УДК 004:654.924.3
DOI 10.17513/snt.40279

МЕТОДИКА ОЦЕНКИ ЗАЩИЩЕННОСТИ ЧЕЛОВЕКО-МАШИННОГО ИНТЕРФЕЙСА ДЛЯ АВТОМАТИЗИРОВАННОГО РАБОЧЕГО МЕСТА ИНТЕГРИРОВАННОЙ СИСТЕМЫ БЕЗОПАСНОСТИ

Тельный А.В., Монахов М.Ю., Николаев А.В., Матвеева Е.А.

ФГБОУ ВО «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых», Владимир, e-mail: andre.izi@mail.ru

Целью исследования является создание методики, с помощью которой можно оценить уровень защищенности информации при ее обработке оператором в человеко-машинном интерфейсе. Данная методика может быть использована для обеспечения управления информационной безопасностью, повышения защищенности объекта от посягательств, снижения уровня ложных срабатываний технических средств интегрированной системы безопасности. Для решения данной задачи применяется система оценок, формируемых группой экспертов по следующим разделам: виды органолептической информации, получаемой оператором (для каждого вида такой информации экспертами оценивается важность обеспечения целостности, конфиденциальности и доступности в зависимости от уровня подсистемы безопасности); перечень факторов, влияющих на защищенность информационных ресурсов для конкретного интерфейса; градации и весовые коэффициенты для факторов, влияющих на защищенность информационных ресурсов для конкретной интегрированной системы безопасности; оценки для распределения значимости факторов, влияющих на защищенность информационных ресурсов по целостности, конфиденциальности и доступности. Защищенность информации человеко-машинного интерфейса предлагается оценивать как евклидово расстояние в пространстве критериев целостности, конфиденциальности и доступности. Данные экспертные оценки были получены и апробированы для оценки различных типов программного обеспечения интегрированных систем безопасности. Предложенная методика может быть использована для: создания системы поддержки принятия решений; оценки качества подготовки и работы конкретных операторов; надежного обеспечения физической защиты конкретного объекта; выбора программных средств интегрированной системы безопасности на объекте защиты.

Ключевые слова: информационная безопасность, интегрированная система безопасности, система контроля и управления доступом, система охранно-тревожной сигнализации, управление информационной безопасностью, система охранного телевидения

ASSESSMENT METHOD OF HUMAN-MACHINE INTERFACE SECURITY FOR AN AUTOMATED WORKPLACE OF AN INTEGRATED SECURITY SYSTEM

Telnyy A.V., Monakhov M.Yu., Nikolaev A.V., Matveeva E.A.

Vladimir State University named after Alexander Grigorievich and Nikolai Grigorievich Stoletov", Vladimir, e-mail: andre.izi@mail.ru

The objective of the study is to develop a methodology for assessing the level of information security when processed by an operator in a human-machine interface. This methodology can be used to ensure information security management, increase the object's security against attacks, and reduce the level of false alarms of technical means of an integrated security system. To solve this problem, a system of assessments formed by a group of experts in the following sections is used: types of organoleptic information received by the operator; for each type of such information, experts assess the importance of ensuring integrity, confidentiality, and availability depending on the level of the security subsystem; a list of factors affecting the security of information resources for a specific interface; gradations and weighting coefficients for factors affecting the security of information resources for a specific integrated security system; assessments for distributing the significance of factors affecting the security of information resources by integrity, confidentiality, and availability. It is proposed to assess the security of human-machine interface information as the Euclidean distance in the space of integrity, confidentiality, and availability criteria. These expert assessments were obtained and tested to assess various types of software for integrated security systems. The proposed methodology can be used for: creating a decision support system; assessing the quality of training and work of specific operators; reliability of ensuring physical protection of a specific facility; selecting software for an integrated security system at the facility being protected.

Keywords: information security, integrated security system, information security management, security alarm system, access control and management system, closed-circuit television system

Введение

При обеспечении процесса охраны объекта для обработки информации используются комплексные аппаратно-программные средства на основе интегрированных систем безопасности (ИСБ). Операторы ИСБ, с одной стороны, являются звеном процесса обработки и управления информационной безопасностью, а с другой – своего рода преобразователями типа представления информации. С помощью анализа восприятий органов чувств оператор получает инфор-

мацию от автоматизированного рабочего места (АРМ) ИСБ и оценивает ее. В основном это информация визуальная (изображения, текст, характер цвета пиктограмм и частота мигания пиктограмм изображения), а также акустическая звуковая, речевая информация. В настоящее время не существует общепринятых методик оценки целостности, доступности и конфиденциальности информации при ее визуальной и акустической обработке человеком-оператором в человеко-машинном интерфейсе АРМ ИСБ. АРМ ИСБ представляет собой программно-аппаратный комплекс, предназначенный для контроля и управления различными системами безопасности (например, системами видеонаблюдения, контроля доступа, пожарной сигнализации и т.д.) с одного центрального места. АРМ обеспечивает функции оперативного контроля, анализа и реагирования на происходящие события в реальном времени.

Цель исследования – на основании методов ситуационного анализа с использованием экспертных оценок специалистов систем охраны и безопасности сформировать методику оценки защищенности человеко-машинного интерфейса в категориях конфиденциальности, целостности и доступности информационных ресурсов, передаваемых человеку-оператору от АРМ ИСБ.

Материалы и методы исследования

Требования к ИСБ, в том числе и к АРМ ИСБ, нормативно регламентированы в [1, 2]. В публикации [3, с. 148–158] дан общий обзор интероперабильности человеко-машинных интерфейсов (ЧМИ). Организации информационной распределенной среды ИСБ посвящена публикация [4]. Семантическая интероперабельность взаимодействия элементов в сетецентрических системах, в том числе при обеспечении информационной безопасности, анализируется в работах [5-7]. Согласно требованиям по обработке информации операторами АРМ ИСБ, вся информация, полученная или переданная через АРМ, должна быть защищена и обрабатываться в соответствии с требованиями к конфиденциальности, целостности и доступности. Все методики оценки качества восприятия оператором АРМ ИСБ информации можно классифицировать по трем основным типам: эргономические (уровень яркости, контраст изображения, время наблюдения, цветоощущение, шумовой фон и т.д.); психофизиологические (психология оператора, его опыт работы, работоспособность и т.д.); программно-технические (технические средства, информационные технологии и системы обработки информации).

Эргономический подход. Эргономические методики представляют собой совокупность методов и средств, обеспечивающих максимально комфортные условия высокоэффективной и безошибочной деятельности оператора на АРМ в ИСБ. При оценке яркостно-контрастных характеристик изображения следует учесть характеристики естественной и искусственной освещенности [8]. При оценке акустических характеристик также учитываются параметры выбранных средств аудиообработки информации и шумовой фон [9]. Вопросам эргономики АРМ посвящены публикации [10, 11].

Психофизиологический подход подразумевает совокупность методов и решений, основанных на психологии человека, его реакцию на звук, яркость и контраст визуальной информации.

Программно-технический подход представляет собой совокупность требований к техническим и программным средствам, применяемым на АРМ для обработки информации. Современные рабочие места мониторинга систем физической защиты характеризуются высокой степенью автоматизации, специализированными компьютерными интерфейсами, отсутствием внешних органов управления и систем индикации. Вся акустическая и визуальная информация поступает оператору только от персонального компьютера. Пользовательские интерфейсы таких систем определяются требованиями и оцениваются существующими стандартами: ГОСТ Р ИСО 14915–1-2016 «Эргономика мультимедийных пользовательских интерфейсов. Часть 1. Принципы проектирования и структура»; ГОСТ 28195-89 «Оценка качества программных средств. Общие положения». Особое внимание при оценке качества интерфейсов отводится сравнительным характеристикам качества отображаемой информации по отношению к зрительным и слуховым возможностям среднестатистического оператора АРМ ИСБ.

При оценке качества восприятия как визуальной, так и акустической информации оператором на АРМ ИСБ можно использовать и комплексный подход с применением экспертных оценок работы оператора на основе опыта и знаний экспертов. Методы ситуационного анализа (морфологический анализ, метод Дельфи, синектики, двухтурового анкетирования, мозгового штурма и пр.) субъективны, однако для вербальных задач информационной безопасности и субъективного восприятия информации человеком в ЧМИ [5-7] методы экспертных оценок, а также методы нечеткой логики оказываются одними из самых используемых.

В данной работе экспертные оценки были сформированы с использованием в качестве экспертов специалистов управления вневедомственной охраны по Владимирской области. Всего в данной работе были задействованы 16 человек. При обработке экспертных оценок эксперты классифицировались по уровню образования и его профилю, а также стажу работы. Эксперты проводили оценки отдельно друг от друга для обеспечения независимости их мнений.

Результаты исследования и их обсуждение

В данной работе из всех подсистем, которые могут быть задействованы в АРМ ИСБ, рассматриваются только базовые подсистемы, в том числе: охранная сигнализация (ОС); тревожная сигнализация (ТС); система контроля и управления доступом (СКУД); охранное телевидение (СОТ). Прочие подсистемы, которые потенциально могут входить в ИСБ, не рассматриваются. Оценка защищенности информационных ресурсов в АРМ ИСБ производится на основании формальной модели, основанной на экспертных оценках специалистов в данной предметной области.

Каждый эксперт в группе для каждой подсистемы безопасности формулирует виды органолептической информации, получаемой оператором от АРМ ИСБ (табл. 1); для каждого вида такой информации формирует экспертные оценки важности обеспечения целостности, конфиденциальности и доступности, причем в зависимости от уровня подсистемы безопасности (табл. 1); формулирует перечень факторов, влияющих на защищенность информационных ресурсов для конкретной АРМ ИСБ, по разделам: технические; программные; организационные и субъективные факторы для конкретного оператора (табл. 2); формулирует градации и в соответствии с ними дает оценку весовым коэффициентам для факторов, влияющих на защищенность информационных ресурсов для конкретной АРМ ИСБ (табл. 2); дает оценку распределения значимости факторов, влияющих на защищенность информационных ресурсов в АРМ ИСБ, по целостности, конфиденциальности и доступности.

Таблица 1

Оценка важности восприятия информации оператором ИСБ по показателям целостности, конфиденциальности и доступности

Индекс j	Характер восприятия информации оператором ИСБ (индекс j)	Важность обеспечения целостности (K_j1)	Важность обеспечения конфиденциальности (K_j2)	Важность обеспечения доступности (K_j3)
Подсистема охранная сигнализация (ОС) в зависимости от класса охраняемого объекта (А1; А2; А3; Б1; Б2)				
1	Тревожное извещение о проникновении (цветовое и текстовое изображение) (А1; А2; А3; Б1; Б2)	1/0,98/0,95/ 0,92/0,9	1/0,95/0,9/ 0,85/0,8	1/0,98/0,98/ 0,98/0,98
2	Тревожное извещение о проникновении (звук) (А1; А2; А3; Б1; Б2)	1/0,98/0,95/ 0,92/0,9	1/0,95/0,9/ 0,85/0,8	1/0,98/0,98/ 0,98/0,98
3	Тревожное извещение о неисправности ОТС объекта (цветовое и текстовое изображение) (А1; А2; А3; Б1; Б2)	1/0,95/0,92/ 0,9/0,85	1/0,95/0,9/ 0,85/0,8	1/0,98/0,95/ 0,95/0,95
4	Тревожное извещение о неисправности ОТС объекта (звук) (А1; А2; А3; Б1; Б2)	1/0,95/0,92/ 0,9/0,85	1/0,95/0,9/ 0,85/0,8	1/0,98/0,95/ 0,95/0,95
5	Тревожное извещение об отсутствии связи с объектом (цветовое и текстовое изображение) (А1; А2; А3; Б1; Б2)	1/0,98/0,95/ 0,92/0,9	1/0,95/0,9/ 0,85/0,8	1/0,98/0,98/ 0,98/0,98
6	Тревожное извещение об отсутствии связи с объектом (звук) (А1; А2; А3; Б1; Б2)	1/0,98/0,95/ 0,92/0,9	1/0,95/0,9/ 0,85/0,8	1/0,98/0,98/ 0,98/0,98
7	Тревожное извещение о снятии с охраны под принуждением (цветовое и текстовое изображение) (А1; А2; А3; Б1; Б2)	1/0,98/0,95/ 0,92/0,9	1/0,95/0,9/ 0,85/0,8	1/0,98/0,98/ 0,98/0,98
8	Тревожное извещение о снятии с охраны под принуждением (звук) (А1; А2; А3; Б1; Б2)	1/0,98/0,95/ 0,92/0,9	1/0,95/0,9/ 0,85/0,8	1/0,98/0,98/ 0,98/0,98
9	Служебное извещение с объекта (переход на резервное питание, вскрытие объекта вне графика охраны и пр.) (цветовое и текстовое изображение) (А1; А2; А3; Б1; Б2)	1/0,95/0,9/ 0,85/0,8	1/0,95/0,9/ 0,8/0,7	1/0,98/0,95/ 0,92/0,9

Продолжение табл. 1

Индекс *j*	Характер восприятия информации оператором ИСБ (индекс *j*)	Важность обеспечения целостности (K_j1)	Важность обеспечения конфиденциальности (K_j2)	Важность обеспечения доступности (K_j3)
10	Служебное извещение с объекта (переход на резервное питание, вскрытие объекта вне графика охраны и пр.) (звук) (А1; А2; А3; Б1; Б2)	1/0,95/0,9/ 0,85/0,8	1/0,95/0,9/ 0,8/0,7	1/0,98/0,95/ 0,92/0,9
11	Информация по адресу объекта и его месте расположения (текст, план) (А1; А2; А3; Б1; Б2)	1/0,95/0,9/ 0,8/0,7	1/0,95/0,9/ 0,85/0,8	1/0,98/0,95/ 0,92/0,9
12	Информация по местам возможного проникновения (текст) (А1; А2; А3; Б1; Б2)	1/0,95/0,9/ 0,8/0,7	/0,95/0,9/ 0,8/0,7	1/0,98/0,95/ 0,92/0,9
13	Информация по режиму работы и график охраны (текст) (А1; А2; А3; Б1; Б2)	1/0,95/0,9/ 0,8/0,7	1/0,95/0,9/ 0,8/0,7	1/0,95/0,9/ 0,9/0,8
14	Информация по адресам собственников (лиц, отвечающих за прием/снятие с охраны) (текст) (А1; А2; А3; Б1; Б2)	1/0,9/0,85/ 0,75/0,65	1/0,95/0,9/ 0,8/0,7	1/0,95/0,9/ 0,9/0,8
15	Информация по типу, количеству, характеру ТСО на объекте (текст, план объекта) (А1;А2;А3;Б1;Б2)	1/0,9/0,85/ 0,75/0,65	1/0,95/0,9/ 0,8/0,7	1/0,95/0,9/ 0,9/0,8
Подсистема тревожная сигнализация (ТС) (А1; А2; А3; Б1; Б2)				
16	Тревожное извещение о нападении (цветовое и текстовое изображение) (А1; А2; А3; Б1; Б2)	1/0,99/0,98/ 0,95/0,92	1/0,95/0,9/ 0,85/0,8	1/0,98/0,98/ 0,98/0,98
17	Тревожное извещение о нападении (звук) (А1; А2; А3; Б1; Б2)	1/0,99/0,98/ 0,95/0,92	1/0,95/0,9/ 0,85/0,8	1/0,98/0,98/ 0,98/0,98
18	Тревожное извещение о неисправности ТС объекта (цветовое и текстовое изображение) (А1; А2; А3; Б1; Б2)	1/0,99/0,98/ 0,95/0,92	1/0,95/0,9/ 0,85/0,8	1/0,98/0,98/ 0,98/0,98
19	Тревожное извещение о неисправности ТС объекта (звук) (А1; А2; А3; Б1; Б2)	1/0,98/0,95/ 0,92/0,9	1/0,95/0,9/ 0,85/0,8	1/0,98/0,95/ 0,95/0,95
20	Тревожное извещение об отсутствии связи с объектом (цветовое и текстовое изображение) (А1; А2; А3; Б1; Б2)	1/0,99/0,98/ 0,95/0,92	1/0,95/0,9/ 0,85/0,8	1/0,98/0,98/ 0,98/0,98
21	Тревожное извещение об отсутствии связи с объектом (звук) (А1; А2; А3; Б1; Б2)	1/0,99/0,98/ 0,95/0,92	1/0,95/0,9/ 0,85/0,8	1/0,98/0,98/ 0,98/0,98
22	Служебное извещение с объекта (переход на резервное питание, авария и пр.) (цветовое и текстовое изображение) (А1; А2; А3; Б1; Б2)	1/0,95/0,9/ 0,85/0,8	1/0,95/0,9/ 0,8/0,7	1/0,98/0,95/ 0,92/0,9
23	Служебное извещение с объекта (переход на резервное питание, авария и пр.) (звук) (А1; А2; А3; Б1; Б2)	1/0,95/0,9/ 0,85/0,8	1/0,95/0,9/ 0,8/0,7	1/0,98/0,95/ 0,92/0,9
24	Информация по адресу объекта и его месту расположения (текст, план) (А1; А2; А3; Б1; Б2)	1/0,95/0,9/ 0,8/0,7	1/0,95/0,9/ 0,85/0,8	1/0,98/0,95/ 0,92/0,9
25	Информация по местам возможного проникновения (текст) (А1; А2; А3; Б1; Б2)	1/0,95/0,9/ 0,8/0,7	/0,95/0,9/ 0,8/0,7	1/0,98/0,95/ 0,92/0,9
26	Информация по режиму работы и график охраны (текст) (А1; А2; А3; Б1; Б2)	1/0,9/0,85/ 0,75/0,65	1/0,95/0,9/ 0,8/0,7	1/0,95/0,9/ 0,9/0,8
27	Информация по типу, количеству, характеру ТСО на объекте (текст, план объекта) (А1; А2; А3; Б1; Б2)	1/0,9/0,85/ 0,75/0,65	1/0,95/0,9/ 0,8/0,7	1/0,95/0,9/ 0,9/0,8
Подсистема контроля и управления доступом (СКУД) классы (4/3/2/1)				
28	Тревожное извещение об НСД в точке доступа (цветовое и текстовое изображение) (классы 4/3/2/1)	1/0,98/ 0,95/0,9	1/0,95/0,9/0,8	1/0,98/ 0,98/0,98
29	Тревожное извещение об НСД в точке доступа (звук) (классы 4/3/2/1)	1/0,98/ 0,95/0,9	1/0,95/0,9/0,8	1/0,98/ 0,98/0,98
30	Тревожное извещение о нарушении графика прохода в точке доступа (цветовое и текстовое изображение) (классы 4/3/2/1)	1/0,98/ 0,95/0,9	1/0,95/0,9/0,8	1/0,98/ 0,98/0,98
31	Тревожное извещение о нарушении графика прохода в точке доступа (звук) (классы 4/3/2/1)	1/0,98/ 0,95/0,9	1/0,95/0,9/0,8	1/0,98/ 0,98/0,98

Продолжение табл. 1

Индекс *j*	Характер восприятия информации оператором ИСБ (индекс *j*)	Важность обеспечения целостности (K_j1)	Важность обеспечения конфиденциальности (K_j2)	Важность обеспечения доступности (K_j3)
32	Тревожное извещение о нарушении порядка (некорректности) прохода в точке доступа (цветовое и текстовое изображение) (классы 4/3/2/1)	1/0,98/ 0,95/0,9	1/0,95/0,9/0,8	1/0,95/ 0,95/0,95
33	Тревожное извещение о нарушении порядка (некорректности) прохода в точке доступа (звук) (классы 4/3/2/1)	1/0,98/ 0,95/0,9	1/0,95/0,9/0,8	1/0,95/ 0,95/0,95
34	Тревожное извещение о неисправности СКУД объекта (цветовое и текстовое изображение) (классы 4/3/2/1)	1/0,98/ 0,95/0,9	1/0,95/0,9/0,8	1/0,95/ 0,95/0,95
35	Тревожное извещение о неисправности СКУД объекта (звук) (классы 4/3/2/1)	1/0,98/ 0,95/0,9	1/0,95/0,9/0,8	1/0,95/ 0,95/0,95
36	Тревожное извещение об отсутствии связи с точками доступа СКУД (цветовое и текстовое изображение) (классы 4/3/2/1)	1/0,98/ 0,95/0,9	1/0,95/0,9/0,8	1/0,98/ 0,98/0,98
37	Тревожное извещение об отсутствии связи с точками доступа СКУД (звук) (классы 4/3/2/1)	1/0,98/ 0,95/0,9	1/0,95/0,9/0,8	1/0,98/ 0,98/0,98
38	Тревожное извещение о превышении попыток доступа (контроллерами) (цветовое и текстовое изображение) (классы 4/3/2/1)	1/0,98/ 0,95/0,9	1/0,95/0,9/0,8	1/0,95/ 0,95/0,95
39	Тревожное извещение о превышении попыток доступа (контроллерами) (звук) (классы 4/3/2/1)	1/0,98/ 0,95/0,9	1/0,95/0,9/0,8	1/0,95/ 0,95/0,95
40	Тревожное извещение о попытке использования недействительного идентификатора в СКУД (контроллерами) (цветовое и текстовое изображение) (классы 4/3/2/1)	1/0,95/ 0,9/0,8	1/0,95/0,9/0,8	1/0,95/0,9/0,9
41	Тревожное извещение о попытке использования недействительного идентификатора в СКУД (контроллерами) (звук) (классы 4/3/2/1)	1/0,95/ 0,9/0,8	1/0,95/0,9/0,8	1/0,95/0,9/0,9
42	Служебное извещение от точек доступа СКУД (переход на резервное питание и пр.) (цветовое и текстовое изображение) (классы 4/3/2/1)	1/0,9/0,8/0,7	1/0,9/0,8/0,7	1/0,9/0,8/0,7
43	Служебное извещение от точек доступа СКУД (переход на резервное питание пр.) (звук) (классы 4/3/2/1)	1/0,9/0,8/0,7	1/0,9/0,8/0,7	1/0,9/0,8/0,7
44	Информация по точке доступа и ее месту расположения (текст, план) (классы 4/3/2/1)	1/0,9/0,8/0,7	1/0,9/0,8/0,7	1/0,9/0,8/0,7
45	Информация по местам возможного проникновения (текст) (классы 4/3/2/1)	1/0,9/0,8/0,7	1/0,9/0,8/0,7	1/0,9/0,8/0,7
46	Информация по режиму работы и график помещения с точкой доступа СКУД (текст) (классы 4/3/2/1)	1/0,9/0,8/0,7	1/0,9/0,8/0,7	1/0,9/0,8/0,7
47	Информация по типу, количеству, характеру точек доступа на объекте (текст, план объекта) (классы 4/3/2/1)	1/0,9/0,8 /0,7	1/0,9/0,8/0,7	1/0,9/0,8/0,7
Подсистема охранного телевидения (СОТ) тип (3/2/1)				
48	Тревожное извещение о фиксации движения на периметре объекта (цветовое и текстовое изображение) (тип СОТ 3/2/1)	1/0,95/0,92	1/0,9/0,8	1/0,9/0,8
49	Тревожное извещение о фиксации движения на периметре объекта (звук) (тип СОТ 3/2/1)	1/0,95/0,92	1/0,9/0,8	1/0,9/0,8
50	Тревожное извещение о фиксации движения внутри объекта (цветовое и текстовое изображение) (тип СОТ 3/2/1)	1/0,98/0,95	1/0,95/0,9	1/0,95/0,9
51	Тревожное извещение о фиксации движения внутри объекта (звук) (тип СОТ 3/2/1)	1/0,98/0,95	1/0,95/0,9	1/0,95/0,9
52	Тревожное извещение о попытке вскрытия аппаратуры и коммуникации СОТ (цветовое и текстовое изображение) (тип СОТ 3/2/1)	1/0,98/0,95	1/0,95/0,9	1/0,95/0,9

Окончание табл. 1

Индекс j	Характер восприятия информации оператором ИСБ (индекс j)	Важность обеспечения целостности (K_j1)	Важность обеспечения конфиденциальности (K_j2)	Важность обеспечения доступности (K_j3)
53	Тревожное извещение о попытке вскрытия аппаратуры и коммуникации СОТ (звук) (тип СОТ 3/2/1)	1/0,98/0,95	1/0,95/0,9	1/0,95/0,9
54	Тревожное извещение о попытке НСД к программным ресурсам СОТ (цветовое и текстовое изображение) (тип СОТ 3/2/1)	1/0,98/0,95	1/0,95/0,9	1/0,95/0,9
55	Тревожное извещение о попытке НСД к программным ресурсам СОТ (звук) (тип СОТ 3/2/1)	1/0,98/0,95	1/0,95/0,9	1/0,95/0,9
56	Служебное извещение с СОТ (переход на резервное питание, окончание емкости регистратора и пр.) (цветовое и текстовое изображение) (тип СОТ 3/2/1)	1/0,92/0,9	1/0,92/0,9	1/0,92/0,9
57	Служебное извещение с СОТ (переход на резервное питание, окончание емкости регистратора и пр.) (звук) (тип СОТ 3/2/1)	1/0,92/0,9	1/0,92/0,9	1/0,92/0,9
58	Информация по адресу объекта и его месту расположения, информация титров (дата, время и пр.) (текст, план) (тип СОТ 3/2/1)	1/0,9/0,8	1/0,9/0,8	1/0,9/0,8
59	Информация по местам возможного проникновения (текст) (тип СОТ 3/2/1)	1/0,9/0,8	1/0,9/0,8	1/0,9/0,8
60	Информация по режиму работы и график охраны (текст) (тип СОТ 3/2/1)	1/0,9/0,8	1/0,9/0,8	1/0,9/0,8
61	Информация по типу, количеству, характеру СОТ на объекте (текст, план объекта) (тип СОТ 3/2/1)	1/0,9/0,8	1/0,9/0,8	1/0,9/0,8

Таблица 2

Весовые коэффициенты для оценки факторов,
влияющих на защищенность информационных ресурсов в АРМ ИСБ

p_i	ФАКТОРЫ	Коэффициент p_i
	Технические факторы	
p_1	Размер экрана монитора: 21” и выше / 19” /17” / 15” и ниже	1,0/0,95/0,9/0,85
p_2	Разрешение экрана монитора: 1920 × 1080 и выше / 1600 × 1024/1280 × 720/1024 × 600/800 × 600/800 × 480/640 × 480	1,0/0,98/0,95/ 0,9/0,85/0,8 /0,7
p_3	Размер минимального элемента пиктограммы пользовательского интерфейса в процентном отношении к размеру экрана: до 20% и выше / до 15% / до 10%/ до 5% / до 1% и менее	1,0/0,95/0,92/ 0,9/0,85
p_4	Яркость и контрастность экрана монитора: отличная / очень хорошая / хорошая/удовлетворительная/плохая / очень плохая (почти ничего не видно)	1,0/0,92/0,85/ 0,75/0,65/0,5
p_5	Уровень звука воспроизведения сообщений в сравнении с уровнем шума в помещении (на сколько дБ звук больше фона): более 15 дБ / более 10 дБ / более 5 дБ / менее 5 дБ	1,0/0,9/0,8/0,6
p_6	Уровень шума в помещении: менее 50 дБ / до 55 дБ/ до 60 дБ/ до 65 дБ/ до 70 дБ/ до 75 дБ/ более 75 дБ/	1,0/0,95/0,9/0,8/ 0,7/0,6/0,5
p_7	Наличие включенных бытовых аудиовизуальных средств (телевизоры, магнитофоны, планшеты и пр.), отвлекающих внимание операторов: нет/есть/	1,0/0,6
p_8	Качество естественной освещенности на рабочем месте: отличная / очень хорошая / хорошая/удовлетворительная /плохая / очень плохая (почти ничего не видно)	1,0/0,92/0,85/ 0,75/0,65/0,5
p_9	Качество средств искусственного освещения на рабочем месте: отличное / очень хорошее / хорошее / удовлетворительное /плохое / очень плохое (почти ничего не видно)	1,0/0,92/0,85/ 0,75/0,65/0,5
p_{10}	Качество функционирования аппаратных средств АРМ ИСБ (наличие отказов, сбоев и пр.): отличное/ очень хорошее / хорошее /удовлетворительное /плохое / очень плохое	1,0/0,92/0,85/ 0,75/0,65/0,5

Окончание табл. 2

p_i	ФАКТОРЫ	Коэффициент p_i
p_{11}	Быстродействие СВТ АРМ ИСБ (среднее время задержки реагирования АРМ ИСБ на типовые действия оператора с ПО): менее 0,1 с / менее 0,5с / до 1 с / до 3 с / до 5 с /более 5 с	1,0/0,9/0,85/ 0,75/0,65/0,5
p_{12}	Срок эксплуатации СВТ: менее 1 года / до 3 лет / от 3 до 5 лет/ от 5 до 8 лет / более 8 лет (в круглосуточном режиме)	1,0/0,95/0,7/ 0,5/0,3
p_{13}	Наличие постороннего, «мешающего» ПО на АРМ ИСБ, используется ли АРМ ИСБ для выполнения других задач: не имеется / имеется	1,0/0,7
	Программные факторы ПО	
p_{14}	Имеется ли актуальный сертификат ИСО 27001: да/нет	1,0/0,85
p_{15}	Апробировано ли данное ПО на других объектах: да/нет	1,0/0,6
p_{16}	Входит ли ПО АРМ ИСБ в список технических средств безопасности: да/нет	1,0/0,6
p_{17}	Соответствует ли АРМ ИСБ требованиям ГОСТ Р 57674-2017: полностью соответствует / частично более чем на 50%/ менее чем на 50% / не соответствует	1,0/0,75/0,55/0,3
p_{18}	Удобство (эргономичность интерфейса): отлично/ очень хорошо / хорошо / удовлетворительно /плохо / очень плохо	1,0/0,9/0,85/ 0,75/0,65/0,5
p_{19}	Размер детализации объектов отображения информации в интерфейсе ПО АРМ ИСБ: отлично/ очень хорошо / хорошо /удовлетворительно /плохо / очень плохо	1,0/0,9/0,85/ 0,75/0,65/0,5
p_{20}	Средняя скорость поступления тревожных извещений оператору АРМ ИСБ: до 1 в час / до 5 в час / до 10 в час / до 20 в час / более 20 в час	1,0/0,95/0,85/ 0,8/0,75
p_{21}	Средняя скорость поступления служебных извещений оператору АРМ ИСБ: до 10 в час / до 20 в час / до 50 в час / до 100 в час / более 100 в час	1,0/0,95/0,85/ 0,8/0,75
	Организационные факторы	
p_{22}	Количество рабочих мест АРМ ИСБ в помещении: одно / два / более двух	1,0/0,9/0,75
p_{23}	Загрузка операторов АРМ ИСБ (по задействованным источникам получения информации от подсистем) ИСБ (объем ТСО на рабочем месте): до 200 номеров / до 400 номеров / до 600 номеров/ свыше 600 номеров	1,0/0,95/0,8/0,65
p_{24}	Дополнительная загрузка операторов АРМ ИСБ (выполнение прочих обязанностей): не имеется / да имеется	1,0/0,75
p_{25}	Режим непрерывной работы операторов ИСБ: 4-часовая смена / 8-часовая смена / 12-часовая смена / суточный режим	1,0/0,92/0,7/0,5
p_{26}	Возможность и организации подмены для чередования режима работы и отдыха оператора АРМ ИСБ: есть/нет	1,0/0,7
	Субъективные факторы оператора	
p_{27}	Наличие опыта (стажа) работы с ПО АРМ ИСБ у оператора: более 5 лет / до 5 лет / до 3 лет/ до 1 года / до 0,5 года /менее 1 месяца	1,0/0,95/0,92/ 0,85/0,75/0,6
p_{28}	Наличие подготовки и качество знания интерфейса ПО АРМ ИСБ оператором: отличное / очень хорошее / хорошее /удовлетворительное /плохое / очень плохое	1,0/0,9/0,85/ 0,75/0,65/0,5
p_{29}	Возраст оператора: до 18 лет / до 30 лет / до 50 лет /до 65 лет/ свыше 65 лет	1,0/0,95/0,85/ 0,75/0,6
p_{30}	Качество слуха оператора: отличное/ очень хорошее / хорошее /удовлетворительное /плохое / очень плохое	1,0/0,9/0,85/ 0,75/0,65/0,5
p_{31}	Качество зрения оператора: отличное/ очень хорошее / хорошее /удовлетворительное /плохое / очень плохое	1,0/0,9/0,85/ 0,75/0,65/0,5
p_{32}	Общее состояние здоровья оператора: отличное/ очень хорошее / хорошее /удовлетворительное /плохое / очень плохое	1,0/0,9/0,85/ 0,75/0,65/0,5
p_{33}	Психоэмоциональное состояние на момент смены, самочувствие оператора: отличное/ очень хорошее / хорошее /удовлетворительное / плохое / очень плохое	1,0/0,9/0,85/ 0,75/0,65/0,5
p_{34}	Уровень недопущения проявления вредных привычек и дисциплинированности (склонность спать на рабочем месте, употреблять спиртные напитки): очень высокий / высокий / средний / низкий / очень низкий	1,0/0,9/0,7/ 0,6/0,5
p_{35}	Уровень исполнительности оператора: очень высокий / высокий / средний / низкий / очень низкий	1,0/0,9/0,7/ 0,6/0,5

Для анализа защищенности информации человеко-машинного интерфейса в АРМ ИСБ предлагается следующий алгоритм действий.

1. При проведении обследования (аудита) конкретного АРМ ИСБ определяются классы (типы) подсистем ИСБ и из таблицы 1 выбирают значения: (K_j1) – важности обеспечения целостности; (K_j2) – конфиденциальности; (K_j3) – доступности. Если какой-то подсистемы в АРМ ИСБ нет, то ее не учитывают. Если какой-то органолептической информации от подсистемы ИСБ в ПО АРМ ИСБ нет, то ее также не учитывают (строки в таблице 1).

2. При проведении обследования (аудита) конкретного АРМ ИСБ определяют конкретные градации проявления факторов по каждому пункту таблицы 2 и определяют весовые коэффициенты для оценки факторов, влияющих на защищенность информационных ресурсов в АРМ ИСБ для каждого p_i.

3. Максимально достижимая защищенность для АРМ ИСБ может быть определена как:

$$P_{max} = \sqrt{\left(\frac{\sum_{n=1}^{N}\left(\sum_{jn=1}^{J_n}\frac{K_{jn}1}{J_n}\right)}{N}\right)^2 + \left(\frac{\sum_{n=1}^{N}\left(\sum_{jn=1}^{J_n}\frac{K_{jn}2}{J_n}\right)}{N}\right)^2 + \left(\frac{\sum_{n=1}^{N}\left(\sum_{jn=1}^{J_n}\frac{K_{jn}3}{J_n}\right)}{N}\right)^2} \quad (1)$$

где $n=1...N$ – количество подсистем безопасности; $K_{jn}1$; $K_{jn}2$; $K_{jn}3$ – весовые коэффициенты по целостности, конфиденциальности и доступности для n-ой подсистемы безопасности; J_n – это количество строк из таблицы 1 по каждой из подсистем безопасности, которые используются (если органолептической информации от подсистемы нет, то ее не учитывают).

4. Для конкретного АРМ ИСБ максимальная защищенность будет определяться по (1) при условии, что $\forall p_i = 1$. Защищенность информации для АРМ ИСБ определяется как евклидово расстояние в пространстве критериев целостности, конфиденциальности и доступности:

$$P = \sqrt{\left(\frac{\sum_{n=1}^{N}\left(\sum_{jn=1}^{J_n}\frac{K_{jn}1}{J_n}\right)}{N}\cdot\left(\frac{q_i1\cdot\sum_{i=1}^{I}p_i}{I}\right)\right)^2 + \left(\frac{\sum_{n=1}^{N}\left(\sum_{jn=1}^{J_n}\frac{K_{jn}2}{J_n}\right)}{N}\cdot\left(\frac{q_i2\cdot\sum_{i=1}^{I}p_i}{I}\right)\right)^2 + \left(\frac{\sum_{n=1}^{N}\left(\sum_{jn=1}^{J_n}\frac{K_{jn}3}{J_n}\right)}{N}\cdot\left(\frac{q_i1\cdot\sum_{i=1}^{I}p_i}{I}\right)\right)^2} \quad (2)$$

где значения p_i берутся из таблицы 2, а значения q_j1; q_j2; q_j3 берутся из таблицы 3.

5. Для окончательной оценки нужна нормировка, тогда реальная защищенность будет такова:

$$P_{APM} = P / P_{max}. \quad (3)$$

При рассмотрении АРМ ИСБ необходимо учитывать, все ли подсистемы безопасности задействованы в ИСБ и каковы уровень (масштаб) и важность подсистемы ИСБ. Для этого реальную подсистему ИСБ необходимо классифицировать согласно требованиям нормативных документов по каждой из подсистем безопасности. Для подсистем охранной и тревожной сигнализации уровень определяется классом охраняемых объектов [12]. В зависимости от стоимости защищаемых предметов и ценностей на объекте, общественной значимости объекта, последствий от возможных посягательств на объект защиты все охраняемые объекты классифицируются по убыванию важности по классам А1; А2; А3; Б1; Б2. Для подсистемы СКУД согласно [13] выделяют по убыванию уровня и важности классы СКУД 4; 3; 2; 1. Для подсистемы СОТ бывают 1-я, 2-я, 3-я группы по убыванию сложности и важности по пункту 5.2.2 нормативного документа [14].

Таблица 3

Распределение значимости факторов, влияющих
на защищенность информационных ресурсов в АРМ ИСБ,
по целостности, конфиденциальности и доступности

p_i	Обеспечение целостности (q_j1)	Обеспечение конфиденциальности (q_j2)	Обеспечение доступности (q_j3)
p_1	0,8	1,0	0,8
p_2	0,8	1,0	0,8
p_3	0,9	1,0	0,9
p_4	0,8	1,0	0,8
p_5	0,9	1,0	0,9
p_6	0,95	0,9	0,8
p_7	0,8	0,9	0,8
p_8	0,8	1,0	0,8
p_9	0,8	1,0	0,8
p_{10}	0,7	0,9	0,8
p_{11}	0,9	0,9	0,6
p_{12}	0,7	0,8	0,7
p_{13}	0,8	0,8	0,8
p_{14}	0,95	0,95	0,95
p_{15}	0,9	0,9	0,9
p_{16}	0,9	0,9	0,9
p_{17}	0,9	0,9	0,9
p_{18}	0,95	1,0	0,85
p_{19}	0,95	1,0	0,9
p_{20}	0,9	1,0	0,8
p_{21}	0,85	1,0	0,9
p_{22}	0,95	0,95	0,95
p_{23}	0,75	0,95	0,75
p_{24}	0,85	0,9	0,75
p_{25}	0,85	0,95	0,85
p_{26}	0,85	0,95	0,85
p_{27}	0,85	0,95	0,9
p_{28}	0,85	0,95	0,9
p_{29}	0,85	0,95	0,9
p_{30}	0,85	0,95	0,9
p_{31}	0,85	0,95	0,85
p_{32}	0,85	0,95	0,85
p_{33}	0,85	0,95	0,85
p_{34}	0,8	0,85	0,8
p_{35}	0,85	0,95	0,85

Представленные в таблицах 1–3 коэффициенты являются обобщенными от группы экспертов субъективными ранжированными оценками, представленными в нормированном виде от 0 до 1 в 20 градациях, то есть с шагом в 0,05. Чем ближе значение показателя к 1, тем более важно обеспечение показателя для выбранного информационного ресурса. Данная таблица для разных АРМ ИСБ, на которых используется одно и то же программное обеспечение, является единой. Методом экспертных оценок была

составлена таблица 2 для учета особенностей конкретного оператора и конкретного рабочего места АРМ ИСБ. В таблице 2 представлены весовые коэффициенты факторов, влияющих на защищенность информационных ресурсов в АРМ ИСБ, в которых были учтены технические, программные, организационные, субъективные факторы конкретного оператора. Для оценки защищенности ЧМИ конкретного рабочего места АРМ ИСБ в пространстве параметров целостности, конфиденциальности и доступности методом экспертных оценок была составлена таблица распределения значимости факторов, влияющих на защищенность информационных ресурсов в АРМ ИСБ (табл. 3). На основании предлагаемой методики для одних и тех же организационных условий и типов операторов АРМ ИСБ была проведена оценка человеко-машинных интерфейсов для АРМ ИСБ «Орион-Про вер.1.20.3.8» (www.bolid.ru); ИСБ «РУБЕЖ-08 вер.3.5.1» (www.sigma-is.ru); ИСБ «Кодос» (www.kodos.ru). Реальных объектов, на которых при одних и тех же условиях «параллельно» установлены разные АРМ ИСБ, не существует по экономическим соображениям. Поэтому апробация результатов была частично виртуальной, т.е. виртуально одинаковыми для разных типов ПО АРМ ИСБ по таблице 2 устанавливались технические, организационные и субъективные факторы. Исходные данные по факторам таблицы 1 и программные факторы по таблице 2 соответствовали разным типам программного обеспечения АРМ ИСБ. Всего анализировались три типа разных начальных виртуально установленных организационных условий и типов операторов АРМ ИСБ (идеальные условия, средние условия и максимально плохие условия). При этом средняя разница в определении нормированного значения оценки защищенности ЧМИ для разных типов используемого ПО составила около 7%, а максимальная разница – 13% для «средних» условий (когда принимались средние значения технических, организационных и субъективных факторов по таблице 2 и исходных данных по факторам таблицы 1). Данные результаты в целом согласуются с субъективным мнением экспертов, которые их оценивали.

Наиболее объективно достоверность результатов применения указанной методики для разных типов АРМ ИСБ оценивается статистически как результат сравнения доли несанкционированных проникновений именно по вине ЧМИ между оператором и конкретным типом АРМ СПИ. При этом можно оценивать очень схожие по условиям объекты с разными АРМ ИСБ или прогнозировать на длительный период состояние защищенности ЧМИ (долю вероятных проникновений по вине ЧМИ) и сравнивать результаты прогноза с фактическим состоянием по окончании периода. Оба варианта вызывают сложности, так как требуют значительного времени сбора данных. Вероятность посягательства на среднестатистический объект защиты составляет несколько попыток в год, а вероятность несанкционированного доступа по вине ЧМИ – несколько процентов от попыток посягательств. Причем за время сбора данных состояние исходных данных может значительно измениться. Другим способом оценки достоверности результатов является корреляция данных расчетов с экспертными мнениями специалистов.

Заключение

Рассмотренные в работе формальная модель и обобщенная методика оценки защищенности информации при ее обработке оператором в АРМ интегрированной системы безопасности являются простым и понятным инструментом, с помощью которого можно оценивать: качество организации работы АРМ ИСБ на конкретном рабочем месте; качество подготовки и работы конкретных операторов; надежность обеспечения физической защиты конкретного объекта; сравнивать между собой разнообразные типы программного обеспечения АРМ ИСБ и выполнять другие задачи. При практическом использовании следует периодически применять данную методику оценки для выявления тенденций и динамики изменения защищенности информационных ресурсов в процессе эксплуатации АРМ ИСБ.

Предлагаемая методика путем расширения экспертных оценок может быть адаптирована для анализа защищенности информации при ее обработке не только для АРМ ИСБ, но и в центрах пожарного мониторинга в системе МЧС, а также для АРМ систем централизованного видеонаблюдения и т.д.

Список литературы

1. ГОСТ Р 57674-2017. Интегрированные системы безопасности. Общие положения. М.: Стандартинформ, 2019. 12 с.

2. Рекомендации по охране особо важных объектов с применением интегрированных систем безопасности. Р 089-2022. М.: ФКУ НИЦ «Охрана». 2022. 96 с.

3. Макаренко С.И. Интероперабельность человеко-машинных интерфейсов / под ред. С.И. Макаренко. СПб.: Наукоемкие технологии, 2023. 185 с.

4. Тельный А.В., Никитин О.Р., Храпов И.В. Об организации информационной распределенной среды интегрированных систем охраны и безопасности // Известия высших учебных заведений. Приборостроение. 2012. Т. 55, № 8. С. 28-32.

5. Макаренко С.И., Соловьева О.С. Семантическая интероперабельность взаимодействия элементов в сетецентри-

ческих системах // Журнал радиоэлектроники. 2021. № 6. С. 13. DOI: 10.30898/1684-1719.2021.6.3.

6. Черницкая Т.Е., Макаренко С.И., Растягаев Д.В. Аспекты информационной безопасности в рамках оценки интероперабельности сетецентрических информационно-управляющих систем. Вестник Российского нового университета. Серия: Сложные системы: модели, анализ и управление. 2020. № 4. С. 113-121. DOI: 10.25586/RNU.V9187.20.04.P.113.

7. Макаренко С.И., Олейников А.Я, Черницкая Т.Е. Модели интероперабельности информационных систем. Системы управления, связи и безопасности. 2019. № 4. С. 215-245. DOI: 10.24411/2410-9916-2019-10408.

8. Методические указания МУК 4.3.3975-24. Методические указания по инструментальному контролю и оценке освещения рабочих мест // Информационно-правовой портал ГАРАНТ.РУ [Электронный ресурс]. URL: https://www.garant.ru/products/ipo/prime/doc/408790461/?ysclid=m1lv23kfuj584294765 (дата обращения: 28.11.2024).

9. Методические указания МУК 4.3.3722-21. Контроль уровня шума на территории жилой застройки, в жилых и общественных зданиях и помещениях // Информационно-правовой портал ГАРАНТ.РУ [Электронный ресурс]. URL: https://www.garant.ru/products/ipo/prime/doc/403287707/?ysclid=m1lvb7959e278375637 (дата обращения: 28.11.2024).

10. Горячкин Б. С. Метод оценки эргономического обеспечения автоматизированной информационной системы // Альманах современной науки и образования. 2016. № 8(110). С. 21-23.

11. Назаренко Н.А., Осетров А.В. Особенности эргономической оценки пользовательских интерфейсов человеко-машинных систем специального назначения // Биотехносфера. 2015. № 1(37). С. 38-43.

12. Методические рекомендации. Обследование и прием под централизованную охрану подразделениями вневедомственной охраны войск национальной гвардии российской федерации объектов, мест проживания и хранения имущества граждан. Р 093. 2024. М.: ФКУ НИЦ «Охрана». 2024. 38 с.

13. Методические рекомендации. Выбор и применение технических средств и систем контроля и управления доступом. Р 064-2017. М.: ФКУ НИЦ «Охрана». 2017. 92 с.

14. ГОСТ Р 51558-2014. Средства и системы охранные телевизионные. Классификация. Общие технические требования. Методы испытаний. М.: Стандартинформ, 2019. 24 с.