УДК 004.056.5

П.Н. Наседкин [1]

[1] *Иркутский государственный университет путей сообщений, г. Иркутск, Российская Федерация*

АНАЛИЗ ВОСТРЕБОВАННОСТИ КОМПОНЕНТОВ УРОВНЯ ПРОГРАММНО-ТЕХНИЧЕСКИХ РЕШЕНИЙ КСЗИ ПРЕДПРИЯТИЯ С ТОЧКИ ЗРЕНИЯ ОБЕСПЕЧЕНИЯ БАЗОВЫХ ТРЕБОВАНИЙ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация. В работе на основе результатов оценивания объектов защиты ИТ-инфраструктуры предприятия в разрезе свойств информации (конфиденциальность, целостность и доступность) проведён анализ востребованности компонент уровня программно-технических решений (ПТР) комплексной системы защиты информации (КСЗИ) предприятия с точки зрения обеспечения основных требований по информационной безопасности (ИБ). В соответствие с ценностью объектов защиты (ОЗ) определены доли участия функциональности комплексов уровня ПТР в общей структуре всех подсистем КСЗИ и в разрезе каждой подсистемы в частности. На основании полученных результатов построены соответствующие диаграммы и таблицы, служащие наглядным инструментом при проведении группировки по востребованности компонент в структуре уровня ПТР КСЗИ и выявления узких мест в ИБ предприятия.

Ключевые слова: информационная безопасность, оценка эффективности, программно-технические решения, группировка по востребованности, функциональность подсистемы, ценность объекта защиты.

P.N. Nasedkin [1]

[1] *Irkutsk State University of Railway Transport, Irkutsk, Russian Federation*

ANALYSIS OF THE DEMAND FOR COMPONENTS OF THE LEVEL OF SOFTWARE AND HARDWARE SOLUTIONS OF THE ENTERPRISE IN TERMS OF PROVIDING BASIC REQUIREMENTS FOR INFORMATION SECURITY

Abstract. In this paper, based on the results of the assessment of the objects of protection of the IT infrastructure of the enterprise in the context of information properties (confidentiality, integrity and availability), the analysis of the demand for components of the level of software and hardware solutions (SHS) of a comprehensive information protection system (CIPS) of the enterprise in terms of the basic requirements for information security (IS). In accordance with the value of the objects of protection (OP) the shares of participation of functionality of complexes of SHS level in the overall structure of all subsystems of CIPS and in the context of each subsystem in particular were determined. Based on the results obtained, the relevant charts and tables were built, which serve as a visual tool for grouping the demand for the components in the structure of CIPS SHS level and identifying bottlenecks in the IS of the enterprise.

Keywords: information security, performance evaluation, software and hardware solutions, grouping by demand, subsystem functionality, value of the object of protection.

Введение. Для достижения целей в области опережающего развития государства в военно-политическом и экономическом направлении, а также обеспечения сохранности и защиты своих информационных активов используются достижения фундаментальной и прикладной науки с привлечением к их реализации высокотехнологичных отраслей (оборонно-промышленный комплексы; атомно-промышленный и атомно-энергетический комплекс; химическая промышленность и др.) [1].

Произошедший за последнее десятилетие стремительный рост как в развитии телекоммуникационных технологий, так и в количестве вредоносных атак на критические информационные инфраструктуры (КИИ) предприятий независимо от формы собственности и их размера требует от руководства данных предприятий своевременного оперативного принятия решений. Основой для этого могут служить количественные оценки состояния уровня программно-технических решений (ПТР) комплексной системы защиты информации (КСЗИ) на примере предприятия ТЭК, рассмотренного в работах [2,3]. Также, должны учитываться в оценке деятельности по обеспечению ИБ и результативности системы менеджмента инфор-

мационной безопасности (СМИБ) ГОСТ Р ИСО/МЭК 27004-2021 [4] с учётом применения ГОСТ Р ИСО/МЭК 27005-2010 [5] в разрезе осуществления менеджмента риска ИБ.

В настоящее время в основе системы обеспечения ИБ (СОИБ) любого предприятия, относящегося к категории предприятий КИИ, как правило можно выделить уровень ПТР в основе которого содержится состав компонент (подсистемы, комплексы и функции, выполняемые ими) этого уровня. Функциональное назначение уровня ПТР КСЗИ состоит в том, чтобы обеспечить ИБ информационных активов предприятия КИИ и конечных точек пользователей, в том числе расположенных вне периметра сети, путём нейтрализации развития сценариев атак [6-9]. Уровень ПТР в структуре КСЗИ образуют основной программно-аппаратный щит противодействия компьютерным атакам. Компоненты уровня ПТР вносят значимый вклад в общий состав структуры КСЗИ предприятия и обеспечивают защиту объектов информатизации различной степени критичности и их значимости (ценности). В связи с чем, возникает задача оценки эффективности функционирования уровня ПТР КСЗИ предприятия [2]. Однако, для получения указанной оценки потребуется обладать информацией о значимости (ценности) компонент, составляющих данный уровень ПТР. С этой целью необходимо провести анализ востребованности компонент в порядке их значимости (ценности) с точки зрения обеспечения требования по ИБ.

В рамках данной работы с учетом объектов защиты (ОЗ) КИИ предприятия и их ценности определим востребованность применяемых компонент уровня ПТР по степени их вклада в функционирование уровня ПТР КСЗИ[2,3], а для этого выполним следующие шаги:

1. Определим ценность ОЗ КИИ предприятия с учетом обеспечения защиты в разрезе свойств информации – конфиденциальность, целостность и доступность;

2. Проведем группировку подсистем уровня ПТР КСЗИ с учетом ценности ОЗ и частоты используемой функциональности комплексов в разрезе подсистем;

3. Определим долю участия функциональности компонент уровня ПТР в общей структуре всех подсистем КСЗИ и в разрезе каждой подсистемы в частности.

Объекты защиты КИИ предприятия и доля участия компонент в функционировании уровня ПТР КСЗИ.

Информационные активы КИИ предприятия в условиях экономической конкуренции и возможных вредоносных воздействий как от внутренней среды, так и внешней требуют от руководства предприятия постоянного внимания к вопросу оценки рисков его информационных активов (ИА) и эффективности используемых механизмов защиты информации. Главные вопросы в области обеспечения защиты ИА предприятия, которые необходимо решать в повседневной деятельности предприятия звучат так: что защищать? от кого защищать? как (каким образом) защищать? Ответ на первый и третий вопрос должен содержать в себе этап по реализации мероприятий по выявлению в структуре предприятия объектов защиты (ОЗ), определения их ценностей и выбора мер программно-технической защиты с учётом обеспечения требований по ИБ. С этой целью в рамках данной статьи был рассмотрен типовой набор объектов защиты в разрезе компонент ПТР КСЗИ, а также определены их ценности информация по которым представлена в таблице 1. Необходимо отметить, что в перечень оцениваемых ОЗ входят и конечные точки автоматизированных рабочих мест (АРМ) пользователей, в том числе и имеющих удалённый доступ к ИА предприятия. Необходимо отметить, что в рамках данной статьи не будут рассматриваться вопросы оценки и эффективности компонент КИИ предприятия в привязке к предоставляемым со стороны провайдеров интернет-сервисов (услуг), а именно: программного обеспечение как услуги (SaaS), инфраструктуры как услуги (IaaS) и платформы как услуги (PaaS).

Принимая во внимание [10], для определения ценности ОЗ введем систему оценки ценностей по шкале от 1 до 4:

1 – реализация риска, воздействующего на свойства информации (конфиденциальность, целостность, доступность) в разрезе ОЗ не несёт последствий для предприятия и его бизнес-процессов;

2 – реализация риска, воздействующего на свойства информации (конфиденциальность, целостность, доступность) в разрезе ОЗ приведет к незначительным потерям для предприятия. Восстановление системы в прежнее работоспособное и исправное состояние возможно без остановки бизнес-процессов;

3 – реализация риска, воздействующего на свойства информации (конфиденциальность, целостность, доступность) в разрезе ОЗ приведет к существенным финансовым потерям и/или окажет значительное негативное влияние на репутацию (имидж) предприятия. Восстановление системы в прежнее работоспособное и исправное состояние возможно, но при условии увеличении временных затрат и/или финансовых ресурсов;

4 – реализация риска, воздействующего на свойства информации (конфиденциальность, целостность, доступность) в разрезе объектов защиты может привести к полной остановке бизнес-процессов, а также к значительным финансовым потерям и/или негативным влияниям на репутацию предприятия.

На основании изложенного, шкала ценности ОЗ предприятия примет вид, который приведен таблице 1.

Таблица 1

Объекты защиты КСЗИ и их ценности

Условное обозначение ОЗ	**Объекты защиты (ОЗ)**		**Конфиденциальность**	**Целостность**	**Доступ ступность**	**Интегральная ценность ОЗ**
	Наименование ОЗ	**Детализация ОЗ**				
1У.	Серверы информационных систем (Серверы ИС)	ИС, обрабатывающие конфиденциальную информацию не содержащую персональные данные (ПДн), а также ИС сторонних организаций, обработка и передача конфиденциальной информации в которых осуществляется в периметре предприятия. Примеры: ИС «Файловый ресурс»; ИС «Автоматизированная система оперативного управления производством, автоматизированная система технологического мониторинга и т.п.	3	4	4	4
2У.		ИС, обрабатывающих персональные данные (ПДн). Примеры: ИС «Адресная книга»; босс-кадровик; ИС «Галактика»; ИС «Служба каталогов Microsoft Active Directory; ИС «Сайт почтовой системы и службы каталога Active Directory». ИС сторонних организаций, обработка и передача ПДн в которых осуществляется в периметре предприятия (клиентское рабочее место. Банк-клиент и др.).	4	4	4	4
3У.	Серверы информационных систем (Серверы ИС)	Информационные системы, обрабатывающие публичную информацию. Примеры:Информационная система «Web-ресурс».	1	2	2	2
4У.		ИС, обрабатывающие открытую информацию. Примеры:ИС «Защита интернет и почтового трафика»; ИС «Сайт почтовой системы и службы каталога Active Directory»» и т.п.	3	3	2	3

Условное обозначение ОЗ	Объекты защиты (ОЗ)		Конфиденциальность	Целостность	Доступ ступность	Интегральная ценность ОЗ
	Наименование ОЗ	Детализация ОЗ				
5У.	АРМ ПТБ (автоматизированное рабочее место с повышенными требованиями к безопасности)	АРМ ИС, обрабатывающие конфиденциальную информацию с повышенными требованиями к безопасности (далее – АРМ ПТБ). Примеры: АРМ ИС как в периметре предприятия, так и выполняющих функции удалённо вне периметра	3	2	2	3
6У.	Автоматизированное рабочее место информационных систем (АРМ ИС)	Автоматизированные рабочие места пользователей информационных систем. Примеры: АРМ ИС пользователя как в периметре предприятия, так и выполняющего функции удалённо вне пери-	2	1	1	2
7У.	Серверы автоматизированных систем управления технологический процессом (Серверы АСУ ТП)	Системы управления производственными объектами с подключением к локальной вычислительной сети (далее –	3	4	4	4
8У.		Системы управления производственными объектами без подключения к ЛВС.	3	4	3	4
9У.	Система хранения данных (СХД)		4	4	4	4
10У.	Активное сетевое оборудование (АСО)		1	3	4	4
11У.	Серверы средств защиты информации (Серверы СрЗИ)		1	3	3	3
12У	АРМ АСУ ТП		3	4	4	4

Ценности ОЗ определяются по каждой позиции ОЗ, как наибольшая оценка, выставляемая экспертным путём с учетом рассмотрения последствий от возможной реализации риска, воздействующего на свойства информации (конфиденциальность, целостность, доступность). С учетом полученных оценок в разрезе ценности ОЗ КИИ предприятия (табл. 1) и принимая во внимание результаты работ [2,3], построим гистограмму (рис. 1), которая показывает какое количество ОЗ КИИ предприятия с учетом их ценности охватывается в разрезе каждой подсистемы уровня ПТР КСЗИ.

Рис. 1. Объекты защиты КИИ предприятия в разрезе подсистем уровня ПТР КСЗИ

Анализ частоты всех задействованных на уровне ОЗ функциональностей подсистем (табл. 2) позволяет сделать вывод о доли их участия (рис. 2), которую можно рассчитать по формуле:

$$K_i = \frac{1}{m} \sum_{j=1}^{m} \Phi_{\Pi}(i, j) * 100\%, \quad (1)$$

где i – определяемый объект защиты; $j = \overline{1,m}$ – порядковый номер функциональности подсистемы; K_i - доля используемых функций по подсистемам для ОЗ, %; m - количество функций подсистем по уровню объекта защиты;

$$\Phi_{\Pi}(i, j) = \begin{cases} 1, \text{если функциональность задействована} \\ 0, \text{ в противном случае} \end{cases};$$

– задействованная функциональность подсистемы в разрезе объекта защиты.

Значения функции $\Phi_{\Pi}(i,j)$ представлены в таблице 2, отражающей связи между ОЗ, защищающими их подсистемами, реализованными в рамках каждой подсистемы функциями и программно-техническими комплексами, обеспечивающими эти функции.

Таблица 2

Матрица инциденций для графа, отражающего связи между ОЗ и защитными подсистемами, – функция $\Phi_{\Pi}(i,j)$

Подсистемы / Объекты защиты	П1			П2		П3		П4		П5		П6		П7		П8			П9
	А1	А2	А3	Б1	Б2	В1	В2	Г1	Г2	Д1	Д2	Е1	Е2	Ж1	Ж2	З1	З2	З3	И
1У.	1	1	1	1	1	1	1	1	1	1	1	0	0	1	1	1	1	1	1
2У.	1	1	1	1	1	1	1	1	1	1	1	0	0	1	1	1	1	1	1
7У.	1	1	1	1	1	1	1	1	1	0	0	0	0	1	1	1	1	1	1
8У.	1	1	1	1	1	1	1	1	1	0	0	0	0	1	1	1	1	1	1
9У.	1	1	1	1	1	0	0	0	0	0	0	1	1	0	0	0	0	0	0
10У.	1	1	1	1	1	0	0	0	0	0	0	1	1	1	1	1	1	1	1
12У.	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	1	1	1	1
4У.	1	1	1	1	1	1	1	1	1	1	1	0	0	1	1	1	1	1	1
5У.	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	1	1	1	0
11У.	1	1	1	1	1	1	1	1	1	0	0	1	1	1	1	1	1	1	1
3У.	1	1	1	1	1	1	1	1	1	1	1	0	0	1	1	1	1	1	1
6У.	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	1	1	1	0

Условные обозначения ОЗ представлены в таблице 1, содержание подсистем на рисунке 1, функциональности подсистем:

- А1 контроль и управление доступом к защищаемым информационным ресурсам;
- А2 контроль и управление доступом к внешним носителям информации и периферийным устройствам;
- А3 контроль доступа к АСО;
- Б1 регистрация и учет действий пользователей и процессов;
- Б2 регистрация событий доступа к внешним устройствам и портам ввода-вывода;
- В1 контроль целостности исполняемых и конфигурационных файлов СрЗИ, компонентов ОС и прикладного ПО;
- В2 контроль неизменности параметров, встроенных СрЗИ и компонентов системного ПО;

- Г1 защита файловой системы от вирусов и вредоносных программ;
- Г2 потоковая защита межсетевого трафика от вирусов и вредоносных программ;
- Д1 контроль каналов утечек защищаемой информации;
- Д2 обнаружение несанкционированного хранения конфиденциальной информации;
- Е1 обеспечение возможности оперативного получения информации о состоянии защищенности;
- Е2 обеспечение автоматизации рутинных задач;
- Ж1 предоставление в виде отчетов информации об обнаруженных уязвимостях с рекомендациями по их устранению;
- Ж2 обеспечение инвентаризации узлов, выявление и идентификация уязвимостей;
- З1 межсетевое экранирование ЛВС;
- З2 обнаружение вторжений в ЛВС;
- З3 обеспечение безопасного функционирования сетевого оборудования;
- И резервное копирование конфигурационных файлов СрЗИ и восстановление данных из резервных копий в случаях сбоев.

Результаты расчетов по формуле (1) приведены на рисунке 2.

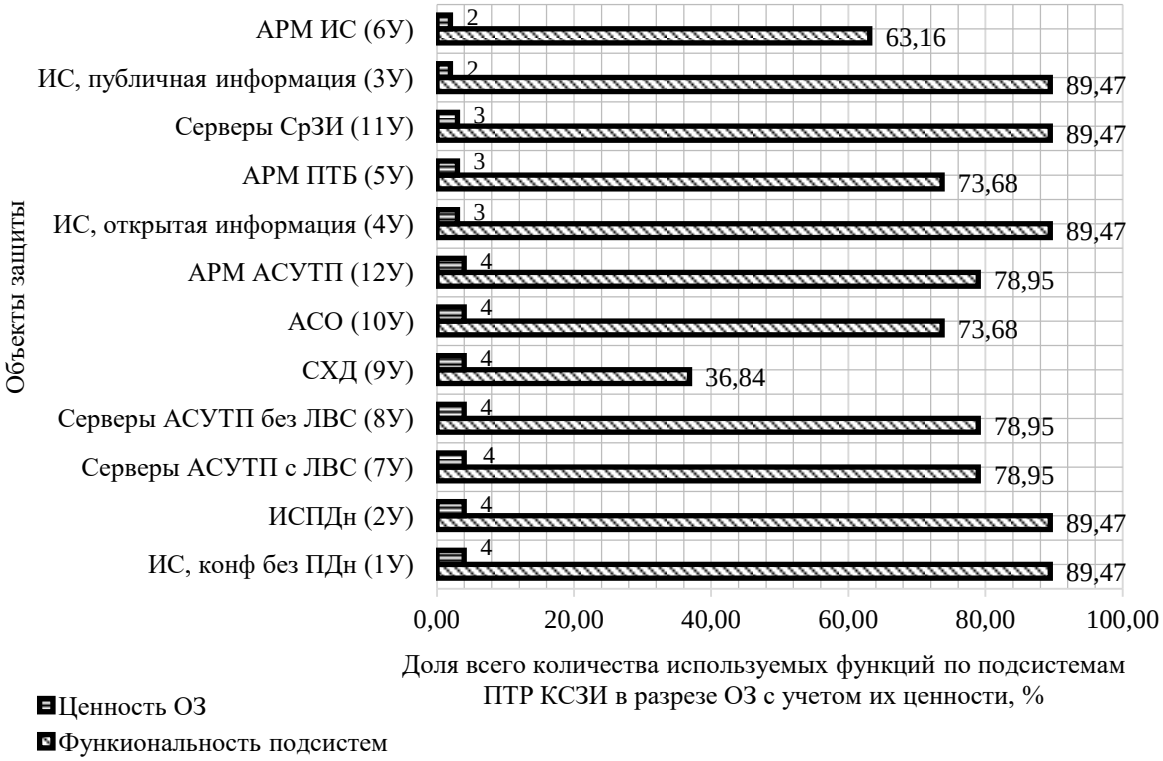

Рис. 2. Доли всего задействованных функций по подсистемам для ОЗ сгруппированных с учётом ценностей

Согласно [2,3] взаимосвязи компонент уровня ПТР КСЗИ для подсистем и функциональностей представлены в таблице 3.

Таблица 3

Взаимосвязи компонент уровня ПТР КСЗИ

П1			**П2**		**П3**		**П4**		**П5**		**П6**		**П7**		**П8**			**П9**
А1	**А2**	**А3**	**Б1**	**Б2**	**В1**	**В2**	**Г1**	**Г2**	**Д1**	**Д2**	**Е1**	**Е2**	**Ж1**	**Ж2**	**З1**	**З2**	**З3**	**И**
К1		К6	К1		К1		К2	К8	К1	–	К11		К12		К8	К9	К6; К7; К8;	К3; К7

П1			П2		П3		П4		П5		П6		П7		П8			П9
А1	А2	А3	Б1	Б2	В1	В2	Г1	Г2	Д1	Д2	Е1	Е2	Ж1	Ж2	З1	З2	З3	И
																	К9	
К4; К8; К10; К14; К15	К15	К8	К2; К4; К5; К6; К8; К9; К10; К12; К13; К14; К15	К15	К12; К13		–	–	К15		–	–	–	–	–	–	–	–

В рамках программно-технических решений для подсистем и функциональностей представленных в таблице 3 выделяются следующие компоненты уровня ПТР КСЗИ (комплексы):

– К1 Комплекс встроенных средств защиты серверов и автоматизированных рабочих машин (АРМ) под управлением операционных систем (ОС) семейства Windows;
– К2 Комплекс антивирусной защиты;
– К3 Комплекс резервного копирования;
– К4 Комплекс защиты среды виртуализации;
– К5 Комплекс сбора, анализа и корреляции событий ИБ;
– К6 Комплекс встроенных средств АСО;
– К7 Комплекс резервного копирования конфигурационных файлов АСО;
– К8 Комплекс межсетевого экранирования;
– К9 Комплекс обнаружения вторжений;
– К10 Комплекс встроенных средств защиты систем хранения данных;
– К11 Комплекс централизованного управления СрЗИ;
– К12 Комплекс анализа защищенности;
– К13 Комплекс контроля целостности;
– К14 Комплекс встроенных средств защиты прикладного программного обеспечения (ППО);
– К15 Комплекс контроля использования информационных ресурсов.

Как показал расчет, наибольшая востребованность в общей структуре всех подсистем КСЗИ без ранжирования их по ценности ОЗ наблюдается у комплексов К1, К8, К15, К12 (табл. 4).

Таблица 4

Группировка доли задействованной функциональности комплексов уровня ПТР КСЗИ в общей структуре всех подсистем КСЗИ без ранжирования их по ценности ОЗ

Условное обозначение комплекса	К1	К8	К15	К12	К13	К6	К9	К2	К4	К7	К10	К11	К14	К3	К5
Доля участия, %	14,9	12,8	12,8	10,6	6,4	6,4	6,4	4,3	4,3	4,26	4,26	4,26	4,3	2,13	2,1

Используя сведения из матрицы инциденций для графа, отражающего связи между ОЗ и защитными подсистемами (табл. 2) наглядно представим в таблице 5 востребованность подсистем по ОЗ с различной ценностью, где: «1» - подсистема востребована; «0» - подсистема не задействована.

Таблица 5

Востребованность подсистем для ОЗ с различной ценностью

Ценность ОЗ	**Объекты защиты (ОЗ)**	**Доля используемых функций по подсистемам для ОЗ, K_i %**	**П1**	**П2**	**П3**	**П4**	**П5**	**П6**	**П7**	**П8**	**П9**
4	ИС, обрабатывающие конфиденциальную информацию не содержащую персональные данные (ПДн), а также ИС сторонних организаций, обработка и передача конфиденциальной информации в которых осуществляется в периметре предприятия.	89,47	1	1	1	1	1	0	1	1	1
4	ИС, обрабатывающих персональные данные (ПДн).	89,47	1	1	1	1	1	0	1	1	1
4	Системы управления производственными объектами с подключением к локальной вычислительной сети (далее – ЛВС)	78,95	1	1	1	1	0	0	1	1	1
4	Системы управления производственными объектами без подключения к ЛВС.	78,95	1	1	1	1	0	0	1	1	1
4	Система хранения данных (СХД)	36,84	1	1	0	0	0	1	0	0	0
4	Активное сетевое оборудование (АСО)	73,68	1	1	0	0	0	1	1	1	1
4	АРМ АСУТП	78,95	1	1	1	1	0	0	0	1	1
3	ИС, обрабатывающие открытую информацию.	89,47	1	1	1	1	1	0	1	1	1
3	АРМ ИС, обрабатывающие конфиденциальную информацию с повышенными требованиями к безопасности (далее – АРМ ПТБ).	73,68	1	1	1	1	1	0	0	1	1
3	Серверы средств защиты информации (Серверы СрЗИ)	89,47	1	1	1	1	0	1	1	1	1
2	Информационные системы, обрабатывающие публичную информацию.	89,47	1	1	1	1	1	0	1	1	1
2	Автоматизированные рабочие места пользователей информацион-	63,16	1	1	1	1	0	0	0	1	0

Ценность ОЗ	**Объекты защиты (ОЗ)**	**Доля используемых функций по подсистемам для ОЗ, K_i %**	**П1**	**П2**	**П3**	**П4**	**П5**	**П6**	**П7**	**П8**	**П9**
	ных систем.										
Итого количество задействованных подсистем по ОЗ:			12	12	10	10	5	3	7	11	10
Частота используемых функциональностей комплексов:			10	14	6	2	3	2	2	6	2
Комплексы, функциональность которых задействована на уровне подсистем:			К1, К4, К6, К8, К10, К14, К15	К1, К2, К4, К5, К6, К8, К9, К10, К12, К13, К14, К15	К1, К12, К13	К2, К8	К1, К15	К11	К12	К6, К7, К8, К9	К3, К7

Из таблицы 5 следует востребованность подсистем для ОЗ с различной ценностью с учётом частоты используемой функциональности комплексов.

Алгоритм формирования перечня группируемых подсистем:

Шаг 1. Выбираем подсистемы, которые имеют наибольшее количество задействованных подсистем по ОЗ;

Шаг 2. В случае, если на шаге 1 выявлены подсистемы, которые имеют равное количество задействованных по ОЗ подсистем, то дальнейшую группировку данных подсистем осуществляем исходя из информации по частоте используемых функциональностей комплексов;

Шаг 3. В случае, если на шаге 2 установлено, что частота функциональности комплексов, используемых по ОЗ имеют равное количество, то дальнейшую группировку подсистем осуществляем исходя из информации о доли задействованной функциональности комплексов уровня ПТР КСЗИ в общей структуре всех подсистем КСЗИ без ранжирования их по ценности ОЗ (табл. 4);

Шаг 4. В случае, если на шаге 3 всё же наблюдается нечёткая граница для проведения дальнейших рассуждений в части группировки подсистем, то требуется руководствоваться экспертными оценками и/или статистическими данными в области обеспечения ИБ на предприятии.

В связи с чем, согласно таблицы 5 наиболее востребованные подсистемы из диапазона от 10 до 12 могут быть сгруппированы в следующем порядке: «П2», «П1», «П8», «П3» (Шаг 1; Шаг 2).

Продолжая анализ востребованности подсистем, мы видим, что «П4» и «П9» задействованы в защите одинакового количества ОЗ (10 объектов) и имеют одинаковую частоту используемых функциональностей комплексов - это 2. В связи с чем, применяем для анализа «Шаг 3» из выше приведённого алгоритма. Согласно информации, представленной в таблице 4 получаем, что:

– для подсистемы «П4» доля участия комплекса «К2» составляет 10,6%, а для «К8» – 12,8%;

– для подсистемы «П9» доля участия комплекса «К3» составляет –2,13%, а для «К7» – 4,26 %.

Для усиления аналитических рассуждений применим «Шаг 4» согласно которого примем к сведению тот факт, что осуществляемые подсистемой «П4» функции направлены на обеспечение антивирусной защиты с задействованием в том числе и доли функциональности комплекса межсетевого экранирования. Отметим, что основу обеспечения ИБ любого предприятии составляют межсетевые шлюзы безопасности (межсетевые экраны – МЭ) реализованные в виде программно-аппаратных комплексов. С помощью МЭ согласно установленных политик ИБ в пределах ИТ –инфраструктуры предприятия обеспечиваются: сегментация вычислительной сети; контроль и управление трафиком, а также потоковая антивирусная защита. В результате изложенного, можно добавить в перечень «П2», «П1», «П8», «П3» (Шаг 1; Шаг 2) по очерёдности следования следующие подсистемы: «П4», «П9».

Иными словами, нами получен базовый перечень подсистем, который необходим для обеспечения основных требований по ИБ на любом предприятии в порядке их востребованности на уровне ПТР КСЗИ: «П2», «П1», «П8», «П3», «П4», «П9».

Далее, для формирования полноценной КСЗИ на уровне ПТР в качестве расширения функциональности по обеспечению ИБ могут быть предложены в дополнение к базовому перечню следующие подсистемы: «П5» (Подсистема контроля использования информационных ресурсов), которая необходима для отслеживания информационных потоков и реагирования на утечки защищаемой информации; «П7» (Подсистема анализа защищённости), которую можно применять для выявления сетевых и программных уязвимостей; «П6» (Подсистема централизованного управления СрЗИ). Данные подсистемы согласно таблицы 5 лежат в диапазоне востребованности от 5 до 7. Применяя алгоритм по определению востребованности подсистем по ОЗ получаем следующий порядок: «П7», «П5», «П6».

Итоговый перечень востребованности подсистем который необходим для обеспечения основных требований по ИБ на предприятии: базовый перечень подсистем в порядке их востребованности – «П2», «П1», «П8», «П3», «П4», «П9»; расширенный перечень подсистем в порядке их востребованности – «П7», «П5», «П6».

Анализ, касающийся доли задействованных функциональностей комплексов по каждой подсистеме уровня ПТР КСЗИ согласно таблицы 3 представлен в таблице 6.

Таблица 6

Доля задействованных функциональностей комплексов в разрезе подсистем уровня ПТР КСЗИ

	П1	**П2**	**П3**	**П4**	**П5**	**П6**	**П7**	**П8**	**П9**
К1	20,00	14,29	33,33	0,00	33,33	0	0	0	0
К2	0	7,14	0	50,00	0	0	0	0	0
К3	0	0	0	0	0	0	0	0	50,00
К4	10,00	7,14	0	0	0	0	0	0	0
К5	0	7,14	0	0	0	0	0	0	0
К6	10,00	7,14	0	0	0	0	0	16,67	0
К7	0	0	0	0	0	0	0	16,67	50,00
К8	20,00	7,14	0	50,00	0	0	0	33,33	0
К9	0	7,14	0	0	0	0	0	33,33	0
К10	10,00	7,14	0	0	0	0	0	0	0
К11	0	0	0	0	0	100,00	0	0	0
К12	0	7,14	16,67	0	0	0	100,00	0	0
К13	0	7,14	16,67	0	0	0	0	0	0
К14	10,00	7,14	0	0	0	0	0	0	0
К15	20,00	14,29	0	0	66,67	0	0	0	0

В соответствие с полученным перечнем (базовый и дополнительный) подсистем по их востребованности на уровне ПТР предприятия представлена полная группировка компонент уровня ПТР КСЗИ с учетом ценности ОЗ с поправкой на долю востребованности задействованных по функциональности комплексов в разрезе подсистем КСЗИ. Результаты группировки компонент по востребованности компонент в структуре уровня ПТР КСЗИ представлены в таблице 7.

Таблица 7

Группировка по востребованности компонент в структуре уровня ПТР КСЗИ

Подсистемы / **Доля функциональности комплексов, %**	**П2**	**П1**	**П8**	**П3**	**П4**	**П9**	**П7**	**П5**	**П6**
7,14	К2, К4, К5, К6, К8, К9, К10, К12, К13, К14								
10		К4, К6, К10, К14							
14,29	К1, К15								
16,67			К6, К7	К12, К13					
20		К1, К8, К15							
25									
33,33			К8, К9	К1				К1	
50					К2, К8	К3, К6			
66,67								К15	
100							К12		К11

Заключение. В работе выполнен анализ востребованности программно-технических компонентов КСЗИ предприятия с позиции ценности объектов защиты и обеспечения основных требований регламентирующих документов ИБ.

В ходе проведённого исследования были построены соответствующие диаграммы и таблицы, отражающие востребованность соответствующих компонентов. Был получен следующий перечень подсистем по востребованности для ОЗ с различной ценностью с учётом частоты используемой функциональности комплексов: базовый перечень подсистем – «П2», «П1», «П8», «П3», «П4», «П9»; дополнительный перечень – «П7», «П5», «П6».

Базовый перечень подсистем содержит в порядке их востребованности на уровне ПТР КСЗИ такие подсистемы, как:

1. П2 (Подсистема регистрации и учета);
2. П1 (Подсистема контроля и управления доступом);
3. П8 (Подсистема обеспечения сетевой безопасности);
4. П3 (Подсистема обеспечения целостности);
5. П4 (Подсистема антивирусной защиты);
6. П9 (Подсистема обеспечения непрерывности функционирования).

Дополнительный перечень подсистем содержит в порядке их востребованности на уровне ПТР КСЗИ следующие подсистемы:

1. П7 (Подсистема анализа защищенности);
2. П5 (Подсистема контроля использования информационных ресурсов);
3. П6 (Подсистема централизованного управления СрЗИ).

Полученный состав по востребованности подсистем, задействованных в их работе комплексов хорошо коррелирует с перечнем подсистем, который используется в нормативном документе Гостехкомиссии России для проведения классификации средств защиты информации от НСД [11].

Как следует из результатов исследования, наибольшую долю задействованной функциональности комплексов уровня ПТР КСЗИ в общей структуре всех подсистем КСЗИ без ранжирования их по ценности ОЗ составляет следующая функциональность:

1. «К1» (Комплекс встроенных средств защиты серверов и автоматизированных рабочих машин (АРМ) под управлением операционных систем (ОС) семейства Windows) – 14,89 % участия;
2. «К8» (Комплекс межсетевого экранирования) – 12,77 % участия;
3. «К15» (Комплекс контроля использования информационных ресурсов) – 12,77 % участия;
4. «К12» (Комплекс анализа защищенности) – 10,64 % участия.

Необходимо отметить, что каждая используемая на уровне ПТР КСЗИ реализация функциональности комплексов в свою очередь может иметь сложную многокомпонентную архитектуру.

Также хотелось бы отметить, что представленная в настоящей работе группировка по востребованности компонент не является окончательной. Возможно в дальнейшем потребуется более глубокая декомпозиция, результаты которой могут быть положены в основу методики оценки информационной безопасности предприятия уровня ПТР КСЗИ и получения агрегированных оценок эффективности защиты информации на предприятии, как это предлагается в работах [12-14].

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Основные направления деятельности Правительства Российской Федерации на период до 2024 года [Электронный ресурс]. – URL: https://docs.cntd.ru/document/554168464 (дата обращения: 01.05.2022).

2. Наседкин, П. Н. Применение нечёткого присоединённого логического вывода в оценке эффективности функционирования комплексной системы защиты информации предприятий / П. Н. Наседкин, Л. В. Аршинский, Н. И. Глухов. — Текст: непосредственный // Теоретические и прикладные вопросы реализации проектов в области информационной безопасности. Материалы межвузовской научно-теоретической конференции (в рамках Сибирского форума «Информационная безопасность – 2021»), 29 ноября – 3 декабря 2021 г.— Новосибирск: Сибирский государственный университет телекоммуникаций и информатики, 2021. — С. 42-52.

3. Глухов, Н. И. Разработка элементов комплексной системы защиты информации предприятия / Н. И. Глухов, П. Н. Наседкин. — Текст : непосредственный // Информационные технологии и математическое моделирование в управлении сложными системами. — 2021. — № 1(9). — С. 35-42.

4. ГОСТ Р ИСО/МЭК 27004-2021. Информационные технологии (ИТ). Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Мониторинг, оценка защищенности, анализ и оценивание [Электронный ресурс]. – URL: https://docs.cntd.ru/document/1200179613/titles (дата обращения: 01.05.2022).

5. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. [Электронный ресурс]. – URL: https://docs.cntd.ru/document/1200084141 (дата обращения: 01.05.2022).

6. Pols, Paul The Unified Kill Chain. Cyber Security Academy [Электронный ресурс]. – URL: https://www.unifiedkillchain.com/assets/The-Unified-Kill-Chain-Thesis.pdf (дата обращения: 18.04.2022).

7. ATT&CK Matrix for Enterprise [Электронный ресурс]. – URL: https://attack.mitre.org/ (дата обращения: 18.04.2022).

8. Какие техники MITRE ATT&CK выявляет PT NAD [Электронный ресурс].–URL: https://mitre.ptsecurity.com/ru-RU/techniques (дата обращения: 18.04.2022).

9. Банк данных угроз безопасности информации ФСТЭК России [Электронный ресурс]. – URL: https://bdu.fstec.ru/threat (дата обращения: 18.04.2022).

10. Ильченко Л.М., Брагина Е.К., Егоров И.Э., Зайцев С.И. Расчет рисков информационной безопасности телекоммуникационного предприятия. Открытое образование. 2018; 22(2):61-70.

11. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования к защите информации // Сборник руководящих документов по защите информации от несанкционированного доступа. – М. : ГТК РФ, 1998. – С. 17–44.

12. Аршинский Л.В. Логико-аксиологический подход к оценке состояния систем // Современные технологии. Системный анализ. Моделирование. Иркутск: ИрГУПС. 2013. №3(39). С. 140-146.

13. Аршинский Л.В. Методика агрегированного оценивания систем с поддержкой ключевых компонентов // Онтология проектирования. 2015. Т. 5. № 2 (16). С. 223-232.

14. Аршинский В.Л., Аршинский Л.В., Доржсурэн Х. Оценка качества функционирования станции Улан-Баторской железной дороги на основе онтологического и продукционного моделирования // Современные наукоемкие технологии, 2018, № 5. С. 16-20.

REFERENCES

1. Key areas of activity of the Government of the Russian Federation for the period up to 2024 [Electronic resource]. - URL: https://docs.cntd.ru/document/554168464 (Accessed: May 01, 2022) (in Russ.).

2. P. N. Nasedkin, L. V. Arshinsky, and N. I. Glukhov. *Primenenie nechyotkogo prisoedinyonnogo logicheskogo vyvoda v ocenke effektivnosti funkcionirovaniya kompleksnoj sistemy zashchity informacii predpriyatij* [Application Of Fuzzy Connected Logical Inference In Assessing The Effectiveness Of Functioning Of Complex Information Security System Of Enterprises]. Teoreticheskie i prikladnye voprosy realizacii proektov v oblasti informacionnoj bezopasnosti. Materialy mezhvuzovskoj nauchno-teoreticheskoj konferencii (v ramkah Si-birskogo foruma «Informacionnaya bezopasnost' – 2021»), 29 noyabrya – 3 dekabrya 2021. — Novosibirsk : Sibirskij gosudarstvennyj universitet telekommunikacij i informatiki [Theoretical and applied issues of information security projects implementation. Proceedings of the Interuniversity Scientific and Theoretical Conference (within the Siberian Forum "Information Security - 2021"), November 29 - December 3, 2021. - Novosibirsk : Siberian State University of Telecommunications and Informatics], 2021. — pp. 42-52.

3. Glukhov N. I., Nasedkin P.N. Razrabotka elementov kompleksnoj sistemy zashchity informacii predpriyatiya [Development of elements of an integrated information protection system of the enterprise] Informacionnye tekhnologii i problemy matematicheskogo modelirovaniya slozhnyh system [Information technologies and problems of mathematical modeling of complex systems]. Irkutsk, IrGUPS, 2011, no. 1(9), pp. 35-42.

4. GOST R ISO/EC 27004-2021. Information technologies (IT). Methods and means of ensuring security. Management of information security. Monitoring, security assessment, analysis and evaluation [Electronic resource]. - URL: https://docs.cntd.ru/document/1200179613/titles (Accessed: May 01, 2022) (in Russ.).

5. GOST R ISO/MECH 27005-2010. Information technology. Methods and means to ensure security. Risk management of information security. [Electronic resource]. - URL: https://docs.cntd.ru/document/1200084141 (Accessed: May 01, 2022) (in Russ.).

6. Pols, Paul The Unified Kill Chain. Cyber Security Academy [Electronic resource]. - URL: https://www.unifiedkillchain.com/assets/The-Unified-Kill-Chain-Thesis.pdf (accessed 18.04.2022).

7. ATT&CK Matrix for Enterprise [Electronic resource]. - URL: https://attack.mitre.org/ (Accessed: April 18, 2022) (in Russ.).

8. What MITRE techniques ATT&CK reveals PT NAD [Electronic resource]. - URL: https://mitre.ptsecurity.com/ru-RU/techniques (Accessed: April 18, 2022) (in Russ.).

9. Data bank of information security threats of FSTEC of Russia [Electronic resource]. - URL: https://bdu.fstec.ru/threat (Accessed: April 18, 2022) (in Russ.).

10. Il'chenko L. M., Bragina E. K., Egorov I. E., Zaitsev S. I. *Raschet riskov informatsionnoi bezopasnosti telekommunikatsionnogo predpriiatiia. Otkrytoe obrazovanie* [Calculation of information security risks of a telecommunications enterprise. Open Education], 2018, No. 2, pp. 61-70, DOI: 10.21686/1818-4243-2018-2-61-70.

11. Guidance document. Automated systems. Protection against unauthorized access to information. Classification of automated systems and requirements for information protection // Collection of guiding documents on information protection from unauthorized access. - Moscow: State Technical Committee of the Russian Federation, 1998. - pp. 17-44. (in Russ.).

12. Arshinskiy, L.V. Logiko-aksiologicheskiy podhod r otsenke sostoyania system [Logical-
axiological approach to the systems state estimation (in Russian)] // So-time technologies. System analysis. Modeling. Irkutsk: IrGUPS. 2013. № 3(39). pp. 140-146.

13. Arshinskiy, L.V. Metodika agregirovannogo otsenivania system s podderzhekoy klyuchevih komponentov [A technique of the aggregate estimation of the systems with the key components support] // Design ontology. 2015. T. 5. № 2 (16). pp. 223-232.

14. Arshinskiy V.L., Arshinskiy L.V., Dorzhsuren H. Otsenka kachestva fukzionirovanya stanzii Ulan-Batorskoy xhelexnoy dorogi na osnove ontologicheskogo I produktivnogo modelirovanya [Quality estimation of Ulan Bator railroad station functioning on the basis of ontological and production modeling]// Modern high technology, 2018, ¹ 5. pp. 16-20.

Информация об авторах

Наседкин Павел Николаевич - ассистент кафедры «Информационные системы и защита информации», Иркутский государственный университет путей сообщений, г. Иркутск, e-mail: nasedkin_pn@irgups.ru

Authors

Pavel Nikolaevich Nasedkin - Postgraduate student, Department of Information Systems, Irkutsk State University of Railways, Irkutsk, e-mail: nasedkin_pn@irgups.ru.

Для цитирования

Наседкин П.Н. Анализ востребованности компонентов уровня программно-технических решений КСЗИ предприятия с точки зрения обеспечения базовых требований по информационной безопасности // «Информационные технологии и математическое моделирование в управлении сложными системами»: электрон. науч. журн. – 2022. – №2(14). – С. 50-64 – DOI: 10.26731/2658-3704.2022.2(14).50-64 – Режим доступа: http://ismm-irgups.ru/toma/214-2022, свободный. – Загл. с экрана. – Яз. рус., англ. (дата обращения: 30.06.2022)

For citation

Nasedkin P.N. Analysis Of The Demand For Components Of The Level Of Software And Hardware Solutions Of The Enterprise In Terms Of Providing Basic Requirements For Information Security. //

Informacionnye tehnologii i matematicheskoe modelirovanie v upravlenii slozhnymi sistemami: ehlektronnyj nauchnyj zhurnal [Information technology and mathematical modeling in the management of complex systems: electronic scientific journal], 2022. No. 2(14). P. 50-64. – DOI: 10.26731/2658-3704.2022.2(14).50-64 [Accessed 30/06/22]