МЕТОДИКА ОЦЕНКИ ЭФФЕКТИВНОСТИ СИСТЕМ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ

Будников С.А.[1], Коваленко С.М.[2], Бочарова А.И.[3]

Цель работы: *разработка методики оценки эффективности создаваемых систем безопасности значимых объектов критической информационной инфраструктуры, позволяющей обосновывать рекомендации по применению организационных и технических мер обеспечения безопасности информации с учетом масштабов негативных последствий, значений эффективности различных мероприятий по обеспечению безопасности, а также эффективности контроля.*

Методы исследования: *для формализации параметров используются методы балльного оценивания, теория эффективности и принятия решений.*

Результат: *разработана методика оценки эффективности систем обеспечения безопасности автоматизированных систем управления технологическим процессом, позволяющая обосновывать рекомендации по применению мер защиты информации по четырем направлениям деятельности по обеспечению безопасности. Выработан порядок балльной оценки эффективности систем обеспечения безопасности автоматизированных систем по сформированному перечню параметров, проверяемых в ходе оценки эффективности систем обеспечения безопасности автоматизированных систем. Определена шкала соответствия уровням состояния безопасности автоматизированных систем управления технологическим процессом. Обоснован показатель эффективности системы безопасности автоматизированных систем управления технологическим процессом, который позволяет оценить выбранный состав мер защиты по организации и планированию, внедрению, контролю состояния, поддержке и совершенствованию системы безопасности и выработать рекомендации по применению мер защиты информации, предлагаемых в справочнике «Группы мер защиты информации» ФСТЭК России. Полученные в работе результаты могут быть использованы при разработке методических рекомендаций по обеспечению безопасности автоматизированных систем управления, являющихся значимыми объектами критической информационной инфраструктуры.*

Научная новизна состоит в том, что использовался обобщенный критерий оценки средневзвешенных отклонений от идеальной альтернативы для значений четырех частных критериев реализуемости мероприятий по организации и планированию, внедрению, контролю состояния, поддержке и совершенствованию системы обеспечения безопасности, позволяющий одновременно оценить эффективность четырех направлений обеспечения безопасности автоматизированных систем управления технологическим процессом.

Ключевые слова: *значимый объект, критическая информационная инфраструктура, меры защиты, система безопасности, теория эффективности.*

DOI:10.21681/2311-3456-2023-3-2-12

Введение

Обеспечение безопасности значимых объектов критической информационной инфраструктуры (далее – КИИ), в том числе являющихся автоматизированными системами управления технологическим процессом (далее – АСУ ТП), имеет важное значение для функционирования как производственного комплекса, так и для обеспечения безопасности страны в целом, поскольку нарушения безопасности таких

1 Будников Сергей Алексеевич, доктор технических наук, профессор, главный научный сотрудник управления ФАУ «ГНИИИ ПТЗИ ФСТЭК России», Москва, Россия. E mail: public.buser@bk.ru

2 Коваленко Сергей Михайлович, аспирант ФАУ «ГНИИИ ПТЗИ ФСТЭК России». Москва, Россия. E mail: skovalenko90@yandex.ru

3 Бочарова Анастасия Ивановна, младший научный сотрудник ФАУ «ГНИИИ ПТЗИ ФСТЭК России». Москва, Россия. E mail: ai.bocharova@yandex.ru

систем могут иметь в качестве исхода значительные негативные последствия для экономики и социальной сферы.

В современных условиях, вместе с развитием перспективных информационных технологий и их широким внедрением в АСУ ТП объектов КИИ, возрастает риск нарушения их функционирования из-за многочисленных компьютерных атак. Вынужденное применение при построении АСУ ТП иностранного оборудования и заимствованного программного обеспечения, имеющего ограниченные возможности по устранению уязвимостей, а также существенное увеличение доли территориально распределенных АСУ ТП является дополнительным фактором для появления новых угроз безопасности информации, обрабатываемой в этих системах.

Перечисленные факторы определяют актуальность совершенствования научно-технического и нормативно-методического обеспечения защиты АСУ ТП от актуальных угроз безопасности информации в новых условиях.

К настоящему времени уже опубликовано значительное количество работ учебного[4] и монографического характера[5] [1], направленных на развитие методического обеспечения по оценке эффективности систем обеспечения безопасности АСУ ТП значимых объектов (ЗО) КИИ. Известны работы теоретического характера, направленные на развитие методологии моделирования и оценки эффективности систем обеспечения безопасности [2-12; 16], также работа Н.М. Масловой[6] Моделированию процесса проведения компьютерной атаки, основанного на представлении атаки марковским случайным процессом с дискретными состояниями и непрерывным временем, посвящена работа [13]. Основные понятия кибербезопасности индустриальных систем, а также новый подход к защите цифровых систем на основе теории управления и функциональной устойчивости представлены в [14]. Кроме того, регулированию вопросов предупреждения и предотвращения реализации угроз безопасности информации в отношении в промышленных объектов и АСУ ТП, относящихся к объектам КИИ, после начала специальной военной операции в нашей стране уделяется повышенное внимание и в нормативно-правовом поле[7, 8].

Однако вопросам оценки эффективности широкого класса мер защиты информации, применяемых в АСУ ТП ЗО КИИ с учетом сложившейся ситуации и возможных негативных последствий до настоящего времени не уделялось должного внимания.

Известно, что для обеспечения устойчивого функционирования ЗО КИИ Российской Федерации при проведении в отношении них компьютерных атак субъектами КИИ создаются системы безопасности (СБ) ЗО КИИ[9]. В соответствии с Требованиями по обеспечению безопасности значимых объектов КИИ Российской Федерации[10] СБ включают в себя правовые, организационные, технические и иные меры, направленные на обеспечение информационной безопасности субъектов КИИ. Указанные группы мер защиты (МЗ) используются комплексно на всех объектах защиты КИИ. Их классификация, парируемые способы реализации угроз и защищаемые объекты и компоненты приведены в «Новом разделе Банка данных угроз безопасности информации»[11].

Состав мер обеспечения безопасности АСУ ТП должен определяться в зависимости от их эффективности, учитывать используемые технологии и структурно-функциональные характеристики АСУ ТП, а также особенности технологического процесса. Многообразие МЗ, разные значения эффективности их применения, неоднородность уровня их применения и реализации делают задачу оценки эффективности МЗ достаточно сложной.

В то же время высока потребность в простой методике, описывающей как соответствующие атрибу-

4 Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. Учеб, пособие для вузов. – М: Горячая линия-Телеком, 2004. – 280 с. ил.

5 Теоретические основы компьютерной безопасности / П.Н. Девянин [и др.]. Москва: Радио и связь, 2000. 192 с.

6 Маслова, Н.А. Методы оценки эффективности систем защиты информационных систем / Н.А. Маслова // «Штучний інтелект». – 2008. – № 4. – С. 253–264.

7 О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации: [указ Президента Российской Федерации от 30.03.2022 № 166]: офиц. текст // Собрание законодательства Российской Федерации / М-во юстиции Российской Федерации. – М. : 2022, № 14 , ст. 2242.

8 О дополнительных мерах по обеспечению информационной безопасности Российской Федерации: [указ Президента Российской Федерации от 01.05.2022 № 250]: офиц. текст // Собрание законодательства Российской Федерации / М-во юстиции Российской Федерации. – М. : 2022, № 18 , ст. 3058.

9 О безопасности критической информационной инфраструктуры Российской Федерации. Федеральный закон РФ от 26.07.2017 № 187 ФЗ // Собрание законодательства Российской Федерации от 31 июля 2017 г. № 31 ст. 4736.

10 Об утверждении Требований по обеспечению безопасности значимых объектов КИИ Российской Федерации. Приказ ФСТЭК России от 25 декабря 2017 г. № 239 [Электронный ресурс] // Электронный фонд правовых и нормативно-технических документов. 2021. – Режим доступа: https://docs.cntd.ru/document/542616931 (дата обращения: 20.02.2023).

11 БДУ – Раздел угроз безопасности информации. [Электронный ресурс]. – Режим доступа: https://bdu.fstec.ru/threat-section/ (дата обращения: 20.02.2023).

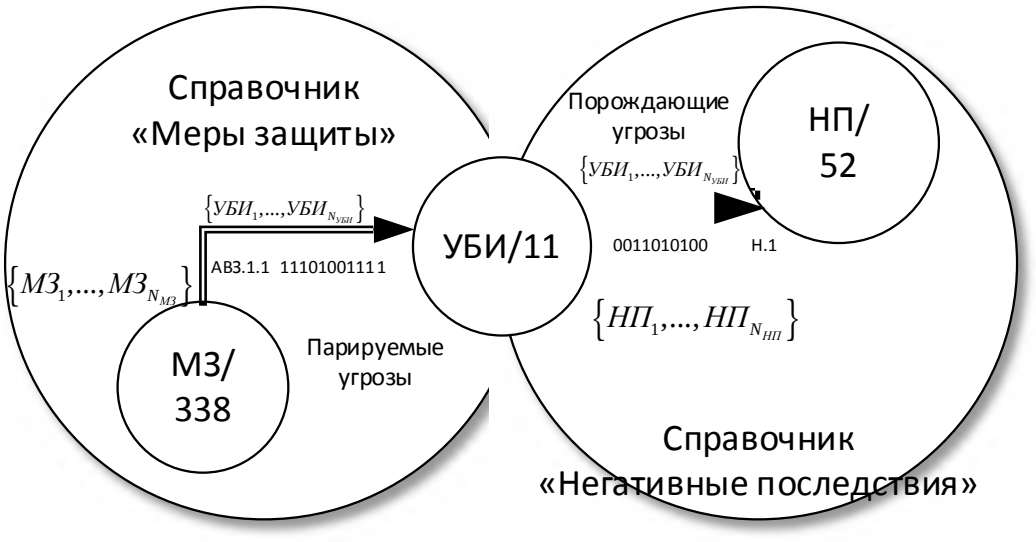

Рис. 1. Схема взаимосвязей данных из справочников «Нового раздела Банка данных угроз безопасности информации»

ты эффективности разнообразных МЗ количественно оцениваются и преобразуются в показатели, служащие основой для принятия решений по применению организационных и технических мер по обеспечению безопасности ЗО КИИ. Это определяет необходимость разработки методики оценивания эффективности СБ ЗО КИИ, позволяющей субъектам КИИ без применения сложных математических методов получать адекватные оценки эффективности СБ ЗО КИИ в целом с учетом их категории значимости (масштаба негативных последствий) и вырабатывать решения по применению совокупности организационных и технических мер.

Постановка задачи

Целью статьи является разработка методики оценки эффективности систем обеспечения безопасности АСУ ТП, позволяющей обосновывать рекомендации по применению мер защиты информации.

Анализ справочников «Нового раздела Банка данных угроз безопасности информации» показывает, что используя данные справочника «Группы мер защиты информации» (338 мер защиты), для уточненных данных можно связать применяемые меры защиты с парируемыми угрозами (УБИ), а используя данные справочника «Раздел угроз безопасности информации» (11 угроз), можно связать УБИ с порождаемыми негативными последствиями (НП) (52 негативных последствия). Схема взаимосвязей данных из этих справочников приведена на рис 1.

В этом случае в качестве показателя применимости $m-$ой МЗ для парирования $y-$ой УБИ можно использовать бинарную величину (индикатор), значение которой определяется из поля «Парируемые угрозы» файла-справочника «Меры защиты»:

$$h_{m,y}=\begin{cases}1, \text{ если поле «Парируемые угрозы»}\\ \text{содержит идентификатор УБИ;}\\ 0, \text{иначе,}\end{cases} \quad (1)$$

где $m=1,M$ – порядковый номер МЗ в справочнике «Меры защиты», $M=338$; $y=1,Y$ – порядковый номер УБИ в справочнике «Раздел угроз безопасности информации», $Y=11$.

Полученная для уточненных в Новом разделе БДУ данных матрица $\mathbf{H}$ размерностью 338x11 представляет собой бинарную матрицу индикаторов наличия взаимосвязи «Меры защиты – Угрозы безопасности информации».

В свою очередь, в качестве показателя «возможности возникновения n-ого негативного последствия при реализации (возникновении) y-ой УБИ» можно использовать бинарную величину, значение которой определяется на пересечении поля «Негативные последствия» и «Угрозы» файла-справочника «Негативные последствия» как:

$$g_{n,y}=\begin{cases}1, \text{ если поле «Негативные последствия»}\\ \text{содержит идентификатор УБИ;}\\ 0, \text{иначе.}\end{cases} \quad (2)$$

где $n=1,N$ – порядковый номер негативного последствия в справочнике «Негативные последствия», $N=52$; $y=1,Y$ – порядковый номер УБИ в справочнике «Раздел угроз безопасности информации», $Y=11$.

Полученная для уточненных в Новом разделе БДУ данных матрица $\mathbf{G}$ размерностью 52x11 представ-

ляет собой бинарную матрицу индикаторов наличия взаимосвязей «Угрозы безопасности информации – Негативные последствия».

Естественно считать[12], что каждая m-ая МЗ вносит в общую итоговую эффективность создаваемой СБ ЗО КИИ по предотвращению (предупреждению) n-го негативного последствия некоторый вклад $w_{m,n}$. Полученные с использованием (1) и (2) бинарные матрицы $\mathbf{H}$ и $\mathbf{G}$ для уточненных данных позволяют сформировать вектор значений степени влияния m-ой меры защиты на возможность предотвращения (предупреждения) возникновения n-го негативного последствия за счет парирования множества y-ых УБИ с использованием нормированного выражения:

$$w_m = \frac{1}{N}\sum_{n=1}^{N}\sum_{y=1}^{Y} h_{m,y}\, g_{n,y}\,. \qquad (3)$$

Несмотря на то, что в соответствии с Требованиями[13] обеспечение безопасности значимых объектов является составной частью работ по созданию, эксплуатации и вывода из эксплуатации значимых объектов, оценка эффективности СБ АСУ ТП независимо от этапа жизненного цикла должна включать оценку реализаций мероприятий по следующим направлениям:

- планирование и разработка мероприятий по обеспечению безопасности АСУ ТП (далее организация);
- реализация (внедрение) мероприятий по обеспечению безопасности АСУ ТП (далее внедрение);
- контроль состояния безопасности АСУ ТП (далее контроля);
- совершенствование безопасности значимых АСУ ТП (далее поддержки уровня).

Каждое из этих направлений является самостоятельной и многокомпонентной группой мероприятий [15], эффективность которой чаще всего оценивается качественно или с привлечением экспертных методов. В этом случае большое число состояний системы, связанных с применением МЗ, может быть разбито на небольшое число классов.

Это позволяет для обобщенной оценки эффективности использовать взвешенные оценки эффективности по 4 направлениям оценивания эффективности СБ АСУ ТП в виде функционала:

$$\mathcal{Э\Phi} = F(k_0 \mathcal{Э\Phi}_0^{ГР}, k_B \mathcal{Э\Phi}_B^{ГР}, k_K \mathcal{Э\Phi}_K^{ГР}, k_П \mathcal{Э\Phi}_П^{ГР}), \qquad (4)$$

где $\mathcal{Э\Phi}$ – обобщенный показатель эффективности СБ АСУ ТП; $\mathcal{Э\Phi}_0^{ГР}$ – групповой показатель эффективности организации безопасности АСУ ТП; $\mathcal{Э\Phi}_B^{ГР}$ – групповой показатель эффективности внедрения мер безопасности в АСУ ТП; $\mathcal{Э\Phi}_K^{ГР}$ – групповой показатель эффективности контроль безопасности в АСУ ТП; $\mathcal{Э\Phi}_П^{ГР}$ – групповой показатель эффективности поддержки уровня обеспечения безопасности в АСУ ТП; $k_O = 0.3$, $k_K = 0.2$, $k_B = 0.3$, $k_П = 0.2$ – весовые коэффициенты значимости направлений оценки эффективности СБ АСУ ТП, $k_0 + k_B + k_к + k_П = 1$.

Групповой показатель эффективности организации безопасности АСУ ТП $\mathcal{Э\Phi}_0^{ГР}$ отражает состояние СБ при решении следующих задач:

- планирование, организация и координация работ по обеспечению информационной безопасности и контроль за ее состоянием;
- выявление угроз безопасности информации и оценка негативных последствий (ущерба), наступление которых возможно в результате реализации угроз безопасности информации;
- обеспечение надежности и эффективности функционирования и безопасности информационных систем, производственных процессов и информационно-технологической инфраструктуры;
- анализ эффективности и контроль за состоянием защищенности АСУ ТП.

В справочнике «Меры защиты» такие меры представлены первыми позициями в группах мер, например: «Разработка правил и процедур (политик) антивирусной защиты». Из всего множества МЗ, приведенных в справочнике, выделяют 127 подгрупп организационных мер, например: АВЗ.0, АУД.0, АУД.6, АУД.7, АУД.8, АУД.10, АУД.11, ДНС.0, ДНС.1, ДНС.2, ДНС.3, ДНС.4, ДНС.5, ДНС.6, ЗИС.0, ЗИС.1, ИПО.3, ИПО.4, ОДТ.0, ОДТ.8, ОПО.0, ОПО.1, ОПО.2, ОПО.3, ОПО.4, ОПС.0, ОЦЛ.0, ПЛН.0, ПЛН.1, ПЛН.2, СОВ.0, УКФ.0, УКФ.1, УПД.0.

С учетом этого групповой показатель эффективности организации безопасности АСУ ТП $\mathcal{Э\Phi}_0^{ГР}$ может быть определен как:

$$\mathcal{Э\Phi}_0^{ГР} = \frac{z_k \cdot \mathcal{Э\Phi}^0}{|\mathbf{M}_O|}\sum_{m\in\mathbf{M}} w_m, \qquad (5)$$

где z_k – коэффициент масштаба возможных негативных последствий, определяемый исходя из категории значимости объекта КИИ ($z_1 = 0.6$ для объектов КИИ

12 Надежность технических систем: Справочник / Ю. К – Беляев, В.А. Богатырев, В.В. Болотин и др.; Под ред. И.А. Ушакова. – М.: Радио и связь, 1985. – 608 с, ил.

13 Об утверждении Требований по обеспечению безопасности значимых объектов КИИ Российской Федерации. Приказ ФСТЭК России от 25 декабря 2017 г. № 239 [Электронный ресурс] // Электронный фонд правовых и нормативно-технических документов. 2021. – Режим доступа: https://docs.cntd.ru/document/542616931 (дата обращения: 20.02.2023).

I категории, $z_2 = 0.8$ для объектов КИИ II категории и $z_3 = 1$ для объектов КИИ III категории); $\mathbf{M}$ – множество мер организации и управления СБ (в рассматриваемом случае $|\mathbf{M}_\text{О}|$=127); $Э\Phi^0$ – интегральное значение реализованности мер организации и управления СБ АСУ ТП, полученное после заполнения опросного листа; w_n – значение эффективности МЗ по парированию УБИ, вычисленное по выражению (3).

Интегральное значение реализованности мер организации и управления СБ АСУ ТП $Э\Phi^0$ определяется после заполнения опросного листа оценки реализованности мер защиты с определением степени реализованности меры защиты.

Эксперту предлагается оценить качество планирования и разработки мероприятий по обеспечению безопасности ЗО КИИ как степень реализованности подмножества реализованных мер защиты. После этого происходит отображение оценок степени реализованности m-ой меры защиты: «Полностью реализована», «Частично реализована», «В основном реализована» или «Полностью реализована» в количественную шкалу интервале $[0,1]$ по 4 уровням градации:

— «Полностью не реализовано» – r_m^O= 0.1;
— «Частично реализовано» – r_m^O= 0,3;
— «В основном реализовано» – r_m^O= 0,7;
— «Полностью реализовано» – r_m^O= 1.

Соответственно интегральная оценка реализованности по направлению планировании и разработки мероприятий по обеспечению безопасности ЗО КИИ определяется как среднее значение реализованности:

$$Э\Phi^O = \frac{1}{|\mathbf{M}_\text{О}|} \sum_{m \in \mathbf{M}} r_m^O, \qquad (6)$$

где $\mathbf{M}$ - множество мер организации и управления СБ; r_m^O - оценка степени реализованности m-ой меры защиты.

Групповой показатель эффективности внедрения мер безопасности в АСУ ТП $Э\Phi_B^{ГР}$ отражает степень реализованности 176 подгрупп из 17 групп организационных и технических мер по обеспечению безопасности, определенных Приказом № 239 ФСТЭК России[14].

Оценка эффективности внедрения мер безопасности в АСУ ТП $Э\Phi_B^{ГР}$ вычисляется по формуле:

$$Э\Phi_B^{ГР} = \frac{z_k \text{-} Э\Phi^B}{|\mathbf{M}_\text{О}|} \sum_{m \in \mathbf{M}} w_m, \qquad (7)$$

где z_k – коэффициент масштаба возможных негативных последствий, определяемый исходя из категории значимости объекта КИИ ($z_1 = 0.6$ для объектов КИИ I категории, $z_2 = 0.8$ для объектов КИИ II категории и $z_3 = 1$ для объектов КИИ III категории); $\mathbf{N}_\text{в}$ – множество внедренных групп организационных и технических мер по обеспечению безопасности $|\mathbf{N}_\text{в}| = 176$; $Э\Phi^B$ – интегральное значение реализованности значение реализованности внедренных организационных и технических мер по обеспечению безопасности АСУ ТП, w_n – значение эффективности МЗ по парированию УБИ, вычисленное по выражению (3).

Соответственно интегральная оценка реализованности по направлению внедрения МЗ определяется как среднее значение реализованности мер:

$$Э\Phi^B = \frac{1}{|\mathbf{M}_\text{в}|} \sum_{m \in \mathbf{M}_\text{в}} r_m^B, \qquad (8)$$

где $\mathbf{M}_\text{в}$ — множество внедренных групп организационных и технических мер по обеспечению безопасности; r_m^B — оценка степени реализованности m-ой меры защиты.

Оценка эффективности контроля уровня обеспечения безопасности в АСУ ТП $Э\Phi_П^{ГР}$ вычисляется по формуле:

$$Э\Phi_K^{ГР} = \frac{z_k \text{-} Э\Phi^K}{|\mathbf{M}_\text{К}|} \sum_{m \in \mathbf{M}} w_m, \qquad (9)$$

где z_k – коэффициент масштаба возможных негативных последствий, определяемый исходя из категории значимости объекта КИИ $z_1 = 0.6$ для объектов КИИ I категории, $z_2 = 0.8$ для объектов КИИ II категории и $z_3 = 1$ для объектов КИИ III категории); $\mathbf{N}_K$ – множество мер, направленных на контроль уровня (состояния) информационной безопасности ($|\mathbf{N}_K|$=4); $Э\Phi^K$ – интегральное значение реализованности МЗ, направленных на контроль уровня (состояния) информационной безопасности, полученное после заполнения опросного листа.

Интегральная оценка реализованности по направлению контроля $Э\Phi^K$ определяется как среднее значение реализованности мер контроля:

$$Э\Phi^K = \frac{1}{|\mathbf{M}_\text{К}|} \sum_{m \in \mathbf{M}_\text{К}} r_m^K, \qquad (10)$$

где $\mathbf{M}_\text{в}$ — множество внедренных групп организационных и технических мер по обеспечению безопасности; r_m^K — оценка степени реализованности m-ой меры защиты.

14 Об утверждении Требований по обеспечению безопасности значимых объектов КИИ Российской Федерации. Приказ ФСТЭК России от 25 декабря 2017 г. № 239 [Электронный ресурс] // Электронный фонд правовых и нормативно-технических документов. 2021. – Режим доступа: https://docs.cntd.ru/document/542616931 (дата обращения: 20.02.2023).

Групповой показатель эффективности поддержки уровня обеспечения безопасности в АСУ ТП $Э\Phi_{П}^{ГР}$ отражает степень реализации следующих мероприятий, направленных на поддержание и развитие уровня (состояния) информационной безопасности:

- управление уязвимостями и обновлениями безопасности программных и программно-аппаратных средств;
- мониторинг и реагирование на события информационной безопасности; в значимом объекте, связанных с обеспечением безопасности;
- восстановление функционирования информационной (автоматизированной) системы в случае возникновения нештатных ситуаций;
- обучение и повышение осведомленности в области информационной безопасности.

К МЗ, направленным на поддержание и развитие уровня (состояния) информационной безопасности, относятся следующие подгруппы мер, например: АВЗ.3 – контроль использования архивных, исполняемых и зашифрованных файлов; АВЗ.4 – обновление базы данных признаков вредоносных компьютерных программ (вирусов); АУД.9 – анализ действий отдельных пользователей; ИАФ.4 – управление средствами аутентификации; ИНЦ.2 – информирование о компьютерных инцидентах; ОДТ.3 – контроль безотказного функционирования средств и систем; ОЦЛ.4 – контроль данных, вводимых в информационную (автоматизированную) систему; СОВ.2 – обновление базы решающих правил; УКФ.2 – управление изменениями; УКФ.4 – контроль действий по внесению изменений; УПД.12 – управление атрибутами безопасности.

Оценка эффективности поддержки уровня обеспечения безопасности в АСУ ТП $Э\Phi_{П}^{ГР}$ вычисляется по формуле:

$$Э\Phi_{П}^{ГР} = \frac{z_k \cdot Э\Phi^{П}}{|\mathbf{M}_{\mathbf{П}}|} \sum_{m \in \mathbf{M}_{\mathbf{П}}} w_m, \qquad (11)$$

где $\mathbf{N}_{\mathbf{П}}$ – множество мер, направленных на поддержание и развитие уровня (состояния) информационной безопасности ($|\mathbf{N}_{\mathbf{П}}|$=29); $Э\Phi^{П}$ – интегральное значение реализованности МЗ, направленных на поддержание и развитие уровня (состояния) информационной, полученное после заполнения опросного листа.

Соответственно интегральная оценка реализованности по направлению планирования и разработки мероприятий по обеспечению безопасности ЗО КИИ определяется как среднее значение реализованности:

$$Э\Phi^{П} = \frac{1}{|\mathbf{M}_{\mathbf{П}}|} \sum_{m \in \mathbf{M}_{\mathbf{П}}} r_m^{П}, \qquad (12)$$

где $\mathbf{M}_{\mathbf{В}}$ - множество внедренных групп организационных и технических мер по обеспечению безопасности; $r_m^{П}$ - оценка степени реализованности m-ой меры защиты.

С использованием этих критериальных и численных значений реализованности МЗ определяются значения реализованности мер $Э\Phi_{О}^{ГР}$, $Э\Phi_{В}^{ГР}$, $Э\Phi_{К}^{ГР}$, $Э\Phi_{П}^{ГР}$ в выражениях (6) – (12).

Одним из требований к обобщенному показателю эффективности СБ является его наглядность. Будем считать, что все частные показатели эффективности СБ независимы, одной размерности и подлежат максимизации. Тогда несколько вариантов оценок эффективности СБ по четырем параметрам удобно и наглядно сравнивать в двумерном виде с использованием лепестковых диаграмм, в которых числа выражены длиной того или иного лепестка[15]. Примером таких оценок может быть представление Центром науки и международных отношений Белфера[16] индексов национальных киберпотенциалов (NCPI) в контексте восьми индикаторов в виде диаграмм[17].

С применением этого подхода обобщенную оценку эффективности СБ следует проводить, используя геометрическую интерпретацию площади фигуры, соответствующей полученным оценкам, на лепестковой диаграмме. Тогда степень соответствия создаваемой СБ удобно оценивать, используя отношения площадей лепестковых диаграмм рассматриваемой и идеальной альтернатив:

$$Э\Phi = \frac{S(Э\Phi_{О}^{ГР}, Э\Phi_{В}^{ГР}, Э\Phi_{К}^{ГР}, Э\Phi_{П}^{ГР})}{S^{И}(Э\Phi_{О}^{*}, Э\Phi_{В}^{*}, Э\Phi_{К}^{*}, Э\Phi_{П}^{*})}, \qquad (13)$$

где S – площадь лепестковой диаграммы эффективности рассматриваемой альтернативы; $S^{И}$ – площадь лепестковой диаграммы эффективности «идеальной» альтернативы, и чем ближе это отношение единичному значению, т.е. чем ближе качество создаваемой СБ к идеальной, полностью соответствующей требованиям по безопасности, тем она лучше.

В системе четырех координат значения эффективности МЗ могут быть представлены четырехугольником, как это показано на рис. 22. Известно, что площадь четырехугольника $Э\Phi_{О}^{*}, Э\Phi_{В}^{*}, Э\Phi_{К}^{*}, Э\Phi_{П}^{*}$

15 Как научиться мыслить образами, используя визуальные аналогии / Хабр [Электронный ресурс]. Режим доступа – https://habr.com/ru/post/345204/ свободный. Загл. с экрана. – Яз. рус.

16 Центр науки и международных отношений Роберта и Рене Белфер –исследовательский центр, расположенный в Школе государственного управления Джона Ф. Кеннеди в Гарвардском университете.

17 National Cyber Power Index 2022 | Belfer Center for Science and International Affairs [Электронный ресурс]. – Режим доступа: https://www.belfercenter.org/publication/national-cyber-power-index-2022.

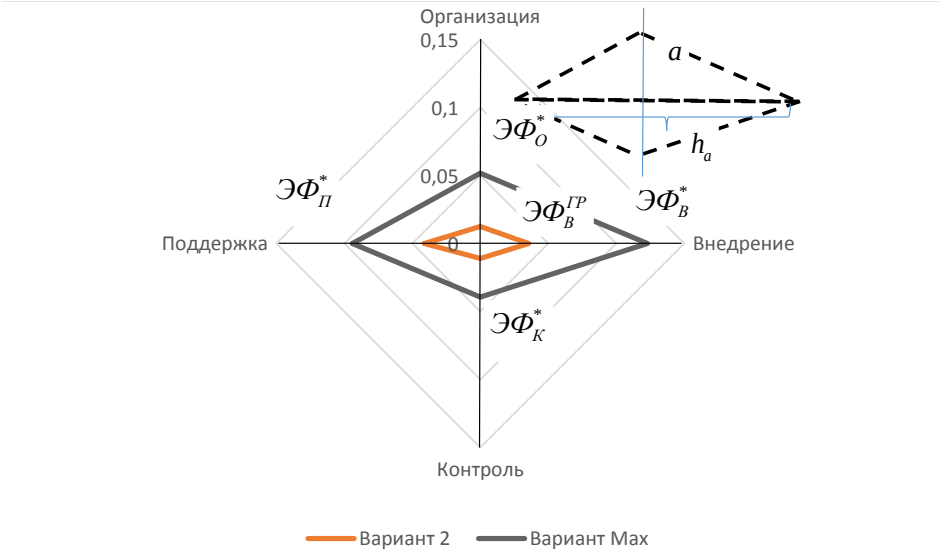

Рис. 2. Представление обобщенной эффективности МЗ по направлениям деятельности

можно записать как сумму площадей двух треугольников $ЭФ_П^*, ЭФ_О^*, ЭФ_В^*$ и $ЭФ_П^*, ЭФ_К^*, ЭФ_В^*$, (см. рис. 22) вида[18]

$$S_{тр} = \frac{1}{2} a h_0, \qquad (14)$$

где $S_{тр}$ – площадь треугольника;

a – длина стороны треугольника;

h_a – высота треугольника.

Тогда площадь четырехугольника $ЭФ_О^*, ЭФ_В^*, ЭФ_К^*, ЭФ_П^*$ с учетом весовых коэффициентов важности направлений обеспечения безопасности k_0, $k_В$, $k_К$ и $k_П$ можно записать как:

$$S = \frac{1}{2}(k_О ЭФ_О^{ГР} + k_К ЭФ_К^{ГР})(k_В ЭФ_В^{ГР} + k_П ЭФ_П^{ГР}). \qquad (15)$$

Обобщенный показатель эффективности текущего варианта СБ АСУ ТП в соответствии с (13) можно записать как отношение площадей четырехугольников для текущего варианта состава МЗ S и «идеального» состава МЗ $S^{И}$[19]

$$ЭФ = \frac{(k_О ЭФ_О^{ГР} + k_К ЭФ_К^{ГР})(k_В ЭФ_В^{ГР} + k_П ЭФ_П^{ГР})}{(k_О ЭФ_О^* + k_К ЭФ_К^*)(k_В ЭФ_В^* + k_П ЭФ_П^*)}, \qquad (16)$$

где $ЭФ_О^*, ЭФ_К^*, ЭФ_В^*, ЭФ_П^*$ – максимальные значения эффективности СБ АСУ ТП в целом при условии полной реализации всех МЗ, $r_m = 1, \forall m$.

Рекомендуется применять следующие категории безопасности (защищенности) АСУ ТП:

«Высокая» – не требуется вмешательств в функционирование системы обеспечения безопасности АСУ ТП;

«Средняя» – требуется внесение изменений в систему обеспечения безопасности АСУ ТП;

«Низкая» – требуется незамедлительное внесение изменений в систему обеспечения безопасности АСУ ТП.

С учетом этих градаций критерии степени безопасности (защищенности) АСУ ТП целесообразно определить, как приведено в табл. 1.

Пример результатов расчета для восьми вариантов состава организационных и технических МЗ в АСУ ТП и варианта с максимальной эффективностью $ЭФ_{max}$ приведен на рис. 3. При этом можно сделать вывод о среднем значении эффективности вариантов от 0.25 до 0.55, что по табл. 1 соответствует «Низким» и «Средним» значениям защищенности.

Сравнительный анализ полученных результатов на рис. 4 показывает, что наибольшим вкладом в обобщенную эффективность СБ АСУ ТП обладают МЗ направления «Внедрения мер безопасности в АСУ ТП», что подчеркивает важность этого процесса при создании СБ АСУ ТП.

В то же время мероприятия, направленные на организацию и контроль, имеют определенный потенциал для приближения к «идеальной» альтернативе.

Таким образом, общая последовательность действий по оценке эффективности систем обеспечения

18 Аленицын А.Г., Бутиков Е.И., Кондратьев А.С. Краткий физико-математический справочник. — Изд. 5-е, испр. — СПб.: «Петроглиф». 2005. — 544 с.: ил.

19 Петровский А.Б. Теория принятия решений: учебник для студ. высш. учеб, заведений / А.Б. Петровский. – М.: Издательский центр «Академия», 2009. – 400 с. – (Университетский учебник. Сер. Прикладная математика и информатика).

Таблица 1

Критерии степени безопасности (защищенности) АСУ ТП

Сравнительная степень защищенности АСУ ТП	Рекомендуемое решение по результатам оценки эффективности	Значение рассчитанной эффективности СБ $ЭФ$
«Низкая»	Требуется незамедлительное внесение изменений в систему обеспечения безопасности АСУ ТП	$0 \le ЭФ \le 0.3$
«Средняя»	Требуется внесение изменений в систему обеспечения безопасности АСУ ТП	$0.3 < ЭФ \le 0.8$
«Высокая»	Не требуется вмешательств в функционирование системы обеспечения безопасности АСУ ТП	$0.8 < ЭФ \le 1$

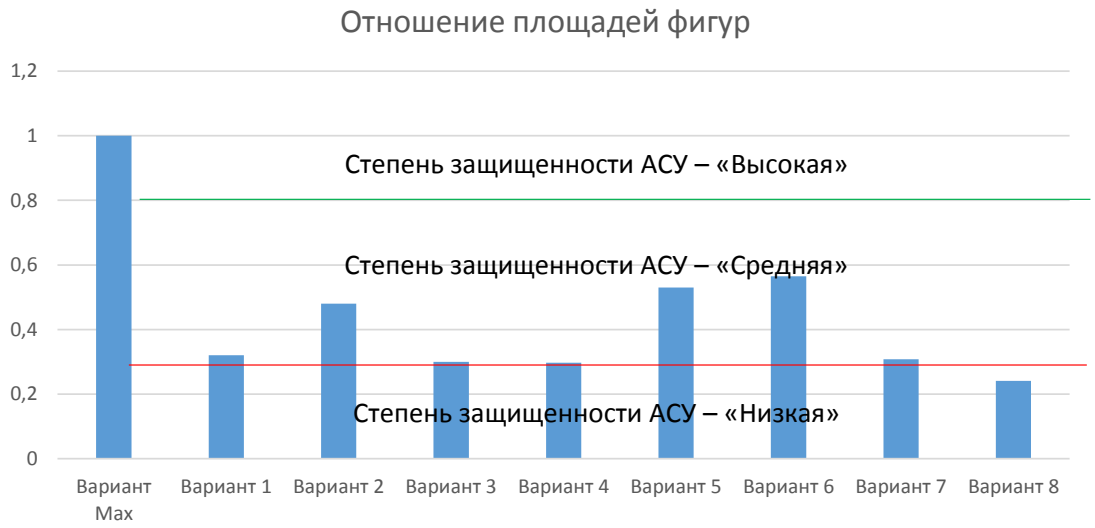

Рис. 3. Значение эффективности вариантов состава МЗ ЗО КИИ

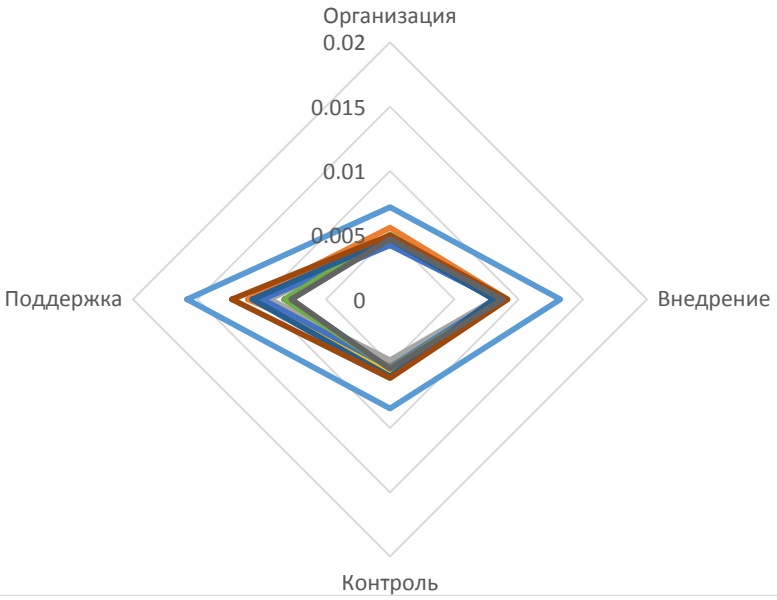

Рис. 4. Распределение вклада мероприятий обеспечения безопасности в общую эффективность

безопасности АСУ ТП ЗО КИИ включает в себя следующие этапы:

1. Используя данные справочника «Группы мер защиты информации», определить состав МЗ, применяемых на ЗО КИИ, и для конкретной модели угроз с задействованием выражения (3) сформировать вектор $\mathbf{W}$ значений эффективности применяемых МЗ.

2. Из выявленного состава МЗ определить подмножества мер на правленные на:

- планирование и разработку мероприятий по обеспечению безопасности АСУ ТП;
- реализацию (внедрение) мероприятий по обеспечению безопасности АСУ ТП;
- контроль состояния безопасности АСУ ТП;
- совершенствование безопасности значимых АСУ ТП.

3. Сформировать опросные листы для балльной оценки по этим направлениям.

4. Провести балльную оценку эффективности принимаемых организационных и технических мер по обеспечению безопасности (реализованность мер организации и планирования безопасности, реализованность мероприятий по внедрению организационно-технических мер защиты, реализованность мероприятий по контролю состояния безопасности, реализованность мероприятий по поддержке и совершенствованию безопасности).

5. Для выявленных подмножеств МЗ расчитать интегральное значение реализованности мер $Э\Phi^{О}$, $Э\Phi^{В}$, $Э\Phi^{К}$, $Э\Phi^{П}$ в соответсвии с приведенными выше шкалами значений.

6. Вычислить групповые показатели эффективности $Э\Phi_{О}^{ГР}$, $Э\Phi_{В}^{ГР}$, $Э\Phi_{К}^{ГР}$, $Э\Phi_{П}^{ГР}$ по выражениям (6), (8), (10), (12) с учетом масштабов негативных последствий Z_k. Зафиксировать значения $Э\Phi_{О}^{ГР}$, $Э\Phi_{В}^{ГР}$, $Э\Phi_{П}^{ГР}$.

7. Установив степень реализованности $r_m = 1$ для $m = 1, M$, вычислить $Э\Phi_{\max}$.

8. Используя выражение (16) и полученые на этапах 5 и 6 результаты, произвести расчет обобщенного показателя эффективности СБ $Э\Phi$, сделать выводы о составе МЗ, их реализуемости на ЗО КИИ.

9. Сформировать предложения и рекомендации по повышению безопасности ЗО КИИ.

Выводы

Таким образом, разработана методика оценки эффективности СБ АСУ ТП, позволяющая обосновывать рекомендации по применению мер защиты информации по следующим направлениям:

- планирование и разработка мероприятий по обеспечению безопасности АСУ ТП;
- реализация (внедрение) мероприятий по обеспечению безопасности АСУ ТП;
- контроль состояния безопасности АСУ ТП;
- совершенствование безопасности значимых АСУ ТП.

Обоснованный показатель эффективности $Э\Phi$ СБ АСУ ТП как степень средневзвешенных отклонений от идеальной альтернативы для значений четырех частных критериев реализуемости мероприятий по организации и планированию, внедрению, контролю состояния, поддержке и совершенствованию СБ в целом позволяет оценить выбранный состав МЗ и выработать рекомендации по применению мер защиты информации, предлагаемых в справочнике «Группы мер защиты информации» ФСТЭК России.

Полученные в работе результаты могут быть использованы при разработке методических рекомендаций по обеспечению безопасности автоматизированных систем управления, являющихся значимыми объектами критической информационной инфраструктуры, и по реализации мер защиты информации, направленных на нейтрализацию актуальных угроз.

Литература

1. Язов Ю.К. Методология оценки эффективности защиты информации в информационных системах от несанкционированного доступа: монография / Ю.К. Язов, С.В. Соловьев. – Санкт-Петербург: Наукоемкие технологии, 2023. – 258 с..
2. Дурденко В.А. Моделирование и оценка эффективности интегрированных систем безопасности объектов, подлежащих обязательной государственной охране / В.А. Дурденко, А.А. Рогожин, Б.О. Баторов // Вестник ВГУ, серия: системный анализ и информационные технологии. – 2018. – № 3. – С. 82–92.
3. Язов Ю.К., Тарелкин М.А., Рубцова И.О. Методический подход к оценке эффективности защиты информации в информационных системах на основе определения возможности опережения мерами защиты процесса реализации угроз // Информация и безопасность. 2019. Т. 22. № 2. С. 220-225.
4. Калашников А.О., Бугайский К.А., Аникина Е.В. Модели количественного оценивания компьютерных атак (Часть 2) // Информация и безопасность. 2019. Т. 22. № 4. С. 529-538.
5. Леньшин А.В., Кравцов Е.В., Славнов К.В. Методика оценки эффективности средств защиты информации на объектах комплексного технического контроля // Радиотехника. 2021. Т. 85. № 1. С. 20-27.

6. Алькаев В.А., Фатеев А.Г. средства анализа защищенности, применяемые для оценки эффективности функционирования средств защиты информации // Инжиниринг и технологии. 2018. Т. 3. № 2. С. 25-28.
7. Кулешов Ю.Е., Сергиенко В.А., Паскробка С.И. Методический подход к оценке эффективности защиты информации // Проблемы инфокоммуникаций. 2018. № 1 (7). С. 45-53.
8. Попов А.Д. Численный метод оценки эффективности систем защиты информации от несанкционированного доступа в автоматизированных информационных системах / В сборнике: Проблемы обеспечения надежности и качества приборов, устройств и систем. Межвузовский сборник научных трудов. Воронеж, 2018. С. 52-60.
9. Титов М.Ю., Трубиенко О.В., Титова М.М. Показатели оценки эффективности систем защиты информации и методы их определения // Промышленные АСУ и контроллеры. 2020. № 1. С. 63-67.
10. Умников Е.В., Атакищев О.И., Грачёв В.А. Применение метода анализа иерархий Саати для оценки эффективности системы защиты информации виртуального полигона // Известия Института инженерной физики. 2022. № 1 (63). С. 99-103.
11. Кляус Т.К., Гатчин Ю.А., Поляков В.И. Методика формирования оптимального состава и оценки эффективности системы защиты информации / В сборнике: Труды Международного научно-технического конгресса «Интеллектуальные системы и информационные технологии - 2019» («ИС & ИТ-2019», «IS&IT'19»). Научное издание: в 2-х томах. 2019. С. 358-360.
12. Миняев А.А. Метод оценки эффективности систем защиты информации территориально распределенных информационных систем / А.А. Миняев, М.Ю. Будько // Информатизация и связь. – 2017. – № 3. – С. 119–121.
13. Будников С.А., Бутрик Е.Е., Соловьев С.В. Моделирование APT-атак, эксплуатирующих уязвимость Zerologon // Вопросы кибербезопасности. 2021. № 6(46). С.47-61. DOI:10.21681/2311-3456-2021-6-47-61
14. Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам / Д. П. Зегжда, Е. Б. Александрова, М. О. Калинин [и др.]. – Москва: Научно-техническое издательство "Горячая линия-Телеком", 2021. – 560 с.
15. Шлыков А.И., Шабуров А.С. О формализации подходов к разработке моделей многокритериальной оценки эффективности систем защиты информации / В сборнике: Автоматизированные системы управления и информационные технологии. Материалы всероссийской научно-технической конференции. В двух томах. Пермь, 2020. С. 408-414.
16. Калашников А.О.1 , Бугайский К.А. Модель количественного оценивания агента сложной сети в условиях неполной информированности // Вопросы кибербезопасности. 2021. № 6(46). С.26-35. DOI:10.21681/2311-3456-2021-6-26-35

METHODOLOGY FOR ASSESSING THE EFFECTIVENESS OF SECURITY SYSTEMS OF AUTOMATED CONTROL SYSTEMS

Budnikov S.A.[20], KovalenkoS.M.[21], Bocharova A.I.[22]

Purpose: *to develop a methodology for evaluating the effectiveness of the created security systems of significant objects of critical information infrastructure, which allows to substantiate recommendations for the application of organizational and technical measures to ensure information security, taking into account the scale of negative consequences, the effectiveness of various security measures, as well as the effectiveness of control.*

Methods: *methods of scoring, efficiency theory and decision-making are used to formalize the parameters.*

Result: *a methodology for evaluating the effectiveness of security systems for automated process control systems has been developed, which makes it possible to substantiate recommendations for the application of information protection measures in four areas of security activities. A* procedure has been developed for scoring the effectiveness of automated systems security systems according to the formed list of parameters checked in the course of assessing the effectiveness of automated systems security systems. The scale of compliance with the levels of the state of safety of automated process control systems is determined. The indicator of the effectiveness of the security system of automated process control systems is substantiated, which allows evaluating the selected composition of protection measures for organizing and planning, implementing, monitoring the state, maintaining and improving the security system and developing recommendations for the application of information protection measures proposed in the reference book "Information protection measures groups» FSTEC of Russia. The results

20 Sergey A. Budnikov, Dr.Sc., Professor, chief researcher of Federal autonomous institution «State Science and Research Experimental Institute of Technical information protection problems of Federal Service for Technical and Export Control». E-mail: public.buser@bk.ru

21 Sergey M. Kovalenko, post-graduate student of Federal autonomous institution «State Science and Research Experimental Institute of Technical information protection problems of Federal Service for Technical and Export Control». E-mail: skovalenko90@yandex.ru

22 Anastasia I. Bocharova, junior researcher of Federal autonomous institution «State Science and Research Experimental Institute of Technical information protection problems of Federal Service for Technical and Export Control». E-mail: ai.bocharova@yandex.ru

obtained in the work can be used in the development of guidelines for ensuring the security of automated control systems, which are significant objects of critical information infrastructure.

Novelty: a generalized criterion for evaluating weighted average deviations from the ideal alternative was used for the values of four particular criteria for the feasibility of measures for the organization and planning, implementation, condition monitoring, support and improvement of the security system, and the procedure for scoring the effectiveness of automated systems security systems was determined according to a specified list of parameters checked during the effectiveness assessment security systems of automated systems.

Keywords: automated process control system, significant object, critical information infrastructure, security measures, security system, efficiency theory.

References

1. Yazov YU.K. Metodologiya otsenki effektivnosti zashchity informatsii v informatsionnykh sistemakh ot nesanktsionirovannogo dostupa: monografiya / YU.K. YAzov, S.V. Solov›yev. – Sankt-Peterburg: Naukoyemkiye tekhnologii, 2023. – 258 s..
2. Durdenko V.A. Modelirovaniye i otsenka effektivnosti integrirovannykh sistem bezopasnosti ob»yektov, podlezhashchikh obyazatel›noy gosudarstvennoy okhrane / V.A. Durdenko, A.A. Rogozhin, B.O. Batorov // Vestnik VGU, seriya: sistemnyy analiz i informatsionnyye tekhnologii. – 2018. – № 3. – S. 82–92.
3. Yazov YU.K., Tarelkin M.A., Rubtsova I.O. Metodicheskiy podkhod k otsenke effektivnosti zashchity informatsii v informatsionnykh sistemakh na osnove opredeleniya vozmozhnosti operezheniya merami zashchity protsessa realizatsii ugroz. Informatsiya i bezopasnost›. 2019. T. 22. № 2. S. 220-225.
4. Kalashnikov A.O., Bugayskiy K.A., Anikina Ye.V. Modeli kolichestvennogo otsenivaniya komp›yuternykh atak (Chast› 2). Informatsiya i bezopasnost›. 2019. T. 22. № 4. S. 529-538.
5. Len›shin A.V., Kravtsov Ye.V., Slavnov K.V. Metodika otsenki effektivnosti sredstv zashchity informatsii na ob»yektakh kompleksnogo tekhnicheskogo kontrolya. Radiotekhnika. 2021. T. 85. № 1. S. 20-27.
6. Al›kayev V.A., Fateyev A.G. sredstva analiza zashchishchennosti, primenyayemyye dlya otsenki effektivnosti funktsionirovaniya sredstv zashchity informatsii. Inzhiniring i tekhnologii. 2018. T. 3. № 2. S. 25-28.
7. Kuleshov YU.Ye., Sergiyenko V.A., Paskrobka S.I. Metodicheskiy podkhod k otsenke effektivnosti zashchity informatsii. Problemy infokommunikatsiy. 2018. № 1 (7). S. 45-53.
8. Popov A.D. Chislennyy metod otsenki effektivnosti sistem zashchity informatsii ot nesanktsionirovannogo dostupa v avtomatizirovannykh informatsionnykh sistemakh. V sbornike: Problemy obespecheniya nadezhnosti i kachestva priborov, ustroystv i sistem. Mezhvuzovskiy sbornik nauchnykh trudov. Voronezh, 2018. S. 52-60.
9. Titov M.YU., Trubiyenko O.V., Titova M.M. Pokazateli otsenki effektivnosti sistem zashchity informatsii i metody ikh opredeleniya. Promyshlennyye ASU i kontrollery. 2020. № 1. S. 63-67.
10. Umnikov Ye.V., Atakishchev O.I., Grachov V.A. Primeneniye metoda analiza iyerarkhiy saati dlya otsenki effektivnosti sistemy zashchity informatsii virtual›nogo poligona. Izvestiya Instituta inzhenernoy fiziki. 2022. № 1 (63). S. 99-103.
11. Klyaus T.K., Gatchin YU.A., Polyakov V.I. Metodika formirovaniya optimal›nogo sostava i otsenki effektivnosti sistemy zashchity informatsii. V sbornike: Trudy Mezhdunarodnogo nauchno-tekhnicheskogo kongressa «Intellektual›nyye sistemy i informatsionnyye tekhnologii - 2019» («IS & IT-2019», «IS&IT›19»). Nauchnoye izdaniye: v 2-kh tomakh. 2019. S. 358-360.
12. Minyayev A.A. Metod otsenki effektivnosti sistem zashchity informatsii territorial›no raspredelennykh informatsionnykh sistem / A.A. Minyayev, M.YU. Bud›ko // Informatizatsiya i svyaz›. – 2017. – № 3. – S. 119–121.
13. Budnikov S.A., Butrik Ye.Ye., Solov›yev S.V. Modelirovaniye APT-atak, ekspluatiruyushchikh uyazvimost› Zerologon. Voprosy kiberbezopasnosti. 2021. № 6(46). S.47-62. 0.4/0.8
14. Kiberbezopasnost› tsifrovoy industrii. Teoriya i praktika funktsional›noy ustoychivosti k kiberatakam / D. P. Zegzhda, Ye. B. Aleksandrova, M. O. Kalinin [i dr.]. – Moskva: Nauchno-tekhnicheskoye izdatel›stvo «Goryachaya liniya-Telekom», 2021. – 560 s.
15. Shlykov A.I., Shaburov A.S. O formalizatsii podkhodov k razrabotke modeley mnogokriterial›noy otsenki effektivnosti sistem zashchity informatsii. V sbornike: Avtomatizirovannyye sistemy upravleniya i informatsionnyye tekhnologii. Materialy vserossiyskoy nauchno-tekhnicheskoy konferentsii. V dvukh tomakh. Perm›, 2020. S. 408-414.