основании применения предлагаемой автором методики диагностики, не нарушает права человека и не становится запретом на профессию. Фактически целенаправленная работа индивида над собой может изменить темперамент личности, и результаты социализации не являются перманентными данными.

Таким образом, сведения, полученные на основе применения социальной диагностики, в сжатые сроки и при сравнительно небольших затратах дают в распоряжение администрации корпорации объективную, достаточно полную количественную информацию по результатам предшествующей социализации работника и его существенных особенностях [Козачок 2007; 2016а].

Важно отметить, что получить такую информацию за короткое время нельзя никакими другими средствами или способами, и, как подтверждает практика, даже длительное наблюдение или отличные рекомендации с прежнего места работы не всегда могут обеспечить необходимую достоверность выводов о конкретных особенностях человека. Кроме того, полученные в ходе проведения диагностики данные можно сопоставлять и сравнивать, а также обнаруживать интересующие тенденции, строить прогнозы и формулировать выводы. Поэтому результаты оценки уровня социализации необходимы в первую очередь для организации целенаправленного управленческого воздействия на персонал корпорации, принятия обоснованных решений по оптимальной расстановке сотрудников, их обучению и актуализации, адекватной мотивации, выявления причин возникновения тех или иных нарушений требований по обеспечению информационной безопасности в корпорации.

Результаты агрегирования данных социальной диагностики представляются в виде совокупности трех оценок: социальной компетентности, социальной готовности и социальной совместимости. Каждая из оценок характеризует выраженность компонента социального ядра личности в значениях на конкретной шкале (все шкалы нормализованы). Таким образом, оценка результатов диагностики отображается на шкале условно от 0 до 100. Нормой для социализации сотрудника считаются значения в диапазоне от 40 до 60 ед. Показатели ниже 40 свидетельствуют о низких результатах социализации личности по конкретному компоненту социального ядра. Поэтому с учетом важности решаемых задач (возможный ущерб корпорации с учетом рисков для подразделений обеспечения информационной безопасности) результаты социализации кандидата должны быть не ниже 60 баллов [Козачок 2012].

В авторской методике предложена трактовка конкретных оценок результатов диагностики, которая включает подробное описание сути критериев оценки. Преимущества такого подхода заключаются в том, что это позволяет:

– администрации, принимающей решение, осознать недопустимость метаморфозы результатов диагностики социального ядра личности в догму, ярлык или штамп, т.е. оценить психологические особенности индивида как свободной в своем формировании личности, его многомерной общественной сущности и свести оценки до значения предсказуемого и программируемого результата;

– рассматривать кандидата или сотрудника подразделения по обеспечению

информационной безопасности более полно, объемно и оценивать его особенности с позиции целевого функционала как работника корпорации;

– отразить оценку навыков, умений и знаний конкретного сотрудника корпорации, усвоенных и приобретенных им вследствие взаимодействия с социумом, что предполагает выделение из полного множества навыков, умений и знаний личности тех, которые напрямую характеризуют ее социализацию;

– прогнозировать эффективность выполнения служебных задач, наращивать темпы роста положительной динамики результативности деятельности;

– провести оценку сложившегося мировоззрения кандидата или сотрудника, понимания им собственной миссии в корпорации;

– оценить организаторские качества кандидата или сотрудника, коммуникативные способности, деловую активность, потребности в самоутверждении и самореализации.

Программный алгоритм выбора рациональных совокупностей субтипов социального ядра личности включает множество возможных комбинаций и представляет 27 позиций. В итоге производится корреляция по совокупности позиций, дифференциация на группы, которые представляют собой однотипные социальные группы, принадлежащие к установленному субтипу. В результате определенные субтипы реализуют похожие принципы по отношению к социуму, для них характерны подобные мотивы деятельности для конкретных условий труда при решении тех или иных задач. Как правило, они однотипно реагируют на внешние раздражители или обстоятельства. Это позволяет прогнозировать эффективность обеспечения информационной безопасности корпорации [Козачок 2005, 2016б].

Новизна подхода и направление дальнейших исследований

Управление обеспечением информационной безопасности корпорации – это комплекс мероприятий по планированию, организации, мотивации и контролю с целью стабилизации или изменения ее состояния для достижения поставленных целей. Планирование и организация деятельности любой системы являются делом обычным, а вот мотивация сотрудников на поддержание порядка и соблюдение требований по обеспечению информационной безопасности в корпорации – это направление, требующее особого внимания и целенаправленного социального управления. Очевидно, что технические аспекты обеспечения информационной безопасности реализуются через правила применения средств защиты информации, и их выполнение гарантирует достижение результата. Однако даже в специально разработанной системе не исключены уязвимости, приводящие к утечкам конфиденциальной информации из-за так называемого человеческого фактора – нарушения правил применения технических средств.

Классическая схема управления информационной безопасностью корпорации достигла предела своих потенциальных возможностей и не позволяет наращивать результативность управления. Социальное управление должно рассматриваться как тонкая настройка классической системы управления корпорацией, что позволит усилить действенность подсистем управления.

Новизна предлагаемого подхода заключается в применении социологического инструментария в системе обеспечения информационной безопасности корпорации, благодаря чему появляется возможность повышения эффективности социального управления.

Направление дальнейших исследований связано с созданием специальных методик оценки социального ядра личности для кандидатов и сотрудников, занимающихся обеспечением информационной безопасности, и для работающих с информацией ограниченного распространения. Результаты оценивания позво-

лят сформировать социологическое обеспечение для администрации корпорации. На их основе администрация сможет принимать обоснованные решения по назначению и перемещению на должности лиц, которые по уровню социального развития способны выполнять работу с конфиденциальной информацией без нарушения требований по обеспечению информационной безопасности.

В заключение хочется подчеркнуть, что подсистема организационного обеспечения информационной безопасности корпорации наиболее критична к нарушениям со стороны персонала. Другие инструменты, кроме социальных и психологических, в этой системе применить не представляется возможным, поэтому и становится очень важной задача создания комплекса мер по отбору кандидатов для работы и их мотивации к исполнению организационных требований обеспечения сохранности информации и недопущению нарушений выработанных требований.

Список литературы:

Велигура А.Н. 2013. О требованиях к модели процесса обеспечения информационной безопасности и подходах к ее созданию. – *Информационная безопасность*. Т. 16. № 1. С. 131-134.

Воронцов С.А., Штейнбух А.Г. 2015. О необходимости совершенствования подходов к обеспечению национальной безопасности России в информационной сфере. – *Наука и образование: хозяйство и экономика; предпринимательство; право и управление*. № 9(64). С. 100-108.

Журавлев Н.Ю., Лобжанидзе Н.Д., Белоусов Р.Г. 2015. Сравнительная характеристика подходов к обеспечению информационной безопасности в РФ и США. – *Актуальные направления научных исследований XXI века: Теория и практика*. № 7-4(18-4). Т. 3. С. 176-179.

Киреева О.Ф. 2013. Социологическая диагностика информационной безопасности информационно-коммуникационной среды. – *Труд и социальные отношения*. № 12. С. 35-42.

Козачок А.В. 2012. *Распознавание вредоносного программного обеспечения на основе скрытых марковских моделей:* автореф. дис. ... к.тех.н. Воронеж: ВГТУ. 19 с.

Козачок В.И. 2005. Диагностика управленческого потенциала персонала федерального органа исполнительной власти. – *Право и образование*. № 2. С. 191-204.

Козачок В.И. 2007. *Социологическое обеспечение процессов формирования аппарата управления в федеральных органах исполнительной власти*: автореф. дис. ... д.соц.н. Орел: Академия ФСО. 51 с.

Козачок В.И. 2012. Исследование существующей системы отбора кандидатов на должности руководителей. – *Среднерусский вестник общественных наук*. № 2. С. 35-38.

Козачок В.И. 2016а. Методология социологического обеспечения формирования аппарата управления. – *Среднерусский вестник общественных наук*. Т. 11. № 4. С. 18-25.

Козачок В.И. 2016б. Подсистема социологического обеспечения реализации кадровой политики. – *Концепция устойчивого развития науки третьего тысячелетия:* сборник научных статей по итогам международной научно-практической конференции. СПб: КультИнформПресс. С. 60-63.

Лазуткин А.Н. 2015. Аудит информационной безопасности на промышленном предприятии. – *Новая наука: Стратегии и векторы развития*. № 5-2. С. 142-144.

Alhogail A. 2015. Design and Validation of Information Security Culture Framework. – *Computers in Human Behavior*. Amsterdam, Netherlands. Vol. 49. P. 567-575.

Beznosov K., Beznosova O. 2007. On the Imbalance of the Security Problem Space and Its Expected Consequences. – *Proceedings of the International Symposium on*

Human Aspects of Information Security & Assurance (HAISA 2007). Vancouver, Canada: University of British Columbia. URL: http://www.emeraldinsight.com/doi/full/10.1108/09685220710831152 (accessed 14.09.2016).

Kearney W., Kruger H. 2016. Can Perceptual Differences Account for Enigmatic Information Security Behaviour in an Organisation? – *Computer Security*. Oxford, UK. Vol. 61. P. 46-58.

Kretzer M., Madche A. 2015. Which Are the Most Effective Measures for Improving Employees' Security Compliance? – *Proceedings of the 36th International Conference on Information Systems (ICIS)*. Fort Worth. P. 1-17.

Rao A. 2014. Less is More?: Investigating the Role of Examples in Security Studies Using Analogical Transfer. – Rao A. et al. *Proceedings of the 2014 Symposium and Bootcamp on the Science of Security*. N.Y., USA. P. 7-12.

Savola R.M. 2007. Towards a Taxonomy for Information Security Metrics. – *Proceedings of the 2007 ACM Workshop on Quality of Protection*. N.Y., USA: ACM. P. 28-30.

Sohrabi Safa N., Von Solms R., Furnell S. 2016. Information Security Policy Compliance Model in Organizations. – *Computer Security*. Oxford, UK. Vol. 56. P. 70-82.

Tu Z., Yuan Y. 2014. Critical Success Factors Analysis on Effective Information Security Management: A Literature Review. – *Proceedings of the 20th Americas Conference on Information Systems*. Savannah. P. 1-18.

Von Solms R., Van Niekerk J. 2013. From Information Security to Cyber Security. – *Computers Security*. Vol. 38. P. 97-102.

Yaokumah W. 2016. Investigation into the State-of-Practice of Operations Security Management Based on ISO/IEC 27002. – *International Journal of Technology Diffusion*. Hershey, PA, USA. Vol. 7. P. 53-72.

KOZACHOK Vasily Ivanivich, *Dr.Sci. (Soc.), Professor; Researcher of Academy of Federal Security Guard Service of the Russian Federation (35 Priborostroitel'naya St, Oryol, Russia, 302034; kosachok@list.ru)*

CORPORATION INFORMATION SECURITY AS AN OBJECT OF SOCIAL MANAGEMENT

Abstract. *This article is devoted to the actualization of the role of human factor in the system of management of corporation information security. The analysis of the confidential information leaks facts according to the major news agencies is carried out and security incidents sources are compared. Dependence in increasing the number of confidential information leaks due to fault of the staff with well-functioning technical information protection system is confirmed. The author proposes to calculate personnel social metrics and outlines proposals of its implementation through the social control mechanisms. Metrics are based on the estimation of procedure of social personality core formation, namely social competence, social compatibility and social readiness of employees for ensuring information security. The article determines scale indicators of social personality core and presents semantic description of their values for the management system of corporation information security.*
Keywords: *information security, corporation, information security incidents, information leakage, information security threats, social management, social competence, social readiness, social compatibility, social personality core*