УДК 658.71.08,519.87
DOI: 10.26467/2079-0619-2020-23-2-20-32

ИССЛЕДОВАНИЕ ПРОФИЛЯ УЯЗВИМОСТЕЙ АВИАЦИОННОГО ПЕРСОНАЛА К СОЦИОИНЖЕНЕРНЫМ АТАКАМ

Ал.К. ВОЛКОВ[1], Ан.К. ВОЛКОВ[1], Л.И. ФРОЛОВА[1]
[1]Ульяновский институт гражданской авиации им. Главного маршала авиации Б.П. Бугаева, г. Ульяновск, Россия

В условиях усиления информационной составляющей авиационной деятельности задача обеспечения авиационной кибербезопасности становится чрезвычайно актуальной. В настоящее время прорабатывается нормативно-правовая база, регламентирующая деятельность в данной области, как со стороны Международной организации гражданской авиации, так и на уровне Российской Федерации. В комплексе угроз авиационной кибербезопасности, к которому относятся умышленные атаки, ошибки сторонних компаний, системные ошибки, природные явления, важное место занимает человеческий фактор. В работе данное негативное явление рассмотрено с точки зрения уязвимости авиационного персонала к социоинженерным атакам. Подобный тип воздействий злоумышленников предполагает набор прикладных психологических и аналитических приемов, способствующих получению конфиденциальной информации или нарушению правил информационной безопасности легитимными сотрудниками компаний. Существующий подход к построению профиля уязвимостей пользователей к социоинженерным атакам предполагает проведение ряда психологических тестов, по результатам которых с использованием регрессионной модели прогнозируются уязвимости пользователя через его психологические особенности. В данной работе ставится несколько иная задача – восстановить профиль уязвимостей авиационного персонала по данным активности в социальной сети. Это связано с тем, что изучение профиля пользователя социальной сети позволит более оперативно решить задачу выбора наиболее уязвимого сотрудника к конкретному типу социоинженерной атаки и внедрять профилактические мероприятия. В работе проведены исследования на базе АО «Международный аэропорт Сургут». В качестве респондентов были выбраны 36 инспекторов по досмотру службы авиационной безопасности. Получены эмпирические данные, включающие анкеты профилей пользователя социальной сети и ряд психологических тестов. С использованием факторного анализа решена задача снижения размерности и выбора наиболее информативных показателей, характеризующих активность пользователя социальной сети. Разработана дискриминантная модель, позволяющая прогнозировать профиль уязвимостей персонала по данным социальной сети. Представлены возможные типы социоинженерных атак на авиационный персонал.

Ключевые слова: кибербезопасность, авиационная безопасность, социоинженерная атака, авиационный персонал, социальная сеть, уязвимость пользователя.

ВВЕДЕНИЕ

В современных условиях информационный ресурс становится важной составляющей экономического и технологического развития авиационной отрасли. Вместе с этим возрастают угрозы в области авиационной кибербезопасности, возможности реализации которых во многом способствует такой фактор, как увеличение масштаба с одновременным усложнением аппаратурной и программной составляющей информационно-телекоммуникационных систем авиапредприятий. К тому же современные воздушные суда представляют собой очень сложные технические системы, которые во многом полагаются на информационно-вычислительные комплексы [1]. С учетом роста сложности программного обеспечения в бортовых системах управления воздушных судов (современная функция самолетовождения включает порядка 850 тыс. строк программного кода) информационная безопасность бортового оборудования не может быть полностью гарантирована. Проблема усложняется тем, что важной составляющей информационной архитектуры современных воздушных судов является информационная система предоставления услуг для пассажиров. По мере повышения производительности персональных компьютеров и гаджетов у злоумышленников появляются реальные возможности к реализации кибератак по беспроводным каналам передачи данных воздушных судов, обеспечивая им доступ к бортовой вычислительной сети. Ряд авиационных экспертов отмечает, довольно сложно

взломать все системы сразу, включая бортовые радиоприемники и бортовую систему адресации и передачи сообщений (Aircraft Communications Addressing and Reporting System, ACARS). Тем не менее, злоумышленник с глубокими знаниями о функционировании бортовой вычислительной системы воздушного судна может преднамеренно вызвать серьезные проблемы относительно ее нормальной работоспособности [2]. В 2013 году исследователь безопасности Хьюго Teco (Hugo Teso) на конференции по кибербезопасности продемонстрировал, что он может манипулировать ACARS, используя свой смартфон на платформе Android [3], тем самым подтверждая уязвимость бортовых сетей передачи данных в комплексе бортового оборудования. В июле 2013 года в результате кибератаки были отключены системы паспортного контроля на терминалах отправления в аэропорту Стамбула, что привело к задержке многих рейсов. В июне 2019 года была зафиксирована кибератака на компанию ASCO Industries, являющейся крупным производителем авиационных деталей. В результате атаки была приостановлена деятельность нескольких заводов компании. Это лишь несколько примеров из множества других, отраженных в работах [4–6], но они оправдывают актуальность задачи обеспечения авиационной кибербезопасности критических информационных систем на воздушном транспорте.

По этой причине Международная организация гражданской авиации (ИКАО) важное внимание стала уделять вопросам нормативно-правового регулирования вопросов обеспечения авиационной кибербезопасности. По результатам 39-й Ассамблеи опубликован документ A39-WP/17 «Решение проблем кибербезопасности в гражданской авиации», затрагивающий вопросы противодействия киберугрозам на авиапредприятиях. На 40-й сессии Ассамблеи ИКАО была утверждена Стратегия в области авиационной кибербезопасности, представленная в документе A40-WP/28. Внесённые изменения в Приложение 17 к Конвенции о международной гражданской авиации закрепляют необходимость разработки каждым государством мер защиты критических важных систем информационных и связных технологий[1]. Меры по обеспечению авиационной кибербезопасности нашли нормативно-правовое закрепление в утвержденной Федеральной системе обеспечения авиационной безопасности (национальной программе авиационной безопасности)[2].

В комплексе угроз авиационной кибербезопасности, к которому относятся умышленные атаки, ошибки сторонних компаний, системные ошибки, природные явления, важное место занимает человеческий фактор. Изначально проблемы человеческого фактора в области кибербезопасности были связаны с недостаточной подготовленностью персонала по вопросам информационной безопасности и осведомленностью в области киберугроз. Однако в процессе развития технических и технологических возможностей средств виртуальной коммуникации данная проблема все больше связывается с деятельностью злоумышленников по применению методов социальной инженерии. Социальная инженерия (social engineering) – это практика получения конфиденциальной информации путем психологического воздействия на легальных пользователей[3]. Все большая вовлеченность авиационного персонала в виртуальную коммуникацию посредством социальных сетей является фактором, способствующим деятельности злоумышленников по установлению психологического профиля и уязвимостях конкретного сотрудника. Изучение профиля пользователя социальной сети позволит злоумышленникам выбрать наиболее уязвимого сотрудника к конкретному типу социоинженерной атаки. Для организации целевых атак на конкретного сотрудника злоумышленники используют фишинговые

[1] Приложение 17 к Конвенции о международной гражданской авиации. Безопасность. Защита международной гражданской авиации от актов незаконного вмешательства. 10-е издание. ИКАО. 2017. 64 с.

[2] Федеральная система обеспечения авиационной безопасности (национальная программа авиационной безопасности): одобрено Межведомственной комиссией по авиационной безопасности, безопасности полетов гражданской авиации и упрощению формальностей. 2019. 110 с.

[3] ГОСТ Р МЭК 62443–2–1–2015. Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 2 – 1. Составление программы обеспечения защищенности (кибербезопасности) системы управления и промышленной автоматики. М.: Стандартинформ, 2015. 158 с.

сайты, фишинговые рассылки, подделывают веб-сайты и затем с помощью электронных писем доставляют на компьютер жертв вредоносное программное обеспечение, зная психологические особенности личности, убеждают перейти по ссылке на фишинговый ресурс или сообщить свои учетные данные различных онлайн-сервисов и электронной почты. Эксплуатация злоумышленниками человеческого фактора может привести к таким последствиям, как кража персональных данных пассажиров, разглашение конфиденциальной информации, сбои в работе паспортного контроля и другой критической инфраструктуры.

Таким образом, уязвимость авиационного персонала к социоинженерным атакам является важной составляющей человеческого фактора в области авиационной кибербезопасности и требует своего научного изучения.

ОБЗОР РЕЛЕВАНТНЫХ РАБОТ

В настоящее время достигнут ряд значительных успехов в исследовании профилей уязвимости пользователей к социоинженерным атакам. Первоначально профиль уязвимости пользователей строился на результатах анкетирования, т. е. по ответам на блок специально разработанных вопросов, характеризующих особенности процесса использования и распространения респондентами идентификационных данных [7, 8, 9]. Впоследствии дополнительно была проведена группа психологических исследований, включая такие тесты, как многофакторный личностный опросник (Р. Кетелл); потребность в поиске новых ощущений (М. Цукерман); склонность к риску (Г. Шуберт); индекс жизненного стиля – психологическая защита (Л. И. Вассерман) и др. В результате была установлена зависимость между профилем уязвимостей пользователя, основанном на проведенном анкетировании, и психологическими особенностями личности, позволяющая автоматизировать процесс построения профиля психологически обусловленных уязвимостей пользователей. В основе процесса построения профиля лежит регрессионная модель, которая и позволяет прогнозировать уязвимости пользователя через его психологические особенности. Выявленное пространство уязвимостей пользователя включает в себя такие факторы, как информационная неосмотрительность; слабый пароль; техническая халатность и установка на получение личной выгоды; техническая неопытность; техническая безграмотность [10]. По результатам исследований разработан комплекс программ для анализа защищенности пользователей информационных систем от социоинженерных атак [11].

ПОСТАНОВКА ЗАДАЧИ

Как видно из проведенного анализа для построения профиля уязвимостей необходимо провести целый ряд психологических тестов, что в условиях реального функционирования авиапредприятия крайне затруднительно ввиду больших временных и ресурсных затрат. Возникает потребность в разработке более гибкой и оперативной методики, позволяющей оперативно проводить диагностику профилей уязвимости авиационного персонала, основываясь на открытых источниках, в частности на данных из социальных сетей. Как следствие необходимо провести исследование, направленное на поиск взаимосвязи между профилем пользователя социальной сети авиационного персонала и психологическими особенностями их личности.

Исследование проводилось в 2019 году на базе АО «Международный аэропорт Сургут». В качестве респондентов были выбраны 36 инспекторов по досмотру. Этот выбор обусловлен тем, что данная категория авиационного персонала непосредственно работает с информацией по вопросам авиационной безопасности, являющейся строго конфиденциальной с грифом «Для служебного пользования», а в некоторых случаях имеющей и более высокий гриф секретности. Возраст респондентов составил от 21 до 51 года, включая лиц женского пола 60 % и мужского пола 40 %. Средний стаж работы сотрудников составил 3,5 года.

Ввиду того, что все респонденты являются пользователями социальной сети ВКонтакте, данная сеть была выбрана как основная. Была разработана анкета профиля пользователя социальной сети, включающая 20 вопросов и направленная на оценку степени интенсивности виртуальной коммуникации.

Респонденты прошли следующие психологические тестирования [12]:

– тип темперамента (Г. Айзенки и С. Айзенки);

– анкета-опросник «Ценностные ориентации» (М. Рокич). Опросник предполагает оценку терминальных и инструментальных ценностей, которые измеряются в рангах от 1 до 18. Чем меньше выставленный ранг, тем более значимой является та или иная ценность.

Важным механизмом обеспечения авиационной кибербезопасности с точки зрения организационной составляющей является создание и поддержание высокого уровня организационной лояльности авиационного персонала. Это связано с тем, что высокий уровень лояльности персонала является фактором, способствующим уменьшению успеха реализации социоинженерных атак злоумышленников. Преданные сотрудники разделяют ценности и цели авиапредприятия, не разглашают коммерческих секретов и сведений для служебного пользования. В связи с этим было проведено тестирование с использованием анкеты-опросника «Шкала организационной лояльности» («Organizational commitment scale»), предложенной Дж. Мейером и Н. Алленом [13]. Анкета позволяет описать трехкомпонентную модель лояльности. Первый компонент характеризует аффективную привязанность (affective commitment scale, ACS), которая описывает степень эмоциональной привязанности персонала к организации. Второй компонент характеризует продолженную лояльность (continuous commitment scale, CCS), которая отражает степень осознания работником того, как затраты, ассоциирующиеся с уходом из организации, связывают его с организацией. Третий компонент характеризует нормативную лояльность (normative commitment scale, NCS), которая описывает степень ощущения работником обязательств перед организацией.

Для обработки полученного эмпирического материала использовался программный пакет STATISTICA. Были задействованы следующие методы математической статистики: корреляционный, факторный и дискриминантный анализы.

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ ПО ВЫЯВЛЕНИЮ ПРОФИЛЯ УЯЗВИМОСТЕЙ АВИАЦИОННОГО ПЕРСОНАЛА

На первом этапе обработки данных был проведен корреляционный анализ для выявления наиболее независимых показателей, характеризующих активность авиационного персонала в социальной сети ВКонтакте. Фрагмент матрицы корреляций представлен в табл. 1 (использовался критерий Пирсона при уровне значимости $p < 0,01$).

Таблица 1
Table 1

Фрагмент матрицы корреляций исходных данных
Fragment of the correlation matrix of the source data

Показатели	**$П_5$**	$П_6$	$П_8$	**$П_9$**	**$П_{10}$**	**$П_{11}$**	$П_{12}$	**$П_{13}$**	**$П_{16}$**	$П_{19}$
1	2	3	4	5	6	7	8	9	10	11
$П_5$	1	-0,012	0,926	0,030	0,100	0,059	0,040	0,061	**0,952**	-0,093
$П_6$	-0,012	1	-0,084	**0,871**	0,057	-0,031	0,346	-0,028	-0,028	-0,072
$П_8$	**0,926**	-0,084	1	0,058	0,193	0,146	0,148	0,196	**0,939**	-0,140
$П_9$	0,030	-0,871	0,058	1	0,422	0,375	0,694	0,412	0,051	-0,066
$П_{10}$	0,100	0,057	0,193	0,422	1	0,844	0,864	**0,921**	0,114	-0,680

Продолжение таблицы 1
Continuance of Table 1

1	2	3	4	5	6	7	8	9	10	11
$П_{11}$	0,059	-0,031	0,146	0,375	**0,844**	1	0,798	**0,877**	0,052	0,054
$П_{12}$	0,040	0,346	0,148	0,694	**0,864**	0,798	1	**0,919**	0,068	-0,064
$П_{13}$	0,061	-0,002	0,196	0,412	**0,921**	0,877	0,919	1	0,085	-0,002
$П_{16}$	**0,952**	-0,028	0,939	0,051	0,114	0,052	0,068	0,085	1	-0,143
$П_{19}$	-0,093	-0,072	-0,140	-0,066	-0,680	0,054	-0,064	-0,002	-0,143	1

В результате анализа были исключены 6 показателей: $П_5$, $П_9$, $П_{10}$, $П_{11}$, $П_{13}$, $П_{16}$.

Следующим этапом обработки данных было проведение факторного анализа по оставшимся 14 показателям в целях выявления наиболее значимых параметров. Согласно критерию Кайзера были оставлены 5 факторов, собственные значения которых превысили 1. Матрица факторных нагрузок (использовался метод варимакс) представлена в табл. 2.

Таблица 2
Table 2

Матрица факторных нагрузок
Factor load matrix

Переменные	Фактор 1	Фактор 2	Фактор 3	Фактор 4	Фактор 5
$П_1$	-0,178	-0,052	-0,299	0,109	-0,160
$П_2$	0,679	-0,023	0,486	0,033	-0,022
$П_3$	**0,804**	0,112	-0,202	0,037	0,261
$П_4$	**0,878**	-0,036	0,080	0,084	-0,107
$П_6$	-0,015	**0,870**	0,156	0,048	-0,056
$П_7$	-0,001	**0,879**	-0,096	-0,040	0,209
$П_8$	**0,882**	-0,061	0,092	0,007	-0,028
$П_{12}$	0,038	0,267	**0,869**	0,015	-0,035
$П_{14}$	-0,024	0,582	0,054	-0,086	0,586
$П_{15}$	0,077	0,115	-0,004	0,127	**0,830**
$П_{17}$	0,055	-0,154	**0,905**	0,075	0,056
$П_{18}$	-0,077	0,053	0,042	-0,141	0,653
$П_{19}$	-0,113	-0,036	-0,051	**-0,867**	0,145
$П_{20}$	0,005	0,060	-0,051	**-0,819**	-0,211

Согласно табл. 2 представим описание факторов (профилей уязвимости). Каждый фактор определяется суммой характеризующих его переменных с учетом определенного веса и знака.

1. В первый фактор вошли такие показатели, как $П_3$ «Количество друзей», $П_4$ «Количество неактивных аккаунтов друзей», $П_8$ «Количество еженедельно добавляемых новых рекомендуемых друзей». Соответственно данный фактор характеризует потребность в социальных отношениях и общении.

2. Второй фактор включает показатели $П_6$ «Количество еженедельно добавляемых новых групп» и $П_7$ «Количество подписок на группы». Данный фактор можно охарактеризовать как поиск социальной поддержки.

3. Третий фактор включает показатели $П_{12}$ «Количество оставленных отзывов комментариев на записи пользователя» и $П_{17}$ «Общее количество фотографий на «стене» страницы пользователя». Фактор характеризует феномен социальной желательности.

4. Четвертый фактор включает показатели $П_{19}$ «Общее количество аудиозаписей» и $П_{20}$ «Общее количество видеозаписей». Фактор отражает поиск новой информации аудио- и видеоформата.

5. Пятый фактор включает показатель $П_{15}$ «Общее количество личных фотографий». Фактор характеризует демонстративное поведение, направленное на привлечение внимания виртуальной аудитории.

Психологические особенности личности авиационного персонала, обусловленные спецификой активности в социальной сети

Для определения устойчивых групп пользователей был проведен кластерный анализ по наиболее значимым показателям в каждом факторе: $П_7$, $П_8$, $П_{15}$, $П_{17}$, $П_{19}$. В качестве правила объединения использовался метод Варда, а в качестве меры близости – манхэттенское расстояние. Дендрограмма кластеров представлена на рис. 1.

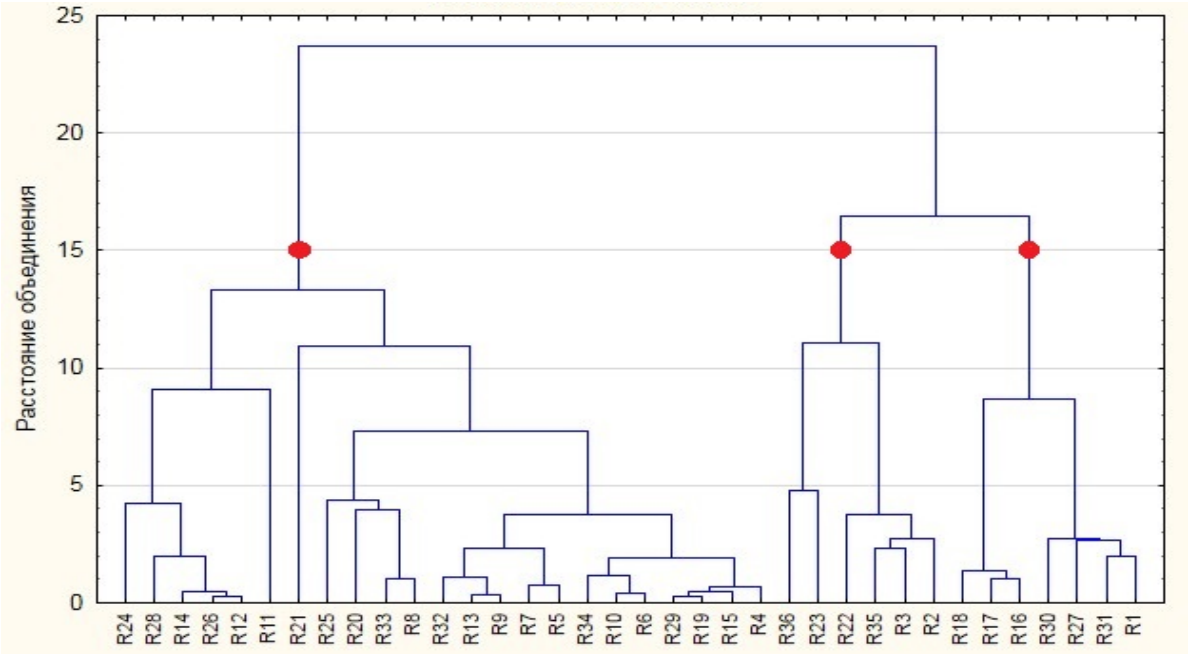

Рис. 1. Дендрограмма наблюдений для исследуемой группы респондентов
Fig. 1. Dendrogram of observations for the group of respondents under study

В данном случае было предложено рассматривать три кластера респондентов. Представим описание каждого кластера.

Кластер 1 – пользователи социальной сети, для которых использование интернет коммуникации направлено прежде всего на поиск социальной поддержки, что связано с большим количеством подписок на различные группы. Большое количество личных фотографий характеризует демонстративное поведение, направленное на привлечение внимания виртуальной аудитории. При этом они имеют наименьшее количество аудио- и видеозаписей и фотографий на «стене» страницы.

Кластер 2 – пользователи социальной сети, которые имеют самое большое количество виртуальных контактов и предпочитают интернет-общение. Предпочитают больше выкладывать фотографий на «стене», которые понравятся другим пользователям, чем публиковать информацию о себе. Это говорит о потребности в социальной желательности со стороны других

пользователей, которая заключается в стремлении представить себя в наилучшем свете, избирательному выбору размещаемой информации.

Кластер 3 – для пользователей социальной сети главной целью нахождения в виртуальном мире является поиск новой аудио- и видеоинформации. Имеют наибольшее количество аудио- и видеозаписей. Используют группы и сообщества, прежде всего, для поиска новой информации.

На основе проведенного анализа, определив основные характеристики активности авиационного персонала в социальной сети, представим описание психологических особенностей личности респондентов в найденных кластерах.

Анализ результатов, полученных с помощью методики «Тип темперамента» Г. Айзенки и С. Айзенки, показал, что в первом кластере преобладают типы: сангвиники (35 %) и холерики (35 %), в меньшем количестве присутствуют флегматики (22 %) и меланхолики (8 %). Основу второго кластера составляют сангвиники (50 %) и флегматики (33 %). В составе третьего кластера доминируют флегматики (57 %), а оставшуюся часть составляют холерики (43 %)

По результатам анализа согласно методике М. Рокича «Ценностные ориентации» общая структура жизненных ценностей в первой и второй группе имеет схожий характер. Доминирующими терминальными ценностями респондентов в первом кластере являются активная деятельная жизнь (ср. = 3,9), счастливая семейная жизнь (ср. = 5,4) и любовь (ср. = 5,5). Во втором кластере активная деятельная жизнь (ср. = 3), наличие хороших и верных друзей (ср. = 3,5) и интересная работа (ср. = 4,5). Преобладающими инструментальными ценностями в обеих группах являются жизнерадостность (ср. = 5,7 для кластера 1 и ср. = 6 для кластера 2), воспитанность (ср. = 5,8 для кластера 1 и ср.= 6,4 для кластера 2). Структура ценностей третьей группы во многом отличается от рассмотренных первых двух. Доминирующими терминальными ценностями являются здоровье (ср. = 4,1), уверенность в себе (ср. = 5,4) и жизненная мудрость (ср. = 5,8). В качестве главных инструментальных ценностей можно выделить ответственность (ср. = 5), честность (ср. = 5,6) и аккуратность (ср. = 5,6).

Результаты, полученные с помощью анкеты-опросника «Шкала организационной лояльности» Дж. Мейера и Н. Аллена, позволили сделать вывод, что общая структура организационной лояльности в рассматриваемых группах имеет идентичный характер. Наибольшее значение имеет показатель аффективной приверженности, который для первой группы составил $ACS_1 = 4{,}3$, для второй группы $ACS_2 = 4{,}4$ и для третьей $ACS_3 = 4{,}5$. Высокая аффективная (эмоциональная) приверженность означает, что авиапредприятие для всего рассматриваемого авиационного персонала имеет большое значение, они переживают свою принадлежность к организации как принадлежность к семье и желают в дальнейшем принадлежать к ней (отношение характеризуется как «Я люблю...»). Значение продолженной приверженности в первой и во второй группе имеет одинаковую величину и составляет $CCS_{1,2} = 3{,}4$. При этом в третьей группе респондентов продолженная приверженность имеет более выраженный характер и близка по значению к аффективной ($CCS_3 = 4{,}3$). Данный факт характеризует то, что воспринимаемые сотрудником издержки и потери, связанные с уходом с авиапредприятия, будут высокими, поэтому такие люди остаются с организацией. Наименьшее значение в структуре организационной лояльности имеет компонента нормативной приверженности, которая для рассматриваемых групп составляет $NCS_1 = 3{,}4$, $NCS_{2,3} = 3{,}1$.

Дискриминантная модель прогнозирования профиля уязвимостей авиационного персонала на основе данных социальной сети

Следующим этапом разрабатываемой диагностической методики является разработка обучаемой модели, в качестве которой будет использована дискриминантная модель. В качестве группирующей переменной в дискриминантном анализе выбраны значения трех полученных кластеров респондентов. В качестве независимых переменных использовались показатели активности пользователя в социальной сети: $П_7$, $П_8$, $П_{15}$, $П_{17}$, $П_{19}$. Показателем качества дискриминации является значение статистики лямбда Уилкса, которая измеряется в диапазоне от 0 до 1 ($\lambda_w = [0; 1]$). Чем меньше значение лямбды Уилкса, тем лучше качество дискриминации. В данном случае значение $\lambda_w = 0{,}046$, что говорит о достаточно хорошем качестве дискриминации. F-критерий равен 21,007 на уровне значимости меньше 0,05. Согласно классификационной матрице процент правильной дискриминации составляет 100 %, т.е. данная разрабатываемая дискриминантная модель может быть использована в качестве обучающей.

Дискриминантная модель представляется в виде системы линейных классификационных уравнений согласно формуле (1)

$$\begin{cases} f_1 = 2{,}521 \cdot П_7 - 0{,}127 \cdot П_8 + 2{,}500 \cdot П_{15} - 1{,}544 \cdot П_{17} + 9{,}378 \cdot П_{19} - 9{,}773, \\ f_2 = 4{,}146 \cdot П_7 - 0{,}532 \cdot П_8 + 4{,}423 \cdot П_{15} - 1{,}560 \cdot П_{17} + 1{,}058 \cdot П_{19} - 8{,}708, \\ f_3 = -1{,}778 \cdot П_7 + 0{,}159 \cdot П_8 - 1{,}833 \cdot П_{15} + 0{,}876 \cdot П_{17} - 3{,}492 \cdot П_{19} - 2{,}030. \end{cases} \quad (1)$$

В табл. 3 представлены результаты анализа характеристик независимых переменных модели. Дополнительный анализ позволит выявить наиболее информативные переменные, тем самым повысив качество дискриминантного анализа.

Таблица 3
Table 3

Характеристики переменных, включенных в модель
Characteristics of variables included in the model

Переменная	Лямбда Уилкса	Частная Лямбда	F-исключить	p-уровень	Толерантность	R^2 (1-Толер.)
$П_7$	**0,094**	**0,493**	**14,888**	**0,000036**	**0,814**	**0,186**
$П_8$	0,047	0,984	0,221	0,802663	0,981	0,019
$П_{15}$	**0,101**	**0,463**	**16,798**	**0,000014**	**0,724**	**0,276**
$П_{17}$	0,057	0,819	3,201	0,055419	0,849	0,151
$П_{19}$	**0,260**	**0,179**	**66,161**	**0,000000**	**0,810**	**0,189**

На основе анализа характеристик (табл. 3) был сделан вывод, что переменные $П_7$, $П_{15}$, $П_{19}$ дают наибольший вклад в общую дискриминацию. Данный вывод сделан исходя из следующих рекомендаций: 1) чем больше значение лямбды Уилкса, тем желательнее присутствие переменной в процедуре дискриминации; 2) чем меньше значение частной лямбды, тем больше вклад переменной в общую дискриминацию; 3) чем меньше толерантность, тем желательней переменная в модели. При этом характеристика F-исключить описывает значения F-критерия, связанные с соответствующей частной лямбдой Уилкса. Значение p-уровень отражает уровни значимости F-критериев.

Определение принадлежности нового респондента к выявленным трем классификационным группам определяется по максимальному значению функции дискриминации. Полученная дискриминантная модель (1) позволит в дальнейшем автоматизировать процесс диагностики профиля уязвимостей авиационного персонала.

Анализ возможных социоинженерных атак злоумышленников

На основе факторного анализа были выявлены переменные, характеризующие особенности активности пользователей социальной сети и связанные с потенциальными уязвимостями к социоинженерным атакам. Было предложено рассматривать их следующим образом: 1) потребность в социальных отношениях и общении; 2) поиск социальной поддержки; 3) феномен социальной желательности; 4) поиск новой информации аудио- и видеоформата; 5) демонстративное поведение. В свою очередь, на основе кластерного анализа были выявлены три профиля пользователей социальной сети, в которых доминирует определенная переменная.

Различные варианты атакующих социоинженерных воздействий и реакции пользователя сети на них зависят от конкретной группы персонала и выраженности той или иной уязвимости, связанной с психологическими особенностями личности.

К примеру, для пользователей из первой группы, ориентированных на демонстративное поведение, нарушитель предпримет действия, способствующие усилению нарциссических качеств личности, чтобы затем использовать это в своих целях. В случае ориентации на различные сетевые группы нарушитель может создать определенную группу, добавить интересующего пользователя и под видом голосования, опроса или форума узнать интересующую информацию.

В силу того, что пользователи во второй группе являются активными участниками виртуального общения и достаточно легко приобретают новые социальные связи, злоумышленник может познакомиться с ними в виртуальной среде и тем или иным способом, используя свое обаяние или другие качества, попытаться выяснить интересующие его сведения.

Относительно третьей группы пользователей можно сказать, что это потенциально наименее уязвимая группа пользователей к социоинженерным атакам на основе социальных сетей.

В табл. 4 представлены некоторые примеры возможных воздействий нарушителей на выделенные группы персонала.

Таблица 4
Table 4

Примеры социоинженерных атак
Examples of social engineering attacks

Группа пользователей	Атакующее воздействие
1 группа	Предложение войти в какую-то привлекательную для пользователя группу Предложение помощи в решении различных проблем в пределах какой-то сетевой группы
2 группа	Виртуальное знакомство с пользователем в социальной сети Отправка письма якобы от друга с «полезным» для пользователя приложением, с установкой которого также внедряется программа-шпион
3 группа	Попытка взломать аккаунт пользователя Попытка подкупа пользователя

С практической точки зрения, полученные результаты могут стать инструментом для выстраивания более эффективной политики правильного выбора средств по профилактике социоинженерных атак злоумышленников на авиационный персонал авиапредприятий.

ЗАКЛЮЧЕНИЕ

На основании проведенного анализа был сделан вывод, что важной составляющей человеческого фактора в области авиационной кибербезопасности является уязвимость авиационного персонала к социоинженерным атакам. Развитие социальных сетей привело к рассмотрению их как важного элемента социоинженерных атак на персонал авиапредприятий.

В статье приводятся результаты исследования, посвященного изучению взаимосвязей между профилем пользователя социальной сети (особенностями активности авиационного персонала в социальной сети) с их психологическими особенностями личности. На основе факторного и кластерного анализа выявлены профили пользователей социальной сети, которые связаны с уязвимостями к социоинженерным атакам. Разработана дискриминантная модель, позволяющая прогнозировать профиль уязвимостей персонала по данным социальной сети. Представлены примеры социоинженерных атак на авиационный персонал.

В дальнейшем планируется увеличить выборку испытуемых и провести более масштабные исследования для уточнения полученных результатов и поиска других, возможно более глубинных, связей между профилем личности в социальной сети и психологическими особенностями.

СПИСОК ЛИТЕРАТУРЫ

1. Кузнецов С.В. Бортовые гетерогенные информационно-вычислительные сети перспективных воздушных судов // Научный вестник МГТУ ГА. 2019. Т. 22, № 2. С. 16–27. DOI: 10.26467/2079-0619-2019-22-2-16-27

2. Paganini P. Cyberthreats against the aviation industry [Электронный ресурс]. Infosec. URL: http://resources.infosecinstitute.com/cyber-threats-aviation-industry/ (дата обращения 25.01.2020).

3. Greenberg A. Researcher says he's found hackable flaws in airplanes' navigation systems. [Электронный ресурс] // Forbes. 10 April, 2013. URL: http://www.forbes.com/sites/andygreenberg/2013/04/10/researcher-says-hes-found-hackable-flaws-in-airplanes-navigation-systems/#67f5622123b7 (дата обращения 25.01.2020).

4. Демин Д.С. Обзор основных киберугроз ключевых субъектов инфраструктуры гражданской авиации / Д.С. Демин, О.Ф. Машошин, А.В. Никитин, В.В. Соломенцев, Ю.М. Колитиевский, И.В. Никитин // Научный вестник ГосНИИ ГА. 2018. № 22 (333). С. 130–143.

5. Demin D. Aspects of cyber-security in civil aviation / D. Demin, V. Shapkin, S. Musin, A. Nikitin, A. Pleshakov, V. Solomentsev // International Journal of Civil Engineering and Technology (IJCIET). 2018. Vol. 9, iss. 9. Pp. 182–189.

6. Быкова В.В Проблемы уязвимости информационных систем предприятий авиационной отрасли: анализ и классификация ошибок / В.В. Быкова, Г.Е. Глухов, А.Н. Шарыпов, П.Е. Черников, С.В. Коваль, А.Ю. Коньков // Научный вестник ГосНИИ ГА. 2019. № 27. С. 56–65.

7. Азаров А.А. Социоинженерные атаки: проблемы анализа / А.А. Азаров, Т.В. Тулупьева, А.В. Суворова, А.Л. Тулупьев, М.В. Абрамов, Р.М. Юсупов / Под. общ. ред. Р.М. Юсупова. СПб.: Наука, 2016. 349 с.

8. Тулупьева Т.В. Социально-психологические факторы, влияющие на степень уязвимости пользователей автоматизированных информационных систем с точки зрения социоинже-

нерных атак / Т.В. Тулупьева, А.Л. Тулупьев, А.Е. Пащенко, А.А. Азаров, М.В. Степашкина // Труды СПИИРАН. 2010. № 1 (12). С. 200–214.

9. Абрамов М.В. Модель профиля компетенций злоумышленника в задаче анализа защищенности персонала информационных систем от социоинженерных атак / М.В. Абрамов, А.А. Азаров, Т.В. Тулупьева, А.Л. Тулупьев // Информационно-управляющие системы. 2016. № 4 (83). С. 77–84. DOI: 10.15217/issn1684-8853.2016.4.77

10. Азаров А.А. Анализ защищенности групп пользователей информационных системы от социоинженерных атак: принцип и программная реализация / А.А. Азаров, М.В. Абрамов, Т.В. Тулупьева, А.Л. Тулупьев // Компьютерные инструменты в образовании. 2015. № 4. С. 52–60.

11. Тулупьев А.Л., Пащенко А.Е., Азаров А.А. Информационная модель пользователя, находящегося под угрозой социоинженерной атаки // Труды СПИИРАН. 2010. № 2 (13). С. 143–155.

12. Практическая психодиагностика: Методики и тесты / Под ред. Д.Я. Райгородского. Самара: БАХРАХ-М, 2002. 667 с.

13. Meyer J.P., Allen N.J. A three-component conceptualization of organizational commitment // Human Resource Management Review. 1991. Vol. 1, iss. 1. Pp. 61–89. DOI: 10.1016/1053-4822(91)90011-Z

СВЕДЕНИЯ ОБ АВТОРАХ

Волков Александр Константинович, кандидат технических наук, доцент Ульяновского института гражданской авиации им. Главного маршала авиации Б.П. Бугаева, oabuvauga@mail.ru.

Волков Андрей Константинович, старший преподаватель Ульяновского института гражданской авиации им. Главного маршала авиации Б.П.Бугаева, oabuvauga@mail.ru.

Фролова Лидия Ивановна, аспирант кафедры летной эксплуатации и безопасности полетов, заместитель начальника отдела дистанционных образовательных технологий Ульяновского института гражданской авиации им. Главного маршала авиации Б.П.Бугаева, frolova.i.lidiya@gmail.com.

RESEARCH OF THE AVIATION PERSONNEL VULNERABILITY PROFILE TO SOCIAL ENGINEERING ATTACKS

Alexander K. Volkov[1], Andrei K. Volkov[1], Lidia I. Frolova[1]
[1]Ulyanovsk Institute of Civil Aviation named after Air Chief Marshal B.P.Bugaev, Ulyanovsk, Russia

ABSTRACT

In conditions of strengthening the informational component of aviation activity, the task of ensuring aviation cybersecurity becomes extremely urgent. Currently, a regulatory framework is being developed that regulates activities in this area, both on the part of the International Civil Aviation Organization and at the Russian Federation level. In the complex of aviation cybersecurity threats, which include deliberate attacks, errors of third-party companies, system errors, natural phenomena, the human factor occupies an important place. In this work, this negative phenomenon is considered from the point of view of the aviation personnel vulnerability to social engineering attacks. Such type of attack by an attacker involves a set of applied psychological and analytical techniques that facilitate the receipt of confidential information or the violation of information security rules by legitimate company employees. The existing approach to building a profile of user vulnerabilities to social engineering attacks involves a series of psychological tests, the results of which are used to predict the user vulnerability through its psychological characteristics. In this work a slightly

different task is posed, the main idea is to restore the vulnerability profile of aviation personnel from activity data in a social network. This is due to the fact that studying the user profile of a social network will more quickly solve the problem of choosing the most vulnerable employee for a particular type of social engineering attack and introduce preventive measures. The research was conducted on the basis of JSC «Surgut International Airport». 36 aviation security inspectors were selected as the respondents. Empirical data have been obtained including profiles of social network user profiles and a number of psychological tests. Using factor analysis the problem of reducing dimensionality and choosing the most informative indicators characterizing the activity of a social network user has been solved. A discriminant model that allows predicting the vulnerability profile of personnel according to the social network has been developed. Possible types of social engineering attacks on aviation personnel are presented.

Key words: cybersecurity, aviation security, social engineering attack, aviation personnel, social network, user vulnerability.

REFERENCES

1. Kuznetsov, S.V. (2019). *On-board heterogeneous information computer networks of perspective aircraft.* Civil Aviation High Technologies, vol. 22, no. 2, pp. 16–27. DOI: 10.26467/2079-0619-2019-22-2-16-27. (in Russian)

2. Paganini, P. (2014). *Cyberthreats against the aviation industry*. Infosec. Available at: http://resources.infosecinstitute.com/cyber-threats-aviation-industry/ (accessed 25.01.2020).

3. Greenberg, A. (2013). *Researcher says he's found hackable flaws in airplanes' navigation systems*. Forbes, 10 April. Available at: http://www.forbes.com/sites/andygreenberg/2013/04/10/researcher-says-hes-found-hackable-flaws-in-airplanes-navigation-systems/#67f5622123b7 (accessed 25.01.2020).

4. Demin, D.S., Mashoshin, O.F., Nikitin, A.V., Solomentsev, V.V., Kolitiyevskiy, Yu.M. and Nikitin, I.V. (2018). *Overview of the main threats key stakeholders of civil aviation infrastructure.* Scientific Bulletin of the State Scientific Research Institute of Civil Aviation, GosNII GA, no. 22 (333), pp. 130–142. (in Russian)

5. Demin, D., Shapkin, V., Musin, S., Nikitin, A., Pleshakov, A. and Solomentsev, V. (2018). *Aspects of cyber-security in civil aviation*. International Journal of Civil Engineering and Technology (IJCIET), vol. 9, issue 9, pp. 182–189. (in Russian)

6. Bykova, V.V., Glukhov, G.Ye., Sharypov, A.N., Chernikov, P.Ye., Koval, S.V. and Konkov, A.Yu. (2019). *Problems of vulnerability of information systems of aviation industry enterprises: analysis and classification of errors*. Scientific Bulletin of the State Scientific Research Institute of Civil Aviation, GosNII GA, no. 27, pp. 56–65. (in Russian)

7. Azarov, A.A., Tulupeva, T.V., Suvorova, A.V., Tulupev, A.L., Abramov, M.V. and Yusupov, R.M. (2016). *Social Engineering Attacks: the Problems of Analysis*, in Yusupova R.M. (Ed.). St.Petersburg: Nauka, 349 p. (in Russian)

8. Tulupyeva, T.V., Tulupyev, A.L., Pashchenko, A.E., Azarov, A.A. and Stepashkin, M.V. (2010). *Social psychological factors that influence the information system users vulnerability degree in regard of socio-engineering attacks.* SPIIRAS Proceedings, no. 1 (12), pp. 200–214. (in Russian)

9. Abramov, M.V., Azarov, A.A., Tulupyeva, T.V. and Tulupyev, A.L. (2016). *Model of malefactor competencies profile for analyzing information system personnel security from social engineering attacks.* Management Information Systems, no. 4, pp. 77–84. DOI: 10.15217/issn1684-8853.2016.4.77. (in Russian)

10. Azarov, A.A., Abramov, M.V., Tulupyeva, T.V. and Tulupyev, A.L. (2015). *The analysis of the information systems "users" groups protection analysis from the social engineering attacks: the principle and program implementation.* Computer tools in education, no. 4, pp. 52–60. (in Russian)

11. Tulupyev, A.L., Pashchenko, A.E. and Azarov, A.A. (2010). *Information model of the user, who may be under the threat of socioengineering attack.* SPIIRAS Proceedings, no. 2 (13), pp. 143–155. (in Russian)

12. Raygorodsky, D.Ya. (Ed.). (2002). *Prakticheskaya psikhodiagnostika: Metodiki i testy* [Practical Psychodiagnostics: Methods and Tests]. Samara: BAKHRAKH-M, 667 p. (in Russian)

13. Meyer, J.P. and Allen, N.J. (1991). *A three-component conceptualization of organizational commitment*. Human Resource Management Review, vol. 1, issue 1, pp. 61–89. DOI: 10.1016/1053-4822(91)90011-Z

INFORMATION ABOUT THE AUTHORS

Alexander K. Volkov, Candidate of Technical Sciences, Associate Professor, Ulyanovsk Institute of Civil Aviation named after Air Chief Marshal B.P.Bugaev, oabuvauga@mail.ru.

Andrei K. Volkov, Assistant Professor, Ulyanovsk Institute of Civil Aviation named after Air Chief Marshal B.P.Bugaev, oabuvauga@mail.ru.

Lidia I. Frolova, Post-graduate student, Flight Operation and Flight Safety Chair, Deputy Head of the Distant Learning Technology Department, Ulyanovsk Institute of Civil Aviation named after Air Chief Marshal B.P.Bugaev, frolova.i.lidiya@gmail.com.

Поступила в редакцию	05.02.2020	Received	05.02.2020
Принята в печать	19.03.2020	Accepted for publication	19.03.2020