ОРГАНІЗАЦІЙНО-ПРАВОВІ ПИТАННЯ БЕЗПЕКИ ІНФОРМАЦІЇ / ORGANIZATIONAL & LAW INFORMATION SECURITY

КАДРОВЫЕ УЯЗВИМОСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ: МЕТОДИКА ОЦЕНКИ

Людмила Астахова

Южно-Уральский государственный университет, Российская Федерация

АСТАХОВА Людмила Викторовна, д.п.н., профессор

Год и место рождения: 1960 год, г. Челябинск, Россия.
Образование: Московский энергетический институт (технический университет), 2006 год.
Должность: профессор кафедры безопасности информационных систем.
Научные интересы: управление информационной безопасностью, подготовка кадров для сферы защиты информации.
Публикации: больше 200 научных публикаций, среди которых монографии, научные статьи и учебно-методическое пособие.
E-mail: **lvastachova@mail.ru**

Аннотация. *В статье представлена методика оценки кадровых уязвимостей информационной безопасности организации, разработанная на основе анализа нормативных документов, классификации причин дестабилизирующих воздействий на информацию ограниченного доступа и психологических тестов.*

Ключевые слова: *методика, оценка, информационная безопасность, кадровая уязвимость.*

Актуальность

Преступления, в том числе в информационной сфере, совершаются людьми. Большинство систем не может нормально функционировать без участия человека. Пользователь системы, с одной стороны, — ее необходимый элемент, а с другой - причина и движущая сила преступления. Вопросы безопасности систем большей частью есть вопросы человеческих отношений и человеческого поведения. Особенно это актуально в сфере защиты информации, т. к. инциденты в ней в подавляющем большинстве случаев происходят по вине сотрудников. В связи с этим существует необходимость в оценке кадровых уязвимостей информационной безопасности организации.

Состояние изученности проблемы

Названная проблема недостаточно исследована в науке. Вопросу анализа защищенности программно-технической составляющей информационных систем посвящено немало внимания, в то время как анализ защищённости пользователей информационных систем, т.е. кадровых уязвимостей информационной безопасности, находится на ранней стадии исследований.

Большой вклад в решение проблемы комплексной оценки персонала внес Г.А. Реймаров. Его работы посвящены методологии и практике использования компьютерных систем, предназначенных для комплексной оценки качества труда руководителей и специалистов промышленности, а также лиц, занятых в научно-производственной сфере [8]. Развитая ученым методология и философия комплексной оценки деятельности персонала ориентирована на отечественную специфику трудовых ресурсов, однако вопросам оценки кадровых уязвимостей информационной безопасности организации внимание не уделяется.

Специфику деятельности по обеспечению информационной безопасности учитывают в своих исследованиях специалисты СПИИРАН, однако их интерес направлен в большей степени на разработку методов поиска вероятности успеха социо-инженерного атакующего воздействия на пользователей информационной системы [1]. В их работах выявляются также взаимосвязи между психологическими особенностями, уязвимостями и возможными действиями пользователя информационной системы в рамках понятия социоинженерных атак [7]. Между тем, необходима методика перехода от исследований профиля

психологических особенностей пользователя к профилю кадровых уязвимостей всех пользователей информационной системы в целом.

Анализ международных и национальных стандартов, методик государственных регуляторов и Центрального Банка России, предпринятый в наших публикациях [3,4], показал, что ни в одном из них в качестве уязвимостей информационной безопасности не названы личностные качества персонала и не определены методы их оценки. Нет личностных качеств и в структуре профессиональных компетенций выпускников вузов, перечисленных в Федеральных государственных образовательных стандартах ВПО. А ведь именно они составляют сущность понятия «человеческий фактор», являющийся зачастую причиной утраты и утечки защищаемой в организации информации. Поэтому проблема отсутствия надежных методик оценки персонала в сфере информационной безопасности, учитывающих личностные качества сотрудников, является весьма актуальной.

Цель

Выявленным противоречием между актуальностью проблемы и ее недостаточной изученностью обусловлена цель настоящей статьи – обосновать вариант методики оценки кадровых уязвимостей информационной безопасности организации.

Метод

Для определения требуемых личностных качеств специалиста, чья деятельность в организации связана с защитой информации, рассмотрим причины, вызывающие дестабилизирующие воздействия на защищаемую информацию, предложенные А.И. Алексенцевым [2].

К преднамеренным причинам ученый отнес: стремление нанести вред (отомстить) руководству или коллеге по работе; стремление обезопасить себя, родных и близких от угроз, шантажа, насилия; воздействие со стороны злоумышленника. Непреднамеренные причины, по его мнению, - это неквалифицированное выполнение операций; халатность, безответственность, недисциплинированность, недобросовестное отношение к выполняемой работе; небрежность, неосторожность, неаккуратность.

Обстоятельствами появления этих причин являются: склонность к развлечениям, пьянству, наркотикам; зависть, обида; тщеславие, самомнение, завышенная самооценка, хвастовство; низкий уровень профессиональной подготовки; излишняя болтливость, привычка делиться опытом, давать советы [2].

Исходя из перечисленных причин и обстоятельств дестабилизирующих воздействий на защищаемую информацию, в данной работе обоснована методика оценки персонала в контексте информационной безопасности, в которой в качестве критериев для оценки выбраны личностные качества человека.

Основные результаты

Созданная методика предназначена для использования в процессе работы с персоналом, начиная с приема сотрудника на работу. В ходе собеседования сотрудник отдела кадров заполняет ответы кандидата на вопросы Анкеты, представленной в таблице 1. Результатом является процентный показатель уязвимости: от 0% (кандидат уязвим с точки зрения безопасности, и представляет угрозу информационной безопасности предприятия) до 100% (кандидат неуязвим и не представляет угрозы). На усмотрение руководства и службы информационной безопасности могут быть выставлены минимальные проходные пороги для различных категорий сотрудников. Категорирование сотрудников необходимо для определения сценария оценки кандидата и заполнения таблицы ответов. Критерии могут быть разными. Например, можно выделить категории, учитывая такие факторы, как ценность информации, с которой необходимо работать сотруднику (аналогично формам допуска к государственной тайне); частота обращения к конфиденциальной информации (КИ): постоянно, периодически, обращение редкое или отсутствует.

Категории сотрудников могут выглядеть следующим образом:

1. Сотрудники постоянно работают с КИ высокой степени важности.
2. Сотрудники периодически работают с КИ высокой степени важности.
3. Сотрудники постоянно работают с КИ средней степени важности.
4. Сотрудники периодически работают с КИ средней степени важности.
5. Сотрудники редко работают с КИ средней степени важности.
6. Сотрудники периодически работают с КИ низкой степени важности.
7. Сотрудники редко работают с КИ низкой степени важности.

Категории могут быть объединены. Например:

I категория включает в себя 1,2,3 позиции;

II категория – 4,5 позиции;

III категория – 6 и 7 позиции.

Оценивать уязвимость кандидата необходимо по факторам, которые представлены в виде блоков: болтливость, злопамятность, хобби, темперамент, наличие вредных привычек, внимательность, стрессоустойчивость, подверженность влиянию, общие представления о необходимости защиты информации.

Излишняя болтливость опасна с точки зрения информационной безопасности, так как сотрудник может раскрыть информацию ограниченного доступа посторонним людям. Болтливость можно оценить в ходе собеседования или попросить рассказать историю на определенную тему, например, о том, как прошел вчерашний день.

Анкета для оценки кандидата

Таблица 1

Категория сотрудника			Исследуемый блок	Вопрос. Иной показатель оценки	Количество баллов за ответ				Сумма баллов в блоке
I	II	III			3	2	1	0	
V	V	V	1. Излишняя болтливость	Просьба рассказать о вчерашнем дне	контролирует свою речь, отвечает кратко	речь лаконична, редко допускает лишнюю информацию	отвечает развернуто, иногда допускает лишнюю информацию	чрезмерно много информации	
V	V			«Вы общительный человек?»	Нет	Скорее нет	Скорее да	Да	
V				В ходе собеседования	контролирует свою речь, отвечает кратко	речь лаконична, редко допускает лишнюю информацию	отвечает развернуто, иногда допускает лишнюю информацию	чрезмерно болтлив	
V	V	V	2. Стремление отомстить руководству или коллеге по работе	«Вы легко прощаете людей?»	Нет	Скорее нет	Скорее да	Да	
V	V			Мнение о предыдущем месте работы	Позитивное	«Обиженный» сотрудник. Не склонен к мести	Невозможно оценить. Отказывается отвечать.	«Обиженный» сотрудник. Склонен к мести	
V	V	V	3. Склонность к развлечениям, пьянству, наркотикам	«Чем Вы увлекаетесь?»	Предполагает постоянное взаимодействие с людьми	Предполагает периодическое взаимодействие с людьми	Предполагает редкое взаимодействие с людьми	Не предполагает взаимодействия с людьми	
V	V			«Как Вы относитесь к проведению свободного времени в большой шумной компании?»	Отрицательно	Скорее отрицательно	Скорее положительно	Положительно	
V	V	V	4. Наличие вредных привычек	«Есть ли у Вас вредные привычки?»	Отсутствуют	Только курение	Только употребление алкоголя	Курение и алкоголь	
V	V	V	5. Внимательность	Психологическое тестирование “Корректурная проба” (Тест Бурдона)	76 – 100% – отличное внимание	51 – 75% – хорошее внимание	26 – 50% – среднее внимание	0 – 25% – плохое внимание	
V	V	V	6. Стрессоустойчивость	Применение провокационного интервью	Не стрессоустойчив	Скорее не стрессоустойчив	Скорее стрессоустойчив	Стрессоустойчив	
V	V			«Насколько легко Вас вывести из себя?»	Сложно	Скорее сложно	Скорее легко	Легко	
V	V	V	7. Подверженность манипуляциям (воздействие со стороны злоумышленника)	«Насколько сложно изменить Ваше мнение?»	Сложно	Скорее сложно	Скорее легко	Легко	
V	V			Тест «Подвержены ли мы манипуляции?» из книги Киры Бурениной	Не подвержен (24-32 балла)	Скорее не подвержен (16-24 балла)	Скорее подвержен (9-16 баллов)	Подвержен (0-8 баллов)	
V				(попытка манипулировать)	Не подвержен	Скорее не подвержен	Скорее подвержен	Подвержен	

Продолжение таблицы 1

V	**V**	**V**	8. Неквали-фицирован-ное выполнение операций	Провокация на разглашение КИ (Сценарий для каждой должности продумывается индиви-дуально)	Не разглашает	Абстрактно ответил	Разглашает детали	Разглашает	
V	**V**	**V**		«Есть ли в вашей работе информация, распространение которой ограничено?»	Присутствует	Скорее присутствует	Не знает	Отсутствует	
V	**V**	**V**	9. Страница в социальной сети	Анализ содержания анкеты, сообщений, фото- и видео-материала	Содержание анкеты позитивно характеризует ее владельца	Содержание анкеты скорее позитивно характеризует ее владельца	Содержание анкеты скорее негативно характеризует ее владельца	Содержание анкеты негативно характеризует ее владельца	
V	**V**			Список интересуемых групп, страниц, на которые подписан пользователь	Список групп не доступен	Групп и страниц мало (до 10), содержание которых позитивно характеризует ее владельца	Групп и страниц немного (10-20), содержание некоторых нега-тивно характери-зует ее владельца	Групп и страниц много (более 20), содержание которых негативно характеризует ее владельца	
V				Уровень конфиденциал ьности страницы	Страница под псевдонимом с минимальным количеством информации	На странице указана информация, которая не дает полного представления о ее владельце	Страница доступна всем пользователям. Анкета достаточно заполнена	Доступно очень много информации, страница открыта для всех пользователей	
V	**V**		10. Обращение на предыдущее место работы	Беседа с руководителем, сотрудниками, которые имеют возможность дать характеристику сотрудникам (секретарь, вахтер)	Отзывы о кандидате позитивные	Отзывы о кандидате скорее позитивные	Отзывы о кандидате скорее негативные	Отзывы о кандидате негативные	
V			11. Запрос по личным данным в поисковых системах	Выявленная информация интерпретируется индивидуально в каждом случае	кандидат неуязвим	кандидат скорее неуязвим	кандидат скорее уязвим	кандидат уязвим	

Излишняя болтливость опасна с точки зрения информационной безопасности, так как сотрудник может раскрыть информацию ограниченного доступа посторонним людям. Болтливость можно оценить в ходе собеседования или попросить рассказать историю на определенную тему, например, о том, как прошел вчерашний день.

Стремление сотрудника отомстить руководству или коллеге может привести к утечке информации во время работы или после увольнения недовольного сотрудника. Оценить риск злого умысла можно, спросив мнение о прошлом месте работы (руководстве, взаимоотношениях в коллективе).

Некоторые увлечения характерны частым взаимодействием с людьми, это увеличивает риск утечки информации. Такими хобби могут быть походы в ночные клубы, групповые спортивные, танцевальные клубы, туризм. Спокойные домашние хобби более безопасны с точки зрения информационной безопасности, например, чтение, работа в саду, рыбалка и др.

Наличие вредных привычек повышает риск утечки информации в неформальной обстановке, например, в курилке во время перерывов, в

компании, находясь при нахождении в состоянии алкогольного опьянения.

Внимательность так же может послужить показателем в процессе оценки персонала. Рассеянный сотрудник может потерять носители с конфиденциальной информацией, а значит, представляет угрозу компании. Внимательность можно оценить с помощью специальных тестов.

Стрессоустойчивого сотрудника сложнее выбить из колеи, а значит, злоумышленнику сложнее добиться информации ограниченного доступа. Слабоустойчивый к стрессам сотрудник плохо контролирует себя в нестабильном состоянии, что может привести к разглашению конфиденциальной информации. Стойкость в стрессовых ситуациях можно выявить методом стресс-интервью. Можно предложить нестандартную ситуацию и узнать о действиях сотрудника в ней.

Подверженный манипуляциям сотрудник может допустить несанкционированный доступ злоумышленника к конфиденциальной информации. Оценить устойчивость к манипуляциям можно с помощью психологического теста «Подвержены ли вы манипуляции?» К. Бурениной [6].

Важнейшим показателем личностных качеств субъекта является наличие у него общих представлений о необходимости защиты конфиденциальной информации. Кандидата необходимо спровоцировать на выдачу тайной информации по профилю предыдущего места работы. Исходя из ответа, необходимо сделать соответствующий вывод об уязвимости претендента на вакансию.

В дополнение к оценке личностных качеств претендента во время собеседования следует использовать недавно появившийся способ - сбор и анализ информации о субъекте с помощью социальных сетей. Личная страничка в сети может многое поведать о жизни человека, его интересах и моральных принципах, а потому ее анализ страницы дополняет оценивание вышеуказанных блоков личностных качеств. Однако этот метод сбора информации о субъекте и его оценки не является предметом рассмотрения в настоящей статье, он должен стать предметом специального исследования.

Факторами для оценки сотрудника могут являться:

− список интересуемых групп, страниц, на которые подписан пользователь (дополнение к блоку о хобби);

− содержание анкеты, сообщений, фото- и видеоматериала (дополнение к блоку о хобби);

− уровень конфиденциальности страницы, т.е. степени ограничения для разных категорий пользователей (дополнение к блоку о наличии общих представлений о необходимости защиты конфиденциальной информации).

Запросы по фамилии, имени и отчеству в поисковых системах могут дать любую информацию о человеке. Выявленную информацию необходимо интерпретировать индивидуально в каждом случае.

Оценивание происходит по 4-балльной шкале по каждому показателю:

0 – кандидат представляет чрезвычайно высокую угрозу информационной безопасности (чрезмерно болтлив, злопамятен, вспыльчив, в свободное время часто находится в окружении больших компаний, рассеян, легко подвергается манипуляциям, без раздумий сообщает тайны);

1 – кандидат представляет большую угрозу информационной безопасности (отвечает развернуто, иногда допускает лишнюю информацию, склонен к злопамятности, вспыльчивости, в свободное время больше склонен находиться в окружении больших компаний, больше склонен к рассеянности, с трудом подвергается манипуляциям, без раздумий сообщает некоторые детали тайной информации);

2 – кандидат представляет небольшую угрозу информационной безопасности (речь лаконична, редко допускает лишнюю информацию, склонен к злопамятности, вспыльчивости, в свободное время больше склонен находиться в кругу семьи, иногда находится в окружении большого количества людей, скорее внимателен, с большим трудом подвергается манипуляциям, на просьбу сообщить тайную информацию раздумывает, отвечает неконкретно);

3 – кандидат не представляет угрозы информационной безопасности (контролирует свою речь, отвечает кратко, совершенно не злопамятен, эмоционально устойчив, в свободное время проводит в семейном кругу, внимателен, устойчив к манипуляциям, не сообщает тайны).

После собеседования происходит расчет коэффициента уязвимости кандидата – P, выраженный в процентах, по формуле:

$$P = \frac{\sum_{i=1}^{N} p_i}{N \cdot 4} \cdot 100\%. \qquad (1)$$

где N – количество выставленных оценок (в том числе оценки «0 баллов»); p_i – количество баллов за i-ый ответ; i – порядковый номер ответа.

Допустим, кандидат относится ко второй категории, по которой, как правило, оцениваются 2 критерия по каждому блоку. Оценены 10 блоков, в каждом блоке по 2 оценки, значит N=20. Баллы выставлены следующим образом:

1 – 2; 2 – 1; 3 – 2; 4 – 3; 5 – 1; 6 – 2; 7 – 0; 8 – 1; 9 – 0; 10 – 3; 11 – 3; 12 – 2; 13 – 1; 14 – 0; 15 – 1; 16 – 0; 17 – 3; 18 – 2; 19 – 1; 20 – 1.

Посчитаем сумму баллов (числитель дроби)

$$\sum_{i=1}^{N} p_i = 2+1+2+3+1+2+0+1+0+3+3+ \\ +2+1+0+1+0+3+2+1+1 = 29.$$

Рассчитаем коэффициент уязвимости кандидата – P по формуле 1.

$$P = \frac{29}{20 \cdot 4} \cdot 100\% = 0{,}37 \cdot 100\% = 37\%.$$

Интерпретация результата может быть такой:

«Коэффициент равен 37%. Показатель ниже 50%, значит, что кандидат представляет угрозу информационной безопасности организации».

Выводы

Таким образом, уникальность разработанной методики заключается, во-первых, в количественном результате оценки сотрудника, которая составляется по различным критериям для оценивания; во-вторых, в возможности проводить оценку в зависимости от категории кандидата, что влияет на глубину проверки; в-третьих, в экономичности, т.к. методика не требует больших финансовых, материальных и трудовых затрат.

Литература

[1] Азаров А.А., Тулупьев А.Л., Соловцов Н.Б., Тулупьева Т.В. Ускорение расчетов оценки защищенности пользователей информационной системы за счет элиминации маловероятных траекторий социо-инженерных атак // Труды СПИИРАН. — 2013. — Вып. 2(25). — С.171-181.

[2] Алексенцев А.И. Понятие и структура угроз защищаемой информации // Безопасность информационных технологий. М., 2000. — № 3.

[3] Астахова Л.В. Проблема идентификации и оценки кадровых уязвимостей информационной безопасности организации // Вестник ЮУрГУ. Серия «Компьютерные технологии, управление, радиоэлектроника». — М., 2013. — № 1. — С.79-83.

[4] Астахова Л.В. Проблема оценки HR-уязвимости объекта защиты информации // Вестник УрФО. Безопасность в информационной сфере. — М., 2011. – № 1. – С.26-33.

[5] Бруннер Е.Ю. Лучше, чем супервнимание: Методики диагностики и психокоррекции: Психология внимания; Оценочные тесты; Развивающие игровые упражнения. Серия: Психологический практикум. — Ростов-на-Дону: Феникс, 2006. — 317 с.

[6] Буренина К. Офис. Стратегия выживания. — М.: Эксмо, 2007. — 112 с.

[7] Ванюшичева О.Ю., Тулупьева Т.В., Пащенко А.Е., Тулупьев А.Л., Азаров А.А. Количественные измерения поведенческих проявлений уязвимостей пользователя, ассоциированных с социоинженерными атаками // Труды СПИИРАН. — 2011. — Вып. 4(19). — С.34-47.

[8] Реймаров Г.А. Комплексная оценка персонала: Инженерный подход к управлению качеством труда. — М. :ЛКИ, 2010. — 424 с.

УДК 331.108.3 (045)

Астахова Л.В. Кадрові вразливості інформаційної безпеки організації: методика оцінки

Анотація. *У статті представлена методика оцінки кадрових вразливостей інформаційної безпеки організації, розроблена на основі аналізу нормативних документів, класифікації причин дестабілізуючих впливів на інформацію обмеженого доступу і психологічних тестів.*

Ключові слова: методика, оцінка, інформаційна безпека, кадрова вразливість.

Astakhova L.V. Human information security vulnerability of organization: methodology of assessment

Abstract. *The article presents the methodology of assessing human vulnerability to information security organization, developed on the basis of the analysis of normative documents, classification of causes of destabilizing impacts on the restricted-access information and psychological tests.*

Keywords: *methodology, assessment, information security, human resources vulnerability.*

Отримано *21 травня 2013 року*, затверджено редколегією *19 червня 2013 року*