УДК 316:42.35
DOI: 10.17223/1998863X/44/17

В.И. Козачок

СОЦИОЛОГИЧЕСКАЯ ОЦЕНКА ПЕРСОНАЛА КАК ФАКТОР ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОРПОРАЦИИ

Статья посвящена проблеме социально-диагностической оценки человека в системе управления обеспечением информационной безопасности корпорации. Рассмотрены не технические меры, а социальные механизмы совершенствования деятельности подразделений по защите информации. В статье подтверждается тенденция роста числа инцидентов утечек информации по вине персонала подразделений обеспечения информационной безопасности. Автор приводит методику социологической оценки готовности персонала к эффективному решению задач по предупреждению утечек конфиденциальной информации. Предлагаемая авторская методика позволяет в кратчайшие сроки и наиболее полно провести диагностику персонала: потенциальных претендентов, работающих сотрудников, обеспечивающих информационную безопасность корпорации.

Ключевые слова: *утечки информации, угрозы информационной безопасности, диагностика персонала, социальное управление, социальная компетентность, социальная готовность, социальная совместимость, социальное ядро личности.*

Введение

По мнению аналитиков 2015 г. стал годом утечек, и не только благодаря нашумевшему взлому аккаунта военного командования Соединенных Штатов Америки в социальных сетях так называемой группировкой «Киберхалифат» или взлому почтового аккаунта Натальи Тимаковой – пресс-секретаря Дмитрия Медведева хакерской группой «Анонимный интернационал» [1]. Именно данные аналитических отчетов [2–4] подтвердили общую сумму ущерба по причине утечек конфиденциальной информации, которая выросла в 2015 г. почти на одну четвертую и превысила 25 млрд долларов США. Каждая значительная утечка информации оценивается суммой потерь в среднем приблизительно 31 млн долларов. Процессы утечек не оставили в стороне и отечественные корпорации, их убытки составляют 6% от общей суммы ущерба [3, 4]. В 2015 г. по сравнению с 2014 г. суммарный ущерб увеличился на 33%. Для всех зафиксированных инцидентов общей является тенденция, выявленная в ходе расследования: почти 37% нарушений случились по вине сотрудников, но не умышленно (сознательно), а из-за невнимательности или вследствие допущенных ошибок [5–8]. По данным компании InfoWatch[2] 37% инцидентов произошли по вине сотрудников, только в первом полугодии 2016 г. 67% случаев утраты данных произошли из-за вины внутреннего нарушителя, при этом 1% происшествий допущены высшими руководителями организаций [3, 4].

[1] InfoWatch – российская компания, специализирующаяся на информационной безопасности в корпоративном секторе. См.: URL: https://www.infowatch.ru/

В современной системе обеспечения информационной безопасности темпы роста числа инцидентов (утечек информации) и, как следствие, наносимого ущерба гораздо выше темпов роста финансовых затрат на защиту информации корпораций [6]. По данным компании PwC[1], в крупных компаниях затраты по этой статье расходов составляют почти 11 млн долларов США, малые компании вынуждены тратить до одного миллиона долларов. Лавинообразный рост числа инцидентов информационной безопасности существенно снижает эффективность значительных финансовых вложений, так как доля ущерба, наносимого утечками, составляет от 40 до 60% [6, 7].

Общая сумма ущерба из-за утечек конфиденциальной информации, по оценке международных экспертов, в 2015 г. выросла на 25% и превысила 25 млрд долларов. За 2015 г. в США произошло 859 утечек информации, в России – 118 инцидентов, в Великобритании – 112 [6]. Поэтому не случайно в экспертной среде 2015 г. назван годом утечек информации.

Распределение известных инцидентов различной направленности выглядит следующим образом: 20,2% инцидентов в медицинских учреждениях, 15,9% – в государственном секторе, 14,9% – в образовательных учреждениях, 10,9% – на предприятиях розничной торговли [6]. Причем стоит отметить, что в госучреждениях «совершенная» система сохранности тайны систематически контролируется специальными подразделениями.

Анализ отчетов и аналитических материалов компании InfoWatch [3, 4] позволил сделать вывод, что распределение утечек информации по воздействию угроз практически не является субстанциальным. Диапазон изменений значений процентов достаточно большой, что подтверждает необходимость внесения корректирующих изменений в существующую систему управления информационной безопасностью. Особое внимание при этом следует обратить на аспекты социального управления информационной безопасностью корпорации, так как за последние три года почти 70% инцидентов произошли по вине персонала, работающего в корпорации.

Более детальный анализ составляющих векторов утечек конфиденциальной информации по категориям виновников позволяет утверждать, что наряду с постепенным снижением числа нарушений со стороны руководителей из года в год возрастает количество инцидентов, происходящих по вине рядовых сотрудников корпораций.

В целом анализ инцидентов, приводящих к утечкам конфиденциальной информации, подтверждает неуклонный рост числа нарушений, с одной стороны, а с другой – прослеживается перекос в сторону совершенствования и финансирования технической стороны обеспечения информационной безопасности корпорации [9, 10]. Проблема заключается в том, что социальный аспект остается вне рамок методического обеспечения, отсутствует инструментарий оценивания готовности персонала корпорации компетентно решать задачи по обеспечению информационной безопасности. Следовательно, система организационно-режимных мер обеспечения информационной безопасности корпорации нуждается в вовлечении механизмов социального управления в арсенал защиты информации [11, 12]. Одним из них является

[1] PwC – группа международных аудиторско-консалтинговых компаний. См.: URL: http://www.pwc.com/

формирование метрик персонала системы обеспечения информационной безопасности, а именно социологического обеспечения [13].

Социологическое обеспечение по результатам диагностики персонала корпорации

Решение практических задач в сфере информационной безопасности определяется прикладными интересами корпораций [14–16], которые связаны с системой отбора, подготовки, расстановки кадров обеспечивающих защиту информации.

Социологическое обеспечение – совокупность информации и алгоритмы ее обработки, связанные с решением следующих задач:

– оценка реального состояния эффективности социального управленческого воздействия на процессы обеспечения информационной безопасности корпорации;

– установление степени влияния определяющих факторов;

– предложение научно-обоснованных рекомендаций по осуществлению требуемых управленческих воздействий по предотвращению инцидентов информационной безопасности.

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 [17].

Формальная постановка задачи по социальной оценке персонала в процессе решения задач обеспечения информационной безопасности корпорации

Формальная постановка задачи

Для описания формальной постановки задачи социальной квалиметрии персонала необходимо ввести ряд обозначений:

$C = \{c_i\}$ – множество значений параметра социальной компетентности (Ск);

$R = \{r_i\}$ – множество значений параметра социальной готовности (Сг);

$E = \{e_i\}$ – множество значений параметра социальной совместимости (Сс);

$i = \overline{1, 3}$ – числовые значения соответствующих категориальных значений (низкий, средний, высокий);

$H = \{h_j\}, j = \overline{1, N}$ – множество сотрудников корпорации;

$T = \{t_k\}, k = \overline{1, M}$ – множество решаемых задач в сфере информационной безопасности;

$Q(h, t)$ – потенциально возможный ущерб от действий сотрудника h при решении задачи t.

Каждого сотрудника корпорации h можно описать в базисе CRE (СкСгСс) с помощью тройки значений:

$$h = < c, r, e >. \quad (1)$$

Необходимо построить отображение при условии минимизации:

$$F : H \to T \mid \min_{H} Q(h, t). \quad (2)$$

Требуется:

Разработать подход эффективного подбора, расстановки и управления персоналом системы обеспечения информационной безопасности корпорации, позволяющий повысить эффективность мероприятий по обеспечению информационной безопасности.

С этой целью провести:

1. Разработку модели социального ядра личности для сотрудников корпорации, обеспечивающих информационную безопасность. Нормировав их уровни сформированности социальной готовности, социальной компетентности, а также социальной совместимости, соотнести оцениваемого кандидата к конкретному субтипу личности.

2. Синтез алгоритма по выбору рациональных подмножеств субтипов социального ядра личности, которая наиболее предпочтительна для работы в подразделении по защите информации в корпорации.

3. Обоснование научно-практических предложений по реализации социального управления обеспечением информационной безопасности корпорации.

Основные допущения:

– программно-аппаратные комплексы и системы обеспечения информационной безопасности являются исправными;

– руководители корпорации имеют возможность фиксации и анализа социально-психологических метрик сотрудников корпорации и кандидатов для работы в системе обеспечения информационной безопасности;

– персонал корпорации в рамках своих должностных полномочий обучен специфике обеспечения информационной безопасности.

Ограничения:

– задача решается в условиях мирного времени;

– корпорация не относится к секретным объектам государства.

В содержании настоящей работы описаны результаты решения первой частной научной задачи исследования.

Итоги диагностики персонала в числовых показателях отображают значение уровня социализации конкретной личности, с одной стороны, и результат самопроецирования человека по отношению к социуму, окружающему его, – с другой. Сведения, полученные в результате диагностики, дают возможность оценить кандидата и его взаимоотношения с обществом и происходящими в нем процессами. Внутренняя мотивация человека и его реальные действия определяются не только и не столько обстоятельствами, а во многом или в основном результатом социализации личности. Пример: если сотрудник, выполняя свои обязанности, в условиях выбора действия или бездействия не ставит во главу угла интересы корпорации в рамках обеспечения информационной безопасности, а считает более важным личную выгоду, то в этих условиях подобная жизненная позиция не является его «личным делом», так как она может нанести или наносит ущерб корпорации. Поэтому предметом детального анализа со стороны руководителей корпорации должны быть особенности результата социализации диагностируемого кандидата. Очевидно, что измеренные показатели социализации изучаемого сотрудника корпо-

рации не представляют собой секретных данных, так как они проявляются им открыто, совершенно осознанно и целенаправленно. Кроме того, показатели социализации остаются практически неизменными на определенном промежутке времени, что позволяет зафиксировать эту информацию, применяя предлагаемую автором методику диагностики, которая не нарушает права личности, и не является запретом на определенную профессию. Исследования подтверждают, что в ходе целенаправленной работы кандидата над собой может измениться не только темперамент, но и результат предшествующей социализации.

Поэтому данные, полученные в результате применения методики социальной диагностики, позволяют в короткий срок и при минимальных затратах обеспечить администрацию корпорации объективной, достаточно полной количественной информацией о результатах предшествующей социализации сотрудника и его значимых особенностях [14]. При этом весьма важным является тот факт, что приобрести данную информацию за столь короткое время не представляется возможным другими способами или средствами. Это подтверждает практика рекрутинговых компаний: даже отличные рекомендации с прежнего места работы или длительное наблюдение за кандидатом не позволяют обеспечить требуемую достоверность оценок и выводов о совокупности конкретных особенностей кандидата. Кроме того, зафиксированные по результатам диагностики сведения позволяют сопоставить и сравнить кандидатов между собой, а при необходимости выявить интересующие тенденции, провести прогнозирование и сформулировать обоснованные выводы. Результат оценки уровня социализации требуется прежде всего для целенаправленной организации управленческого воздействия на сотрудников корпорации. Оптимальная расстановка сотрудников, их обучение и актуализация их адекватной мотивации, выявление реальных причин, приведших к тем или иным нарушениям требований обеспечения информационной безопасности в корпорации [18], немыслимы без принятия обоснованных социально выверенных управленческих решений.

Модель социального ядра личности сотрудника

Социальное ядро личности отражает результаты процессов социализации человека на протяжении его развития, образования и взаимодействия с сотрудниками и обществом. Понятие ядра личности подробно рассматривается в психологии как полуизменяемая часть индивида, сформированная по максимуму в детстве и на первых этапах развития структура. По мнению А.Н. Леонтьева, «личность человека „производится“ – создается общественными отношениями» [18]. Очевидно, что не только психическое становление личности индивида, но и ее социальное развития обеспечивает формирование полноценного члена общества. Проведенные автором исследования [17] позволяют утверждать о существовании социального ядра личности, представленного триединой структурой: социальной компетентности, социальной готовности и социальной совместимости. Предложенный автором подход не противоречит существующим подходам в психологии и позволяет уточнить отдельные положения в социологии управления.

Судить о сформированности или не сформированности той или иной составляющей части социального ядра конкретного человека можно тогда, ко-

гда выполнено шкалирование полученных результатов диагностической оценки личности кандидата на должность по обеспечению информационной безопасности корпорации. Графическое представление интервальных шкал значений диагностики показывает различные варианты распределения результатов (рис. 1).

Результат агрегирования полученных сведений социальной диагностики представлен в виде набора трех оценок, при этом каждая из них отражает сформированность составляющей социального ядра личности в абсолютных величинах на конкретной шкале. Таким образом, результат оценивания заносится на шкалу в интервале от 0 до 100. Социализация сотрудника считается нормой, если результат диагностики находится в диапазоне 40–60 единиц. Низкими результатами социализации личности считаются показатели ниже 40 по конкретной составляющей социального ядра. Учитывая важность и сложность задач по обеспечению информационной безопасности, а также последствия возможного ущерба для корпорации с учетом существующих рисков результат социализации предпочтительного кандидата должен быть выше 60 баллов [19].

Рис. 1. Интервальные шкалы оценивания компонентов социального ядра человека

Каждой интервальной шкале оценивания компонент социального ядра диагностируемого сотрудника дан содержательный шифр, который при записи обозначается биграммой от собственного названия:

– Ск – шкала социальной компетентности;
– Сг – шкала социальной готовности;
– Сс – шкала социальной совместимости.

Интерпретация результатов измерений

Трактовка конкретных оценок результатов диагностики требует подробного описания сути и критериев оценивания социальной готовности личности к выполнению задач по защите информации. С одной стороны, такая интерпретация позволит администрации, принимающей решение, осознать недопустимость метаморфозы результатов диагностики социального ядра личности в догму, ярлык или штамп, с другой – является подходом редуцирования индивида как свободной в своем формировании личности многомерной общественной сущности до значения предсказуемого и программируемого на необходимый результат объекта. Поэтому представленная совокупность сведений о диагностических шкалах позволяет рассматривать кандидата или сотрудника подразделения по обеспечению информационной безопасности более полно, объемно и оценивать его особенности с позиции целевого функционала как работника корпорации. Исследования показывают, что по данным шкалам требуется проводить оценивание не только штатных сотрудников подразделений по обеспечению информационной безопасности, но и

всех работников корпорации, связанных с обработкой конфиденциальной информации. Эти сотрудники в процессе работы в той или иной мере решают задачи по обеспечению неразглашения или недопущению хищения конфиденциальной информации в ходе повседневной деятельности.

В процедуре диагностики социального ядра конкретного лица социальная компетентность личности (Ск) отражает оценку навыков, умений и знаний конкретного сотрудника корпорации, усвоенных и приобретенных им вследствие взаимодействия с социумом, это предполагает выделение из полного множества навыков, умений и знаний личности тех, которые напрямую характеризуют ее социализацию. Социальная компетентность личности – это способность правильно ориентироваться в социальном пространстве.

Оценки в интервале **от 60 до 100 баллов** означают, что кандидат обладает исключительными способностями, которые позволят ему организовать рациональное взаимодействие в коллективе корпорации на основе имеющихся интеллекта и сформированных компетенций. Благодаря этому диагностируемый кандидат не испытывает сложностей при выполнении должностных обязанностей. Кроме того, его результаты обладают устойчивой положительной динамикой в деятельности корпорации. Высокие потенциальные возможности кандидата не ограничивают пределов его карьерного роста.

Полученные оценки в интервале **40–60 баллов** позволят сопоставить диагностируемого кандидата с типовым среднестатистическим индивидом. Администрация корпорации сможет оценить степень соответствия его образования, соответствует ли он квалификационным требованиям к конкретной должности, и как при наличии профессиональной и специальной подготовки кандидат справится с имеющимся объемом задач на конкретной должности. В целом имеющиеся опыт и навыки дают возможность работать производительно, эффективно и грамотно. Однако постоянство высоких результатов деятельности потребует значительных усилий со стороны кандидата. На определенном этапе при изменении статуса сотрудника возможны сбои, так как диагностируемый кандидат обладает ограниченным запасом определенных возможностей.

Показатели диагностической оценки социальной компетентности кандидата **менее 40 баллов** свидетельствуют о том, что в процессе диагностики исследуемая личность, несмотря на выполнение квалификационных требований по образовательному цензу, не продемонстрировала минимального набора необходимых компетенций. Этот факт обусловливает прогноз низкой эффективности при выполнении служебных задач, отсутствие необходимой самостоятельности. Слабые задатки к осмыслению происходящих событий и рациональному познанию не позволяют наращивать темпы положительной динамики и результативности деятельности; человек испытывает сложности в решении больших объемов разнородных нетиповых задач. Именно поэтому для такого кандидата потребуется значительная по объему и времени формирующе-развивающая доподготовка в целях повышения уровня «социальной компетентности».

Диагностика социальной готовности (Сг) кандидата позволяет провести оценку его сложившегося мировоззрения, отношения и понимания собственной миссии в социальной действительности. Собственно, через призму его

мировоззрения кандидат воспринимает окружающую действительность, перерабатывает поступившую информацию, реализует принятые им решения.

Когда результаты диагностического оценивания по шкале социальной готовности **превосходят 60 баллов**, диагностируемый кандидат характеризуется повышенной активностью по осуществлению принятых решений, а его превосходные организаторские качества и настойчивость позволяют вовлечь в эти процессы других сотрудников корпорации и подтверждают лидерский характер диагностируемого. Обычно такие кандидаты испытывают постоянную потребность в работе, решении сложных и нестандартных задач, а также познании нового. Как правило, кандидаты такого типа отличаются высокой нормативностью поведения и постоянным стремлением соответствовать духовным, моральным и нравственным нормам общества, при невозможности получения удовлетворенности условиями быта или работы стараются изменить положение вещей, высокоэффективно и рационально используют как личное, так и рабочее время в корпорации.

Оценка в интервале **40–60 баллов** представляет, что диагностируемый кандидат обладает хорошими организаторскими качествами, систематически проявляет деловую активность, обязательность и дисциплинированность. Достаточные потребности в самоутверждении и самореализации выражаются в формировании конкретных целей и оптимальных программ их достижения, время при этом используется рационально. Кандидат данного типа соблюдает принятые в коллективе корпорации правила поведения, но способен по некоторым позициям отстаивать личное мнение в створе общепринятых моральных и нравственных норм. Неудовлетворенность обстоятельствами на работе или в быту иногда служит причиной проявления деловой инициативности.

Оценки в интервале **от 0 до 40 баллов** характеризуют диагностируемого кандидата как человека со слабыми организаторскими и деловыми качествами и поэтому сниженной социальной активностью: присущая пассивность обусловливает низкое проявление потребности в познании и труде. Поведение оцениваемого кандидата на работе в корпорации не всегда соответствует общепринятым нормам в коллективе. Отмечается неудовлетворенность условиями быта и работы, но кандидат не принимает никаких усилий для изменения сложившегося положения дел. Личное и рабочее время распределяется малорационально, возможно накопление незавершенных основных задач с ликвидацией методами «авралов» сверх рабочего времени. Такой тип оцениваемого кандидата догматичен, практически всегда лоялен к общественному мнению, в первую очередь лидеров или руководителей, обладающих высоким авторитетом или властью. Воспринимает верность общепринятых представлений как внешнюю непреодолимую силу, поэтому не принимает на себя ответственность за истинность своих и чужих суждений, отдает предпочтение авторитетным суждениям. Если выявляет в общепринятом мнении противоречие, то просто игнорирует его. Очень часто такой кандидат является высокоинтеллектуальной личностью с широкой эрудицией и блестящим образованием.

Интервальная шкала социальной совместимости (Сс) кандидата отражает устойчивое свойство личности выстраивать, а также поддерживать межличностные отношения с окружающими людьми. Понятие социальной совместимости следует рассматривать более широко, чем просто морально-психологический климат в подразделении корпорации. Социальная совме-

стимость подразумевает ее проявление как в устойчивых коллективах (семья, работа, друзья, партнеры), так и в эпизодических отношениях (общественные места, общественный транспорт и др.). Именно социальная совместимость кандидата в коллективе подразделения информационной безопасности определяет результативность работы команды в целом и отдельных сотрудников в частности, гордость за принадлежность к коллективу и результатам, полученным в ходе совместных действий, взаимовыручку, сплоченность команды, будущее успешное развития всего коллектива подразделения.

Высокой оценкой по шкале социальной совместимости считается результат от **60 баллов и более,** он показывает, что кандидат целиком адаптировался в конкретной социальной среде, для него характерны значительная потребность в согласованном взаимодействии с каждым членом команды и высокая социальная мобильность на основе добротных коммуникативных способностей. Взаимоотношения в коллективе и со случайными людьми диагностируемый кандидат строит на основе личных материальных и духовных потребностей. Доброжелательность и непосредственность во взаимодействии с коллегами позволяют оцениваемому кандидату в коллективе строить выверенные межличностные отношения, а широкий круг друзей и знакомых позволяет верно определить род и сферу занятий, а также поддерживать свое материальное положение. Кроме того, умение сотрудничать с разными людьми способствует повышению результативности его труда, что в целом положительно влияет на динамику общих результатов деятельности команды. Вероятно, такой кандидат более успешен при командном решении задач по обеспечению информационной безопасности и способен эффективно руководить коллективом.

Оценки в интервале **40–60 баллов** позволяют утверждать, что кандидат обладает обычными способностями межличностной социально-психологической совместимости. При этом общение не является доминирующей потребностью в его деятельности, однако кандидат обладает хорошими коммуникативными способностями и испытывает значительную потребность в разумном взаимодействии с социумом. Его работа и ее результативность в основном определяются умением классически строить взаимоотношения с членами команды, хотя в основном эти отношения носят, как правило, сугубо деловой характер. Устойчивая система внутренних установок и стереотипов, сформированная у кандидата, позволяет адекватно оценивать коллег, а также при необходимости привлекать их к реализации актуальных задач по обеспечению информационной безопасности корпорации.

Результаты оценивания **ниже 40 баллов** свидетельствуют о том, что диагностируемый кандидат соответствует такому типу личности, для которого социальное взаимодействие – это не потребность, а производственная или коммерческая необходимость. Низкие показатели коммуникативности и недостаточная социальная мобильность предопределяют значительные трудности в коллективной работе при решении задач по обеспечению информационной безопасности в корпорации. Обычно человек такого типа чувствует себя комфортно в условиях, когда порученная ему задача требует лишь персональных усилий, отсутствует потребность в привлечении других сотрудников команды. В любом коллективе подобные работники практически малоза-

метны, хотя могут и успешно решают сложные и важные задачи, не требующие согласованных действий с коллегами.

Сочетание трех интервалов диагностических оценок на трех шкалах служит основой для формирования полного множества оценивания результатов измерений. Число гипотетически возможных комбинаций субтипов оцениваемых кандидатов равно 27 [20]. Множество комбинаций субтипов в интервале: наилучший кандидат – **ВВВ** (высокие значения показателей социальных компетентности, готовности и совместимости кандидата), наихудший – **ННН** (низкие значения составляющих социального ядра диагностируемого кандидата), – приведены в таблице.

Результаты диагностики социального ядра личности

Позиции	Ск	Сг	Сп		Позции	Ск	Сг	Сс
01	***В***	***В***	***В***		15	***Н***	***С***	***В***
02	***В***	***В***	***С***		16	***Н***	***В***	***Н***
03	***С***	***В***	***В***		17	***Н***	***Н***	***В***
04	***В***	***С***	***В***		18	***В***	***Н***	***С***
05	***С***	***С***	***В***		19	***С***	***Н***	***В***
06	***В***	***С***	***С***		20	***В***	***Н***	***Н***
07	***С***	***В***	***С***		21	***С***	***С***	***Н***
08	***С***	***С***	***С***		22	***Н***	***С***	***С***
09	***В***	***В***	***Н***		23	***С***	***Н***	***С***
10	***В***	***Н***	***В***		24	***Н***	***С***	***Н***
11	***Н***	***В***	***В***		25	***Н***	***Н***	***С***
12	***С***	***В***	***Н***		26	***С***	***Н***	***Н***
13	***В***	***С***	***Н***		27	***Н***	***Н***	***Н***
14	***Н***	***В***	***С***					

Примечание. Ск – социальная компетентность; Сг – социальная готовность; Сс – социальная совместимость; ***В*** – высокий уровень, более 60; ***С*** – средний уровень, от 40 до 60; ***Н*** – низкий уровень, менее 40.

Рассмотрение приведенного в таблице полного множества возможных комбинаций результатов измерений (составляющие социального ядра кандидата) позволило разделить их на три группы. Результаты измерений, соответствующие позициям 21–27, свидетельствуют об очевидной незавершенности процессов социализации личности и нежелательности использовать таких сотрудников для решения задач по обеспечению информационной безопасности. Совокупность позиций 14–17 соответствует группе кандидатов с несформированной социальной компетентностью, а результаты измерений с 18-й до 20-й позиции определяют кандидатов с низкой социальной готовностью. Потенциально конфликтными, что неприемлемо для подразделений обеспечения информационной безопасности, являются кандидаты, набравшие по результатам диагностики оценки, соответствующие 12-й и 13-й позициям. Оцениваемый кандидат характеризуется как профессионал при получении результатов диагностики, соответствующих позиции 08. В свою очередь, подмножество позиций с 09-й по 11-ю определяют типаж недоученного, бесцельного и несовместимого сотрудника корпорации. Особенную

группу представляет совокупность позиций 01–07, соответствующих характеристике так называемых готовых (позиции с 01 по 04), а также потенциально готовых (позиции с 05 по 07) кандидатов к успешному решению задач по обеспечению информационной безопасности.

Таким образом, множество кандидатов с определенной комбинацией результатов по шкалам оценивания сформируют однотипную социальную группу, принадлежащую к установленному субтипу. Сотрудники такого субтипа 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, такие кандидаты однотипно реагируют на внешние раздражители или обстоятельства [21].

Заключение

Предлагаемая автором методика позволяет эффективно использовать социологический инструментарий в системе обеспечения информационной безопасности корпорации. Данная методика успешно апробирована ПАО «Орелтекмаш». В результате применения данной методики осуществляется реорганизация системы социального управления. Методика апробирована в малых и средних корпорациях. Результаты оценивания социального ядра личности позволят сформировать социологическое обеспечение, на основе которого администрация корпорации 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.

Литература

1. *Хакерские атаки* – 2015. URL: https://www.gazeta.ru/tech/2015/12/24/ 7989839/best-hacks-2015.shtml (дата обращения: 09.11.2016).

2. *Аналитика*. Международные новости утечек информации, ежегодные аналитические отчеты и статистика по инцидентам за прошедшие годы URL: http://www.infowatch.ru/analytics/reports# (дата обращения: 14.09.2016).

3. *Глобальное* исследование утечек конфиденциальной информации в 2015 году // InfoWatch. URL: https://www.infowatch.ru/sites/default/files/report/analytics/russ/InfoWatch_Global_Report_2015.pdf (дата обращения: 14.05.2018).

4. *Глобальное* исследование утечек конфиденциальной информации в 2016 году // InfoWatch. URL: https://www.infowatch.ru/sites/default/files/report/analytics/russ/InfoWatch_Global_Report_2016.pdf (дата обращения: 14.05.2018).

5. *Ruiz R., Winter R., Amatte F.* The leakage of passwords from home banking sites: a threat to global cyber security? // Journal of Payments Strategy & Systems. 2017. Т. 11, № 2. С. 174–186.

6. *Управление* киберрисками во взаимосвязанном мире : глобальное исследование по вопросам обеспечения информационной безопасности // PricewaterhouseCoopers. 2015. URL: http://www.pwc.ru/ru/riskassurance/ publications/assets/managing-cyberrisks.pdf (дата обращения: 25.07.2016).

7. *Thomas K. et al.* Data Breaches, Phishing, or Malware?: Understanding the Risks of Stolen Credentials // Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2017. С. 1421–1434.

8. *Das S. et al.* Breaking! A Typology of Security and Privacy News and How It's Shared // Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems. ACM, 2018. С. 1–12.

9. *Data* loss prevention. Insights on governance, risk and compliance. Keeping your sensitive data out of the public domain // Ernst & Young. 2011. URL: http://www.ey.com/Pub-

lication/vwLUAssets/EY_Data_Loss_Prevention/$FILE/EY_Data_Loss_Prevention.pdf (accessed: 14.05.2018).

10. *Козачок А.В.* Распознавание вредоносного программного обеспечения на основе скрытых марковских моделей : дис. … канд. техн. наук. Воронеж, 2012.

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

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

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

14. *Savola R.M.* Towards a Taxonomy for Information Security Metrics // Proceedings of the 2007 ACM Workshop on Quality of Protection. New York : ACM, 2007. P. 28–30.

15. *Von Solms R., Van Niekerk J.* From information security to cyber security // Computers Security. 2013. Vol. 38. P. 97–102.

16. *Киреева О.Ф.* Социологическая диагностика информационной безопасности информационно-коммуникационной среды // Труд и социальные отношения. М. : Академия труда и социальных отношений. 2013. №. 12. С. 35–42.

17. *Козачок В.И.* Социологическое обеспечение процессов формирования аппарата управления в федеральных органах исполнительной власти : автореф. дис. ... д-ра социол. наук. Орел, 2007. 51 с.

18. *Психологические* теории личности URL: http://studbooks.net/1340405/psihologiya/psihologicheskie_teorii_lichnosti (дата обращения: 17.05.18).

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

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

21. *Козачок В.И.* Информационная безопасность корпорации как объект социального управления // Власть. 2017. Т. 284, № 5. С. 74–82.

Vasiliy I. Kozachok, Academy of Federal Security Service of the Russian Federation (Moscow, Russian Federation).

E-mail: kosachok@list.ru

Vestnik Tomskogo gosudarstvennogo universiteta. Filosofiya. Sotsiologiya. Politologiya – Tomsk State University Journal of Philosophy, Sociology and Political Science. 2018. 44. pp. 169–182.

DOI: 10.17223/1998863X/44/17

SOCIOLOGICAL ASSESSMENT OF PERSONNEL AS A FACTOR IN ENSURING CORPORATION INFORMATION SECURITY

Keywords: information leakage; information security threats; personnel diagnostics; social management; social competence; social readiness; social compatibility; social core of personality.

The article is devoted to the problem of a person's social diagnostic assessment in the corporate information security management system. Non-technical information security techniques and social mechanisms to improve information security management are considered. The article confirms the tendency of increasing the number of information leaks due to the information security units faults. The author gives the description of staff readiness sociological assessment methodology to prevent confidential data leakage. The author's methodology is based on the results of corporation information security management sociological support. It means providing top managers (or information security staff) with relevant generalised and systematised information required to make management decisions based on the results of corporate employees sociological examination. The personality social core model for information security staff was developed. The levels of social readiness, social competence and social compatibility are normalised, which makes it possible to correlate the assessed candidate to a specific subtype from 27 hypothetically possible ones. The author's research allows stating that assessing a person's social core formation level makes it possible to permit a specific employee or candidate to work at an information security unit. The proposed author's methodology provides decision-makers with tools for personnel diagnostics and assesses potential applicants or employees from information security staff.

References

1. Korotkin, A. (2015) *Khakerskiye ataki – 2015* [Hacker attacks – 2015]. [Online] Available from: https://www.gazeta.ru/tech/2015/12/24/ 7989839/best-hacks-2015.shtml. (Accessed: 9th November 2016).

2. InfoWatch. (n.d.) *Analitika. Mezhdunarodnyye novosti utechek informatsii, yezhegodnyye analiticheskiye otchety i statistika po intsidentam za proshedshiye gody* [Analytics. International news leaks, annual analytical reports and incident statistics for past years]. [Online] Available from: http://www.infowatch.ru/ana-lytics/reports#. (Accessed: 14th September 2016).

3. InfoWatch. (2015) *Global'noye issledovaniye utechek konfidentsial'noy informatsii v 2015 godu* [Global investigation of leakage of confidential information in 2015]. [Online] Available from: https://www.infowatch.ru/sites/default/files/report/analytics/russ/InfoWatch_Global_Report_2015.pdf. (Accessed: 14th May 2018).

4. InfoWatch. (2016) *Global'noye issledovaniye utechek konfidentsial'noy informatsii v 2016 godu* [Global research on leakage of confidential information in 2016]. [Online] Available from: https://www.infowatch.ru/sites/default/files/report/analytics/russ/InfoWatch_Global_Report_2016.pdf. (Accessed: 14th May 2018).

5. Ruiz, R., Winter, R. & Amatte, F. (2017) The leakage of passwords from home banking sites: A threat to global cyber security? *Journal of Payments Strategy & Systems*. 11(2). pp. 174–186.

6. PricewaterhouseCoopers. (2015) *Upravleniye kiberriskami vo vzaimosvyazannom mire. Global'noye issledovaniye po voprosam obespecheniya informatsionnoy bezopasnosti* [Management of cyberries in an interconnected world. Global research on the issues of information security]. [Online] Available from: http://www.pwc.ru/ru/riskassurance/ publications/assets/managing-cyberrisks.pdf. (Accessed: 25th July 2016).

7. Thomas, K. et al. (2017) Data Breaches, Phishing, or Malware?: Understanding the Risks of Stolen Credentials. *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2017. pp. 1421–1434.

8. Das, S. et al. (2018) Breaking! A Typology of Security and Privacy News and How It's Shared. *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. ACM, 2018. pp. 1–12.

9. Ernst & Young. (2011) *Data loss prevention. Insights on governance, risk and compliance. Keeping your sensitive data out of the public domain*. [Online] Available from: http://www.ey.com/Publication/vwLUAssets/EY_Data_Loss_Prevention/$FILE/EY_Data_Loss_Prevention.pdf. (Accessed: 14th May 2018).

10. Kozachok, A.V. (2012) *Raspoznavaniye vredonosnogo programmnogo obespecheniya na osnove skrytykh markovskikh modeley* [Malware detection based on hidden Markov models]. Engineering Cand. Diss. Voronezh.

11. Zhuravlev, N.Yu., Lobzhanidze, N.D. & Belousov, R.G. (2015) Sravnitel'naya kharakteristika podkhodov k obespecheniyu informatsionnoy bezopasnosti v RF i SSHA [Comparative characteristics of approaches to ensuring information security in the Russian Federation and the USA]. *Aktual'naya napravleniya nauchnykh issledovaniy XXI veka: Teoriya i praktika.* 7–4 (3). pp. 176–179.

12. Vorontsov, S.A. & Shteynbukh, A.G. (2015) O neobkhodimosti sovershenstvovaniya podkhodov k obespecheniyu natsional'noy bezopasnosti Rossii v informatsionnoy sfere [On the need to improve approaches to ensuring the national security of Russia in the information sphere]. *Nauka i obrazovaniye: khozyaystvo i ekonomika; predprinimatel'stvo; pravo i upravleniye*. 9(64). pp. 100–108.

13. Kozachok, V.I. (2012) Issledovaniye sushchestvuyushchey sistemy otbora kandidatov na dolzhnosti rukovoditeley [The research of the existing system of selection of candidates for leadership positions]. *Srednerusskiy vestnik obshchestvennykh nauk – Central Russian Journal of Social Sciences*. 2. pp. 35–38.

14. Savola, R.M. (2007) Towards a Taxonomy for Information Security Metrics. *Proceedings of the 2007 ACM Workshop on Quality of Protection*. New York, USA: ACM. pp. 28–30.

15. Von Solms, R. & Van Niekerk, J. (2013) From information security to cyber security. *Computers Security*. 38. pp. 97–102. DOI: 10.1016/j.cose.2013.04.004

16. Kireyeva, O.F. (2013) Information- and communications environment: sociological diagnostics of information security. *Trud i sotsial'nyye otnosheniya – Labour and Social Relations*. 12. pp. 35–42. (In Russian).

17. Kozachok, V.I. (2007) *Sotsiologicheskoye obespecheniye protsessov formirovaniya apparata upravleniya v federal'nykh organakh ispolnitel'noy vlasti* [Sociological support of the processes of formation of the administrative apparatus in the federal executive bodies]. Abstract of Sociology Dr. Diss. Orel.

18. Studbooks.net. (n.d.) *Psikhologicheskiye teorii lichnosti* [Psychological Theories of Personality]. [Online] Available from: http://studbooks.net/1340405/psihologiya/psihologicheskie_teorii_lichnosti. (Accessed: 17th May 2018).

19. Kozachok, V.I. (2016) Methodology of sociological support of management staff formation. *Srednerusskiy vestnik obshchestvennykh nauk – Central Russian Journal of Social Sciences*. 11(4). pp. 18–25. (In Russian). DOI: 10.12737/21314

20. Kozachok, V.I. (2005) Diagnostika upravlencheskogo potentsiala personala federal'nogo organa ispolnitel'noy vlasti [Diagnostics of managment personnel potential of the federal executive body]. *Pravo i obrazovaniye – Law and Education*. 2. pp. 191–204.

21. Kozachok, V.I. (2017) Corporation Information Security as an Object of Social Management. *Vlast' – Power*. 284(5). pp. 74–82. (In Russian).